

FOR A GOOD **REASON** **GRUNDIG**

en

Owner's Manual

Transmission

GEC-D2201AR 1 channel video encoder

GEC-D2201AR.25.1.04.10.2011
© ASP AG



Content:			
1. Introduction	1	11. Storage Management	45
2. Important Safety Instructions	1	12. Recording	47
3. Package Contents	2	13. File Location	48
4. Installation	2	14. Camera Control	49
1. Connections	3	15. View Log File	50
2. System Requirements	4	16. View User Information	51
3. Ceiling/Wall Mounting	5	17. View Parameters	53
5. Deleting the Existing GRUNDIG Viewer	7	18. Factory Default	53
6. Accessing the Video Server	8	19. Software Version	54
7. Browser-based Viewer Introduction	14	20. Software Upgrade	55
8. Home Page	15	21. Maintenance	56
9. System Related Settings	17	10. Streaming Settings	57
1. Host Name & System Time Setting	17	1. Video Format	57
2. Security	18	2. Video Compression	58
3. Network	25	3. Video OCX Protocol	60
4. DDNS	32	4. Video Frame Rate	61
5. Mail	33	5. Audio	62
6. FTP	34	11. PTZ Settings	63
7. HTTP	35	12. Logout	65
8. Application (Alarm Settings)	35	13. CMS Software Introduction	65
9. Motion Detection	40	14. Internet Security Settings	66
10. Tampering	43	15. GRUNDIG Viewer Download Procedure	69
		16. Install UPnP Components	71

1. Introduction

This Video Server provides a stable platform for transmission from traditional analogue CCTV cameras to an IP-based system.

With the ability to select H.264 or MJPEG video compression, the Video Server offers scalability and efficient use of network bandwidth. By combining the Video Server with a NVR that can receive IP signals from the internet, users can upgrade analogue cameras to become an IP-based surveillance system that reduces the wiring costs and maximises the convenience of distant surveillance applications.

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 products to one 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 product. 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 unauthorised 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

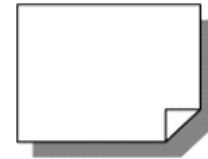
These parts are included:



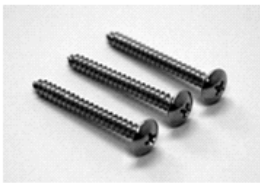
Video Server (Encoder)



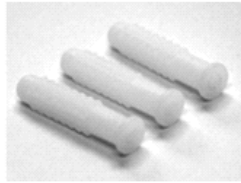
**DC Jack Cable with
screw terminal block
(Length: 300mm)**



Quick Guide



**M4A Pan Head
Self-Tapping Screw**



**M4 Plastic Anchors
(Length: 35 mm)**



**CD
(Software and Documentation)**

4. Installation

Do not install this product 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.

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.

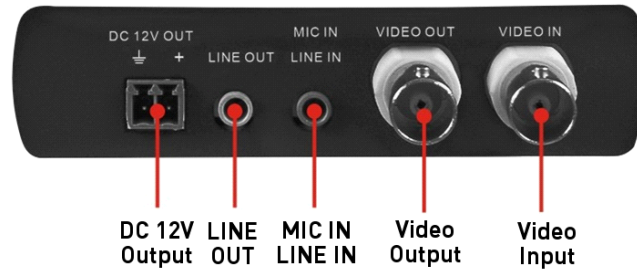
When installing the unit, fasten it securely and firmly. A falling unit may cause personal injury.

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

4.1. Connections

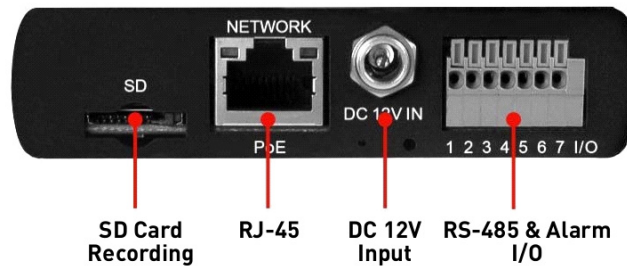
The definition for each connector on the Video Server will be given as follows.

The connectors on the front panel are as shown below.



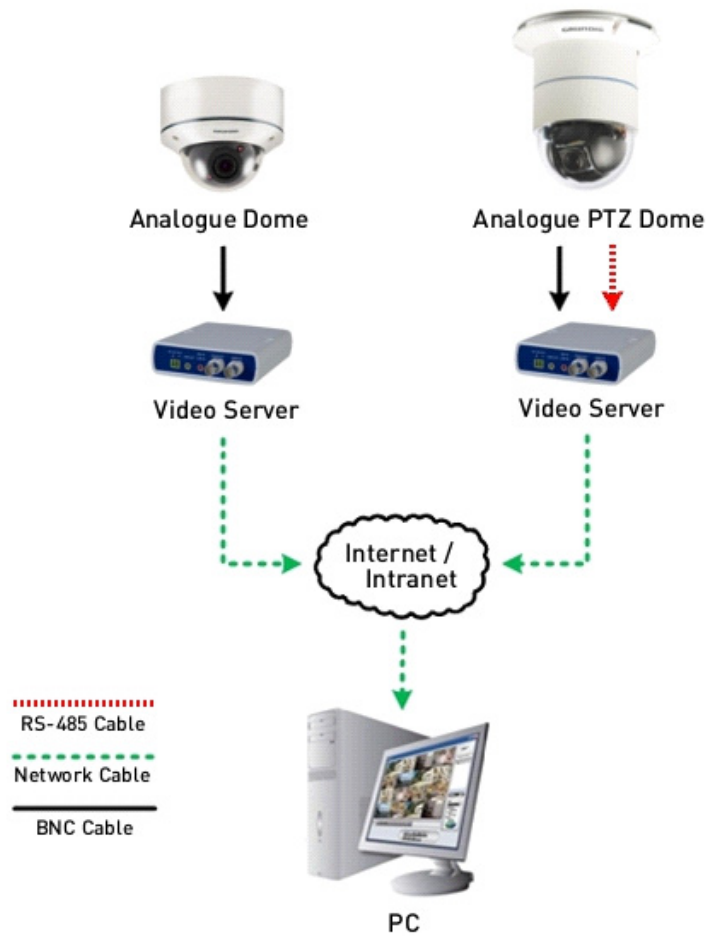
Connector	Definition
DC 12V OUT	Power Output
LINE OUT	Audio Output
MIC IN /LINE IN	Audio Input and Microphone Input
VIDEO OUT	Analogue BNC Video Output to Monitor
VIDEO IN	Analogue BNC Video Input to Video Server

The connectors on the rear panel are as shown below.



Connector	Pin No.	Definition
SD Card Recording	-	Micro SD Card Inserting Slot
NETWORK / PoE (RJ-45)	-	10/100