VSS Nederland
Video Systems

FOR A GOOD REASON GRUNDIG

en

Owner´s Manual

IP Cameras & Domes

GCI-H0522V	720P HD IP Colour Fixed Dome Camera
GCI-K0322V	1080P Full HD IP C/B&W AV Fixed Dome w/ IR LED

GCI-H0522V.12.1.31.01.2011

Design and specifications are subject to change without notice

Content:

1. Introduction

This GRUNDIG IP Dome Camera is capable of serving real time streaming and makes the images run more smoothly. In addition to MJPEG real time streaming, this camera develops H.264 codec to apply for high resolution digital broadcast.

With a compact and sophisticated mechanical design, this IP Dome Camera is easily installed and aesthetic. Additionally, the IP Dome Camera's vandal proof cover (IK10) can protect the camera from heavy damage.

These instructions apply to the following products. For the different properties of the products please refer to the table.

Model	HD	IR-LED
GCI-H0522V	720p	-
GCI-K0322V	1080P	✓

2. Important Safety Instructions

Be sure to use only the standard adapter that is specified in the specification sheet. Using any other adapter could cause fire, electrical shock, or damage to the product. Incorrectly connecting the power supply or replacing battery may cause explosion, fire, electric shock, or damage to the product. Do not connect multiple cameras to a single adapter. Exceeding the capacity may cause abnormal heat generation or fire.

Do not place conductive objects (e.g. screwdrivers, coins or any metal items) or containers filled with water on top of the camera. Doing so may cause personal injury due to fire, electric shock, or falling objects.

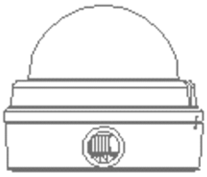
If any unusual smells or smoke come from the unit, stop using the product. In such case, immediately disconnect the power source and contact the service center. Continued use in such a condition may cause fire or electric shock.

If this product fails to operate normally, contact the nearest service center. Never disassemble or modify this product in any way. (GRUNDIG is not liable for problems caused by unauthorized modifications or attempted repair.)

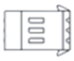
To prevent fire or electric shock, do not expose the inside of this device to rain or moisture.

3. Package Contents

These parts are included:



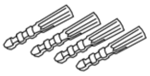
Camera



Power Terminal Block

(not included for GCI-K0522V)

Self Tapping Screws (x4)

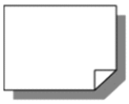


Plastic Screw Anchors (x4)

Rubber Washers (x4)

DC Jack Cable

Security Torx



Quick Guide

CD (Software and Manuals)

4. Installation

Do not install in a location subject to high temperature (over 50°C), low temperature (below -10°C), or high humidity. Doing so may cause fire or electric shock. Keep out of direct sunlight and heat radiation sources. It may cause fire. Avoid aiming the camera directly towards extremely bright objects such as sun, as this may damage the image sensor.

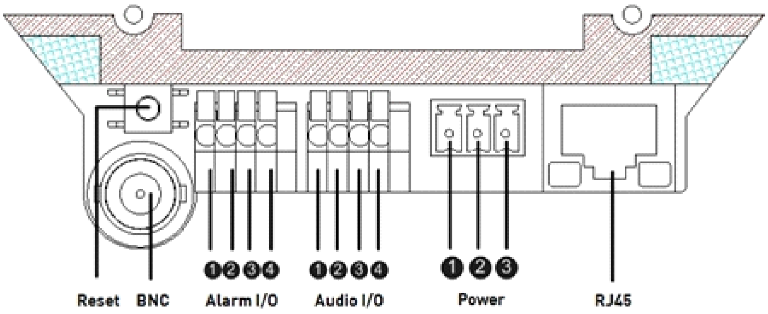
Do not install the unit in humid, dusty, or sooty locations. Doing so may cause fire or electric shock. Install it in a place with good ventilation.

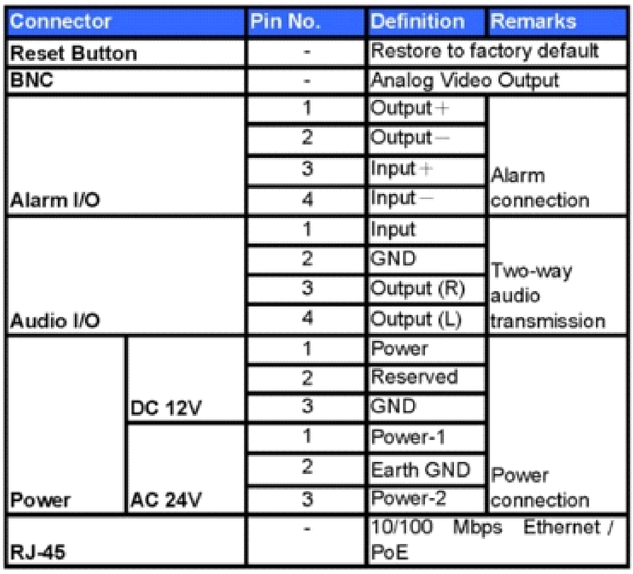
When installing the camera, fasten it securely and firmly. A falling camera may cause personal injury.

If you want to relocate the already installed product, be sure to turn off the power and then move or reinstall it.

4.1. 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	

4.2. System Requirements

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

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 XP / Windows VISTA / 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

4.3. Power Connection

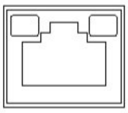
Make sure the camera's power cable is correctly and firmly connected; refer to the pin definition table in section 4.1. Camera's Connectors. If using Power over Ethernet (PoE), make sure Power Sourcing Equipment (PSE) is in use in the network.

4.4. 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 RJ45 connector of the IP 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 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.



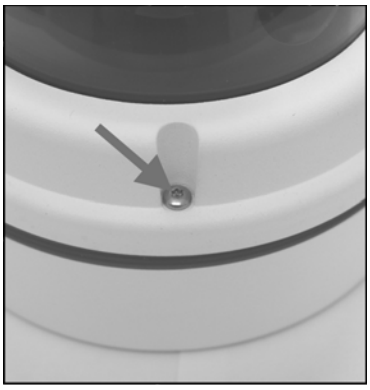
Green Link Light indicates good network connection.
Orange Activity Light flashes for network activity indication.

4.5. Hard Ceiling

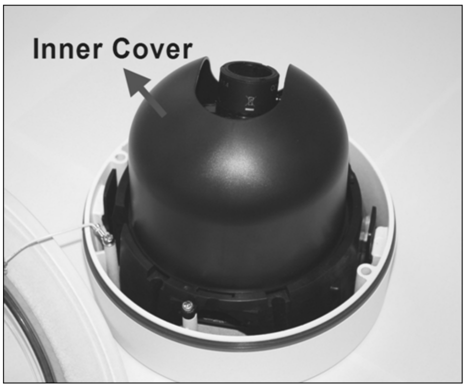
This IP Dome Camera can be installed directly on a wall or ceiling. Please note that the wall or ceiling must have enough strength to support the IP Dome Camera.

Follow the steps below to install the IP Dome Camera:

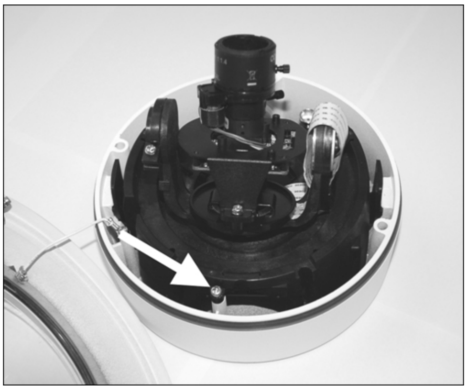
Step 1:
Unpack the IP Dome Camera package and take out the IP Dome Camera.



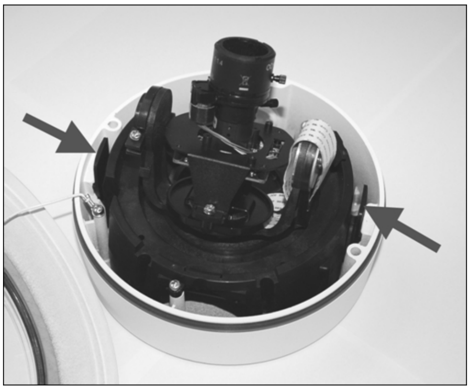
Step 2:
Use a Security Torx to unscrew the two Torx screws on the side of the Dome Cover, as shown in the figure, and open the Dome Cover. The Security Torx is included in the package.



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 picture.

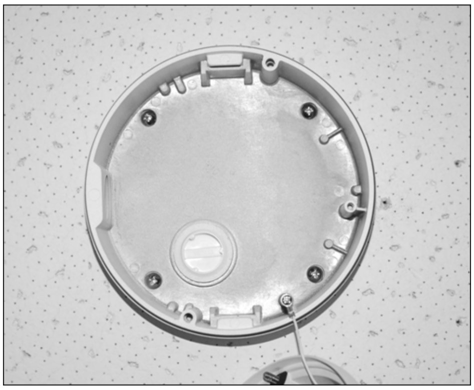


Step 5:
Press the sides of the snap-on module, as indicated in the figure, and detach it from the Dome Camera's housing.

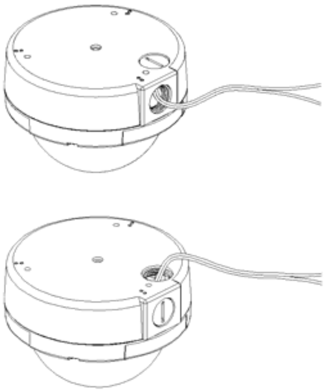
Step 6:
Mark the positions of the four screw holes on the base of the Dome Camera at the chosen installation location.

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

Step 8:
Put the anchors into these drilled holes.

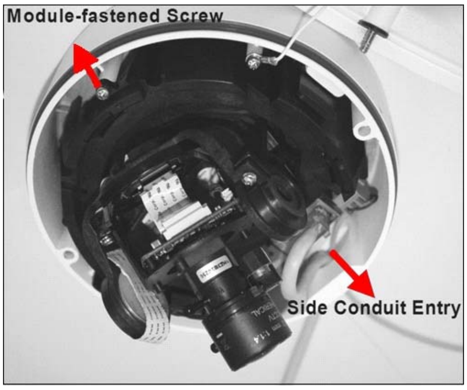


Step 9:
Fasten the Dome Camera's housing with four self tapping screws. Please use the supplied rubber washers for sealing the self tapping screws.



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.

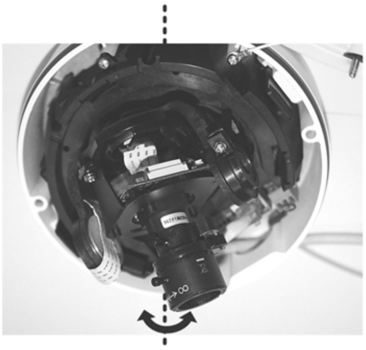


Step 12:
Attach the snap-on module into the Dome Camera housing, and screw the module-fastened screw tightly to secure the camera module.
NOTE: The terminal blocks should face the side conduit entry, as shown in the figure.

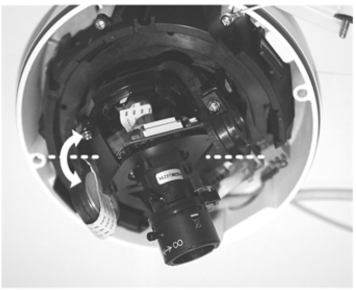
Step 13:
Connect the power and network outputs.
NOTE: The Power Cable is omitted if using PoE.

Step 14:
Access the camera browser-viewer for viewing images. Please refer to 6. Accessing the Camera for further details. Users can also use the camera's BNC connector for video output. To use the BNC output, first you need to configure the video format in the sub-menu "Video Format" (in the Streaming main-menu) either as MJPEG+BNC or as H.264+BNC. Please refer to section 10.1. Video Format. In the default setting, there will be no signal for the BNC output.

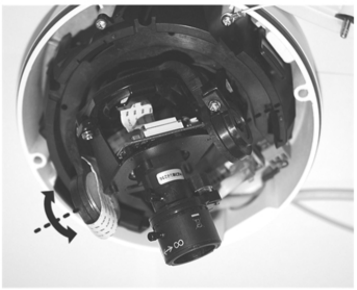
Step 15:
Adjust the camera to a desired angle, as shown below. Pan adjustment range is nearly 360°; rotation angle range approaches 270°. The Tilt is adjustable between -10° ~ 90°.



Pan Adjustment

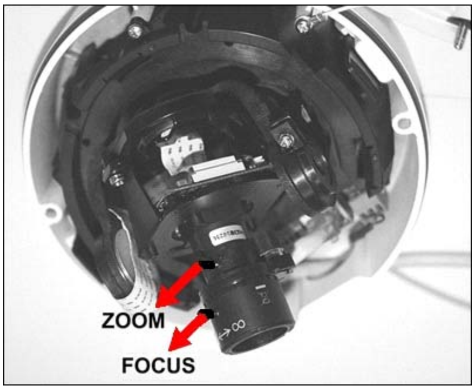


Rotation Adjustment



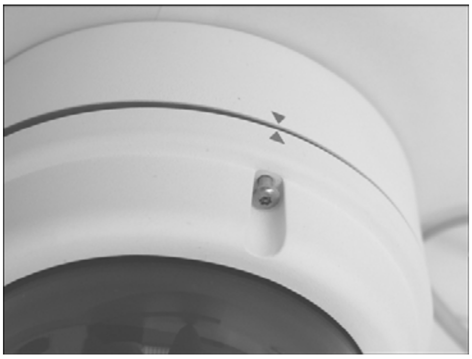
Tilt Adjustment

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



Step 16:
Adjust the zoom ring screw to set the desired zoom; subsequently, modifying the focus ring screw to set the desired focal length.

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

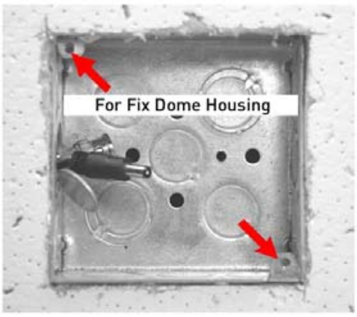


Step 18:
Replace the Dome Cover back, aligning the arrow mark on the Dome Cover with the one on the housing as shown in the picture.

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.

4.6. 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. In the picture below you can see a 4S Mount Electrical Box.

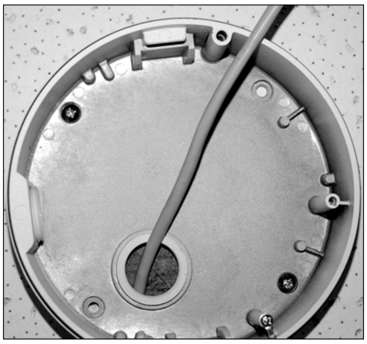


4S Mount Electrical Box

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 4.5. 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 cross head screw first. Then press the sides of camera module and pull it out of 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 the Camera for further details. Users can also use the camera's BNC connector for video output. To use the BNC output, first you need to configure the video format in the sub-menu "Video Format" (in the Streaming main-menu) either as MJPEG+BNC or as H.264+BNC. Please refer to section 10.1. Video Format. In the default setting, there will be no signal for the BNC output.

Step 8:
Position the camera at a desired angle by Pan/Tilt/Rotation adjustment.

Step 9:
Adjust the camera's focal length and focus via zoom and focus ring screws.

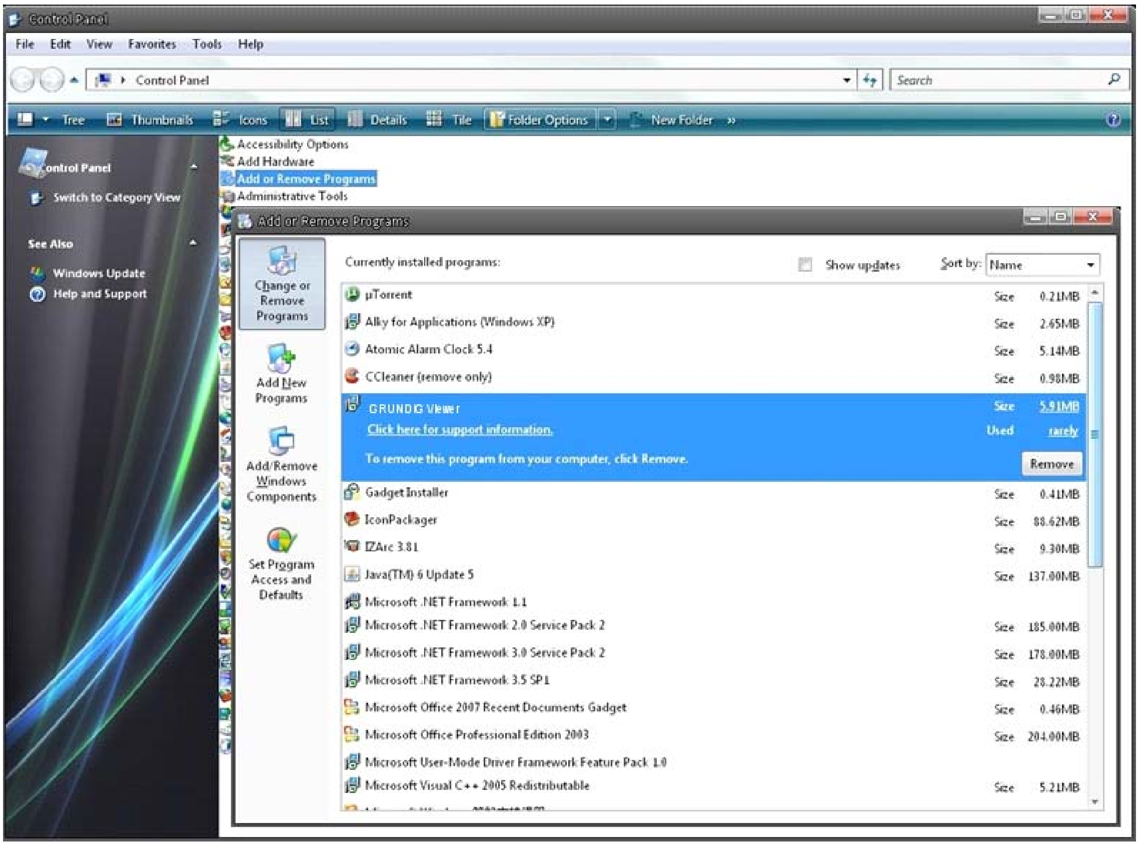
Step 10:
Replace the Dome Cover back, aligning the arrow mark on the Dome Cover with the one on the housing.

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.

5. Deleting the Existing GRUNDIG Viewer

For users who have installed the GRUNDIG Viewer for 1.3 Megapixel Series IP Cameras on the PC, please first delete the existing GRUNDIG Viewer from the PC before accessing this IP Camera.

Deleting the GRUNDIG Viewer :
Click "Control Panel", and then click on "Add or Remove Programs". In the "Currently installed programs" list, select "GRUNDIG Viewer" and click the button "Remove" to uninstall the existing GRUNDIG Viewer as shown in the figure below.

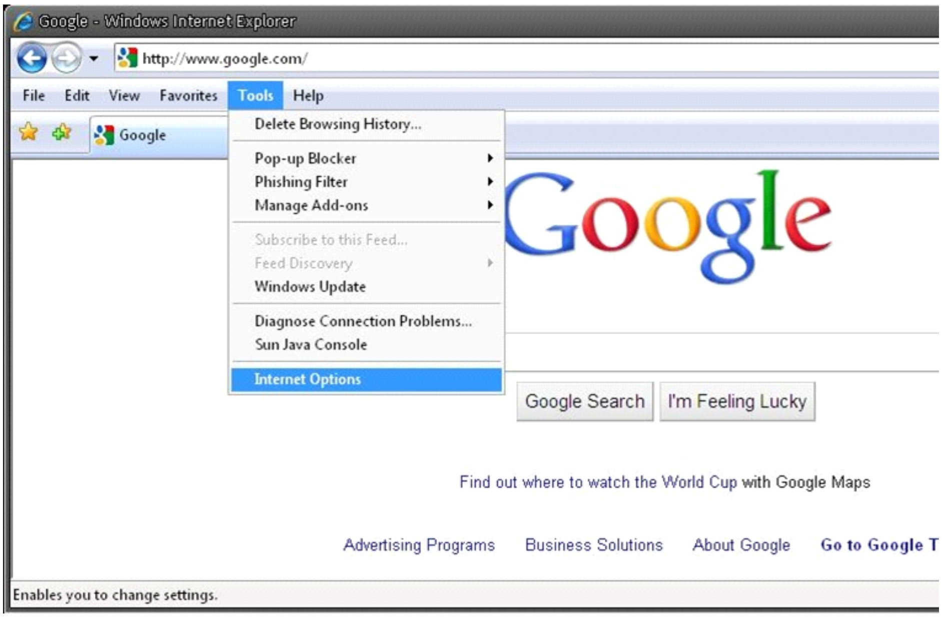


Currently installed programs: □ Show updates Sort by: Name

µTorrent	Size	0.21MB
Alky for Applications (Windows XP)	Size	2.65MB
Atomic Alarm Clock 5.4	Size	5.14MB
CCleaner (remove only)	Size	0.98MB
GRUNDIG Viewer	Size	5.91MB
Click here for support information.	Used	rarely
To remove this program from your computer, click Remove.		
Gadget Installer	Size	0.41MB
IconPackager	Size	88.62MB
IZArc 3.81	Size	9.30MB
Java(TM) 6 Update 5	Size	137.00MB
Microsoft .NET Framework 1.1		
Microsoft .NET Framework 2.0 Service Pack 2	Size	185.00MB
Microsoft .NET Framework 3.0 Service Pack 2	Size	178.00MB
Microsoft .NET Framework 3.5 SP1	Size	28.22MB
Microsoft Office 2007 Recent Documents Gadget	Size	0.46MB
Microsoft Office Professional Edition 2003	Size	204.00MB
Microsoft User-Mode Driver Framework Feature Pack 1.0		
Microsoft Visual C++ 2005 Redistributable	Size	5.21MB

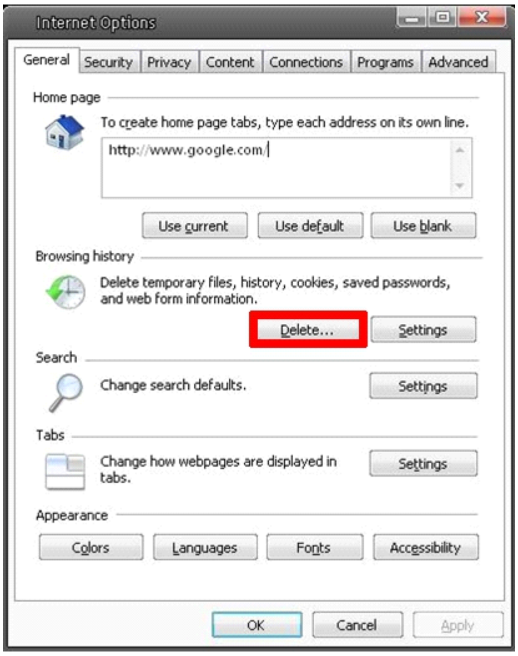
Deleting Temporary Internet Files :
To improve the browser performance, it is suggested to clean up all the files in the Temporary Internet Files. The procedure is as follows (for other web browsers please read the corresponding manuals):

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



Enables you to change settings.

STEP 2: Click on “Delete” in the first pop-up window. Then tap the “Delete Files” in the “Temporary Internet files” section in the next pop-up window.



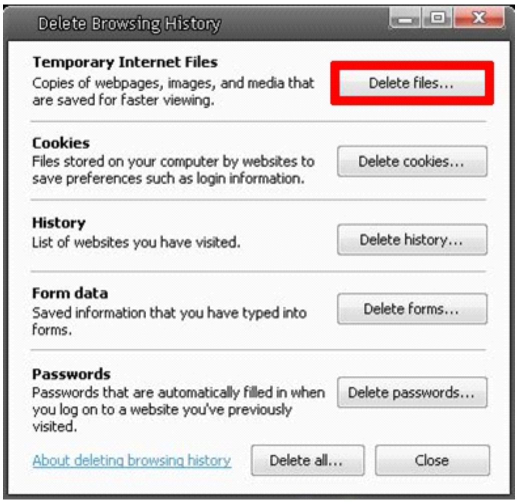
To create home page tabs, type each address on its own line.

http://www.google.com/

Delete temporary files, history, cookies, saved passwords, and web form information.

Change search defaults.

Change how webpages are displayed in tabs.



Temporary Internet Files
Copies of webpages, images, and media that are saved for faster viewing.

Cookies
Files stored on your computer by websites to save preferences such as login information.

History
List of websites you have visited.

Form data
Saved information that you have typed into forms.

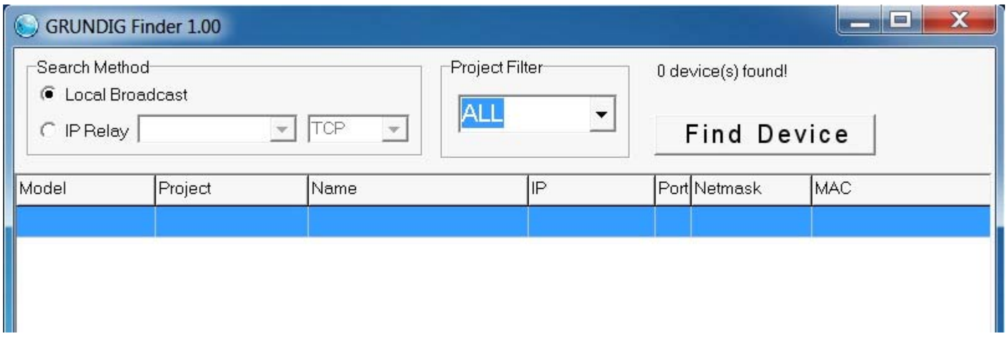
Passwords
Passwords that are automatically filled in when you log on to a website you've previously visited.

6. Accessing the Camera

For initial access to the IP Camera, users can search the camera through the installer program: GRUNDIG Finder.exe, which can be found on the supplied CD.

GRUNDIG Finder Software Setup :

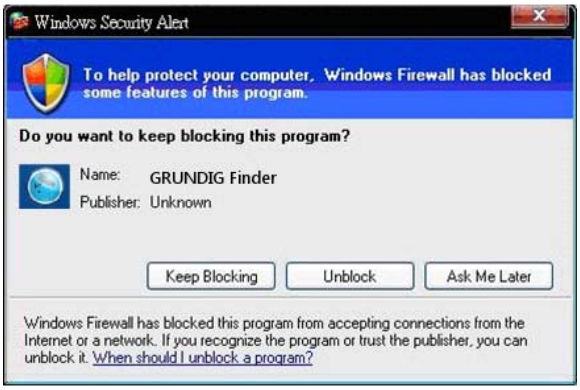
Step 1: Double-click on the program GRUNDIG Finder.exe (see the icon below); its window will appear as shown below. Then click the "Find Device" button.



0 device(s) found!

Model	Project	Name	IP	Port	Netmask	MAC

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



To help protect your computer, Windows Firewall has blocked some features of this program.

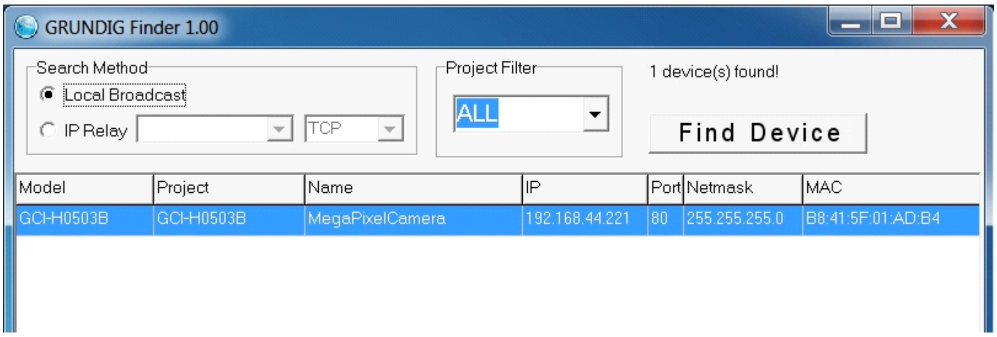
Do you want to keep blocking this program?

Name: GRUNDIG Finder
Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Device Search :

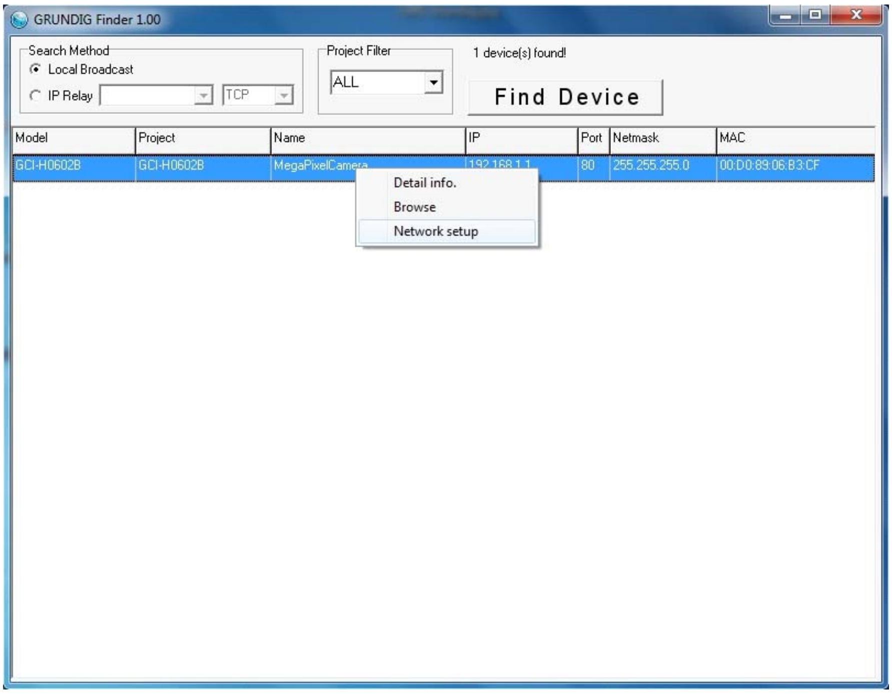
Step 3: Click "Find Device" again, and all the IP devices found will be listed on the page, as shown in the picture below. The IP Camera's default IP address is: 192.168.1.1.



1 device(s) found!

Model	Project	Name	IP	Port	Netmask	MAC
GCI-H0503B	GCI-H0503B	MegaPixelCamera	192.168.44.221	80	255.255.255.0	B8:41:5F:01:AD:B4

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



GRUNDIG Finder 1.00

Search Method
● Local Broadcast
○ IP Relay TCP

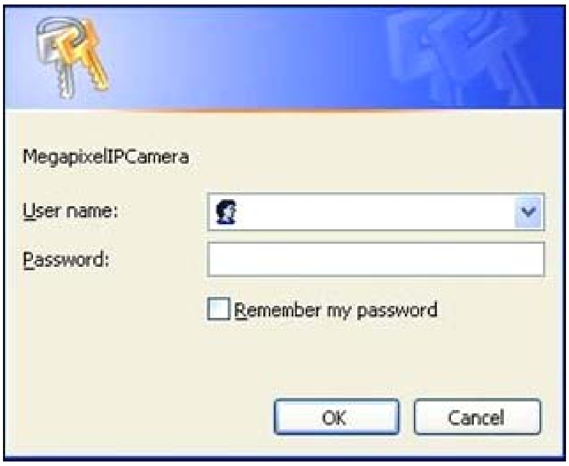
Project Filter ALL

1 device(s) found!

Find Device

Model	Project	Name	IP	Port	Netmask	MAC
GCI-H0602B	GCI-H0602B	MegaPixelCamera	192.168.1.1	80	255.255.255.0	00:D0:89:06:B3:CF

Step 5: Then the dialogue box for entering the default username and password (as shown below) will appear for logging in to the IP Dome Camera.



MegapixelIPCamera

User name:

Password:

□ Remember my password

The default login ID and password for the Administrator are:

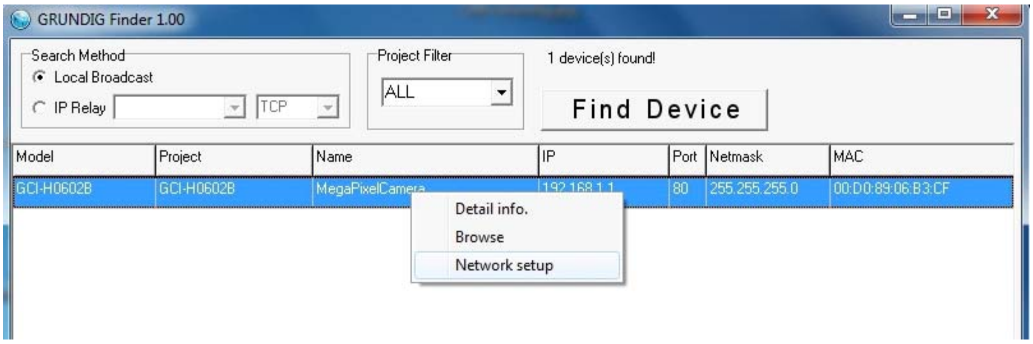
Login ID: admin
Password: 1234

NOTE: ID and password are case sensitive.
It is strongly advised that administrator's password be altered for security concerns. Refer to section 9.2. 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, e.g. 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 of which you would like to change the network property. On the selected item, right-click and select "Network Setup". Meanwhile, record the IP Camera's MAC address, for future identification.



GRUNDIG Finder 1.00

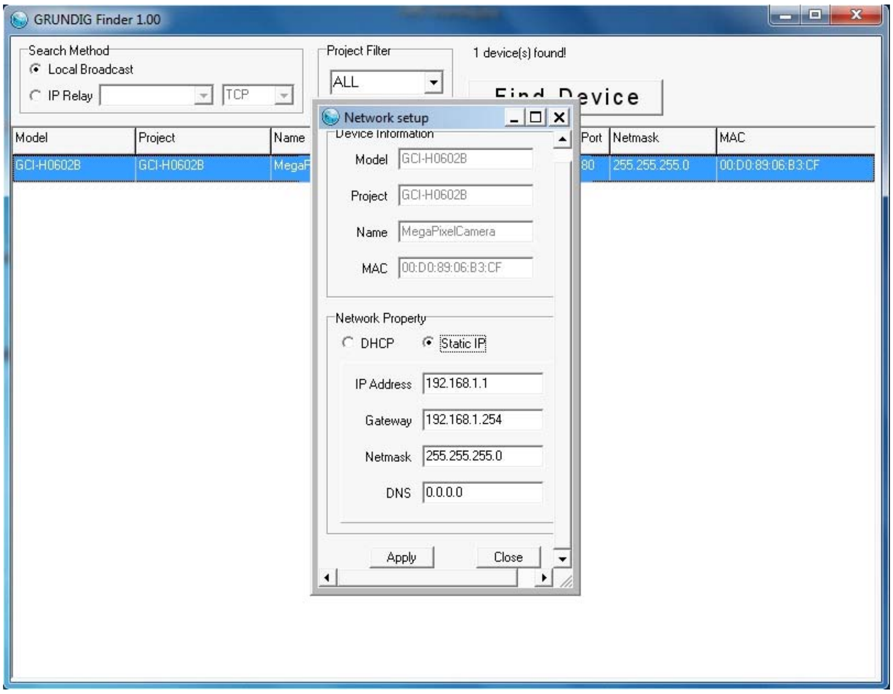
Search Method: ● Local Broadcast ○ IP Relay [ ] TCP

Project Filter: ALL

1 device(s) found!

Model	Project	Name	IP	Port	Netmask	MAC
GCI-H0602B	GCI-H0602B	MegaPixelCamera	192.168.1.1	80	255.255.255.0	00:D0:89:06:B3:CF

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



GRUNDIG Finder 1.00

Network setup

Device Information

Model: GCI-H0602B

Project: GCI-H0602B

Name: MegaPixelCamera

MAC: 00:D0:89:06:B3:CF

Network Property: ○ DHCP ● Static IP

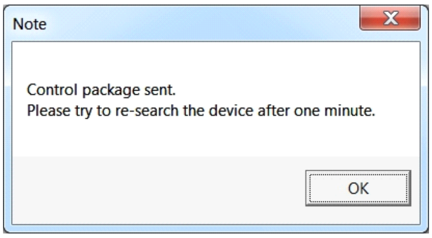
IP Address: 192.168.1.1

Gateway: 192.168.1.254

Netmask: 255.255.255.0

DNS: 0.0.0.0

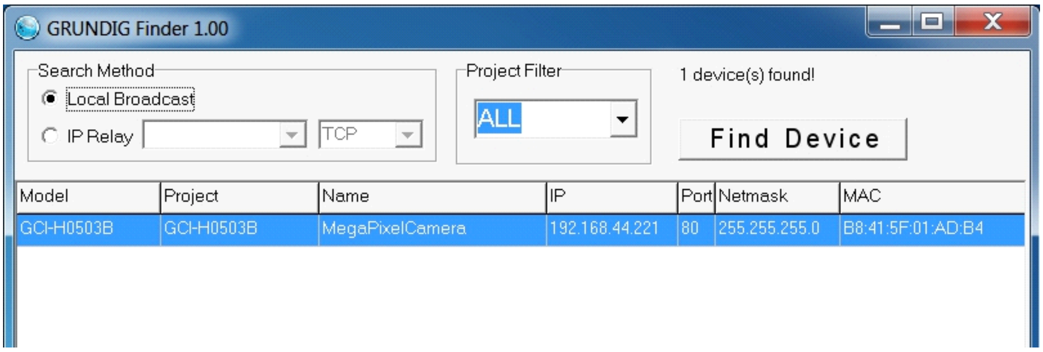
Step 3: Click "OK" on the Note of setting change. Wait for one minute to re-search the IP Camera.



Note

Control package sent.
Please try to re-search the device after one minute.

Step 4: Click the "Find Device" button to 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.



GRUNDIG Finder 1.00

Search Method: ● Local Broadcast ○ IP Relay [ ] TCP

Project Filter: ALL

1 device(s) found!

Model	Project	Name	IP	Port	Netmask	MAC
GCI-H0503B	GCI-H0503B	MegaPixelCamera	192.168.44.221	80	255.255.255.0	B8:41:5F:01:AD:B4

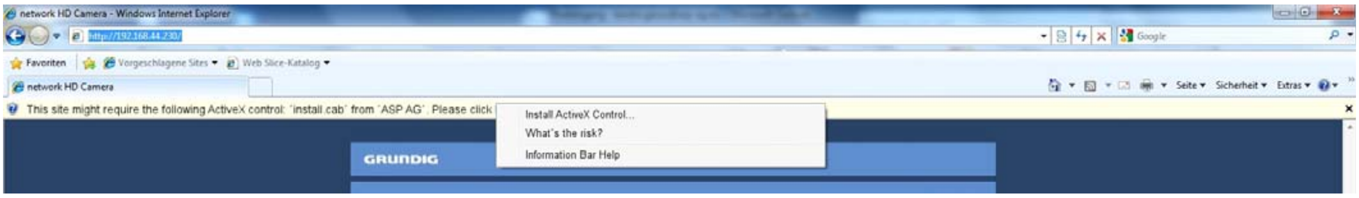
Step 5: Enter User name and Password to access the IP Camera.

Installing the GRUNDIG Viewer Software Online :

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

If the Web browser doesn't allow the GRUNDIG Viewer installation, please check the Internet security settings or ActiveX controls and plug-ins settings (see 14. 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 picture below). Right-click on the Information Bar and select "Install ActiveX Control..." to allow the installation.

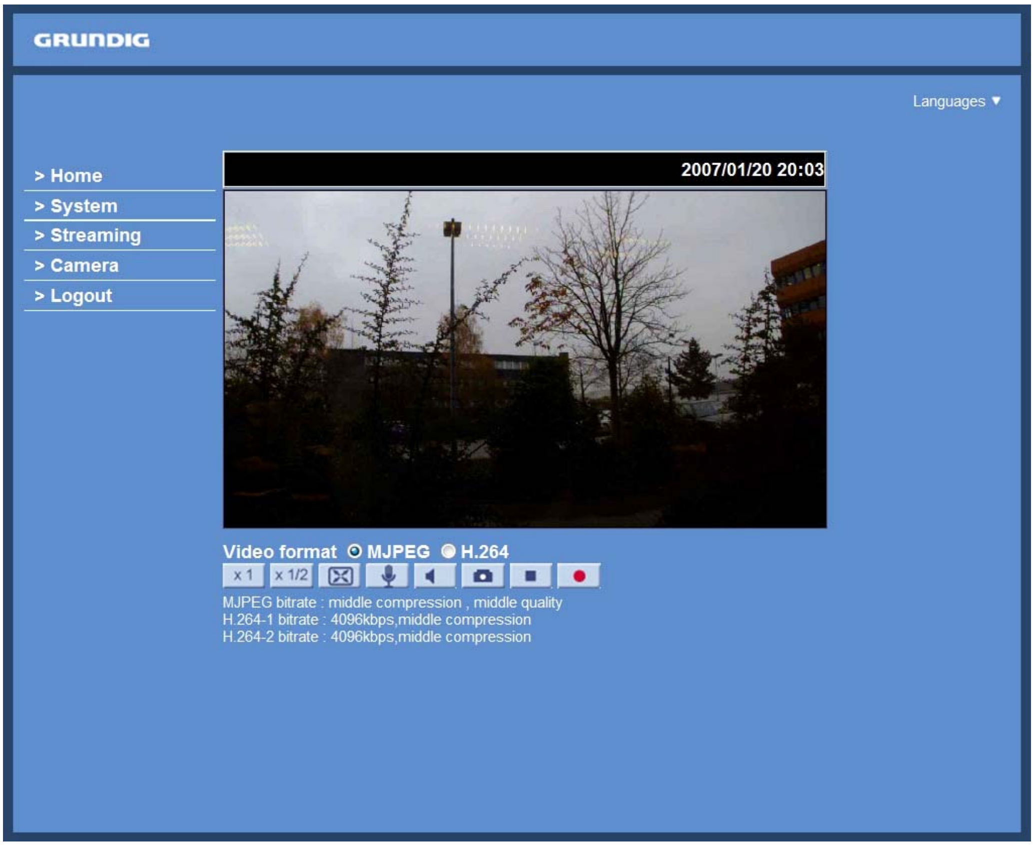


This site might require the following ActiveX control: 'install.cab' from 'ASP AG'. Please click

Then the security warning window will pop up. Click "Install" to carry on software installation.

Click "Finish" to close the GRUNDIG Viewer window when download is finished. For the detailed software download procedure, please refer to chapter 10. GRUNDIG Viewer Download Procedure.

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



Video format ● MJPEG ○ H.264

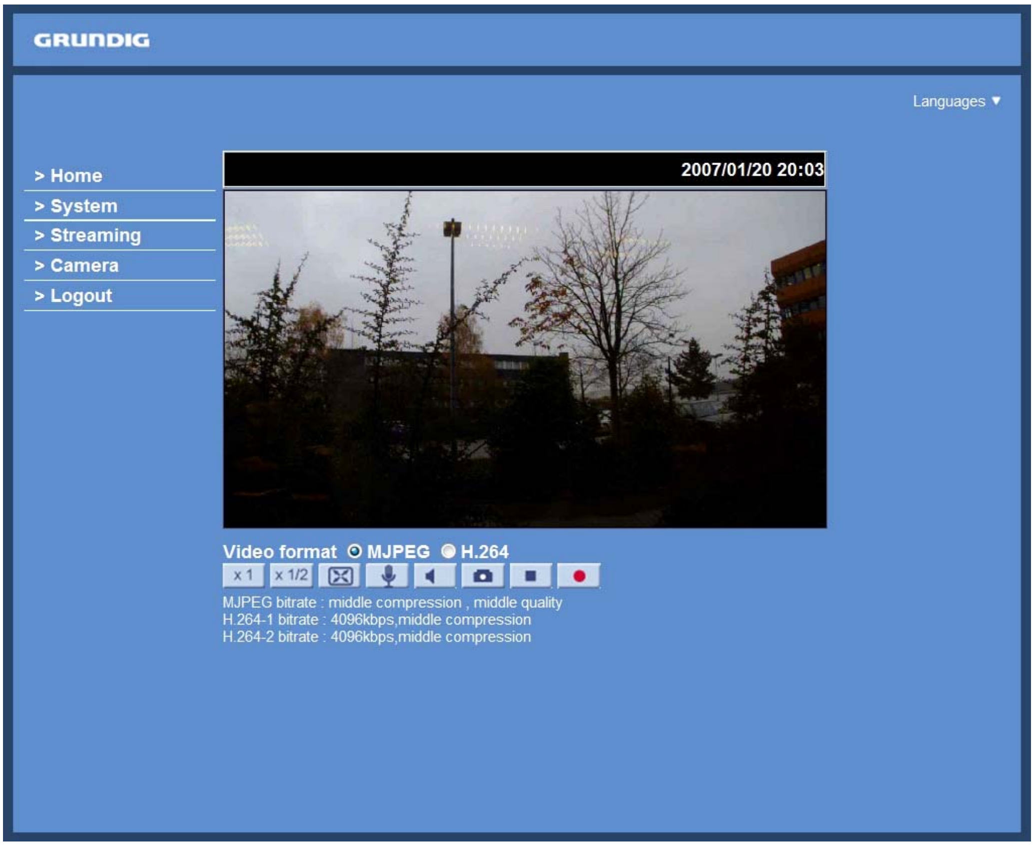
MJPEG bitrate : middle compression , middle quality
H.264-1 bitrate : 4096kbps,middle compression
H.264-2 bitrate : 4096kbps,middle compression

Administrator/User Privileges :
"Administrator" represents the person who can configure the IP Camera and who authorizes users to have access to the camera; "User" refers to whoever has access to the camera with limited authority, i.e. to enter Home and Camera setting pages.

Image and Focus Adjustment :
This image appears on the Home page when successfully accessing to the IP Camera. Adjust zoom and focus as necessary to produce a clear image.

7. Browser-based Viewer Introduction

The picture below shows the Home page of the IP Camera's viewer window.



Video format ● MJPEG ○ H.264

MJPEG bitrate : middle compression , middle quality
H.264-1 bitrate : 4096kbps,middle compression
H.264-2 bitrate : 4096kbps,middle compression

There are five tabs on the left (Home, System, Streaming, Camera and Logout) and one tab on the right (Languages).

Home :
Users can monitor the live video of the targeted area.

System setting :
The administrator can set host name, system time, admin password, network related settings, etc. Further details will be interpreted in chapter 9. System Related Settings.

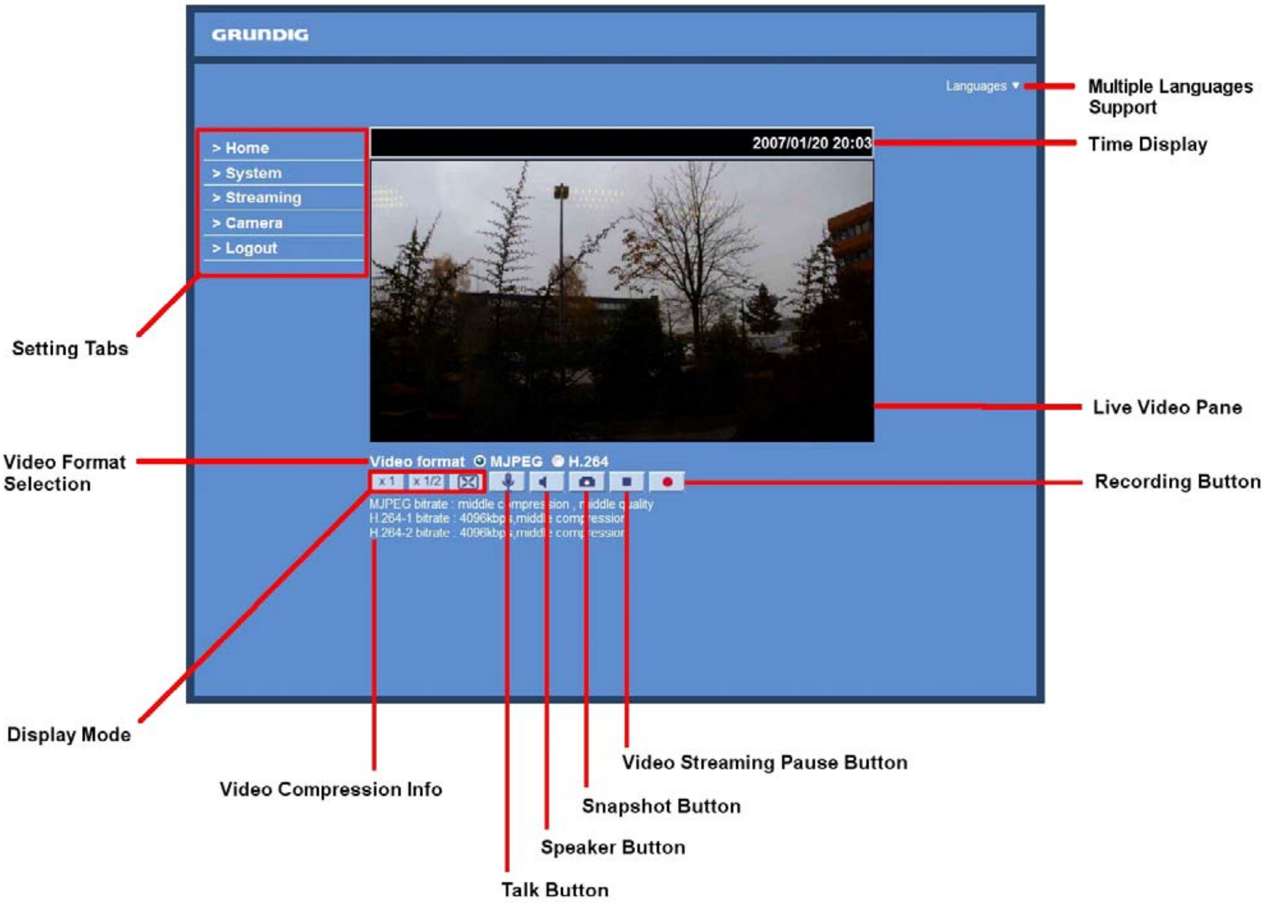
Camera setting :
Users can adjust various camera parameters.

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

Languages : Please choose one of the supported languages (German, English or French).

8. Home Page

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



Video format ● MJPEG ○ H.264

MJPEG bitrate : middle compression , middle quality
H.264-1 bitrate : 4096kbps,middle compression
H.264-2 bitrate : 4096kbps,middle compression

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

Display Mode (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 9.2. Security: User >> Add user >> Talk/Listen for further details. This function is only open to the "User' who has been granted this privilege by the Administrator.
Please note that additional equipment will be necessary.

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:\. For changing the storage location, please refer to section 9.13. File Location for further details.

NOTE: Users with Windows 7 operating system need to follow the following procedure to be able to use the Snapshot function. First you need to log on to your computer as an Administrator. Then you go to Windows Start menu, click with the right mouse button on your Internet Browser and select in the appearing pop-up window "Run as Administrator". Afterwards you can log in to your camera as usual (as an administrator or user).

Video Streaming Stop/Restart button (stop/restart) :
If you 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.

Recording button (on/off) :
Press the button and the recordings from the Live View will be saved to the location specified in the "File Location" (snapshot) page. The default storage location for the recording is: C:/. See section 9.13. File Location for further details.

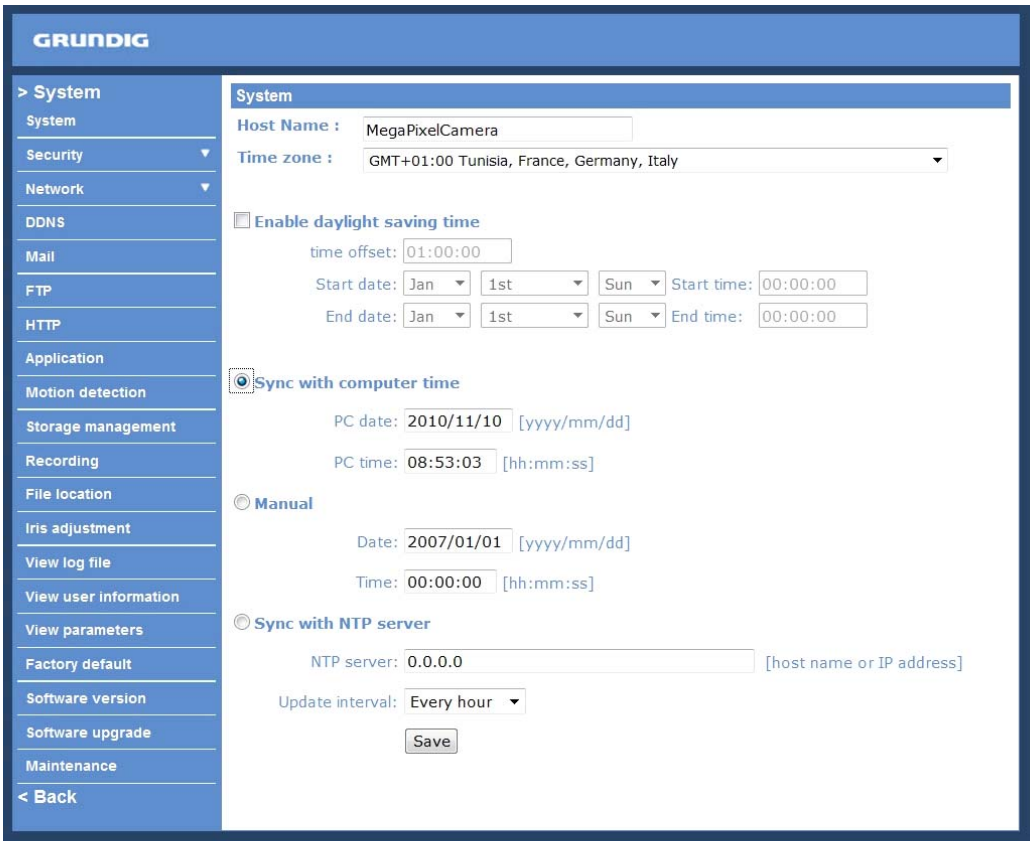
NOTE: Users with Windows 7 operating system who want to use the Recording function, need to follow the procedure in the NOTE below the "Snapshot button" section in this chapter.

Multiple Languages Support :
Multiple languages are supported for the viewer window interface.

9. System Related Settings

The picture 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 the Administrator.



System

Host Name : MegaPixelCamera

Time zone : GMT+01:00 Tunisia, France, Germany, Italy

□ Enable daylight saving time

time offset: 01:00:00

Start date: Jan 1st Sun Start time: 00:00:00

End date: Jan 1st Sun End time: 00:00:00

● Sync with computer time

PC date: 2010/11/10 [yyyy/mm/dd]

PC time: 08:53:03 [hh:mm:ss]

○ Manual

Date: 2007/01/01 [yyyy/mm/dd]

Time: 00:00:00 [hh:mm:ss]

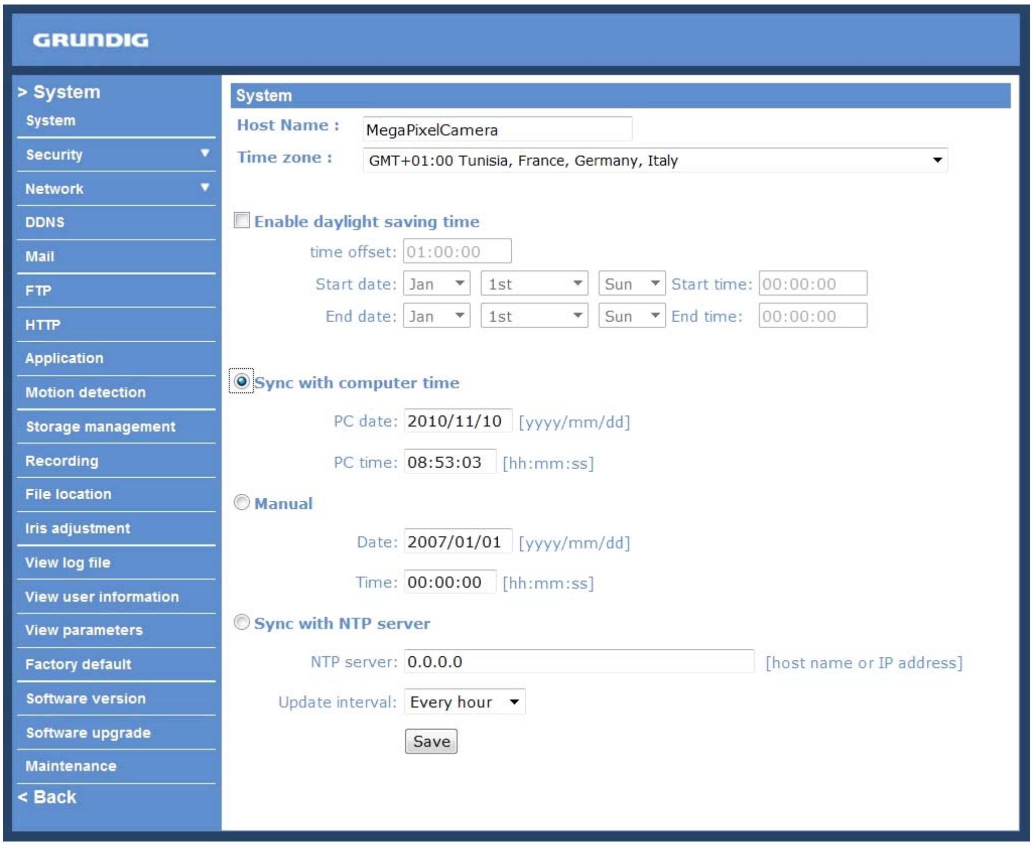
○ Sync with NTP server

NTP server: 0.0.0.0 [host name or IP address]

Update interval: Every hour

9.1. Host Name and System Time Setting

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



System

Host Name : MegaPixelCamera

Time zone : GMT+01:00 Tunisia, France, Germany, Italy

□ Enable daylight saving time

time offset: 01:00:00

Start date: Jan 1st Sun Start time: 00:00:00

End date: Jan 1st Sun End time: 00:00:00

● Sync with computer time

PC date: 2010/11/10 [yyyy/mm/dd]

PC time: 08:53:03 [hh:mm:ss]

○ Manual

Date: 2007/01/01 [yyyy/mm/dd]

Time: 00:00:00 [hh:mm:ss]

○ Sync with NTP server

NTP server: 0.0.0.0 [host name or IP address]

Update interval: Every hour

Host Name :
The name is for camera identification (max. 30 characters). If alarm function (see section 9.8. Application) is enabled and is set to send an alarm message by Mail/FTP, the host name entered here will display in the alarm message.

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 synchronise with the PC's.

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

Sync with NTP server :
Network Time Protocol (NTP) is an alternate way to synchronise your camera's clock with a NTP server. Please specify the server you wish to synchronise 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.

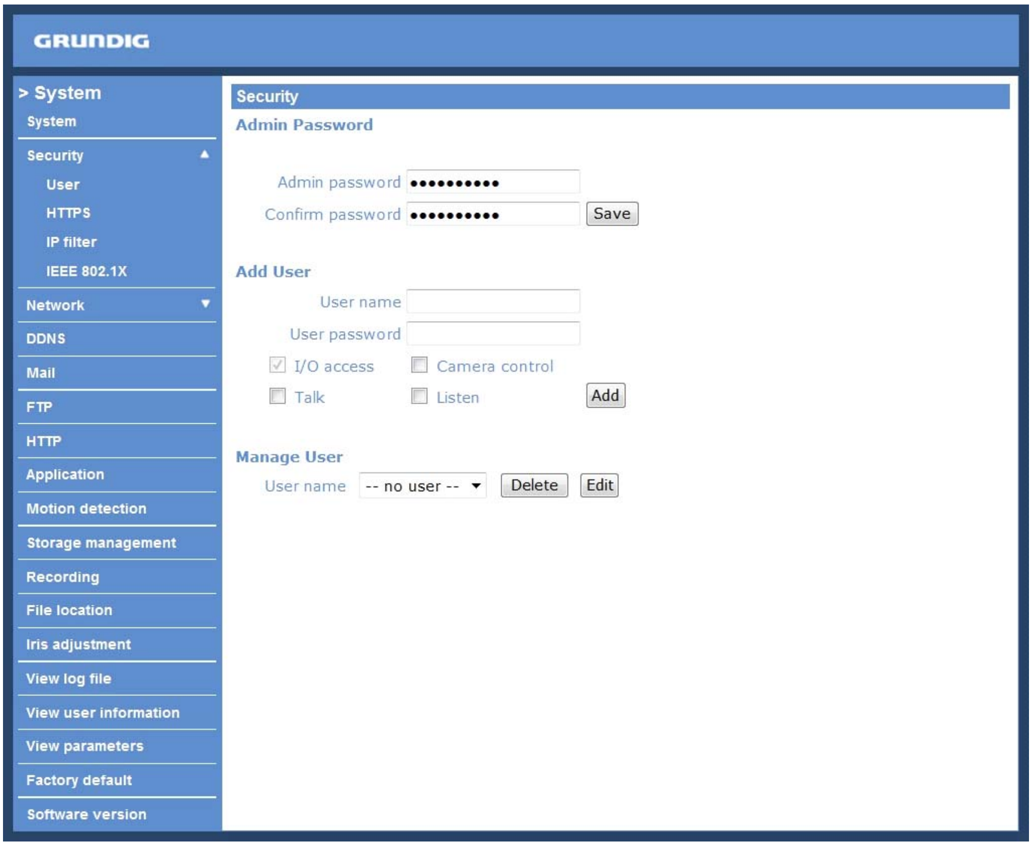
NOTE: Press < Save > to confirm the new setting.

9.2. Security

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

<User> :

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



Security

Admin Password

Admin password ••••••••••

Confirm password •••••••••• Save

Add User

User name

User password

☑ I/O access ☐ Camera control

☐ Talk ☐ Listen Add

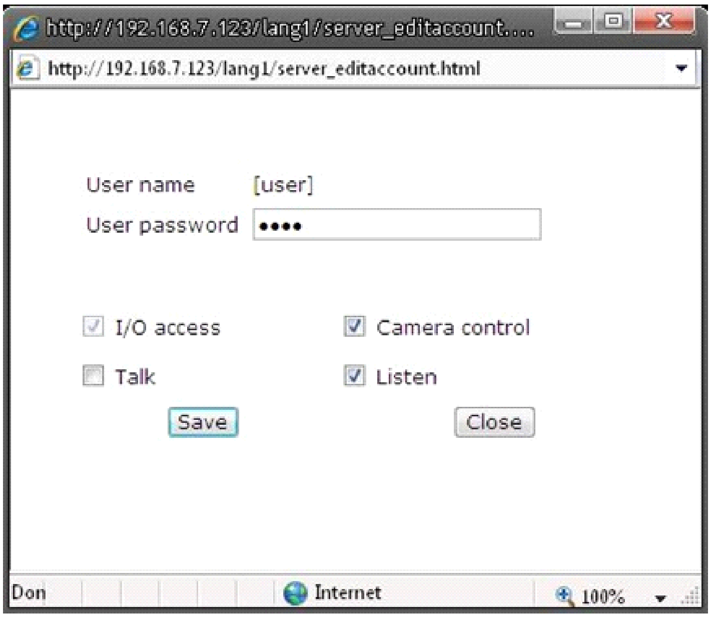
Manage User

User name -- no user -- Delete Edit

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

Admin Password :
Change the administrator's password by putting in 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 digits.

Add User :
Type the new user's name and password and click <Add> to add the new user. The user name can have up to 16 characters, the password up to 14 characters. The new user will be displayed in the user name list. A maximum of 20 user accounts can be set. To each user the privileges of "Camera control", "Talk" and "Listen" can be assigned.



http://192.168.7.123/lang1/server_editaccount.html

User name [user]

User password ••••

☑ I/O access ☑ Camera control

□ Talk ☑ Listen

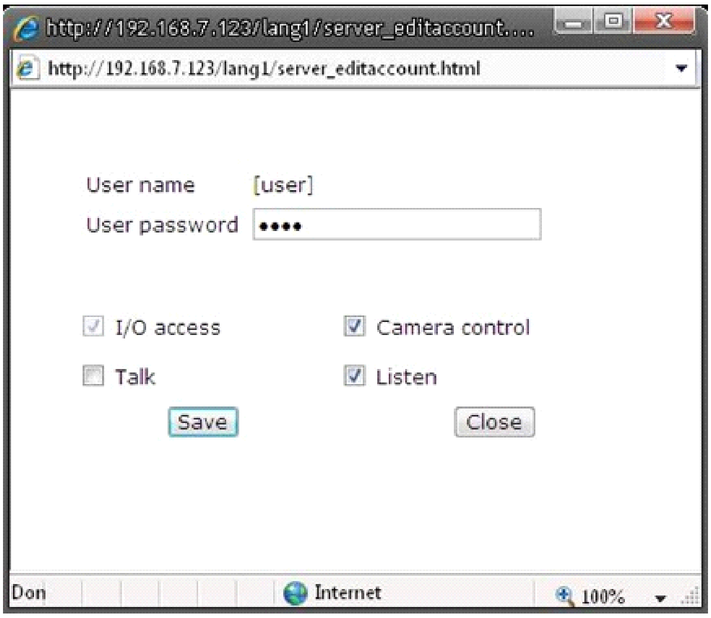
- I/O access:
This item supports fundamental functions that enable users to view video when accessing the camera.

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

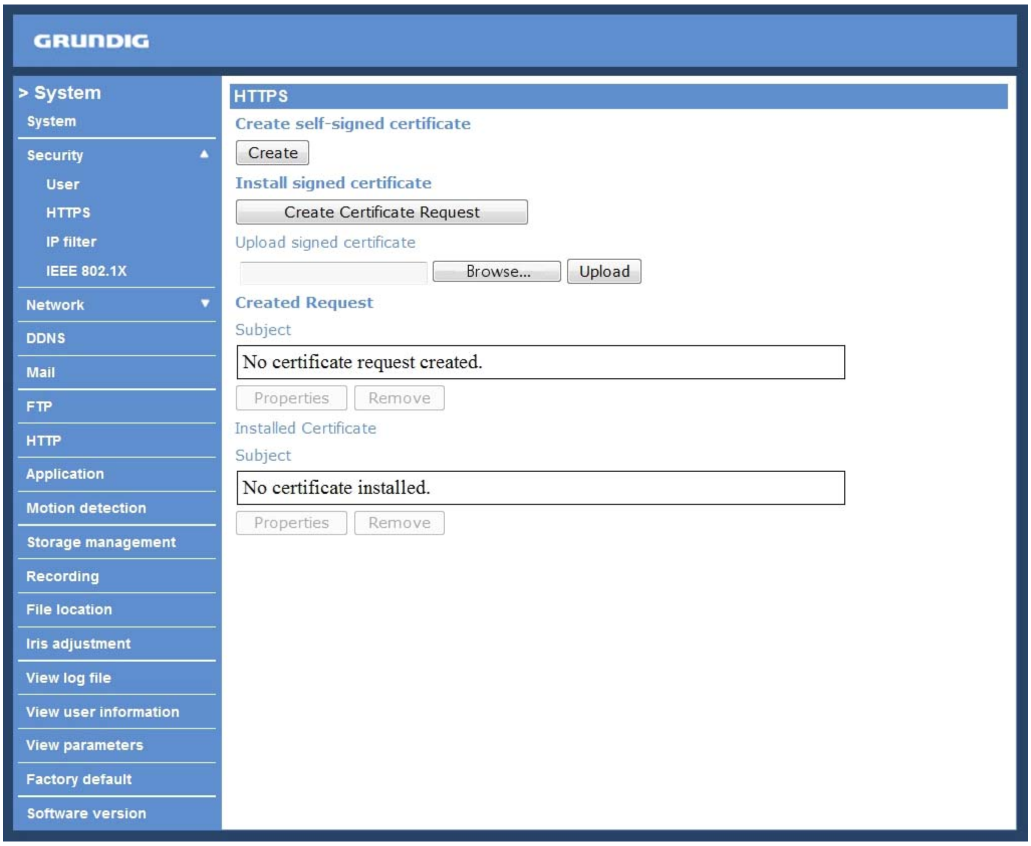
☑ I/O access ☑ Camera control
□ Talk ☑ Listen

Save
Close
Don
Internet
100%

<HTTPS> :

<HTTPS> allows secure connections between the IP Camera and the web browser using the <Secure Socket Layer (SSL)> or the <Transport Layer Security (TLS)>, which prevent 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.

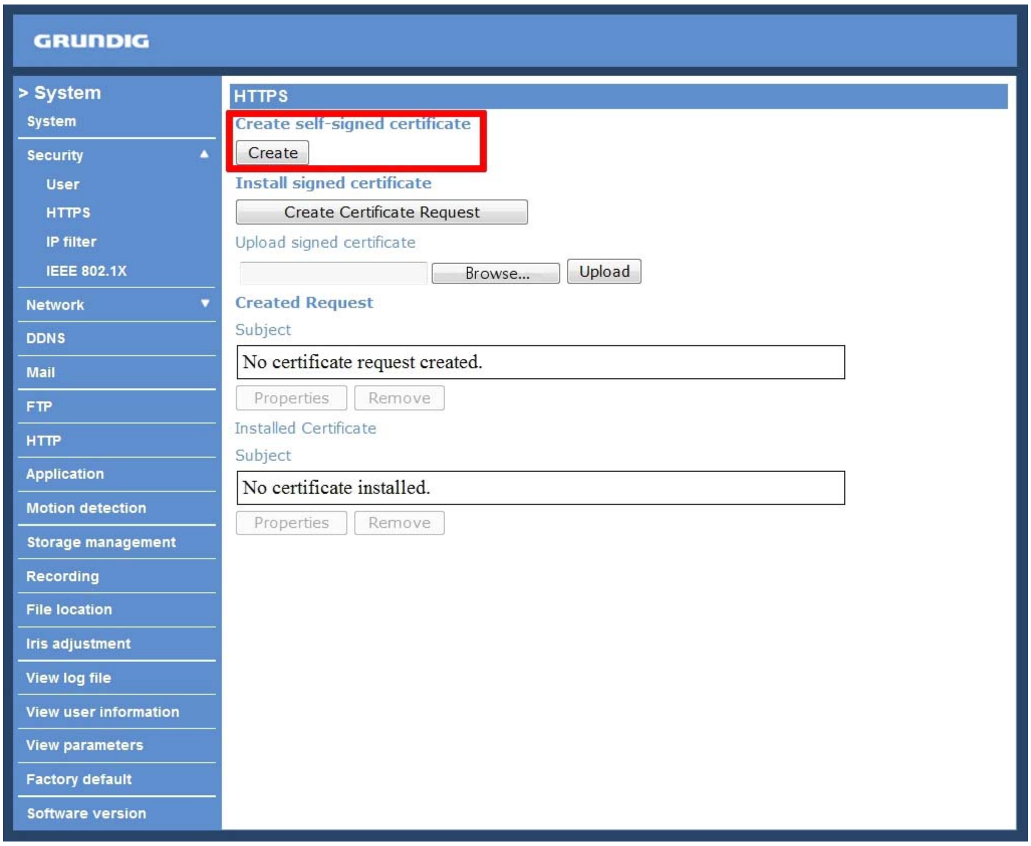


No certificate request created.

No certificate installed.

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.



No certificate request created.

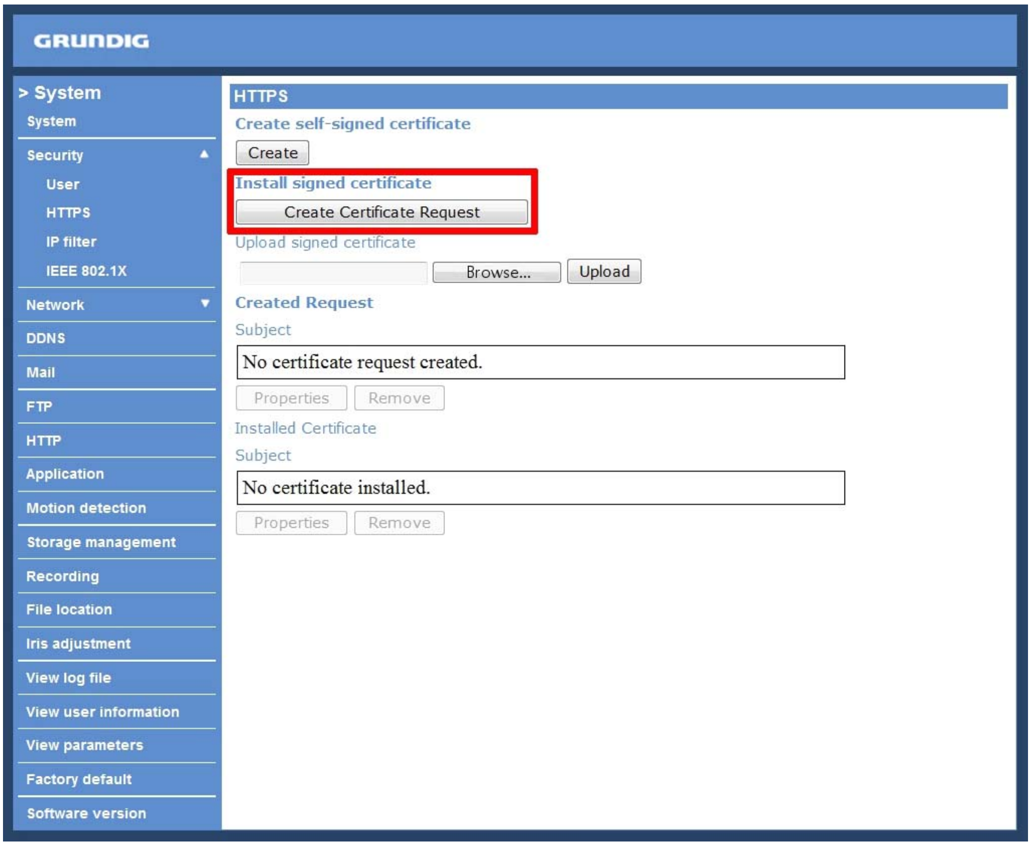
No certificate installed.

Click the <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.

Provide the requested information in the Create Dialog. Please refer to the following Provide the Certificate Information for more details.

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.

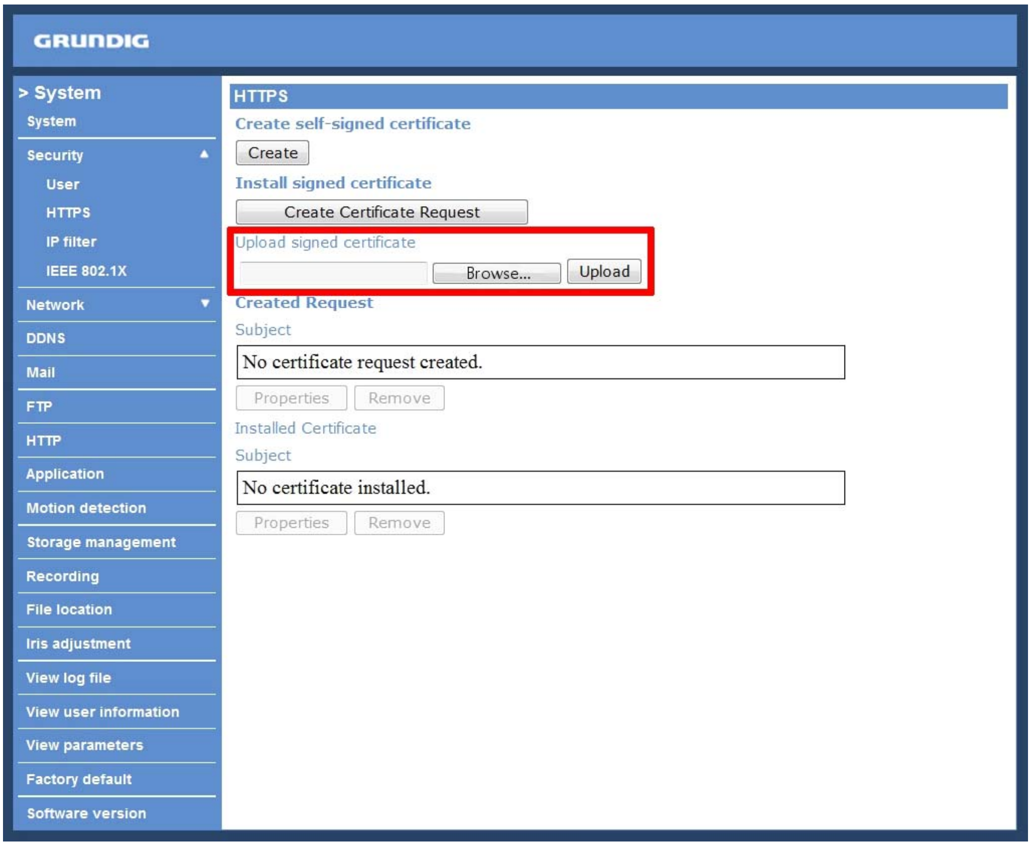


No certificate request created.

No certificate installed.

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.

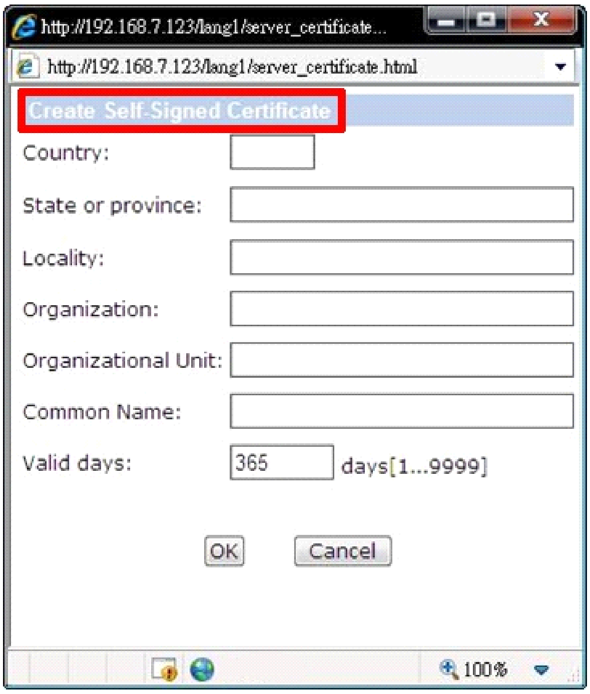
When the signed certificate is returned, install it by uploading the signed certificate.



No certificate request created.

No certificate installed.

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

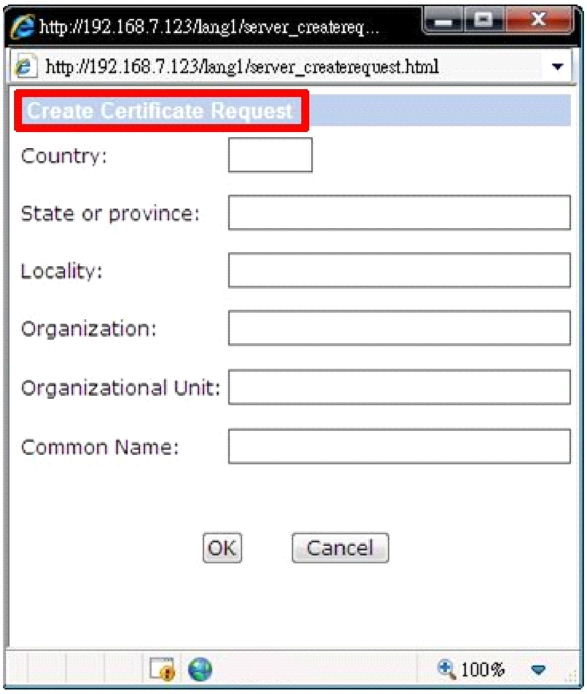


http://192.168.7.123/lang1/server_certificate...

http://192.168.7.123/lang1/server_certificate.html

Create Self-Signed Certificate

Country:	
State or province:	
Locality:	
Organization:	
Organizational Unit:	
Common Name:	
Valid days:	365 days[1...9999]



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:	
Organizational Unit:	
Common Name:	

- Country:
Enter a 2-letter combination code to indicate the country the certificate will be used in. For instance, type in “GB” to indicate Great Britain.

- State or province:
Enter the local administrative region.

- Locality:
Enter other geographical information.

- Organisation:
Enter the name of the organisation to which the entity identified in “Common Name” belongs.

- Organisation Unit:
Enter the name of the organisational unit to which the entity identified in “Common Name” belongs.

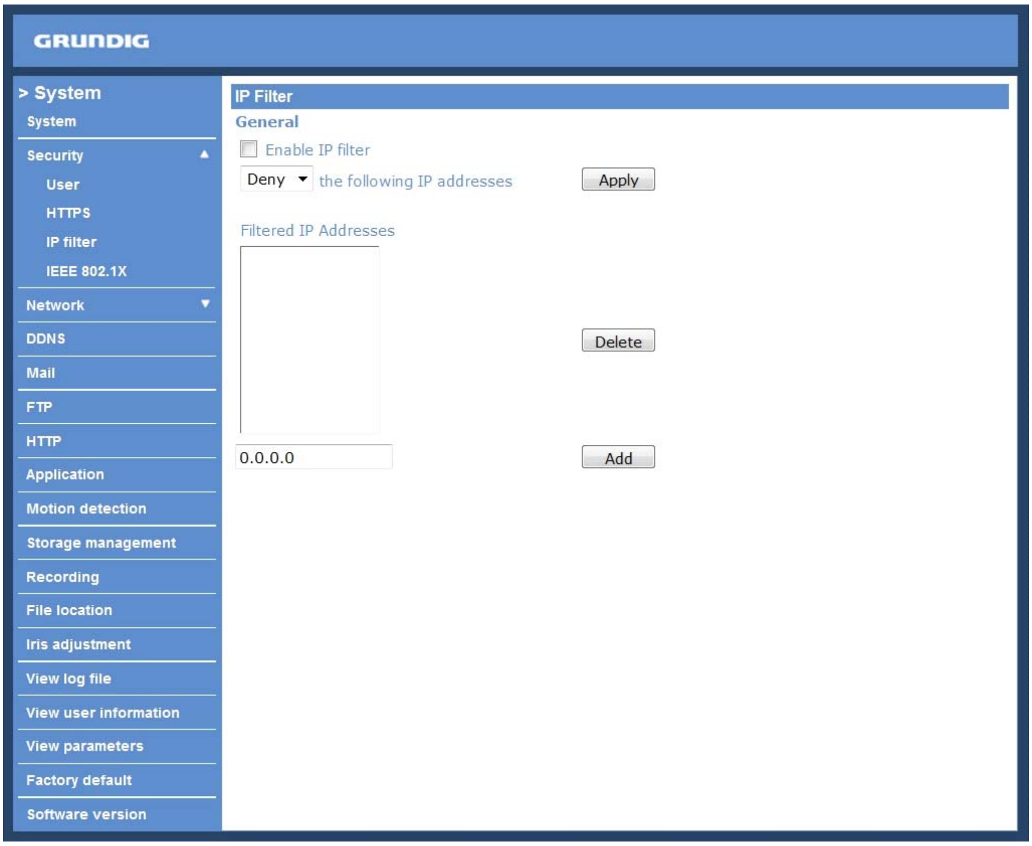
- Common Name:
Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).

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

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

<IP Filter> :

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



IP Filter

General

☐ Enable IP filter

Deny ▾ the following IP addresses

Filtered IP Addresses

0.0.0.0

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 behaviour.

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

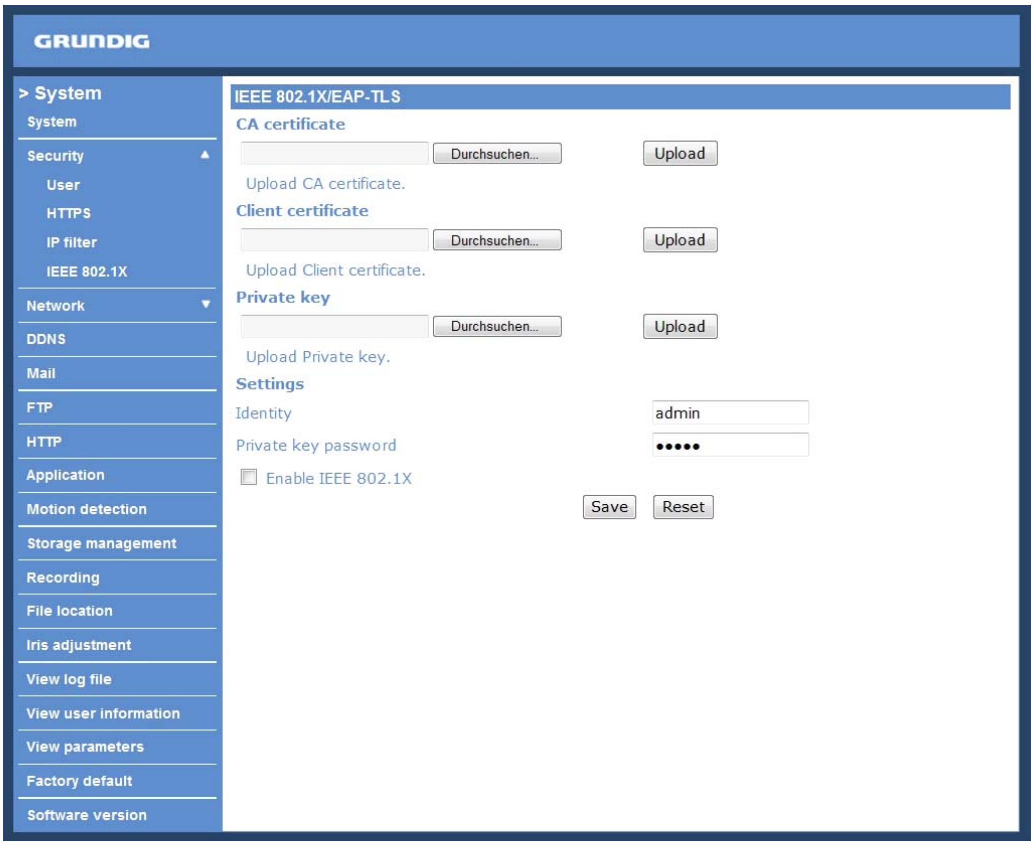
The Filtered IP Addresses list box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.

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

<IEEE 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 the network administrator to receive certificates, user IDs and passwords.



IEEE 802.1X/EAP-TLS

CA certificate

Upload CA certificate.

Client certificate

Upload Client certificate.

Private key

Upload Private key.

Settings

Identity	admin
Private key password	•••••

□ Enable IEEE 802.1X

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.

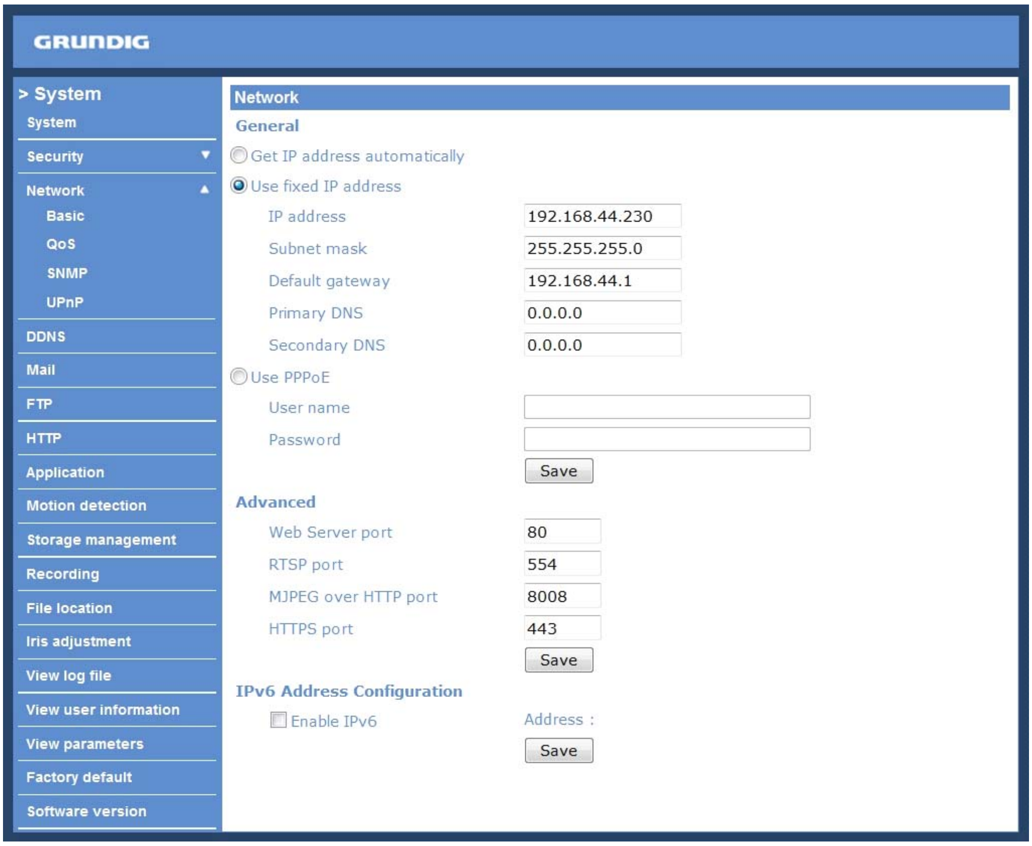
- Private Key Password:
Enter the password (maximum 16 characters) for your user identity.

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

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

9.3. Network

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



Network

General

○ Get IP address automatically

● Use fixed IP address

IP address	192.168.44.230
Subnet mask	255.255.255.0
Default gateway	192.168.44.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

○ Use PPPoE

User name	
Password	

Save

Advanced

Web Server port	80
RTSP port	554
MJPEG over HTTP port	8008
HTTPS port	443

Save

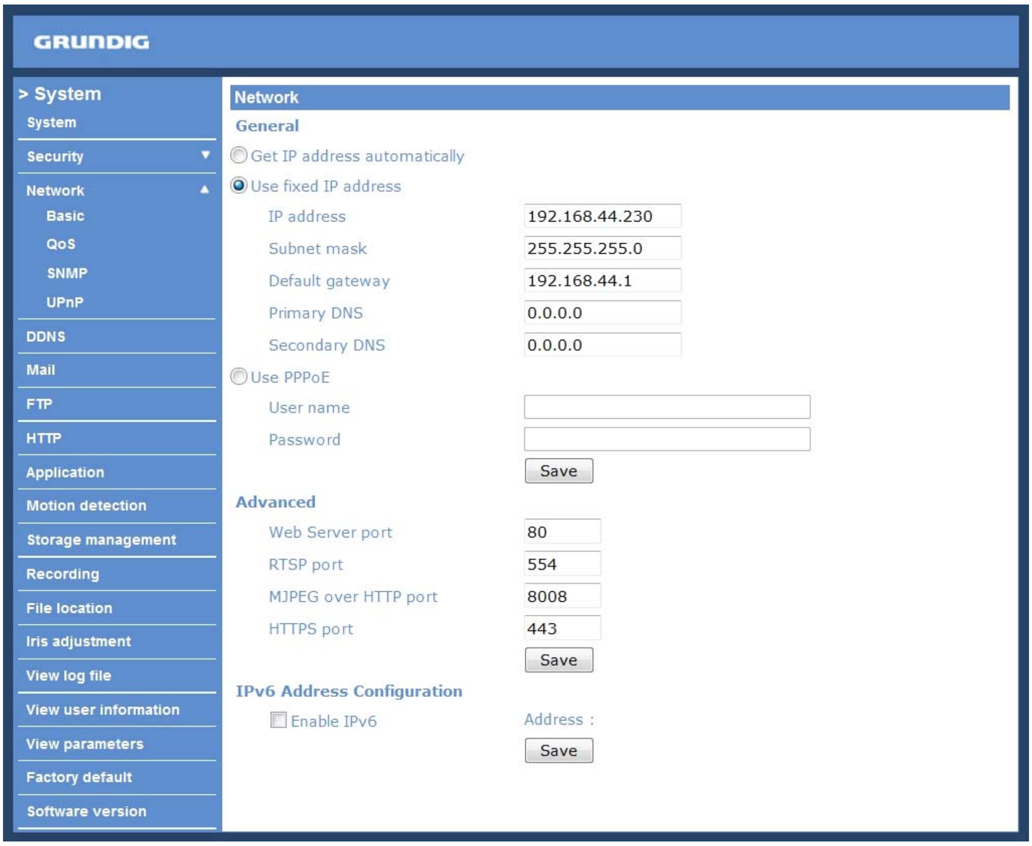
IPv6 Address Configuration

□ Enable IPv6 Address :

Save

<Basic> :

Users can choose to connect to the IP Camera through a 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.


Network

General

○ Get IP address automatically

● Use fixed IP address

IP address 192.168.44.230
Subnet mask 255.255.255.0
Default gateway 192.168.44.1
Primary DNS 0.0.0.0
Secondary DNS 0.0.0.0

○ Use PPPoE

User name
Password

Save

Advanced

Web Server port 80
RTSP port 554
MJPEG over HTTP port 8008
HTTPS port 443

Save

IPv6 Address Configuration

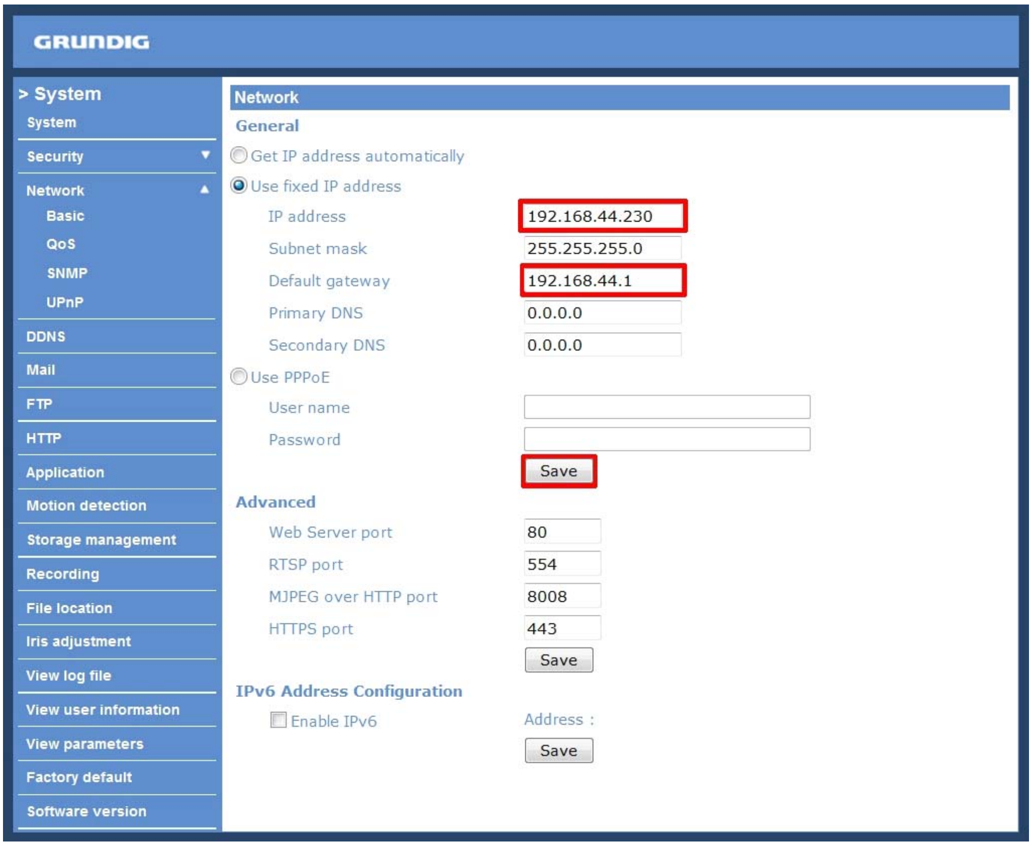
□ Enable IPv6 Address :

Save

Get IP address automatically (DHCP):
The camera's default setting is "Use fixed IP address". Please refer to the previous section 6. Accessing the Camera for login with the default IP address.
If "Get IP address automatically" is selected, after the IP Camera restarts, users can search the IP address through the installer program "GRUNDIG Finder.exe", which can be found in the "GRUNDIG Finder" folder on the supplied CD.

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

Use a fixed IP address :
To setup a 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, e.g. 192.168.7.123; then go to the Default Gateway (explained later) and type in the appropriate setting, e.g. 192.168.7.254. Press "Save" to confirm the new setting.



Network

General

○ Get IP address automatically

● Use fixed IP address

IP address 192.168.44.230

Subnet mask 255.255.255.0

Default gateway 192.168.44.1

Primary DNS 0.0.0.0

Secondary DNS 0.0.0.0

○ Use PPPoE

User name

Password

Save

Advanced

Web Server port 80

RTSP port 554

MJPEG over HTTP port 8008

HTTPS port 443

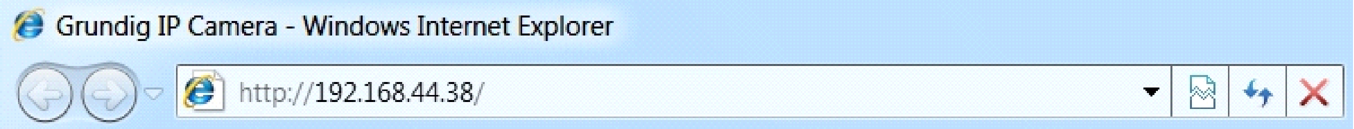
Save

IPv6 Address Configuration

□ Enable IPv6 Address :

Save

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



Grundig IP Camera - Windows Internet Explorer

http://192.168.44.38/

- 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 subnets. An invalid gateway setting will fail the transmission to destinations in different subnets.

- 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 users must be informed about 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 users 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.

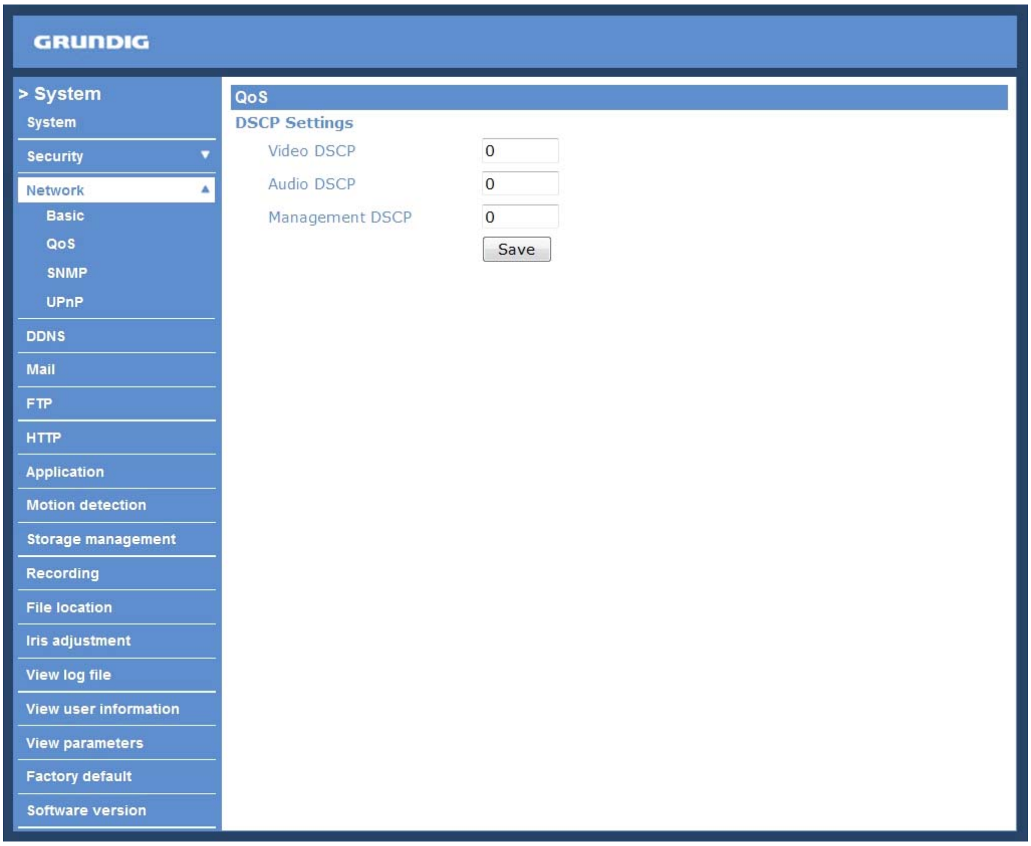
- HTTPS port:
The default setting of HTTPS Port is 443; the setting range is from 1024 to 65535.

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.

<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

Video DSCP 0

Audio DSCP 0

Management DSCP 0

DSCP Settings :
The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled.

The IP Camera uses the following QoS Classes: Video, Audio and Management.

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

- Audio:
This setting is only available for the IP Cameras which support audio.

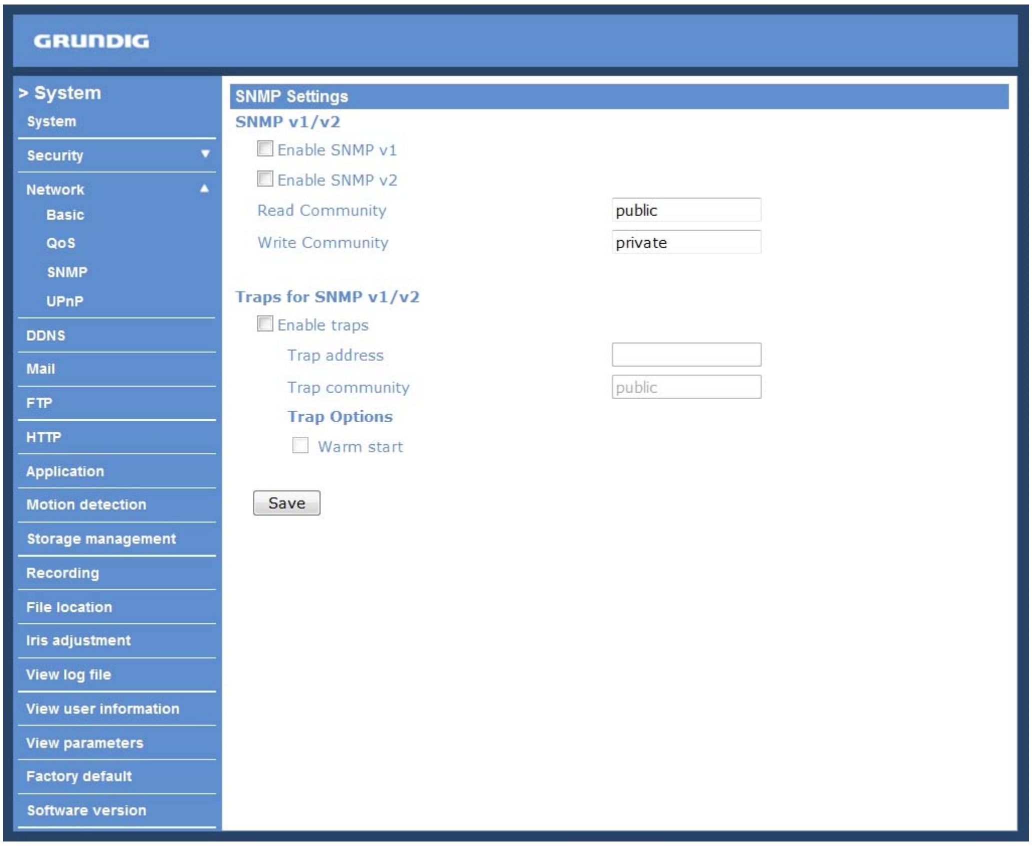
- Management:
This class consists of HTTP traffic: Web browsing.

Click the "Save" button to complete the setting.

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

<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.



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

SNMP v1/v2 :
- Enable SNMP:
Select the version of SNMP to use by checking the box.

- Read Community:
Specify the community name which has read-only access to all supported SNMP objects. The default value is "public".

- Write Community:
Specify the community name which has read/write access to all supported SNMP objects (except read-only objects). The default value is "private".

Traps for SNMP v1/v2 :

Traps are used by the IP Camera to send messages to a management system about 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.

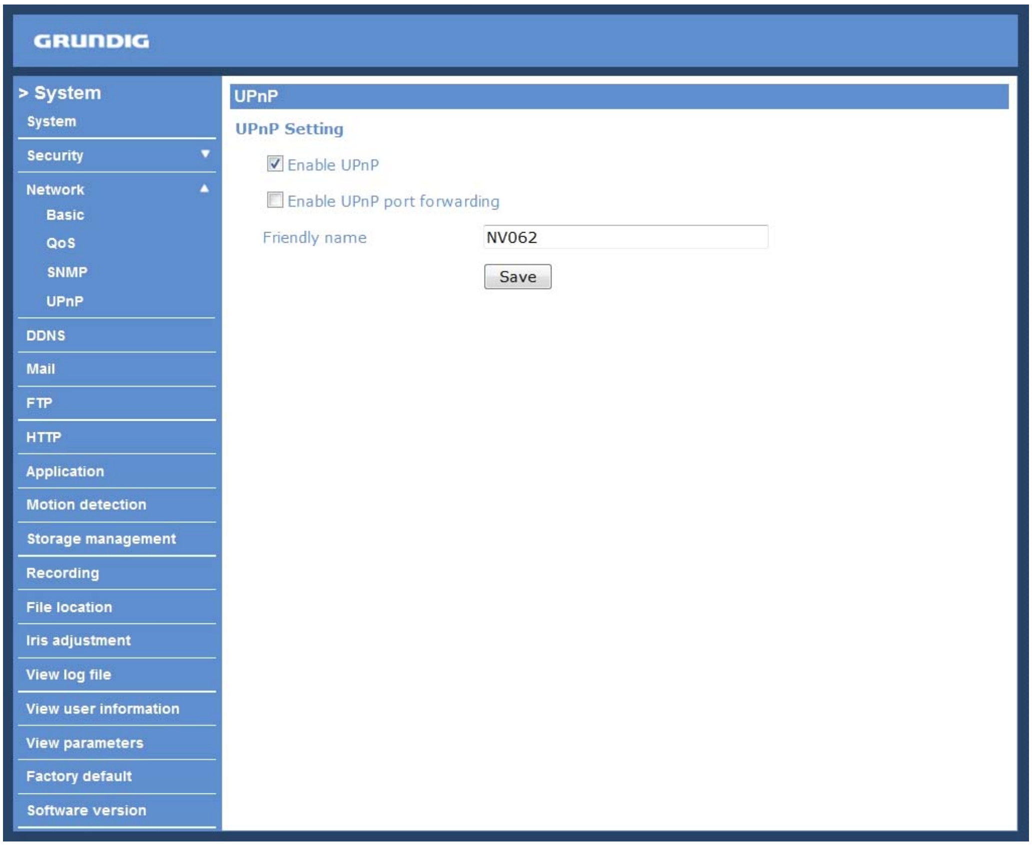
Trap Option :

- Warm Start:

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

Click the “Save” button to complete the setting.

<UPnP> :



UPnP

UPnP Setting

☑ Enable UPnP

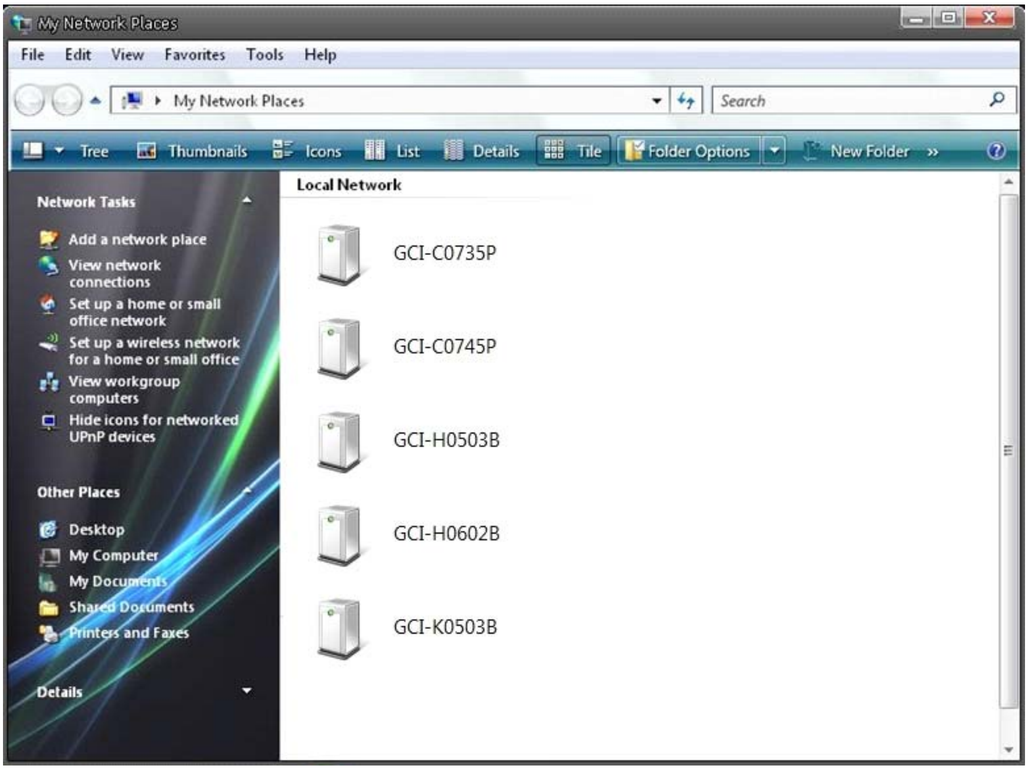
□ Enable UPnP port forwarding

Friendly name: NV062

UPnP Setting :

- Enable UPnP:

When the UPnP is enabled, 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.



NOTE: To enable this function, please make sure the UPnP component is installed on your computer. Please refer to chapter 16. 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.

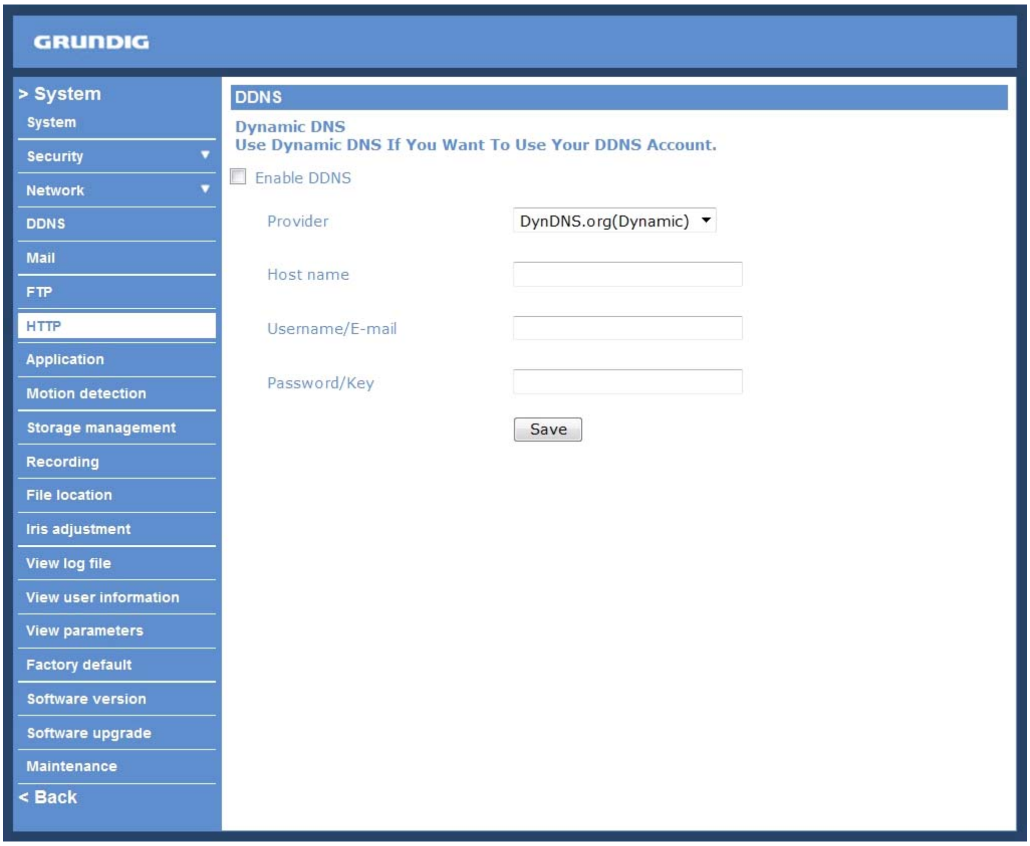
NOTE: To enable this function, please make sure that your router supports UPnP and is activated.

- Friendly name:

Set the name for the IP Camera for identity.

9.4. DDNS

The Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronised 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 that others can connect to it through this name.



DDNS

Dynamic DNS
Use Dynamic DNS If You Want To Use Your DDNS Account.

□ Enable DDNS

Provider: DynDNS.org(Dynamic)

Host name:

Username/E-mail:

Password/Key:

Enable DDNS :
Check the item to enable DDNS.

Provider :
Select one DDNS host from the provider list.

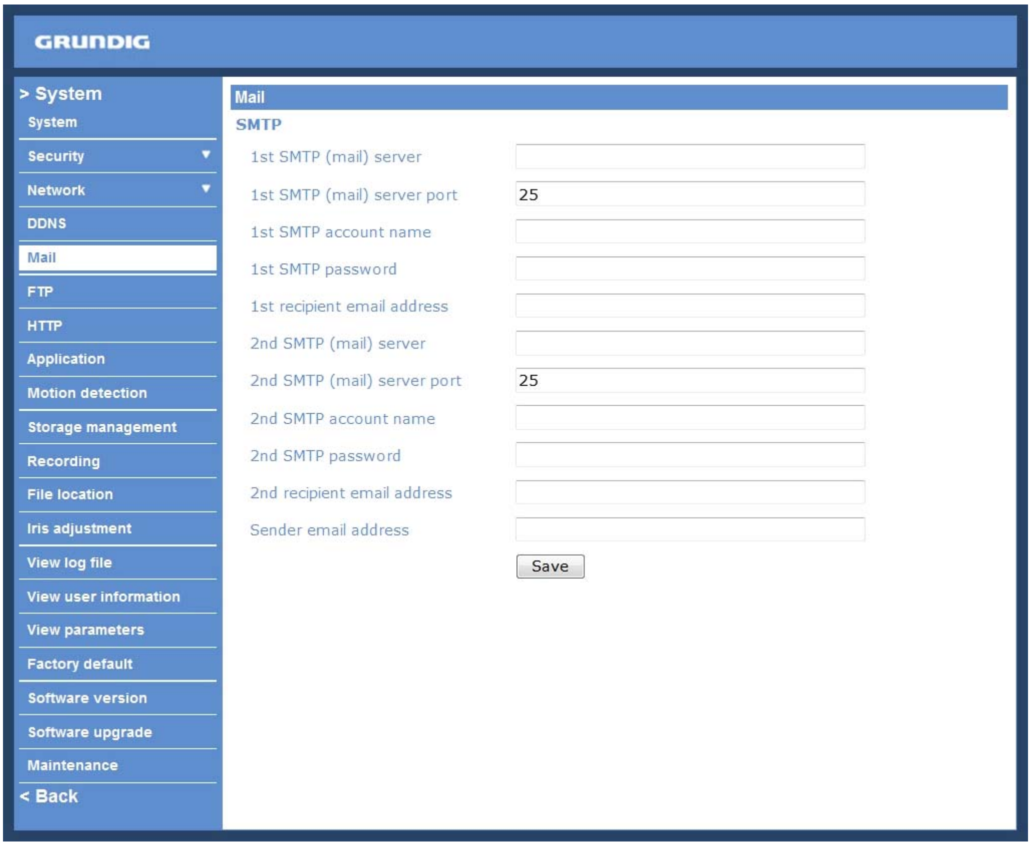
Host name :
Enter the registered domain name in the field.

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

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

9.5. Mail

The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when a motion is detected. 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 to whom the message text is transferred. The configuration page is shown below:



Mail

SMTP

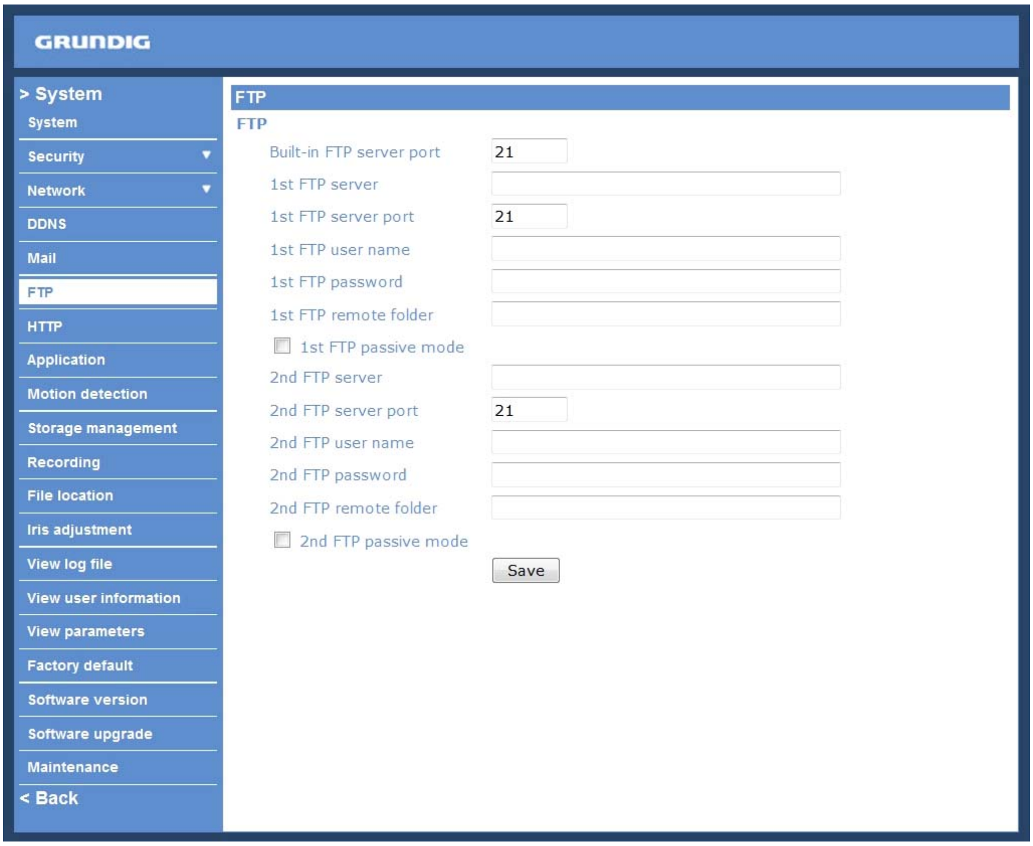
1st SMTP (mail) server	
1st SMTP (mail) server port	25
1st SMTP account name	
1st SMTP password	
1st recipient email address	
2nd SMTP (mail) server	
2nd SMTP (mail) server port	25
2nd SMTP account name	
2nd SMTP password	
2nd recipient email address	
Sender email address	

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

Click the "Save" button to save the changes.

9.6. FTP

The Administrator can set to sending alarm messages to a specific File Transfer Protocol (FTP) site when motion is detected. Users can assign an 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. Click "Save" when the setting is finished.



FTP

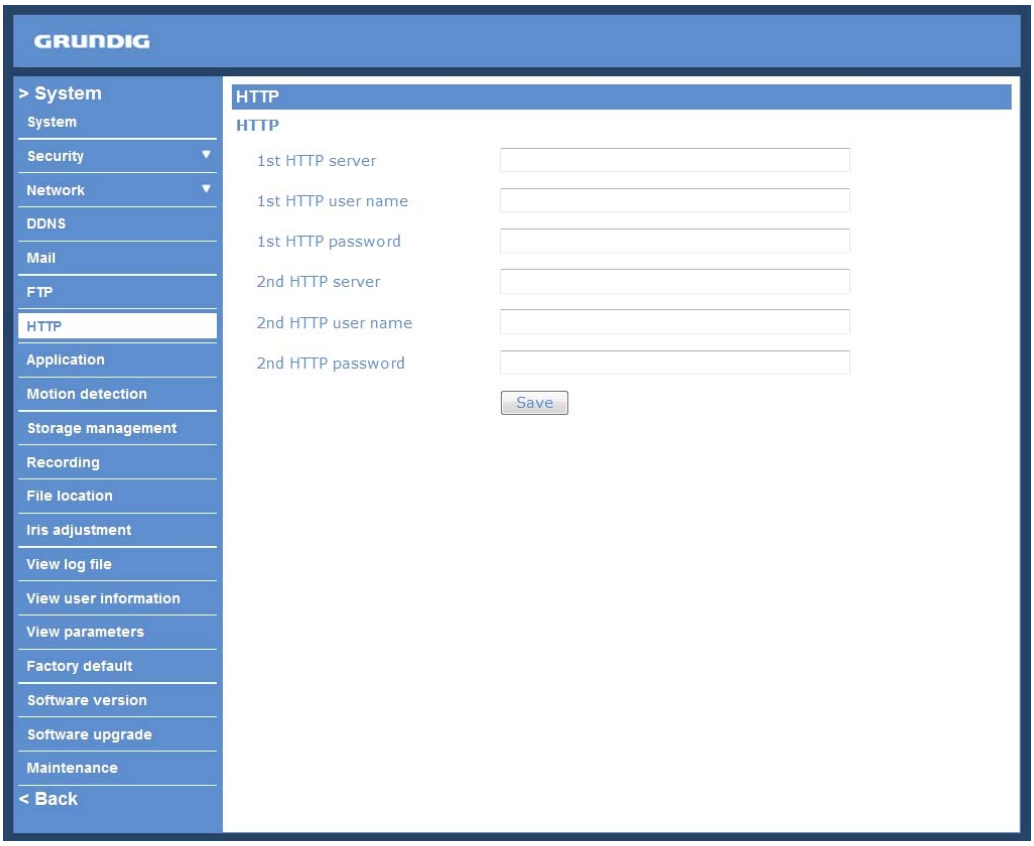
FTP

Built-in FTP server port	21
1st FTP server	
1st FTP server port	21
1st FTP user name	
1st FTP password	
1st FTP remote folder	
□ 1st FTP passive mode	
2nd FTP server	
2nd FTP server port	21
2nd FTP user name	
2nd FTP password	
2nd FTP remote folder	
□ 2nd FTP passive mode	

Save

9.7. 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 the setting is finished.

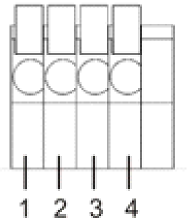


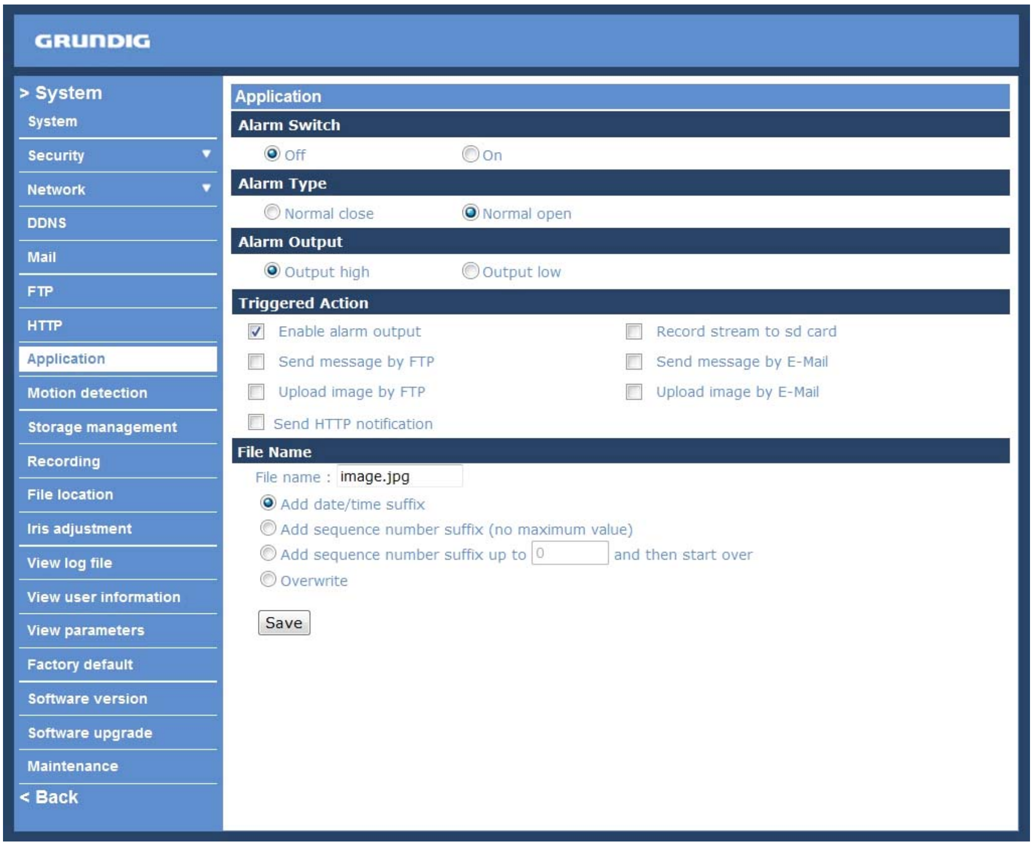
Please refer to: 9.8. Application: Send HTTP notification / 9.9. Motion Detection for HTTP Notification settings.

9.8. Application (Alarm Settings)

The IP Camera equips one alarm input and one relay output for cooperating with the alarm system to catch events' images. Refer to the 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-





Application

Alarm Switch

● Off ○ On

Alarm Type

○ Normal close ● Normal open

Alarm Output

● Output high ○ Output low

Triggered Action

☑ Enable alarm output ☐ Record stream to sd card

☐ Send message by FTP ☐ Send message by E-Mail

☐ Upload image by FTP ☐ Upload image by E-Mail

☐ Send HTTP notification

File Name

File name : image.jpg

● Add date/time suffix

○ Add sequence number suffix (no maximum value)

○ Add sequence number suffix up to 0 and then start over

○ Overwrite

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.

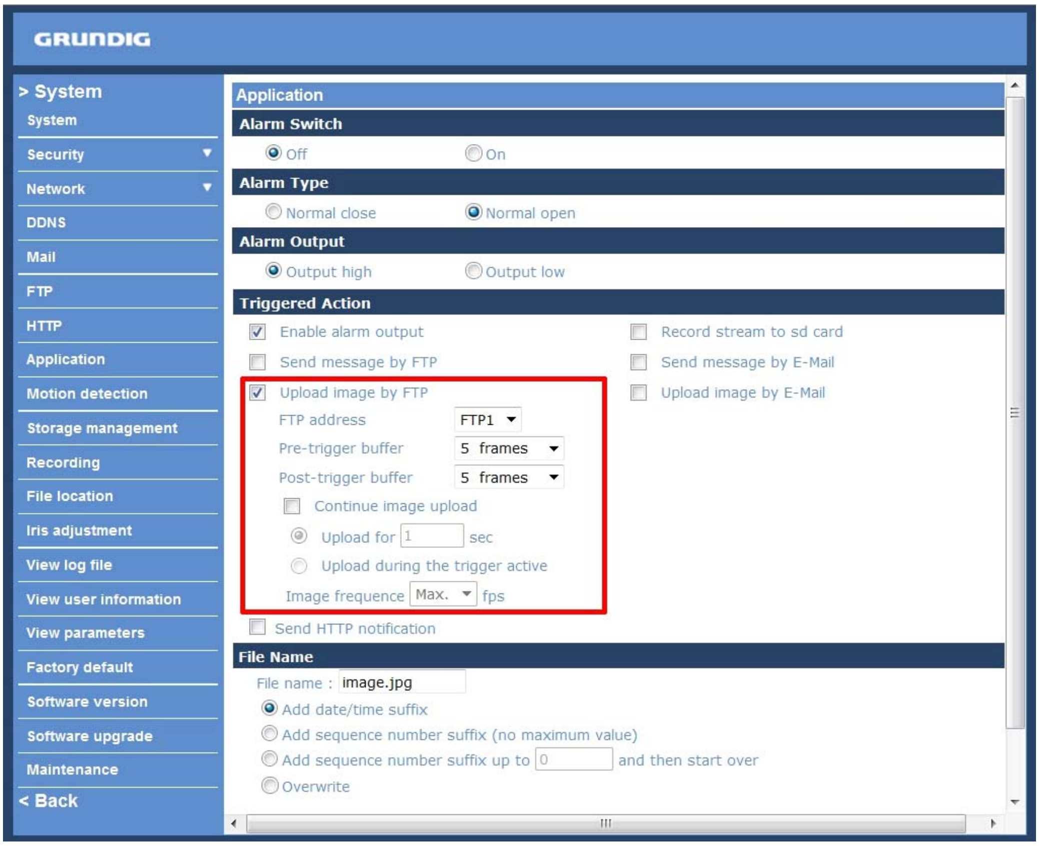
Alarm Output :
Define alarm output signal as “high” or “low” for the normal alarm output status according to the current alarm application.

Triggered Action (Multi-option) :
The Administrator can specify alarm actions that will take place when motion is detected. 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 choose to send an alarm message by FTP and/or by E-Mail when a 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 the alarm is triggered, event images will be uploaded to the appointed FTP site.



Application

Alarm Switch
● Off ○ On

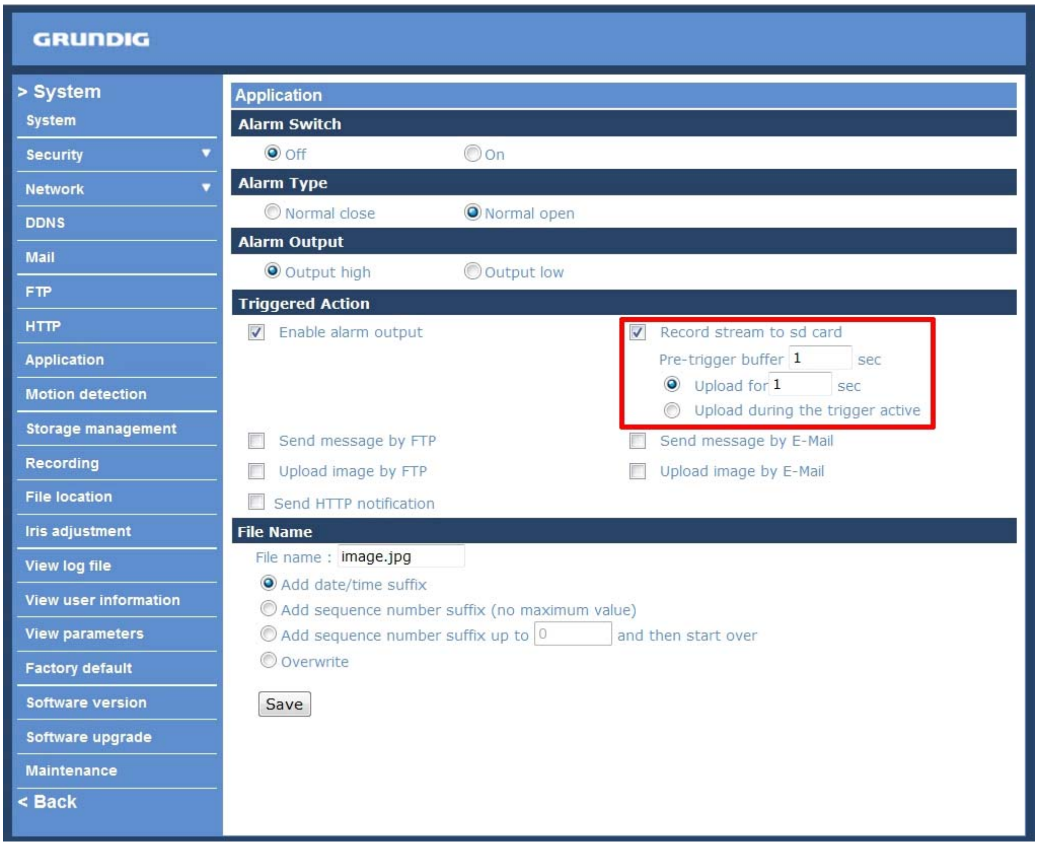
Alarm Type
○ Normal close ● Normal open

Alarm Output
● Output high ○ Output low

Triggered Action
☑ Enable alarm output
□ Record stream to sd card
□ Send message by FTP
□ Send message by E-Mail
☑ Upload image by FTP
□ Upload image by E-Mail
FTP address: FTP1
Pre-trigger buffer: 5 frames
Post-trigger buffer: 5 frames
□ Continue image upload
● Upload for 1 sec
○ Upload during the trigger active
Image frequence Max. fps
□ Send HTTP notification

File Name
File name : image.jpg
● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

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



Application

Alarm Switch
● Off ○ On

Alarm Type
○ Normal close ● Normal open

Alarm Output
● Output high ○ Output low

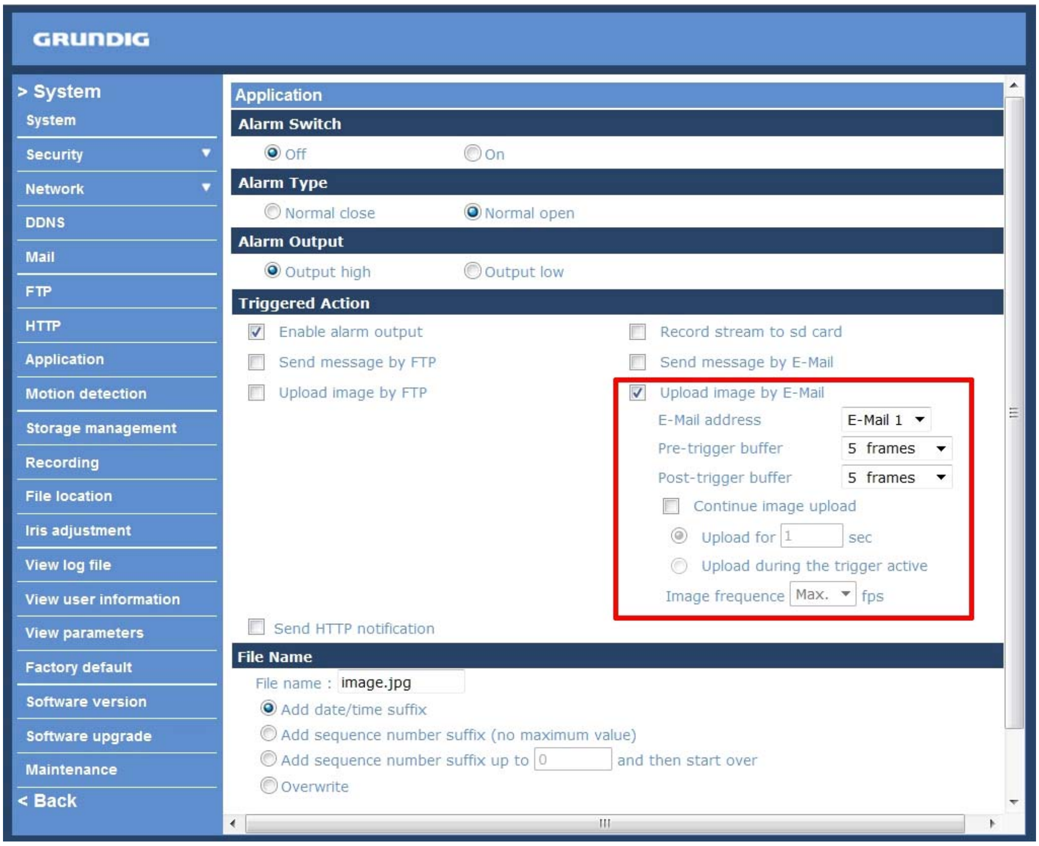
Triggered Action
☑ Enable alarm output
☑ Record stream to sd card
Pre-trigger buffer 1 sec
● Upload for 1 sec
○ Upload during the trigger active
□ Send message by FTP
□ Send message by E-Mail
□ Upload image by FTP
□ Upload image by E-Mail
□ Send HTTP notification

File Name
File name : image.jpg
● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.12. 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.



Application

Alarm Switch

● Off ○ On

Alarm Type

○ Normal close ● Normal open

Alarm Output

● Output high ○ Output low

Triggered Action

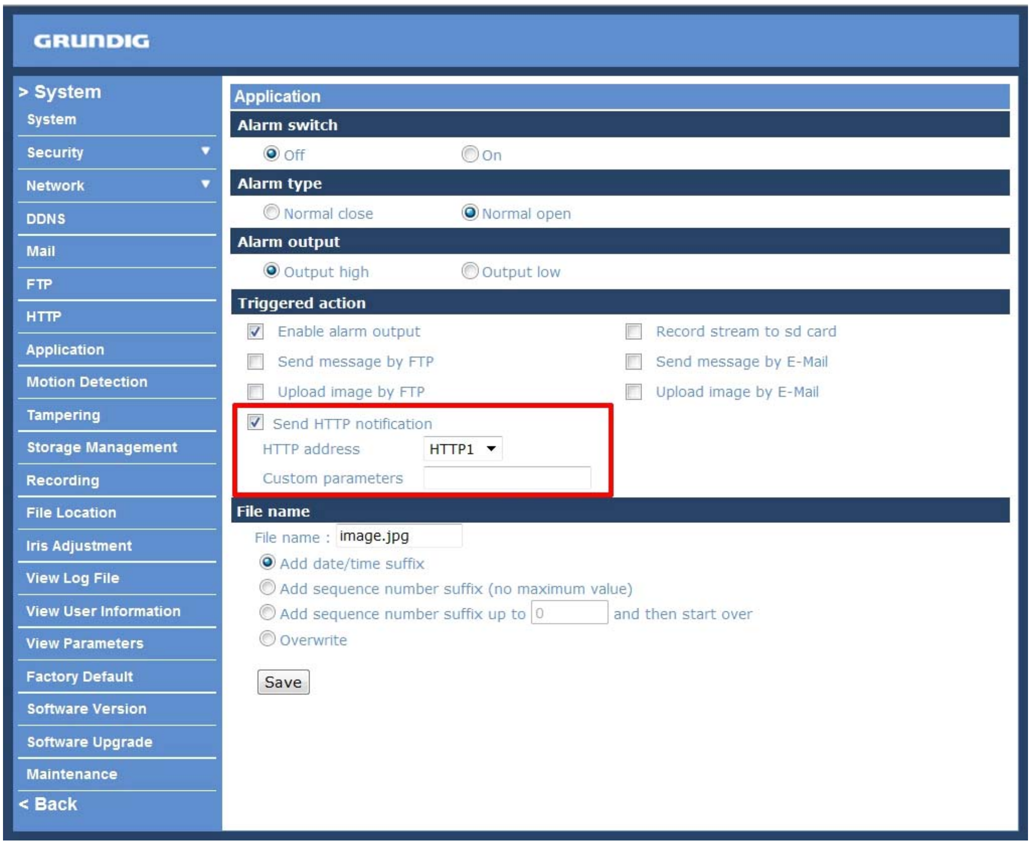
☑ Enable alarm output
□ Record stream to sd card
□ Send message by FTP
□ Send message by E-Mail
□ Upload image by FTP
☑ Upload image by E-Mail
E-Mail address: E-Mail 1
Pre-trigger buffer: 5 frames
Post-trigger buffer: 5 frames
□ Continue image upload
● Upload for 1 sec
○ Upload during the trigger active
Image frequence Max. fps
□ Send HTTP notification

File Name

File name : image.jpg
● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

NOTE: Make sure SMTP or FTP configuration has been completed. See section 9.5. Mail and 9.6. FTP for further details.

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



Application

Alarm switch
● Off ○ On

Alarm type
○ Normal close ● Normal open

Alarm output
● Output high ○ Output low

Triggered action
☑ Enable alarm output □ Record stream to sd card
□ Send message by FTP □ Send message by E-Mail
□ Upload image by FTP □ Upload image by E-Mail
☑ Send HTTP notification
HTTP address: HTTP1
Custom parameters:

File name
File name : image.jpg
● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

File Name :
Enter a file name into the blank box, e.g. 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 up to _ and then start over:
File Name: imageXX.jpg
X: Sequence Number

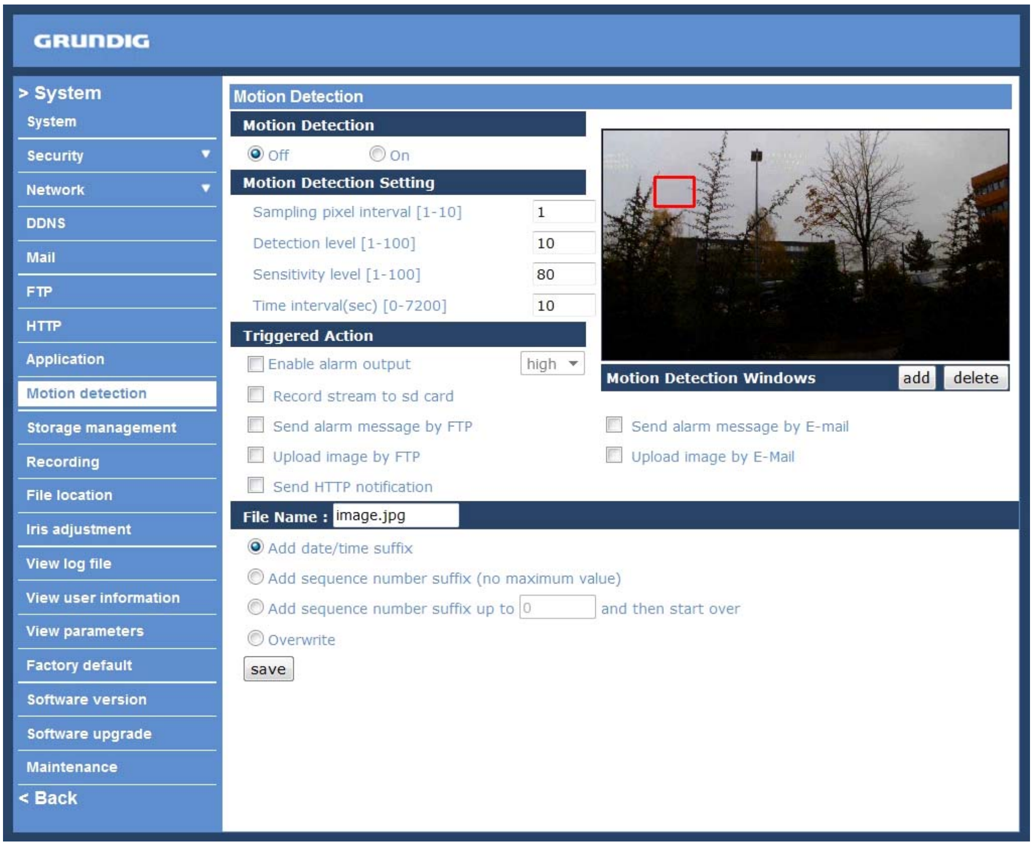
The file name suffix will end at the number being set. For example, if the setting is "10" the file name will start from 00, end at 10, and then start all over again.

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

Save :
After completing all the settings mentioned above, please click on the Save button to save all the settings in this page.

9.9. Motion Detection

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



Motion Detection

Motion Detection

● Off ○ On

Motion Detection Setting

Sampling pixel interval [1-10]	1
Detection level [1-100]	10
Sensitivity level [1-100]	80
Time interval(sec) [0-7200]	10

Triggered Action

□ Enable alarm output high

□ Record stream to sd card

□ Send alarm message by FTP □ Send alarm message by E-mail

□ Upload image by FTP □ Upload image by E-Mail

□ Send HTTP notification

File Name : image.jpg

● Add date/time suffix

○ Add sequence number suffix (no maximum value)

○ Add sequence number suffix up to 0 and then start over

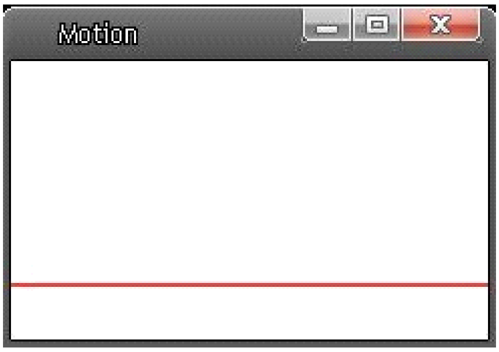
○ Overwrite

save

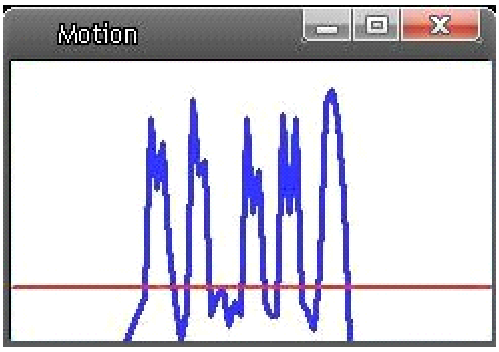
In the Motion Detection setting page is a frame (Motion Detection Window) displayed in the Live View Pane. The Motion Detection Window is for defining the motion detection area. To change the size of the Motion Detection Window, move the mouse cursor to the edge of the frame and draw it outward/inward.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

Up to 10 Motion Detection Windows can be set. Press the “Add” button under the Live View 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 the Motion Detection function is activated, the pop-up window (Motion) with indication of motion will be shown.



When motion is detected, the signals will be displayed in 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 the System section: Motion Detection. The default setting is Off.

Motion Detection Setting :
Users can adjust various parameters of Motion Detection in this section.

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

- Detection level [1-100]:
The default level is 10. This item is to set the 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 as changing, the 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 accordingly lower.

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

Triggered Action (Multi-option) :
The Administrator can specify alarm actions that will take place when the alarm is triggered. 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.

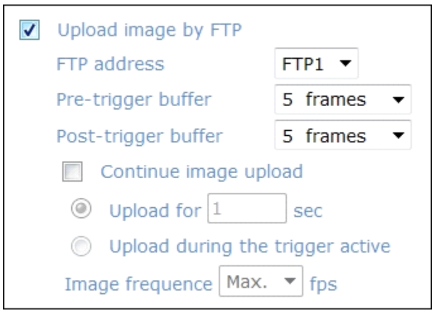
- Record stream to SD Card:
Select this item, and the Motion Detection recording will be stored on a Micro SD/SDHC card when motion is detected.

NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.12. Recording for further details.

- Send Alarm Message by FTP/E-Mail:
The Administrator can choose to send an alarm message by FTP and/or by E-Mail when a 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 picture below. When a motion is detected, event images will be uploaded to the appointed FTP site.



☑ Upload image by FTP

FTP address: FTP1

Pre-trigger buffer: 5 frames

Post-trigger buffer: 5 frames

□ Continue image upload

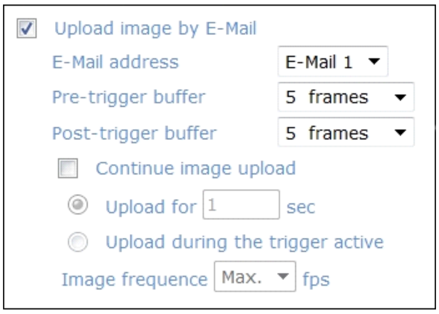
● Upload for 1 sec

○ Upload during the trigger active

Image frequence Max. fps

- 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 picture below. When a motion is detected, event images will be sent to the appointed e-mail address.



☑ Upload image by E-Mail

E-Mail address: E-Mail 1

Pre-trigger buffer: 5 frames

Post-trigger buffer: 5 frames

□ Continue image upload

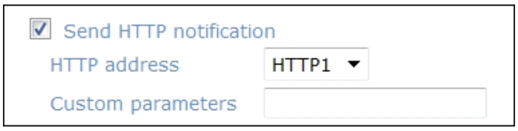
● Upload for 1 sec

○ Upload during the trigger active

Image frequence Max. fps

- Send HTTP notification:

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



☑ Send HTTP notification

HTTP address: HTTP1

Custom parameters:

NOTE: Make sure SMTP or FTP configuration has been completed. See section 9.5. Mail and 9.6. FTP for further details.

File Name :

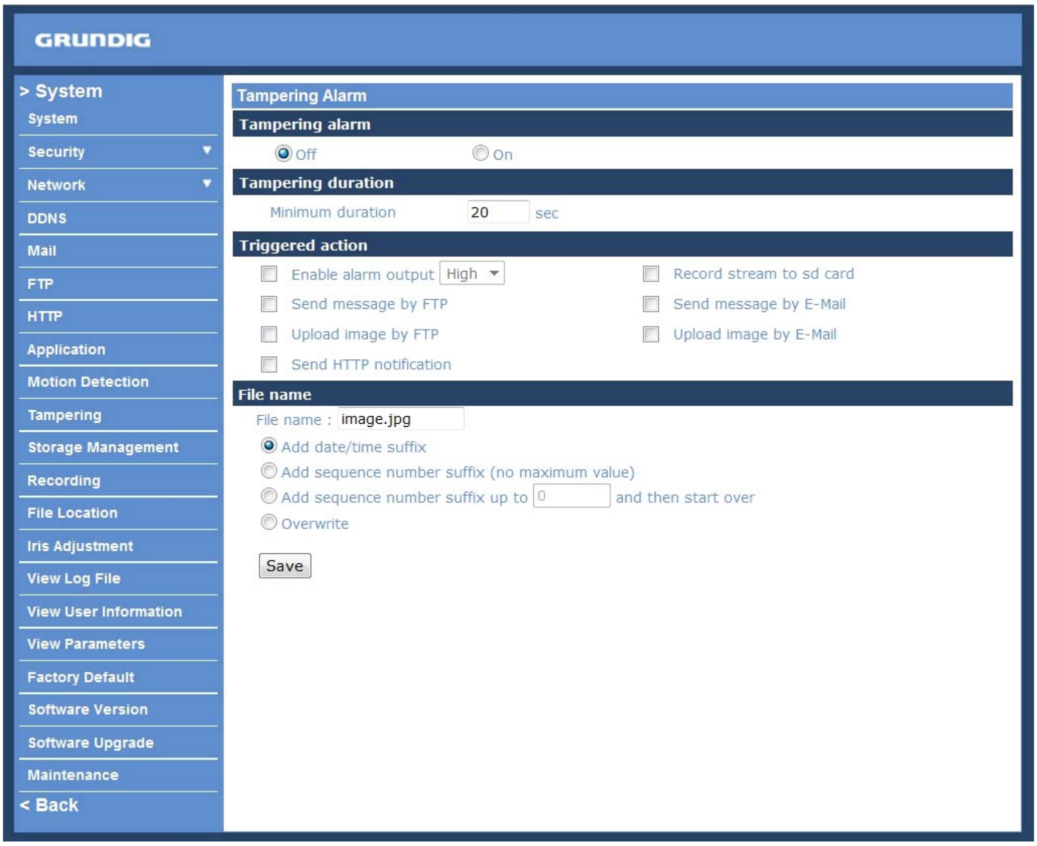
The uploaded image's filename format can be set in this section. Please select the one that meets your requirements.

Save :

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

9.10. Tampering

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



Tampering Alarm

Tampering alarm

● Off ○ On

Tampering duration

Minimum duration 20 sec

Triggered action

□ Enable alarm output High □ Record stream to sd card

□ Send message by FTP □ Send message by E-Mail

□ Upload image by FTP □ Upload image by E-Mail

□ Send HTTP notification

File name

File name : image.jpg

● Add date/time suffix

○ Add sequence number suffix (no maximum value)

○ Add sequence number suffix up to 0 and then start over

○ Overwrite

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 the Tampering Alarm function in the Tampering Alarm setting page. The default setting is Off.

Tampering Duration :
The Minimum Tampering Duration is the time for video analysis to determine whether any camera tampering has occurred. Minimum Duration can also be interpreted as defining the Tampering threshold; longer duration represents a 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 place when tampering is detected. All options are listed as follows:

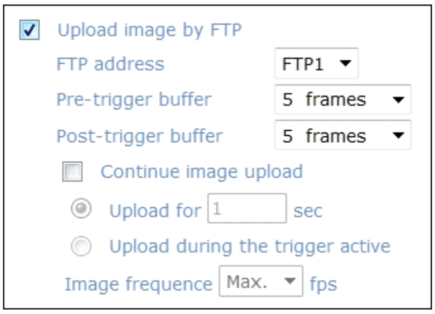
- Enable Alarm Output:
Check this item and select the predefined type of alarm output to enable alarm relay output when tampering is detected.

- Record stream to SD Card:
Select this item, and the Tampering Alarm recording will be stored on a 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 9.12. 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 FTP

FTP address: FTP1

Pre-trigger buffer: 5 frames

Post-trigger buffer: 5 frames

□ Continue image upload

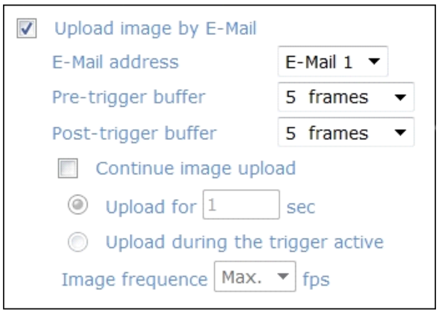
● Upload for 1 sec

○ Upload during the trigger active

Image frequence Max. fps

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

- 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.



☑ Upload image by E-Mail

E-Mail address: E-Mail 1

Pre-trigger buffer: 5 frames

Post-trigger buffer: 5 frames

□ Continue image upload

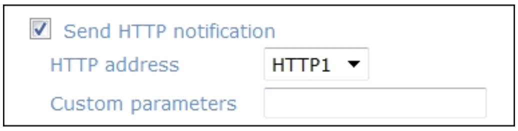
● Upload for 1 sec

○ Upload during the trigger active

Image frequence Max. fps

NOTE: Make sure SMTP or FTP configuration has been completed. See section 9.5. Mail and 9.6. 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.



☑ Send HTTP notification

HTTP address: HTTP1

Custom parameters:

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

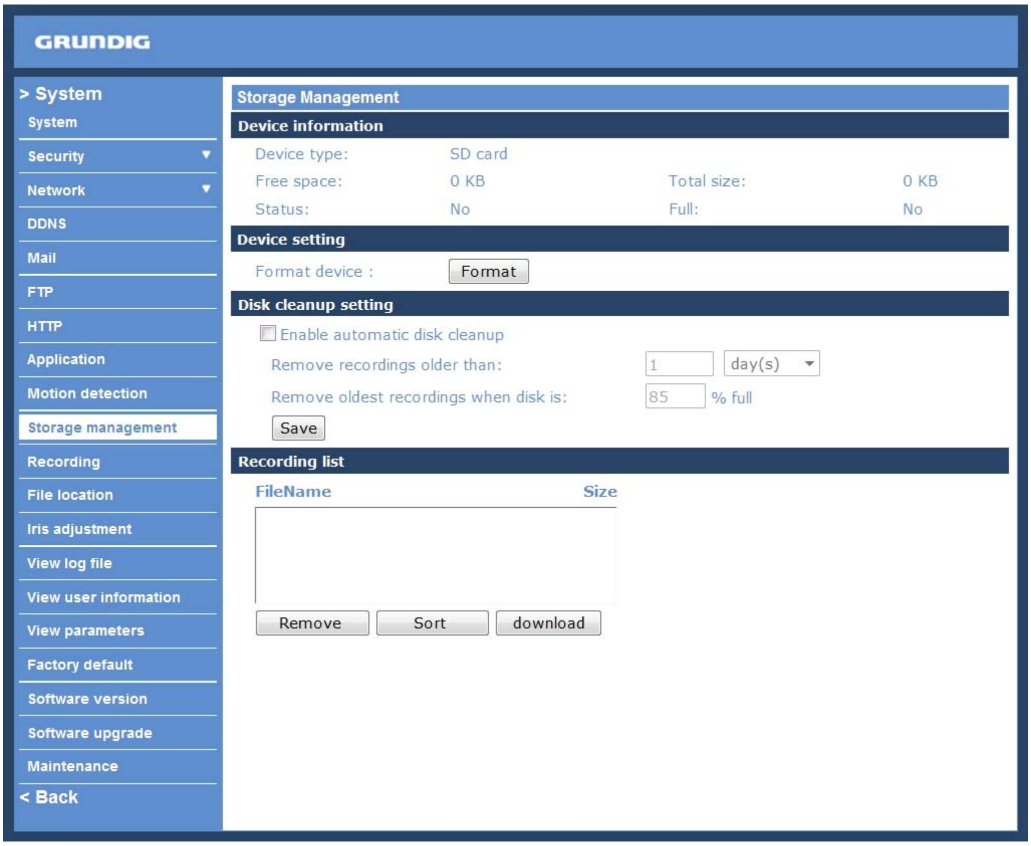
Save :
Click the Save button to save all the Tampering Alarm settings mentioned above.

9.11. Storage Management

Users can store local recordings on a Micro SD/SDHC card up to 16 GB. 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 9.12. Recording) for activation.

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



Storage Management

Device information

Device type: SD card

Free space: 0 KB   Total size: 0 KB

Status: No   Full: No

Device setting

Format device : Format

Disk cleanup setting

☐ Enable automatic disk cleanup

Remove recordings older than: 1 day(s)

Remove oldest recordings when disk is: 85 % full

Save

Recording list

FileName	Size

Remove   Sort   download

Device Information :
When users insert the Micro SD/SDHC card, the card information such as the memory capacity and status will be shown in the Device Information section. For the memory card being successfully installed, its status shall be shown in the “Device information” section in the Storage Management page.

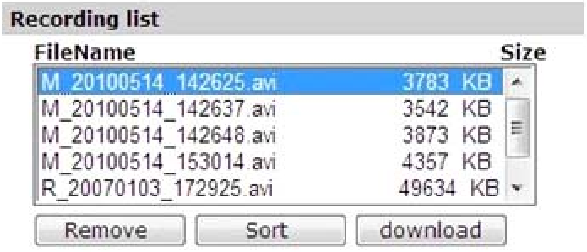
Device Setting :
Press the “Format” button to format the memory card.

Disk Cleanup Setting :
Users can enable an 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).

If the recording modus is set to Always and at the same time the event recording (when a motion detection or an alarm takes place) is also turned on, in this case, when an event occurs, the event will be recorded first, afterwards the camera will return to normal recording mode.

When the recording mode is set to “Always” (consecutive recording) in the submenu "Recording" and the Micro SD/SDHC card recording is also allowed to be enabled when triggered by events, once the events occur, the system will immediately implement the recorded events to the memory card. After events recording, the IP Camera will return to regular recording mode.



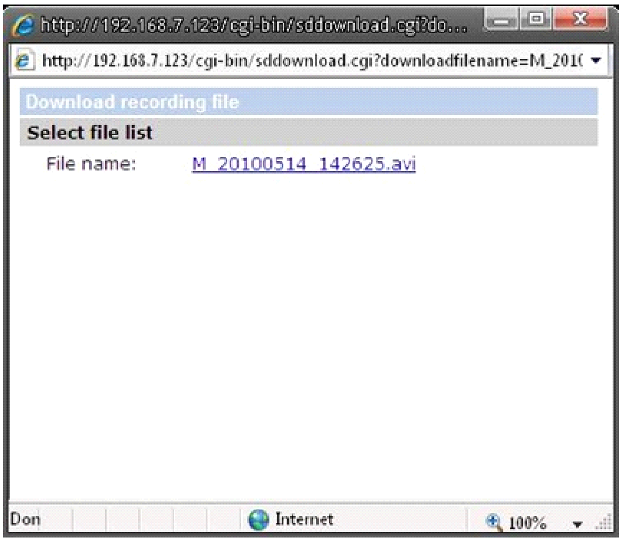
Recording list

FileName	Size
M_20100514_142625.avi	3783 KB
M_20100514_142637.avi	3542 KB
M_20100514_142648.avi	3873 KB
M_20100514_153014.avi	4357 KB
R_20070103_172925.avi	49634 KB

- 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.

- 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.



http://192.168.7.123/cgi-bin/sddownload.cgi?do...

http://192.168.7.123/cgi-bin/sddownload.cgi?downloadfilename=M_201(

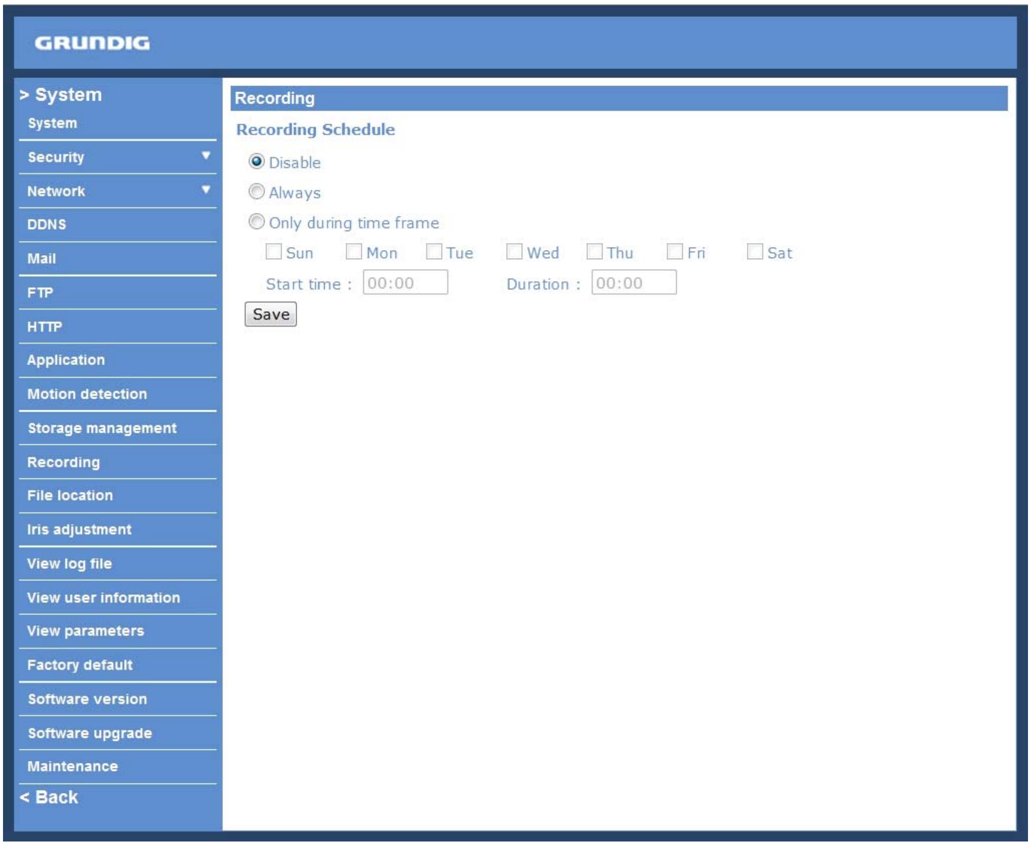
Download recording file

Select file list

File name: M_20100514_142625.avi

9.12. Recording

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



Recording

Recording Schedule

● Disable

○ Always

○ Only during time frame

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Start time : 00:00 Duration : 00:00

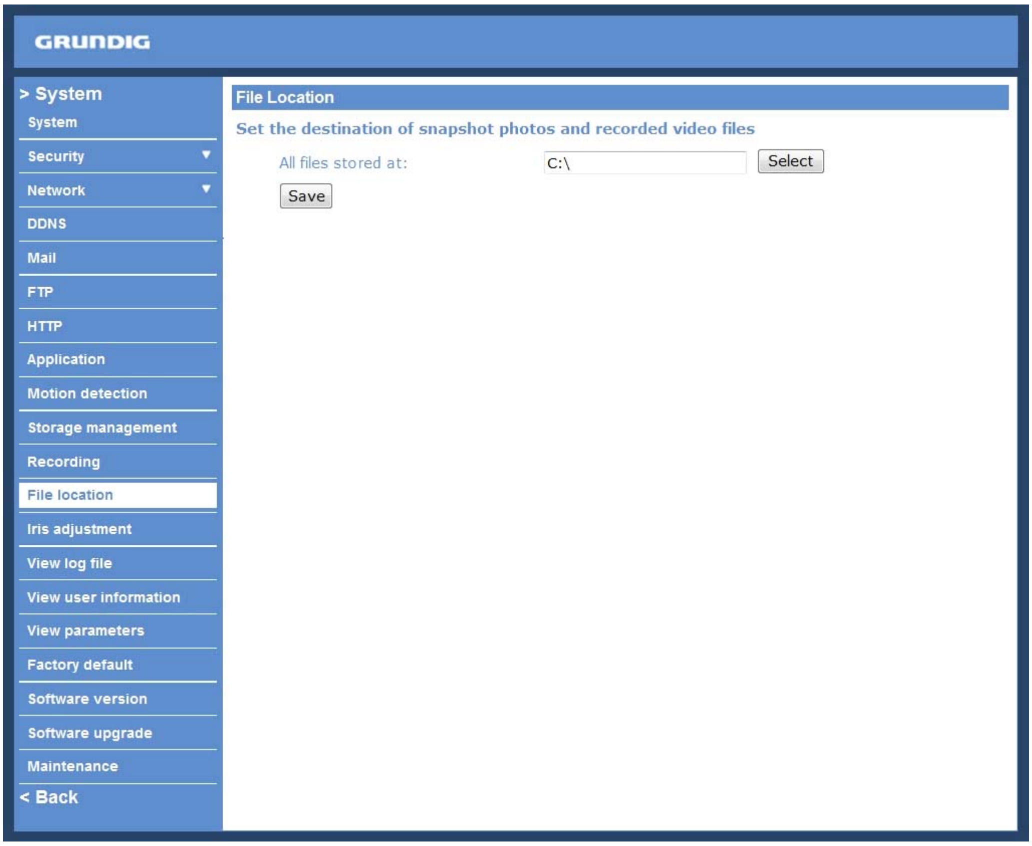
Activating Micro SD/SDHC Card Recording :
Two types of schedule mode are offered: "Always" and "Only during time frame". Users can setup the time frame to fit the recording schedule or choose “Always” to allow the Micro SD/SDHC Card Recording to be activated all the time.
Please click on the “Save” button to confirm the schedule mode.

Terminating Micro SD/SDHC Card Recording :
Select “Disable” to terminate the recording function.

9.13. File Location

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

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



File Location

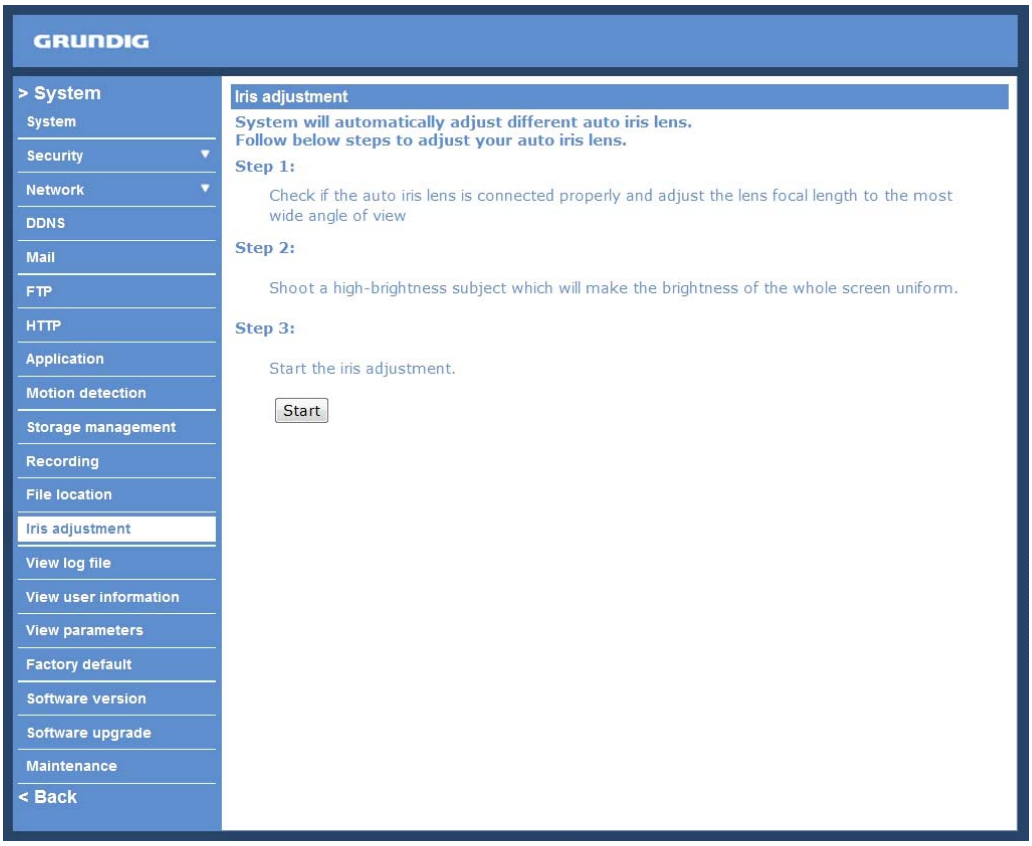
Set the destination of snapshot photos and recorded video files

All files stored at: C:\

NOTE: Users with Windows 7 operating system need to follow the following procedure to be able to use the Snapshot and Recording function. First you need to log on to your computer as an Administrator. Then you go to Windows Start menu, click with the right mouse button on your Internet Browser and select in the appearing pop-up window “Run as Administrator”. Afterwards you can log in to your camera as usual (as an administrator or user).

9.14. Iris Adjustment

For users who use an auto-iris lens, when it is required to undertake an iris adjustment, please refer to the iris adjustment procedure in the sub-menu Iris Adjustment to adjust the iris.



Iris adjustment

System will automatically adjust different auto iris lens.
Follow below steps to adjust your auto iris lens.

Step 1:

Check if the auto iris lens is connected properly and adjust the lens focal length to the most wide angle of view

Step 2:

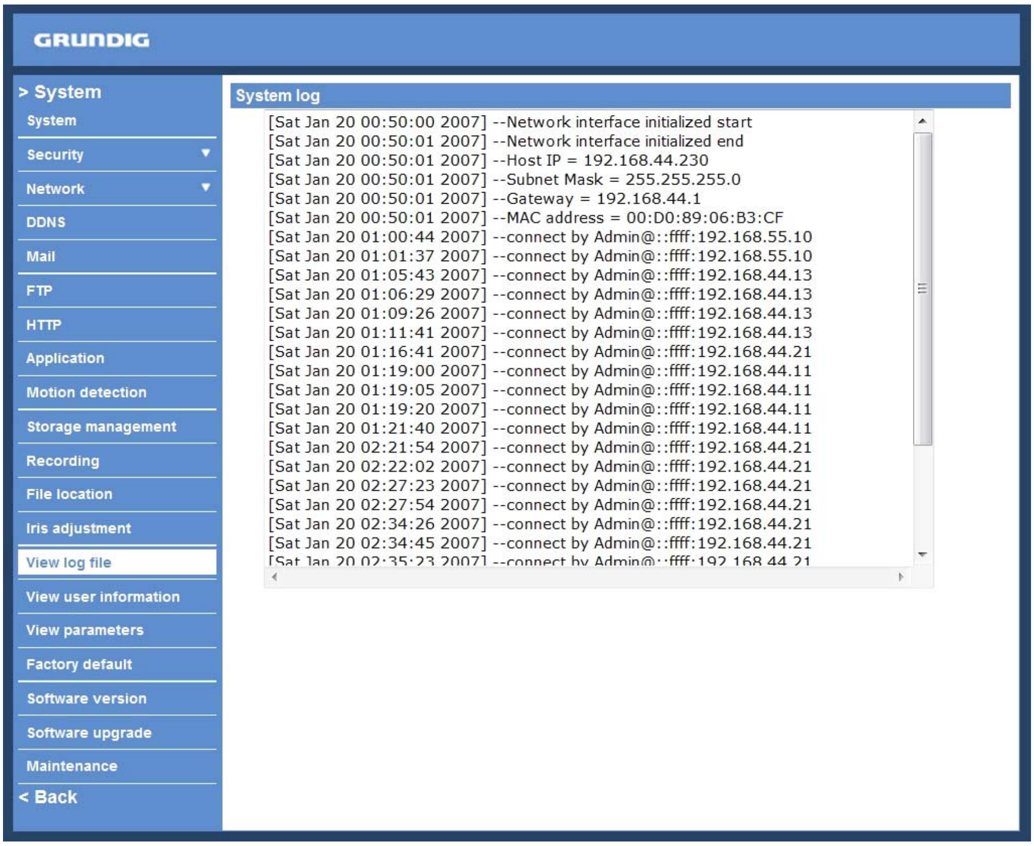
Shoot a high-brightness subject which will make the brightness of the whole screen uniform.

Step 3:

Start the iris adjustment.

9.15. View Log File

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



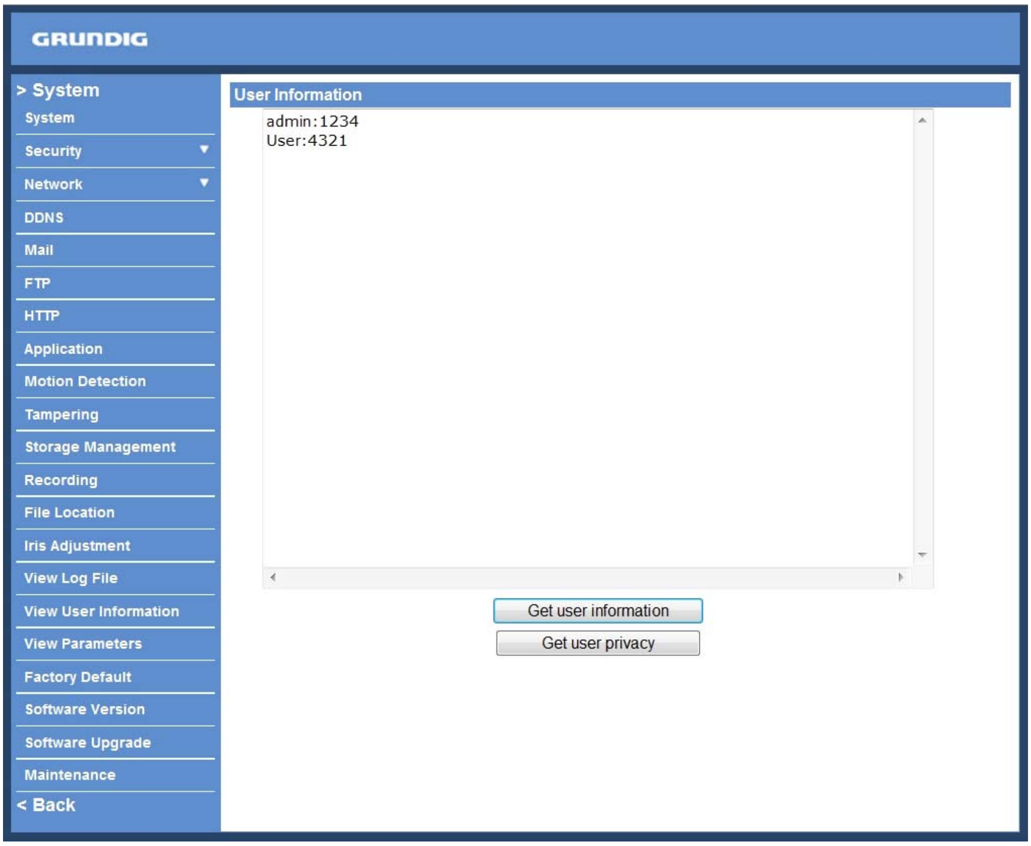
System log

```
[Sat Jan 20 00:50:00 2007] --Network interface initialized start
[Sat Jan 20 00:50:01 2007] --Network interface initialized end
[Sat Jan 20 00:50:01 2007] --Host IP = 192.168.44.230
[Sat Jan 20 00:50:01 2007] --Subnet Mask = 255.255.255.0
[Sat Jan 20 00:50:01 2007] --Gateway = 192.168.44.1
[Sat Jan 20 00:50:01 2007] --MAC address = 00:D0:89:06:B3:CF
[Sat Jan 20 01:00:44 2007] --connect by Admin@::ffff:192.168.55.10
[Sat Jan 20 01:01:37 2007] --connect by Admin@::ffff:192.168.55.10
[Sat Jan 20 01:05:43 2007] --connect by Admin@::ffff:192.168.44.13
[Sat Jan 20 01:06:29 2007] --connect by Admin@::ffff:192.168.44.13
[Sat Jan 20 01:09:26 2007] --connect by Admin@::ffff:192.168.44.13
[Sat Jan 20 01:11:41 2007] --connect by Admin@::ffff:192.168.44.13
[Sat Jan 20 01:16:41 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 01:19:00 2007] --connect by Admin@::ffff:192.168.44.11
[Sat Jan 20 01:19:05 2007] --connect by Admin@::ffff:192.168.44.11
[Sat Jan 20 01:19:20 2007] --connect by Admin@::ffff:192.168.44.11
[Sat Jan 20 01:21:40 2007] --connect by Admin@::ffff:192.168.44.11
[Sat Jan 20 02:21:54 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 02:22:02 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 02:27:23 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 02:27:54 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 02:34:26 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 02:34:45 2007] --connect by Admin@::ffff:192.168.44.21
[Sat Jan 20 02:35:23 2007] --connect by Admin@::ffff:192.168.44.21
```

9.16. View User Information

The Administrator can view each user's login information and their privileges (see section 9.2. Security).

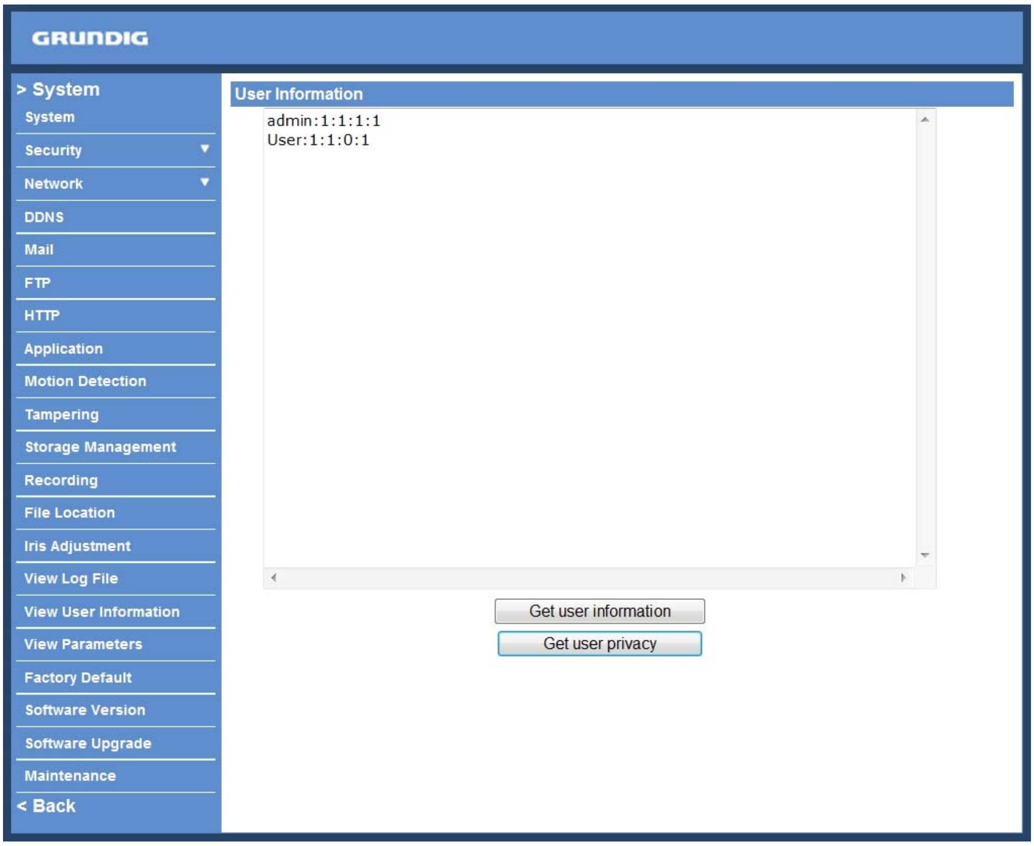
View User Login Information :
All the users in the network will be listed in the "User Information" zone, as shown below. The picture below shows: User: 4321
This indicates that one user's login username is: User, and the password is: 4321



```
admin:1234
User:4321
```

View User Privilege :

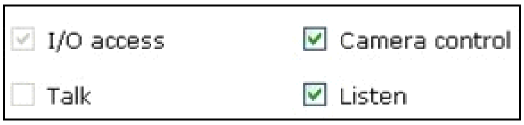
If you press “Get user privacy” at the bottom of the page, the Administrator will be able to view each user’s privileges.



```
admin:1:1:1:1
User:1:1:0:1
```

As the picture above shows: User: 1:1:0:1

1:1:0:1 = I/O access : Camera control : Talk : Listen (see 9.2. Security)

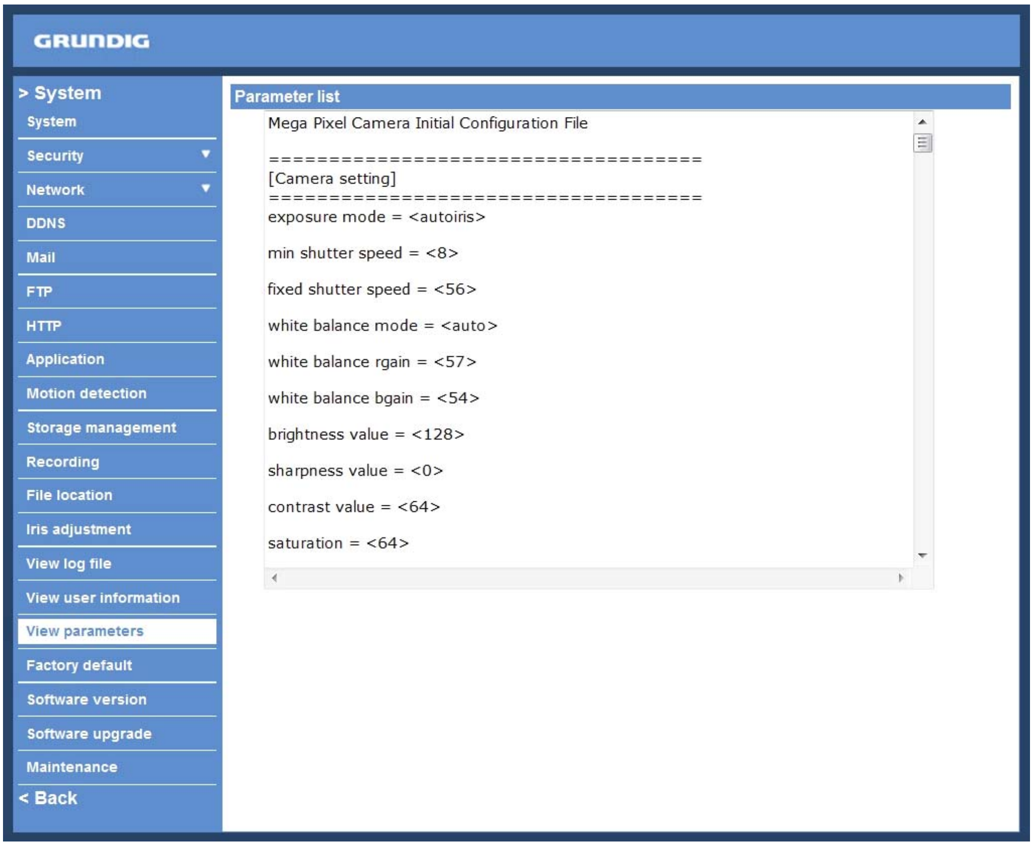


☑ I/O access	☑ Camera control
□ Talk	☑ Listen

This denotes that the user has been granted the privileges of I/O access, Camera control and Listen.

9.17. View Parameters

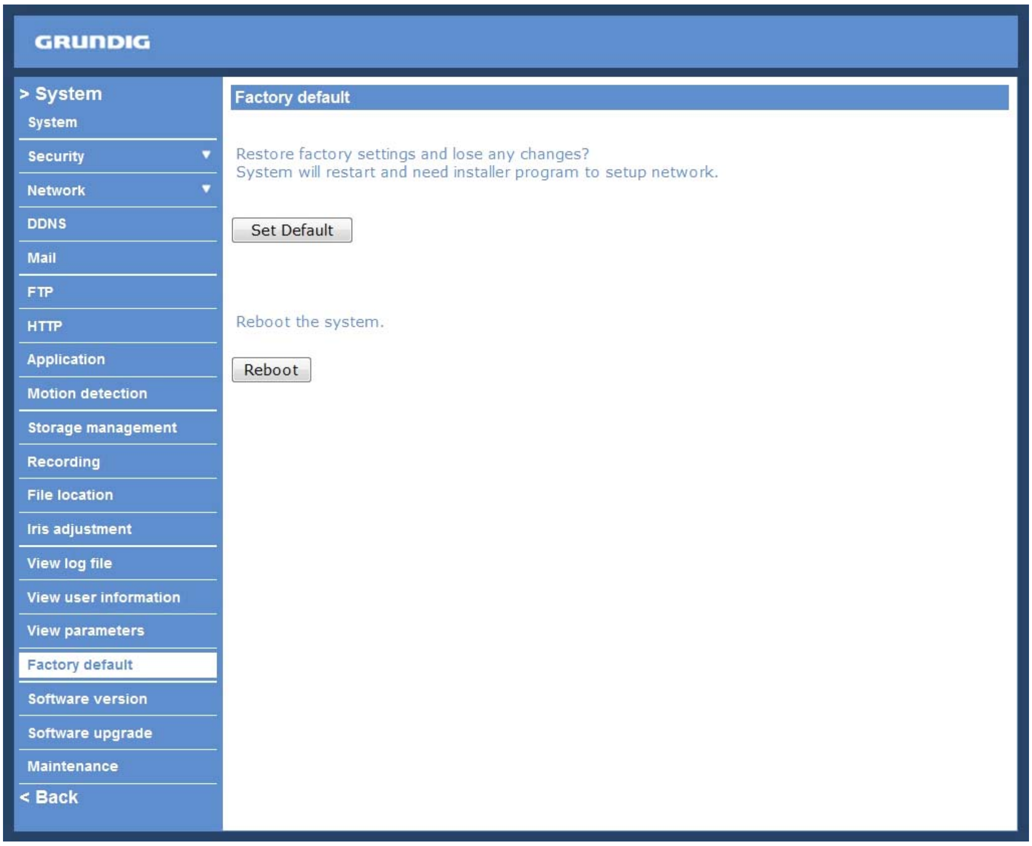
Click on this item to view the entire system's parameter setting.



```
Mega Pixel Camera Initial Configuration File

====================================
[Camera setting]
====================================
exposure mode = <autoiris>

min shutter speed = <8>

fixed shutter speed = <56>

white balance mode = <auto>

white balance rgain = <57>

white balance bgain = <54>

brightness value = <128>

sharpness value = <0>

contrast value = <64>

saturation = <64>
```

9.18. Factory Default

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



Restore factory settings and lose any changes?
System will restart and need installer program to setup network.

Reboot the system.

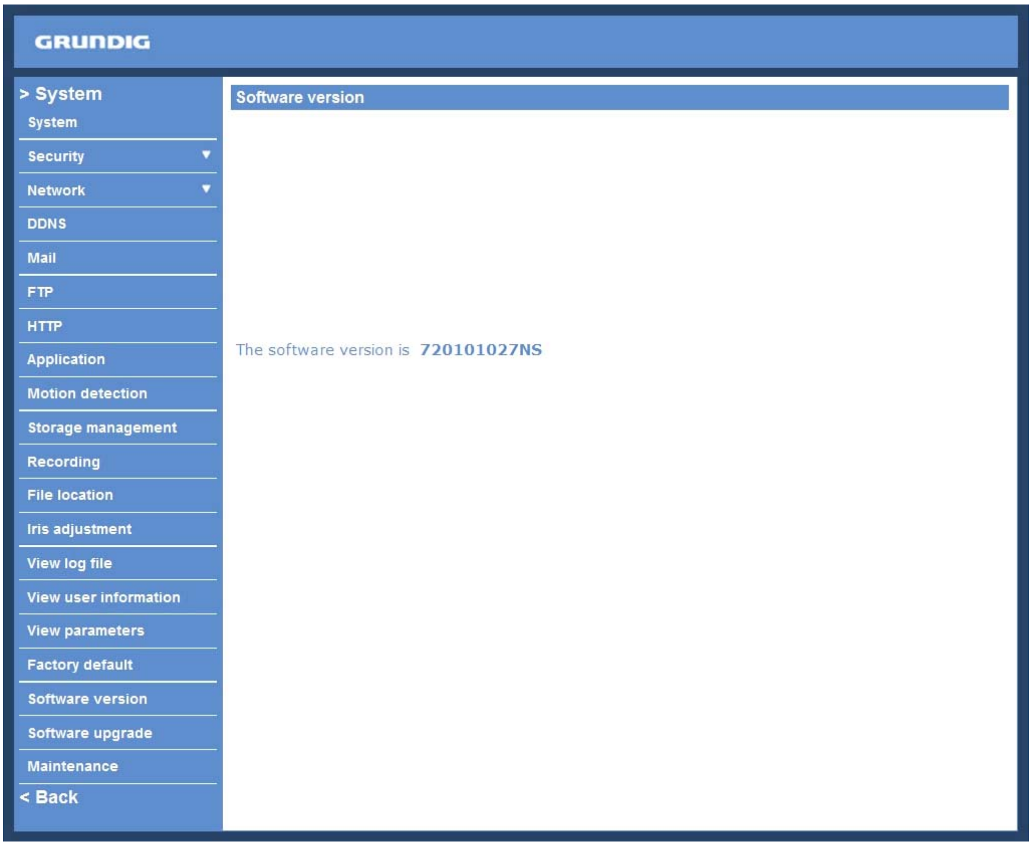
Set Default :
Click on the “Set Default” button to recall the factory default settings. Then the system will restart in 30 seconds.

NOTE: The IP address will be restored to default.

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

9.19. Software Version

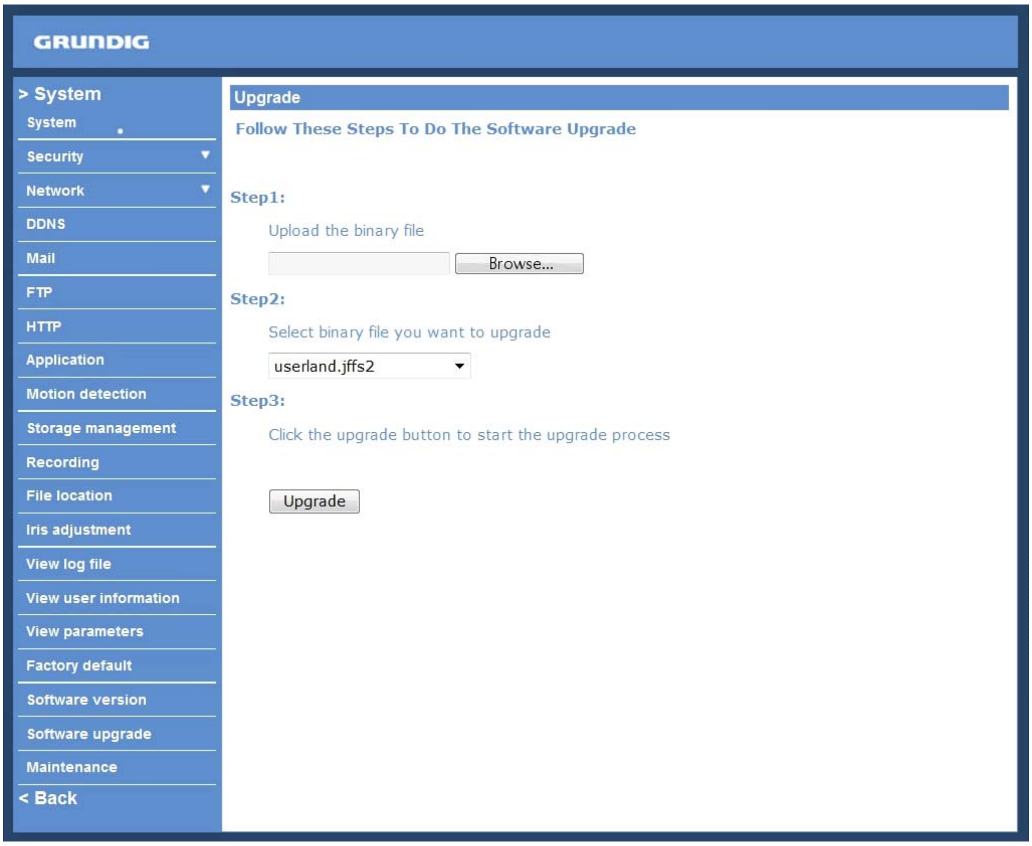
The current software version is displayed in the software version page, which is shown in the picture below.



The software version is 720101027NS

9.20. Software Upgrade

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



Follow These Steps To Do The Software Upgrade

Step1:

Upload the binary file

Step2:

Select binary file you want to upgrade

userland.jffs2

Step3:

Click the upgrade button to start the upgrade process

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

The procedure of a software upgrade is as follows:

Step 1: Click “Browse” and select the binary file to be uploaded, e.g. 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 100% is reached, the upgrade process is finished.
After the upgrade process is finished, the viewer will return to the Home page.

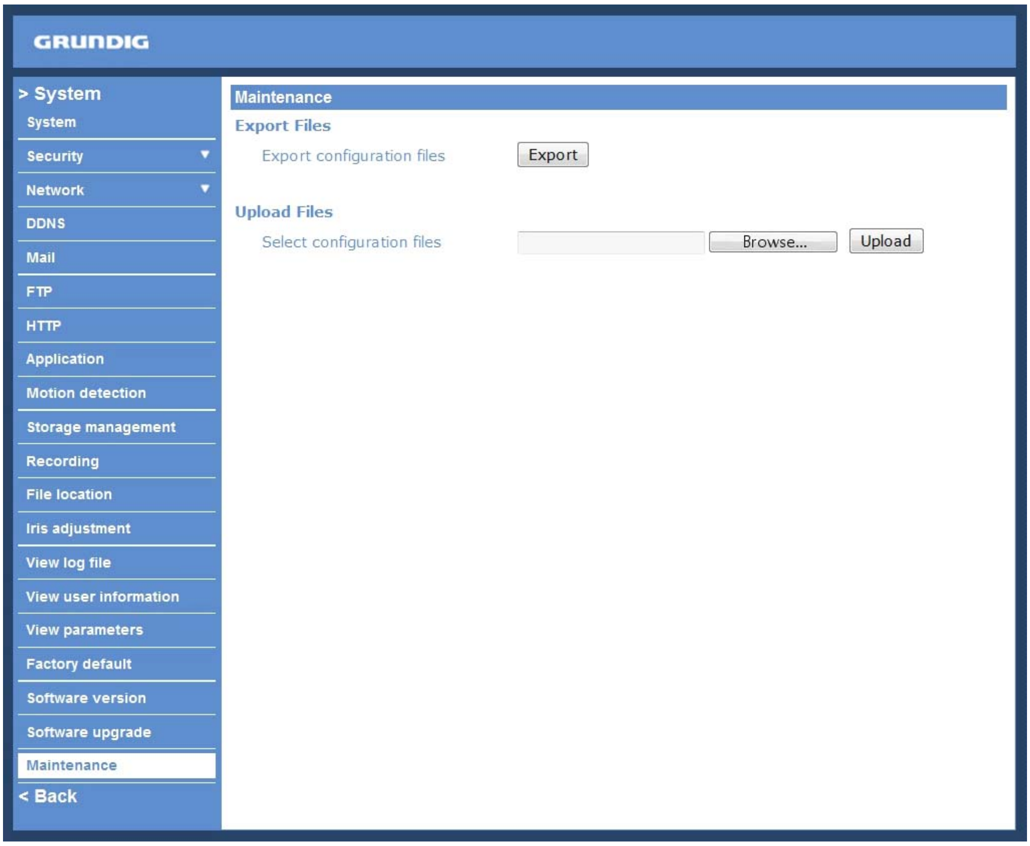
Step 4: Close the video browser.

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

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

9.21. Maintenance

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



Maintenance

Export Files

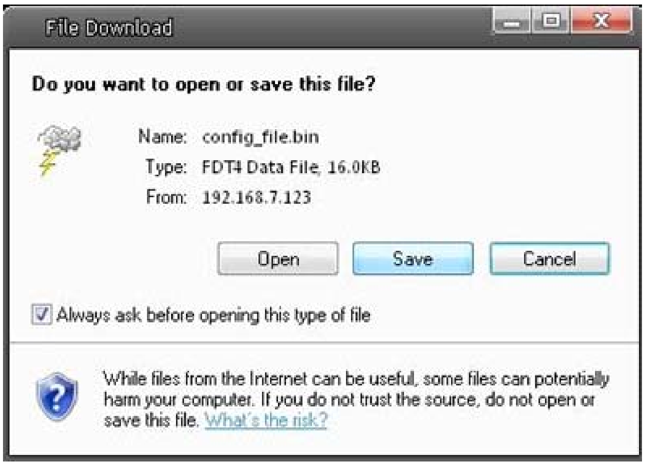
Export configuration files

Upload Files

Select configuration files

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 up as shown below. Click "Save" and specify a desired location for saving the configuration file.



File Download

Do you want to open or save this file?

Name: config_file.bin

Type: FDT4 Data File, 16.0KB

From: 192.168.7.123

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file.

Upload :

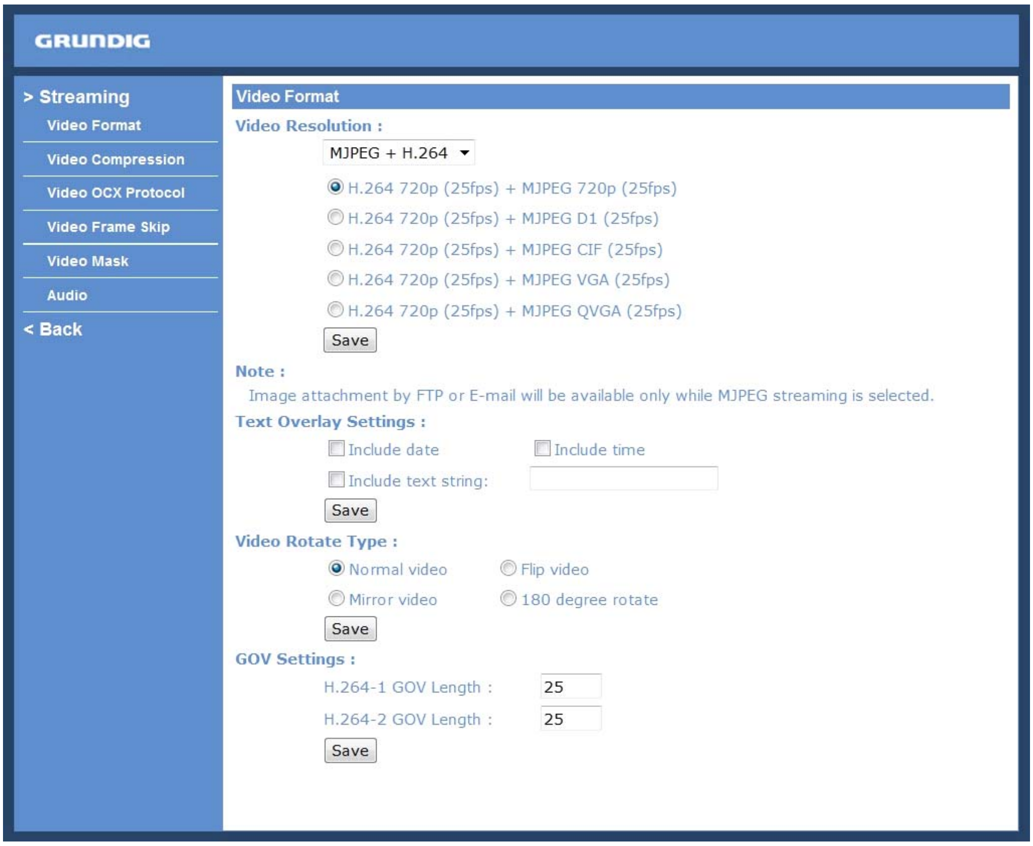
To copy an existing configuration file to the IP Camera, please first click on "Browse" to select the configuration file, and then press the "Upload" button for uploading.

10. Streaming Settings

Press the tab "Streaming" on 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.

10.1. Video Format

The video setting page is shown below:



Video Format

Video Resolution :

MJPEG + H.264

● H.264 720p (25fps) + MJPEG 720p (25fps)
○ H.264 720p (25fps) + MJPEG D1 (25fps)
○ H.264 720p (25fps) + MJPEG CIF (25fps)
○ H.264 720p (25fps) + MJPEG VGA (25fps)
○ H.264 720p (25fps) + MJPEG QVGA (25fps)

Save

Note :

Image attachment by FTP or E-mail will be available only while MJPEG streaming is selected.

Text Overlay Settings :

□ Include date □ Include time
□ Include text string:

Save

Video Rotate Type :

● Normal video ○ Flip video
○ Mirror video ○ 180 degree rotate

Save

GOV Settings :

H.264-1 GOV Length : 25
H.264-2 GOV Length : 25

Save

Video Format :
Resolution for MJPEG & H.264 format includes:
- H.264 720p (25fps) + MJPEG 720p (25fps)
- H.264 720p (25fps) + MJPEG D1 (25fps)
- H.264 720p (25fps) + MJPEG CIF (25fps)
- H.264 720p (25fps) + MJPEG VGA (25fps)
- H.264 720p (25fps) + MJPEG QVGA (25fps)

For MJPEG & BNC:
- MJPEG 720p (25fps) + BNC Output

For MJPEG only:
- MJPEG 1080p (12fps)
- MJPEG SXGA (25fps)

For H.264 & H.264:
- H.264 720p (25fps) +H.264 D1 (25fps)
- H.264 720p (25fps) + H.264 CIF (25fps)
- H.264 720p (25fps) + H.264 VGA (25fps)
- H.264 720p (25fps) + H.264 VGA (25fps)
- H.264 720p (25fps) + H.264 QVGA (25fps Baseline)

For H.264 & BNC:
- H.264 720p (25fps) + BNC Output

For H.264 only:
- H.264 1080p (12fps)
- H.264 SXGA (25fps)

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

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

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

The following are descriptions of different video rotation types.

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

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

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

Click "Save" to confirm the setting.

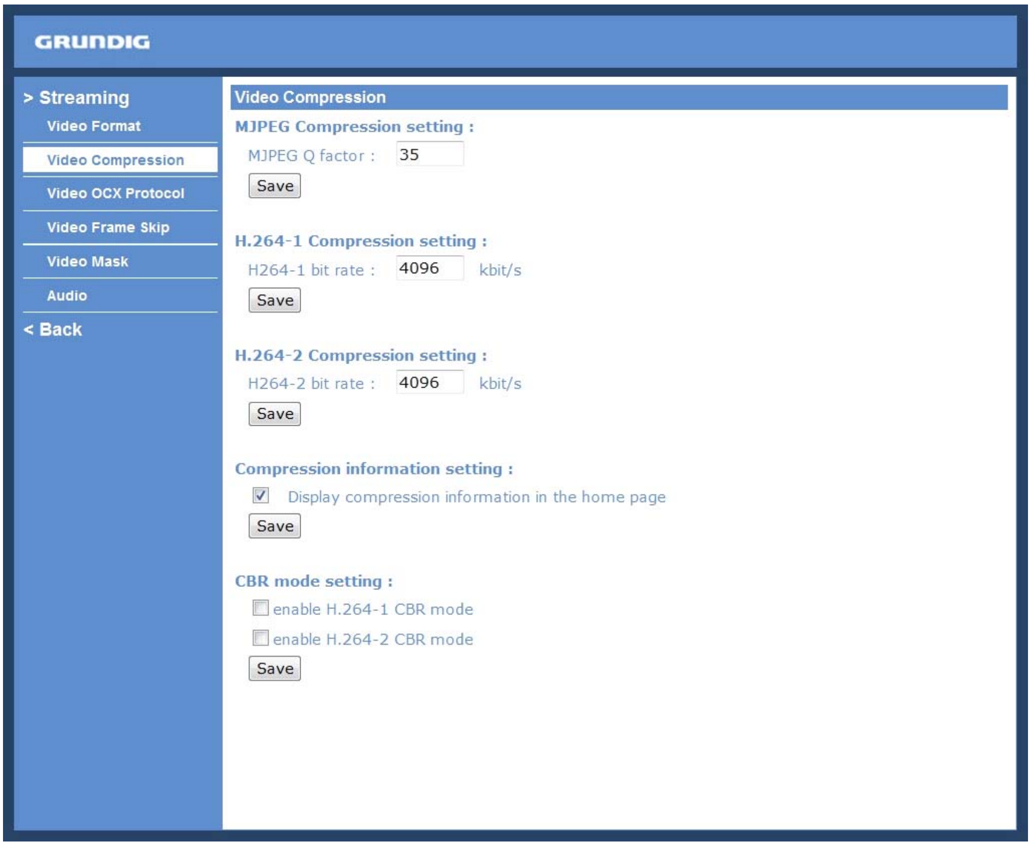
GOV Settings :
Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. Longer GOV means decreasing the frequency of I-frames.
Click "Save" to confirm the GOV setting.

10.2. Video Compression

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

MJPEG Compression Settings:
A higher value implies higher bit rates and a higher visual quality. The default setting is 35; the setting range is from 1 to 70.
Click “Save” to confirm the setting.

H.264-1 / H.264-2 Bit Rate:
The default setting is 4096 kbps; the setting range is from 64 to 8192 kbps.
Click “Save” to confirm the setting.



Video Compression

MJPEG Compression setting :
MJPEG Q factor : 35

H.264-1 Compression setting :
H264-1 bit rate : 4096 kbit/s

H.264-2 Compression setting :
H264-2 bit rate : 4096 kbit/s

Compression information setting :
☑ Display compression information in the home page

CBR mode setting :
□ enable H.264-1 CBR mode
□ enable H.264-2 CBR mode

MJPEG Q (Quality) factor :
A higher value implies higher bit rates and a higher visual quality. The default setting of the MJPEG Q factor is 35; the setting range is from 1 to 70.

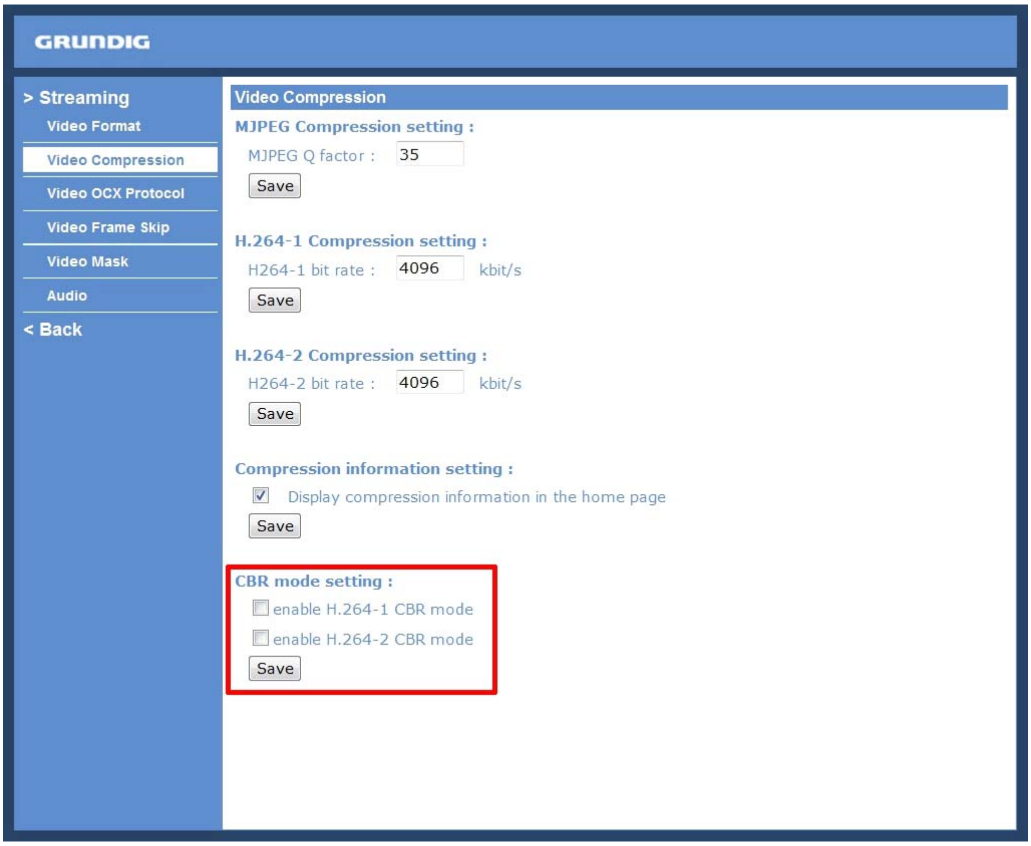
H.264-1 / H.264-2 bit rate :
The default setting of H.264-1 / H.264-2 is 4096 kbps; the setting range is from 64 to 8192 kbps.

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 can become the preferred bit rate mode if the bandwidth available is limited. It is important to take into account the image quality when you choose to use CBR mode.

Click “Save” to confirm the setting.



GRUNDIG

> Streaming
- Video Format
- Video Compression
- Video OCX Protocol
- Video Frame Skip
- Video Mask
- Audio

< Back

Video Compression

MJPEG Compression setting :

MJPEG Q factor : 35

Save

H.264-1 Compression setting :

H264-1 bit rate : 4096 kbit/s

Save

H.264-2 Compression setting :

H264-2 bit rate : 4096 kbit/s

Save

Compression information setting :

☑ Display compression information in the home page

Save

CBR mode setting :

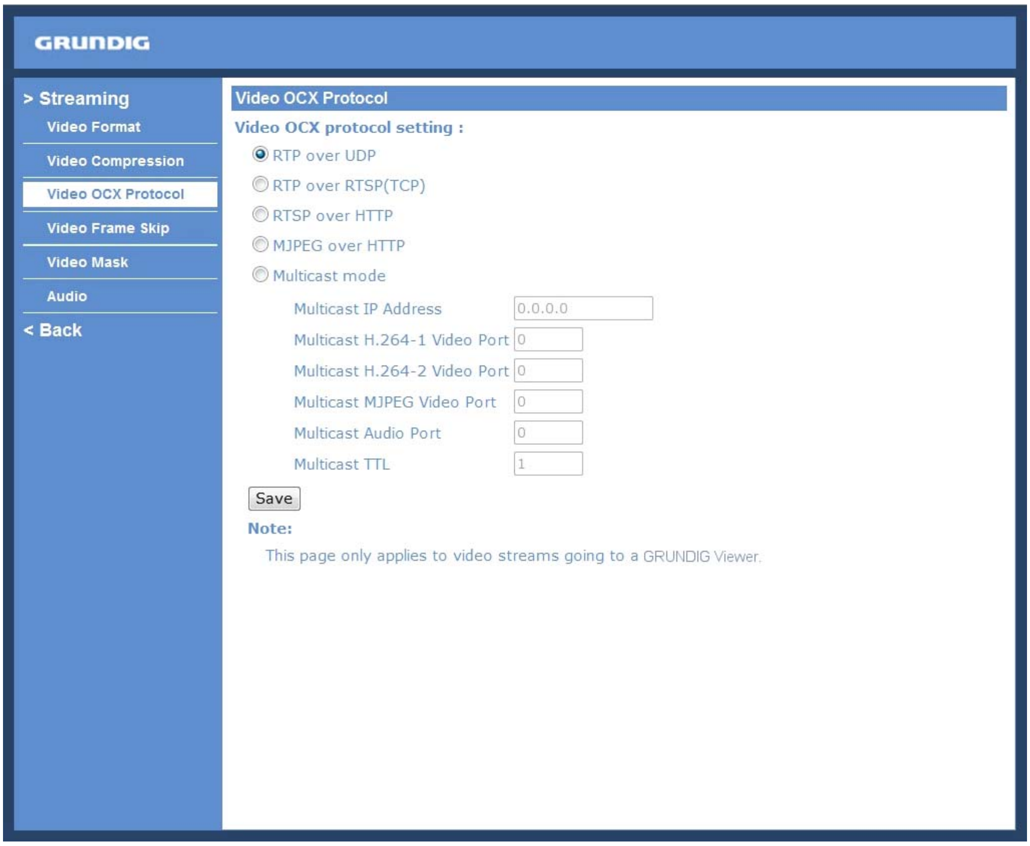
□ enable H.264-1 CBR mode

□ enable H.264-2 CBR mode

Save

10.3. 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 Video OCX Protocol page is as follows:



Video OCX Protocol

Video OCX protocol setting :

● RTP over UDP
○ RTP over RTSP(TCP)
○ RTSP over HTTP
○ MJPEG over HTTP
○ Multicast mode

Multicast IP Address	0.0.0.0
Multicast H.264-1 Video Port	0
Multicast H.264-2 Video Port	0
Multicast MJPEG Video Port	0
Multicast Audio Port	0
Multicast TTL	1

Note:

This page only applies to video streams going to a GRUNDIG Viewer.

Video OCX protocol setting options include:

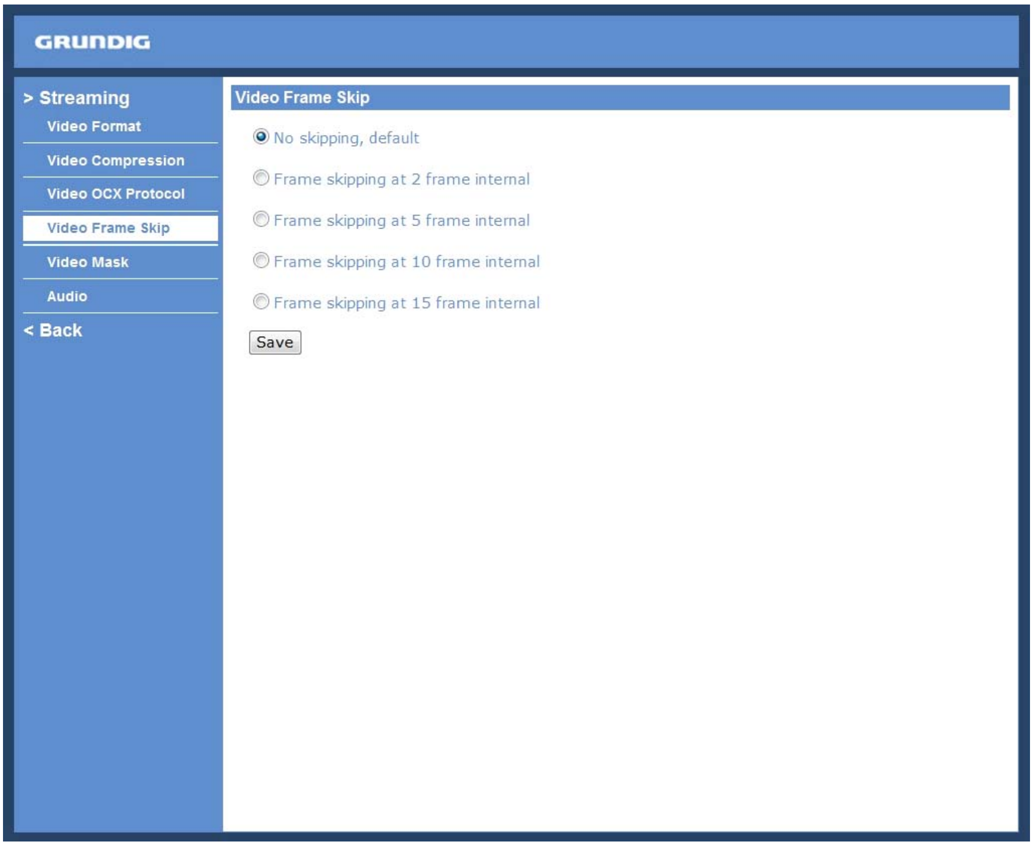
- RTP over UDP / RTP over RTSP (TCP) / RTSP over HTTP / MJPEG over HTTP
(Select a mode according to your data delivery requirements.)

- 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.

10.4. Video Frame Skip

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



Video Frame Skip

● No skipping, default

○ Frame skipping at 2 frame internal

○ Frame skipping at 5 frame internal

○ Frame skipping at 10 frame internal

○ Frame skipping at 15 frame internal

Video Frame Skip options include:

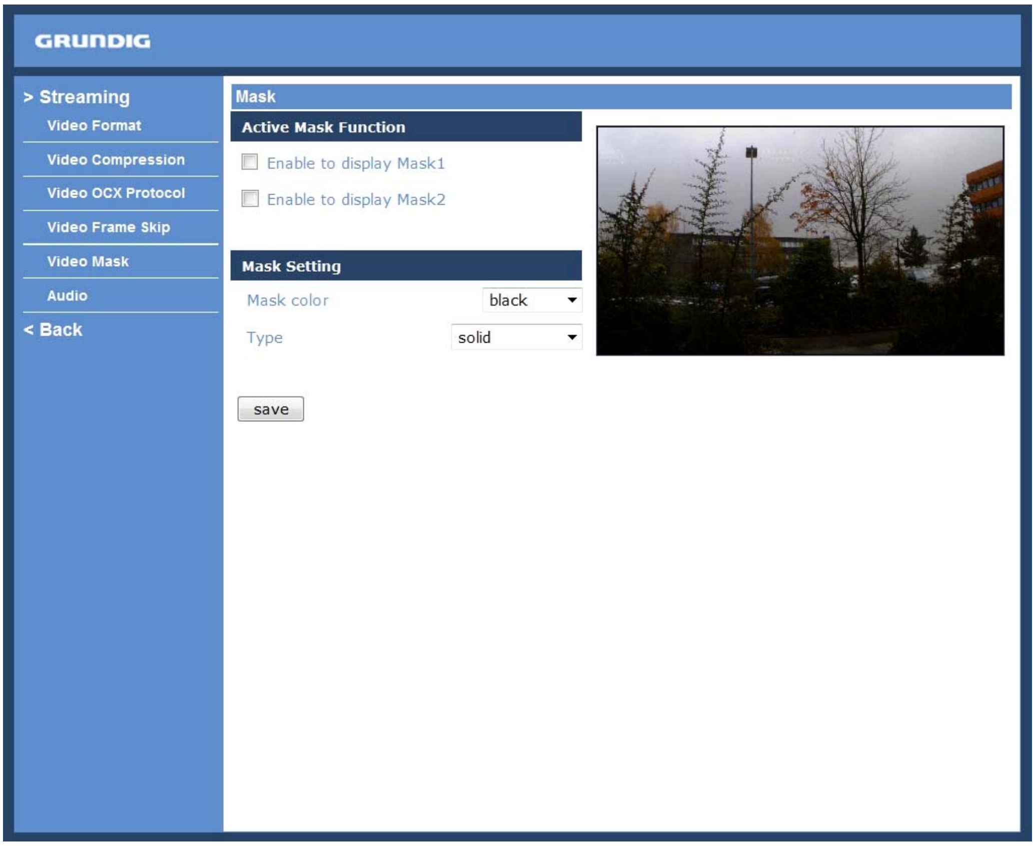
- No skipping, default
- Frame skipping at 2 frame interval
- Frame skipping at 3 frame interval
- Frame skipping at 4 frame interval
- Frame skipping at 5 frame interval
- Frame skipping at 10 frame interval
- Frame skipping to 15 frame interval

Click “Save” to confirm the setting.

NOTE: Higher frame skipping rate will decrease video smoothness.

10.5. Video Mask

There are up to five video masks which can be set by the users.



Active Mask Function

□ Enable to display Mask1

□ Enable to display Mask2

Mask Setting

Mask color: black

Type: solid

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 in order to adjust the mask's size and place it on the target zone.

NOTE: It is suggested to set the Video Mask twice as big as 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 colour:

The selection of Mask colours includes red, black, white, yellow, green, blue, cyan, and magenta.

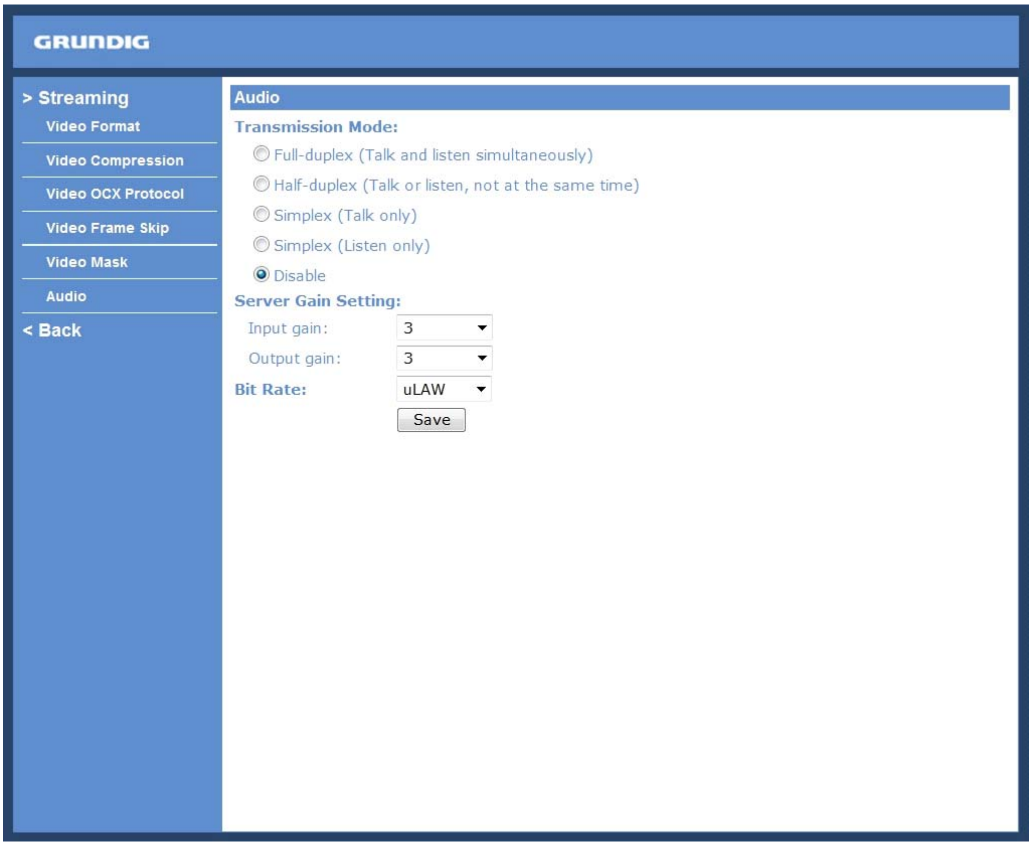
- Type:

Select to change the mask type as solid or transparent.

Click "Save" to confirm the setting.

10.6. Audio

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



Transmission Mode:

○ Full-duplex (Talk and listen simultaneously)

○ Half-duplex (Talk or listen, not at the same time)

○ Simplex (Talk only)

○ Simplex (Listen only)

● Disable

Server Gain Setting:

Input gain: 3

Output gain: 3

Bit Rate: uLAW

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”.

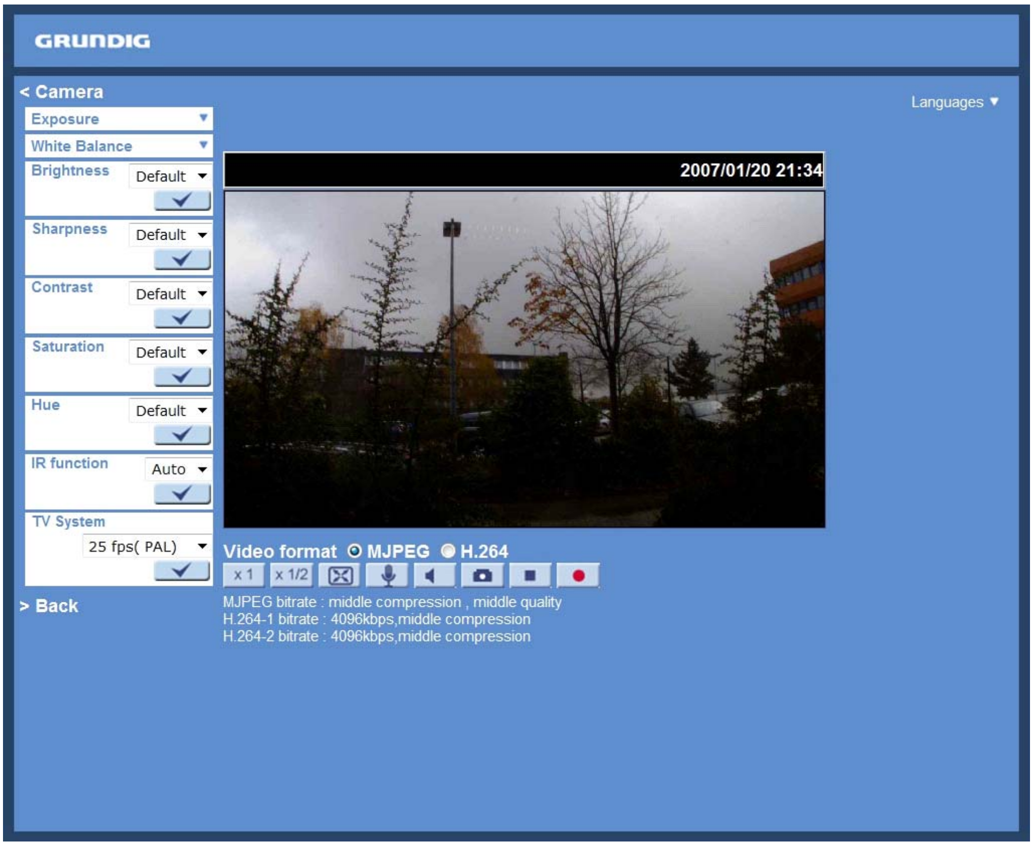
Bit Rate :

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. A higher bit rate signifies a higher audio quality and requires a bigger bandwidth.

Click “Save” to confirm the setting.

11. Camera Settings

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



Brightness: Default

Sharpness: Default

Contrast: Default

Saturation: Default

Hue: Default

IR function: Auto

TV System: 25 fps(PAL)

2007/01/20 21:34

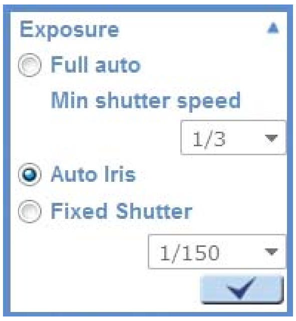
Video format ● MJPEG ○ H.264

MJPEG bitrate : middle compression , middle quality
H.264-1 bitrate : 4096kbps,middle compression
H.264-2 bitrate : 4096kbps,middle compression

NOTE: Camera settings and function buttons may vary depending on the camera model.

11.1. Exposure Setting

The Exposure pull-down menu is as follows:



○ Full auto
Min shutter speed: 1/3
● Auto Iris
○ Fixed Shutter: 1/150

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 a 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 can select the suitable shutter speed according to the environmental luminance.

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

Auto Iris Mode :
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.

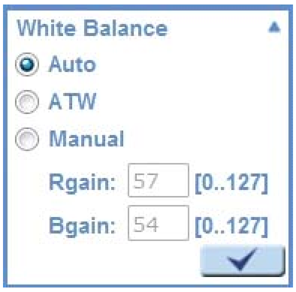
NOTE: The minimum shutter speed will vary depending on the setting in Full Auto Mode.

Fixed Shutter Mode :
In this mode, a fixed shutter speed can be selected from the drop-down menu. The shutter speed range is from 1/10000 to 1 (1/1.5) sec. with 19 (18) options. Users can choose a suitable shutter speed according to the environmental illumination.

Press < √ > to confirm the new setting.

11.2. White Balance Setting

The White Balance pull-down menu is as follows:



White Balance

● Auto
○ ATW
○ Manual

Rgain: 57 [0..127]
Bgain: 54 [0..127]

A camera needs to find a reference colour temperature, which is a way of measuring the quality of a light source, for calculating all the other colours. 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 colour temperature of some light sources for reference.

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

Auto Mode :
The Auto Balance White mode is suitable for an environment with a light source having a colour temperature ranging from 2700 ~ 7600K.

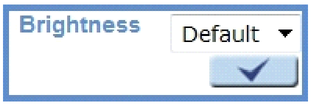
ATW Mode (Auto Tracing White Balance) :
With the Auto Tracking White Balance function, the white balance in a scene will be automatically adjusted while temperature colour is changing. The ATW Mode is suitable for environments with a light source having a colour temperature in the range roughly from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

Manual Mode :
In this mode, users can change the White Balance value manually via specifying R-Gain and B-Gain; the range of R/B-Gain is from 0 to 255.

Press < √ > to confirm the new setting.

11.3. 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.

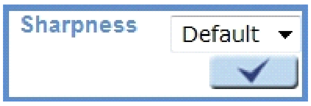


Brightness: Default

11.4. Sharpness Setting

Sharpness Setting

Increasing the sharpness level can make the image look sharper; it especially enhances the object's edges. Press < √ > to confirm the new setting.



Sharpness: Default

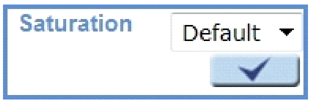
11.5. Contrast Setting

The camera image contrast level is adjustable; please choose from a range of -6 to +19. Press < √ > to confirm the new setting.

Contrast: Default

11.6. Saturation Setting

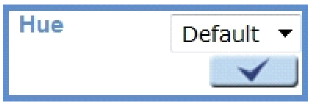
The camera image saturation level is adjustable; please select from a range of -6 to +19.
Press < √ > to confirm the new setting.



Saturation: Default

11.7. Hue Setting

The camera image hue level is adjustable; please select from a range of -12 to +13. Press < √ > to confirm the new setting.



Hue: Default

11.8. IR Function

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

IR function: Auto

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 always be on.

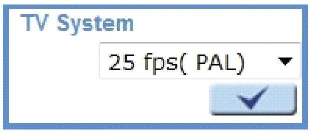
Light Off Mode :
In this mode, IR LED lights will always be off.

Press < √ > to confirm the new setting.

11.9. TV System Setup

Select the video format that matches the present TV system.

Press < √ > to confirm the new setting.

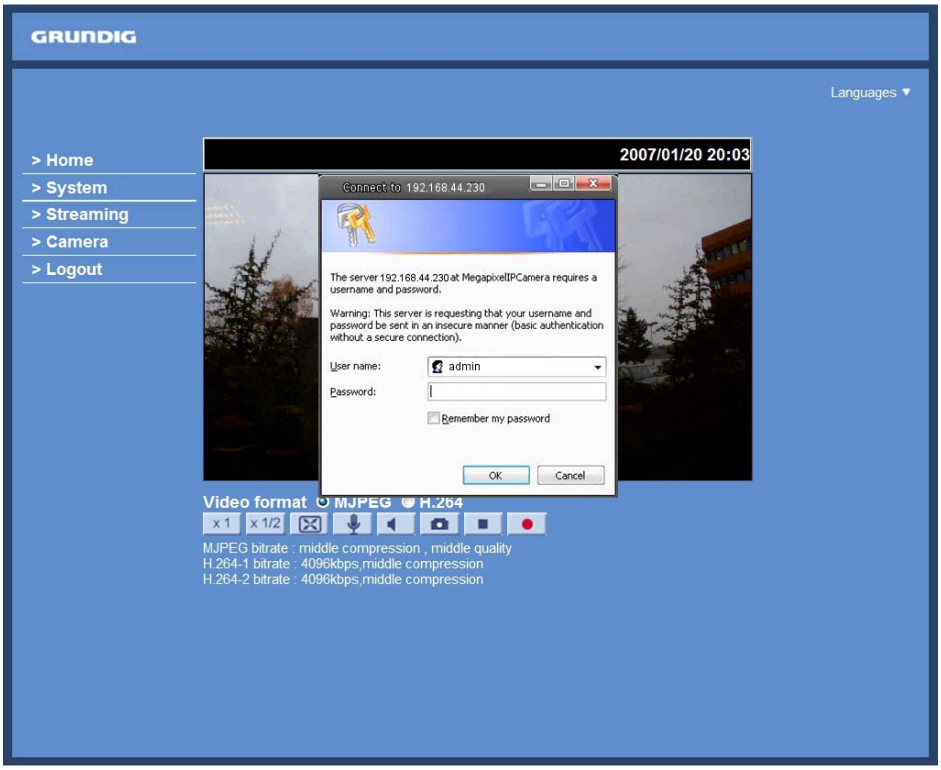


TV System

25 fps(PAL)

12. Logout

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



The server 192.168.44.230 at MegapixelIPCamera requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password:

□ Remember my password

Video format ○ MJPEG ○ H.264

MJPEG bitrate : middle compression , middle quality

H.264-1 bitrate : 4096kbps,middle compression

H.264-2 bitrate : 4096kbps,middle compression

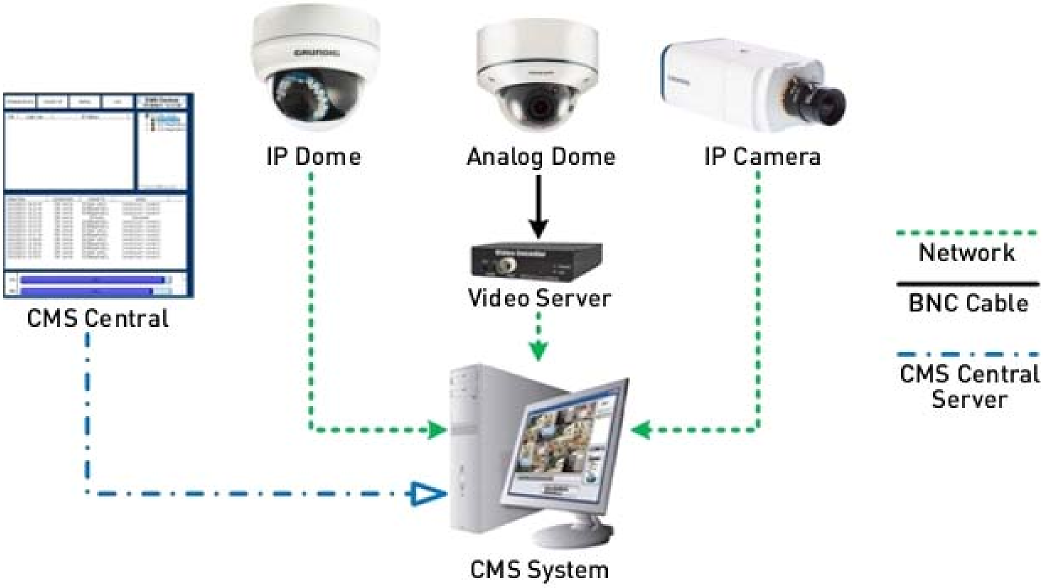
13. CMS Software Introduction

The Central Management System (CMS) software bundles the IP cameras into one system. Offering powerful functionalities via intuitive interface, it is a centralized monitoring solution for your video surveillance equipments.

It gives the user access to monitor multiple IP Cameras, 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.



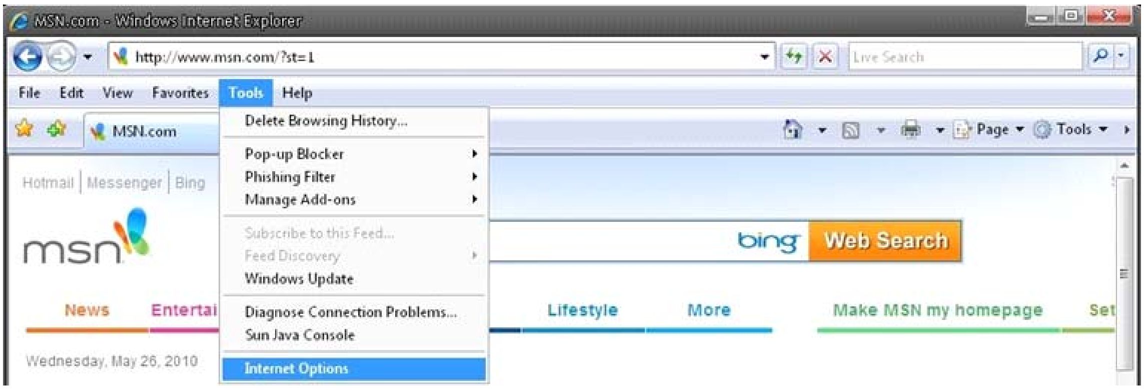
14. Internet Security Settings

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

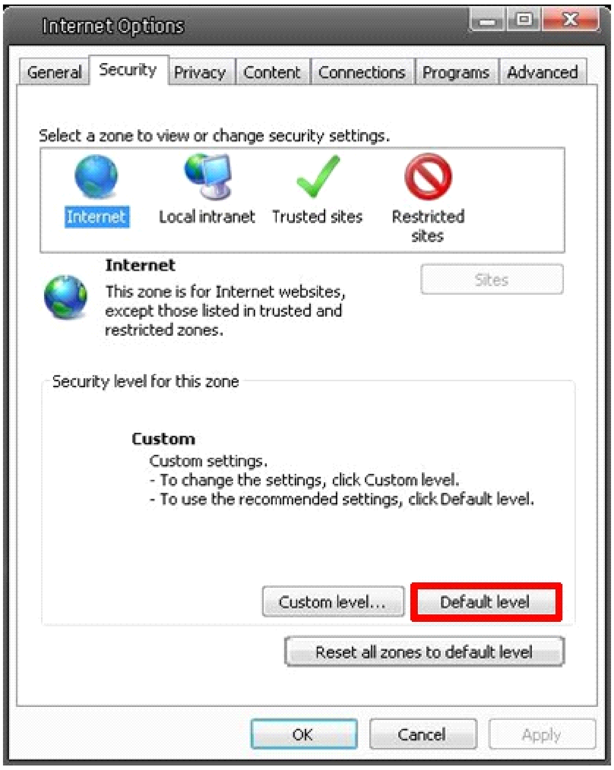
Internet Security Level : Default

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>.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Custom

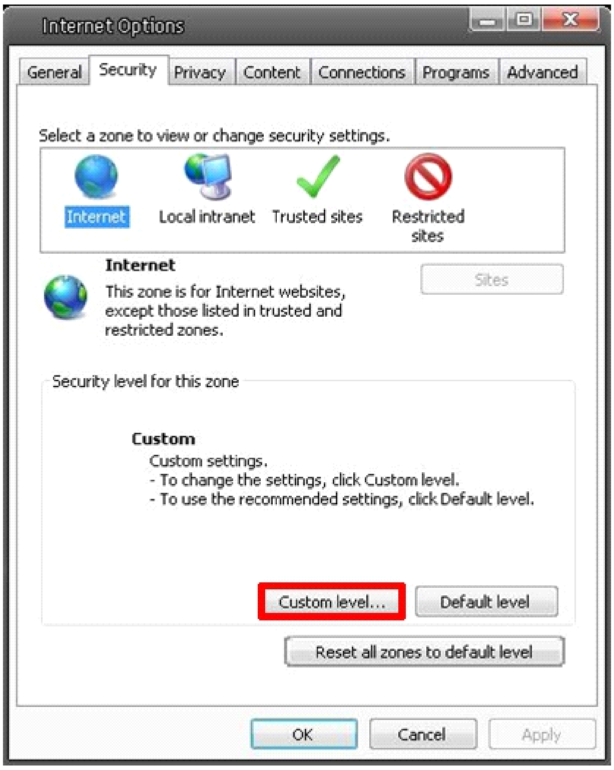
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

Step 4: Down the page, press "Default Level" (see the picture 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-in Settings :

Step 1~3: Refer to the previous section above.

Step 4: Down the page, press "Custom Level" (see the picture below) to change ActiveX controls and plug-in settings.



Select a zone to view or change security settings.

Internet

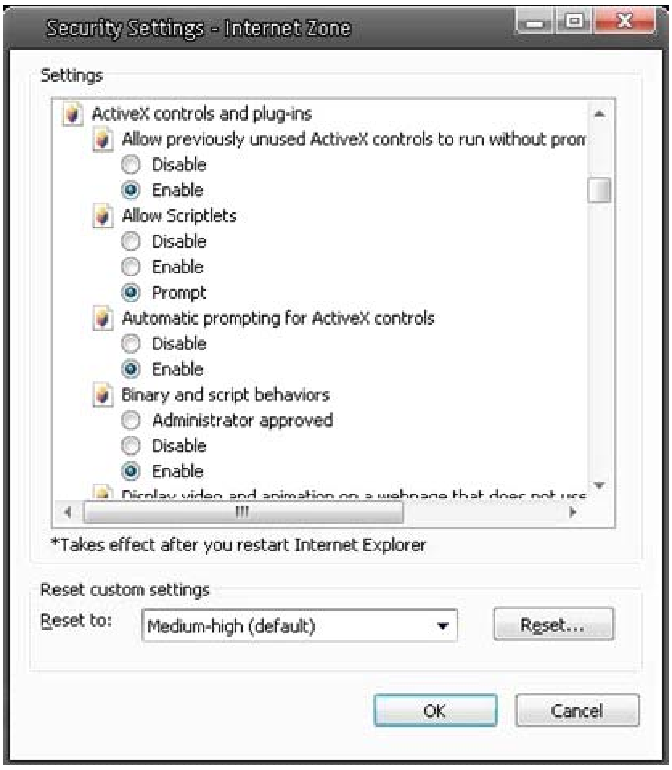
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

The Security Settings screen is displayed as shown below:



Security Settings - Internet Zone

Settings

ActiveX controls and plug-ins

Allow previously unused ActiveX controls to run without prom

○ Disable

● Enable

Allow Scriptlets

○ Disable

○ Enable

● Prompt

Automatic prompting for ActiveX controls

○ Disable

● Enable

Binary and script behaviors

○ Administrator approved

○ Disable

● Enable

Display video and animation on a webpage that does not use

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

Step 5: Under "ActiveX controls and plug-ins", set ALL items (as listed below) to <Enable> or <Prompt>. Please note that the items may vary depending on the Internet Explorer version you are using.

ActiveX controls and plug-in 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 as safe for scripting

Step 6: Click <OK> to accept the settings and to close the Security screen.

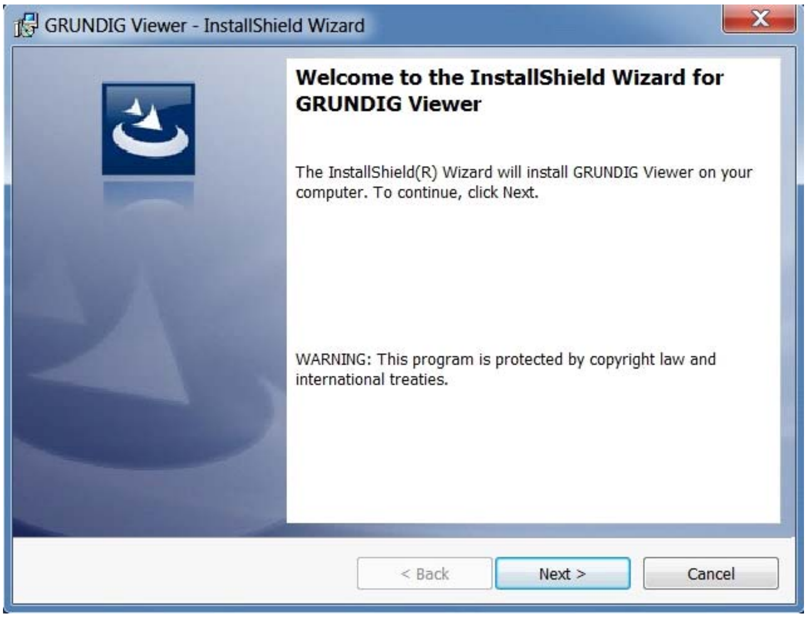
Step 7: Click <OK> to close the Internet Options screen.

Step 8: Close the browser window, and restart a new one later for accessing the IP Camera.

15. GRUNDIG Viewer Download Procedure

The procedure of GRUNDIG Viewer software download is specified as follows:

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



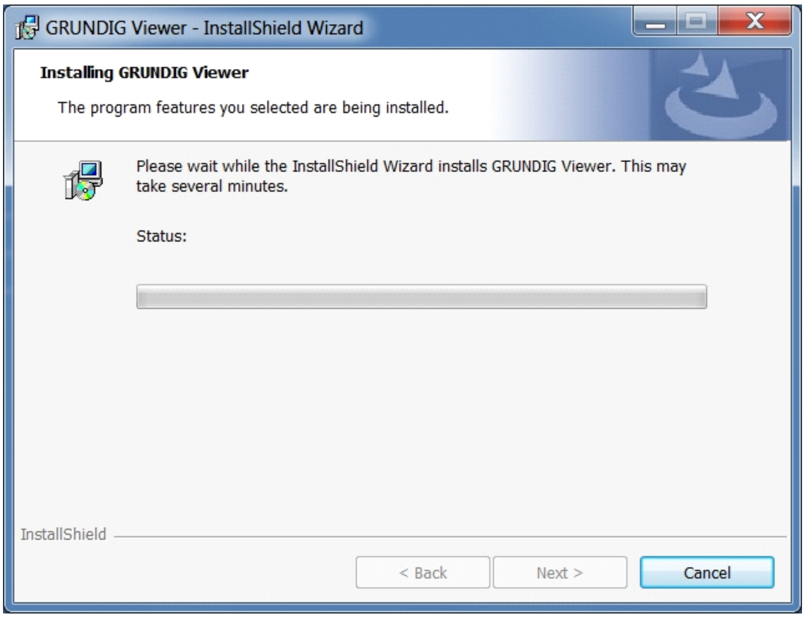
GRUNDIG Viewer - InstallShield Wizard

Welcome to the InstallShield Wizard for GRUNDIG Viewer

The InstallShield(R) Wizard will install GRUNDIG Viewer on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



GRUNDIG Viewer - InstallShield Wizard

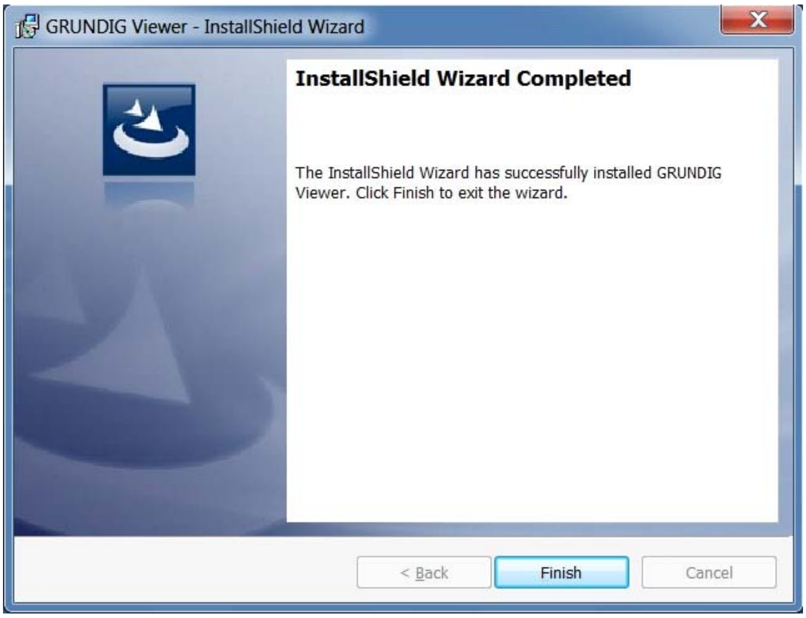
Installing GRUNDIG Viewer

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs GRUNDIG Viewer. This may take several minutes.

Status:

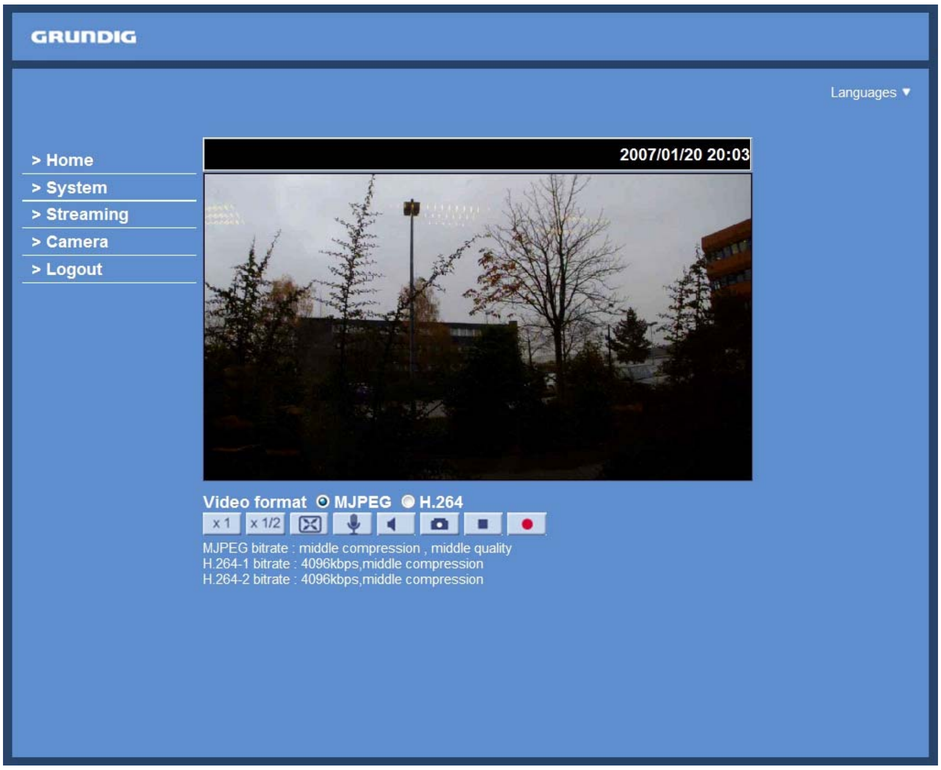
Step 3: Click "Finish" to close the GRUNDIG Viewer installation page.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed GRUNDIG Viewer. Click Finish to exit the wizard.

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



Video format ◉ MJPEG ○ H.264

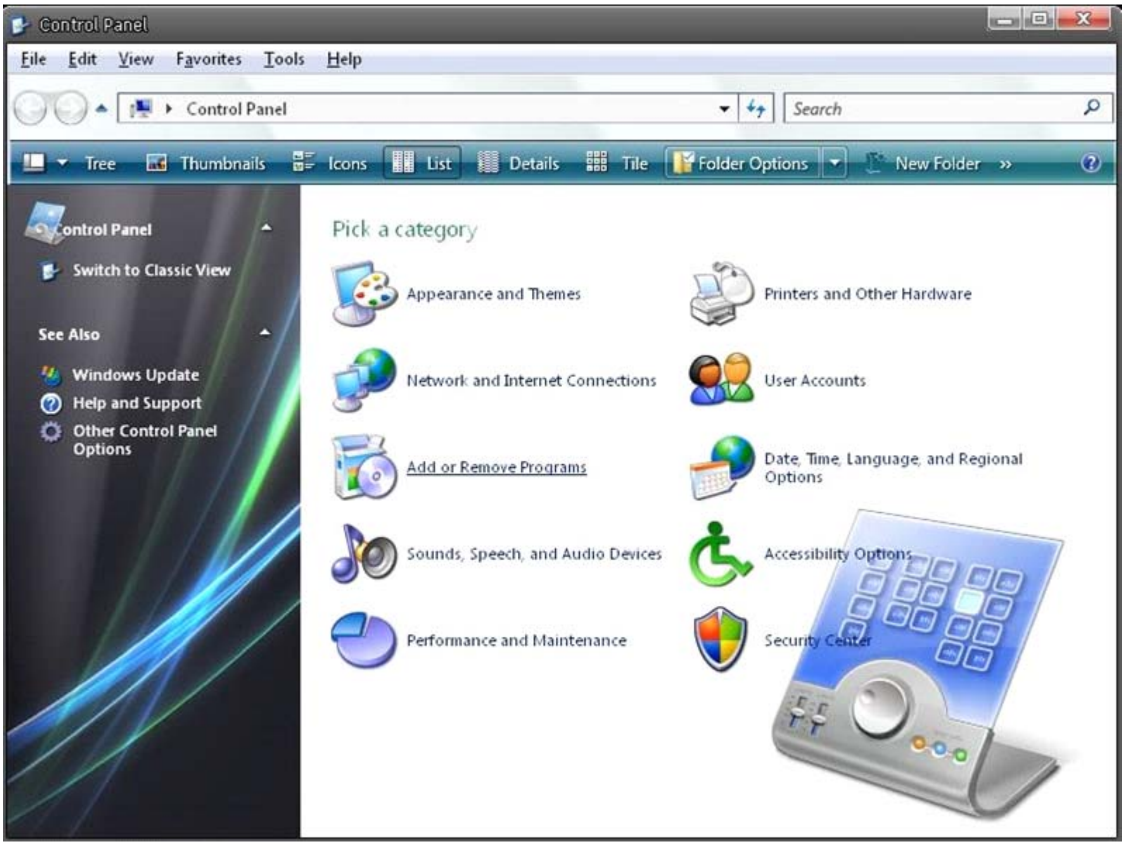
MJPEG bitrate : middle compression , middle quality
H.264-1 bitrate : 4096kbps,middle compression
H.264-2 bitrate : 4096kbps,middle compression

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

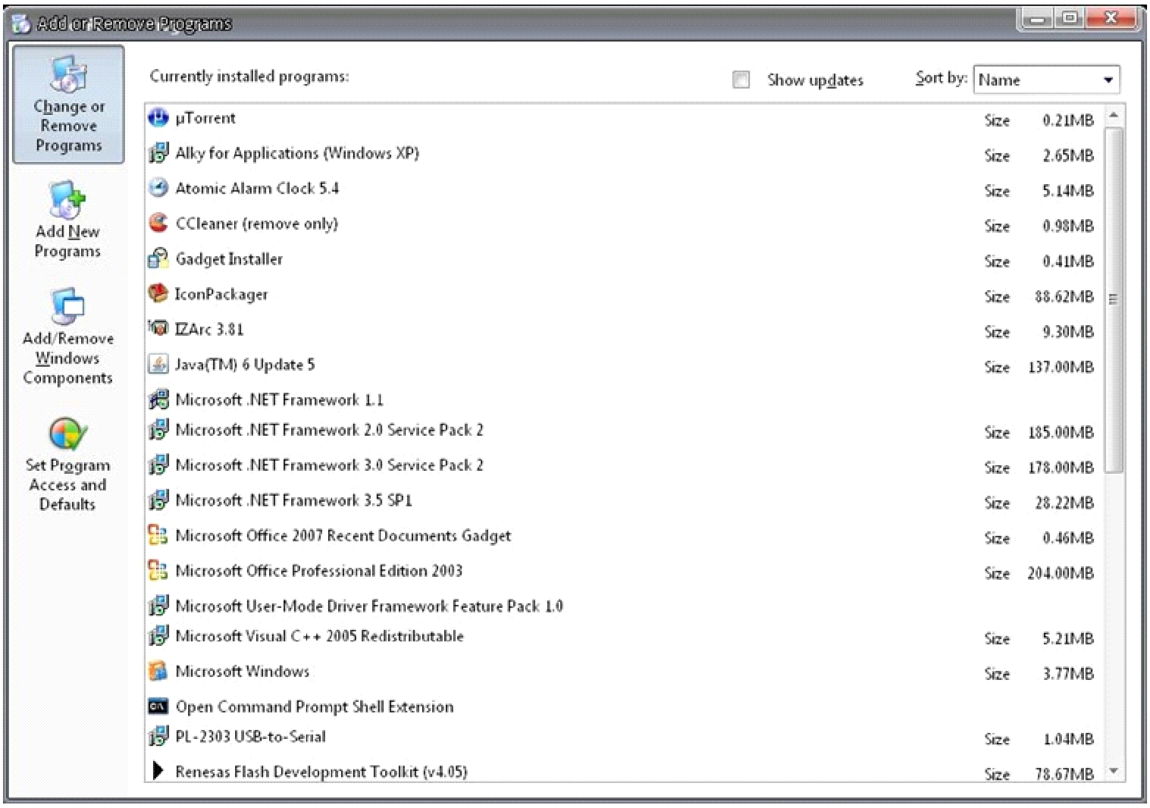
16. Install UPnP Components

Please follow the instructions below to install UPnP components. (The procedure is for Windows XP, for other systems please refer to the corresponding manuals.)

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

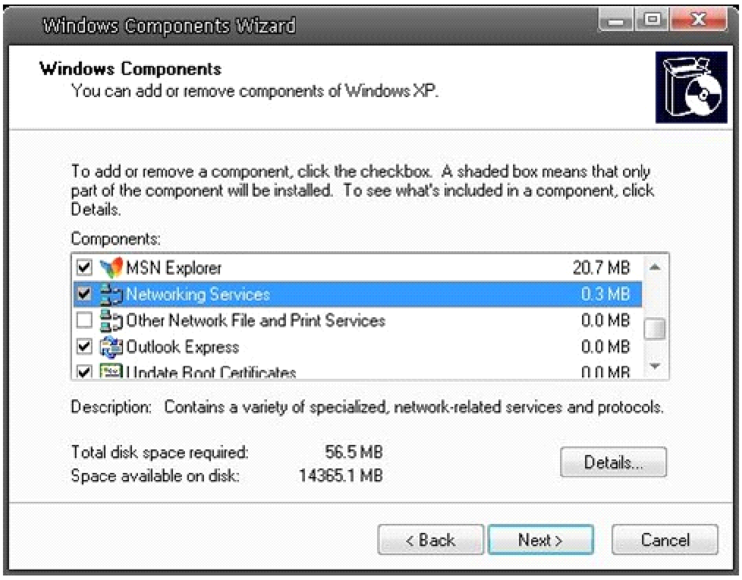

Control Panel
File Edit View Favorites Tools Help
Control Panel
Search
Tree Thumbnails Icons List Details Tile Folder Options New Folder
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Other Control Panel Options
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Add or Remove Programs
Date, Time, Language, and Regional Options
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance
Security Center

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


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Currently installed programs:
□ Show updates
Sort by: Name

µTorrent	Size	0.21MB
Alky for Applications (Windows XP)	Size	2.65MB
Atomic Alarm Clock 5.4	Size	5.14MB
CCleaner (remove only)	Size	0.98MB
Gadget Installer	Size	0.41MB
IconPackager	Size	88.62MB
IZArc 3.81	Size	9.30MB
Java(TM) 6 Update 5	Size	137.00MB
Microsoft .NET Framework 1.1		
Microsoft .NET Framework 2.0 Service Pack 2	Size	185.00MB
Microsoft .NET Framework 3.0 Service Pack 2	Size	178.00MB
Microsoft .NET Framework 3.5 SP1	Size	28.22MB
Microsoft Office 2007 Recent Documents Gadget	Size	0.46MB
Microsoft Office Professional Edition 2003	Size	204.00MB
Microsoft User-Mode Driver Framework Feature Pack 1.0		
Microsoft Visual C++ 2005 Redistributable	Size	5.21MB
Microsoft Windows	Size	3.77MB
Open Command Prompt Shell Extension		
PL-2303 USB-to-Serial	Size	1.04MB
Renesas Flash Development Toolkit (v4.05)	Size	78.67MB

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



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

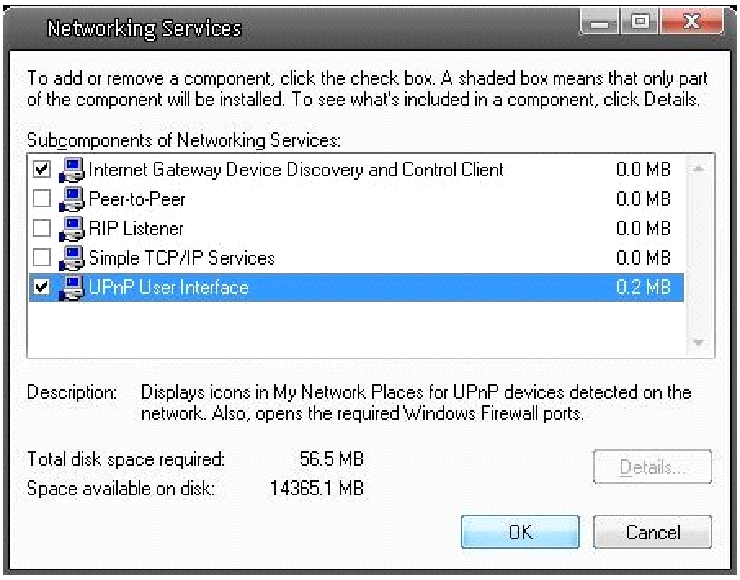
☑ MSN Explorer	20.7 MB
☑ Networking Services	0.3 MB
□ Other Network File and Print Services	0.0 MB
☑ Outlook Express	0.0 MB
☑ Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 56.5 MB

Space available on disk: 14365.1 MB

Step 4: Select “UPnP User Interface” in the Networking Services’ subcomponents list and then click “OK”.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

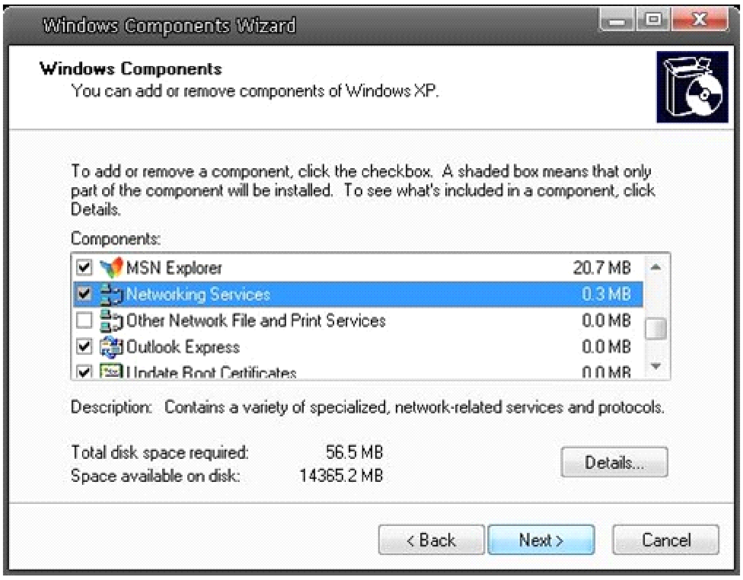
☑ Internet Gateway Device Discovery and Control Client	0.0 MB
□ Peer-to-Peer	0.0 MB
□ RIP Listener	0.0 MB
□ Simple TCP/IP Services	0.0 MB
☑ UPnP User Interface	0.2 MB

Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.

Total disk space required: 56.5 MB

Space available on disk: 14365.1 MB

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



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

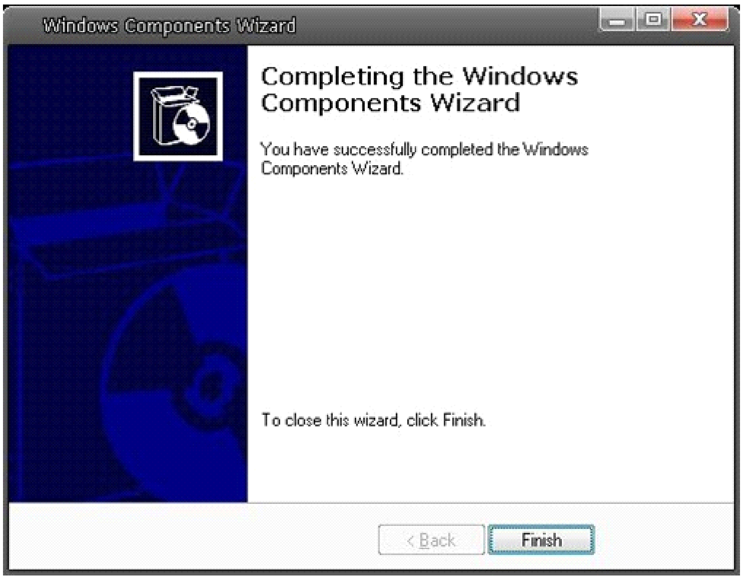
☑ MSN Explorer	20.7 MB
☑ Networking Services	0.3 MB
□ Other Network File and Print Services	0.0 MB
☑ Outlook Express	0.0 MB
☑ Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 56.5 MB

Space available on disk: 14365.2 MB

Step 6: Click "Finish" to complete the installation.



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

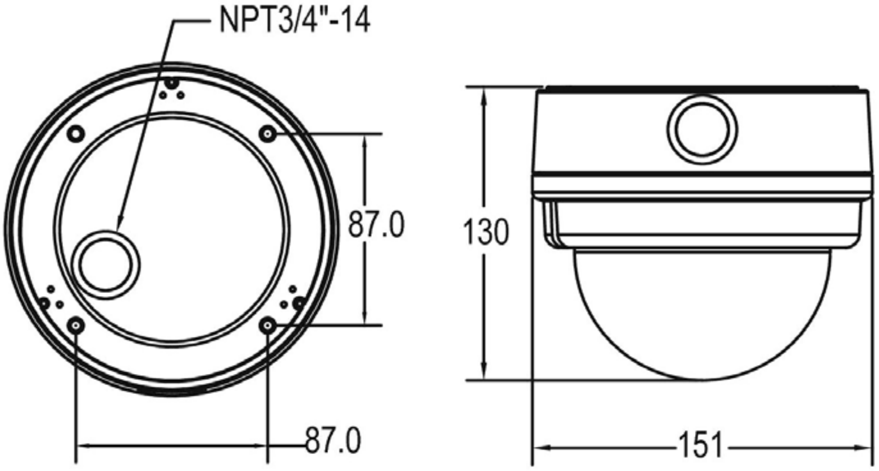
Specifications GCI-H0522V

Image Sensor	1/2.5" CMOS Aptina, 2 megapixel
Pixels - total	1920(H) x 1080(V), Full HD
Sensitivity	0.2 lux @ F1.2
Lens Drive Type	Auto iris, DC
Lens Focal Length	3.3 ~ 12 mm
Viewing Angle	71° ~ 21°
Motion Detection	On/ Off/ Sensitivity/ Area setting
Privacy zones	2 zones, rectangle
White Balance	ATW, AWB, Manual
Shutter Speed	1 sec to 1/10,000 sec
Camera ID	20 character
Alarm Inputs	1
Alarm Outputs	1
Web Browser	MS Internet Explorer 6.0 (or higher)
Number of Clients	Up to 20 users
Video Compression	Dual stream: H.264+H.264, H.264+MJPEG, MJPEG+BNC or H.264+BNC
Video Resolution	Full HD 1920 x 1080 (12 fps), 720P 1280 X 720 (25 fps)
Network Protocol	IPv4, IPv6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, 802.1X and SNMP
SD memory	Micro SD/SDHC
Alarm Event	Alarm Input, Motion Detection or Schedule: Image transfer or alarm message by FTP, Image transfer or alarm message by E-mail, recording on SD-card, enable alarm output and send HTTP notification
Audio Compression	G.726 ADPCM, G.711
LED Indicator	Power, link, active
Video Outputs	1Vpp, BNC
Input/Output sockets	Video Out(BNC), Power(3-Pin Term), RJ-45, Micro SD Card Slot, Alarm Terminal 4-Pin (Alarm In 2-Pin, Alarm Out 2-Pin), Audio (4-Pin)
Firmware Upgrade	Firmware upgrade by Web Browser
Configuration	Upload & Download configuration on remote PC
Protection Rating	IP66
Operating Temperature	-10°C ~ +50°C
Humidity	10 ~ 90% no condensation
Regulation	CE, FCC, RoHS Compliant
Supply Voltage	12 VDC / 24 VAC / PoE IEEE 802.3af
Power Consumption	5.5 W
Weight	0.8 kg
Dimensions (wxhxd)	Ø 151 x 130.5 mm

Specifications GCI-K0322V

Sensitivity	0.2 lux @ F1.4 (Colour) / 0.02 lux @ F1.4 (B&W)
Max. IR Distance	15/25 m (according to scene reflexion)
Power Consumption	8.9 W
Weight	0.8 kg
Dimensions (wxhxd)	Ø 151 x 130.5 mm

Dimensions


NPT3/4"-14
87.0
87.0
130
151

EC Declaration of Conformity

GCI-H0522V	720P HD IP Colour Fixed Dome Camera
GCI-K0322V	1080P Full HD IP C/B&W AV Fixed Dome w/ IR LED

It is hereby certified that the products meet the standards in the following relevant provisions:

EC EMC Directive 2004/108/EC
Low Voltage Directive 2006/95/EC

Applied harmonized standards and technical specifications:

EN 55022 Class A (2006 + A1: 2007)
EN 61000-3-2 (2006)
EN 61000-3-3 (1995 + A1: 2001 + A2: 2005)
EN 50130-4 (1995 + A1: 1998 + A2: 2003)

ASP AG
Lüttringhauser Str. 9
42897 Remscheid
Germany

Remscheid, 31.01.2011

Ludwig Bergschneider
CEO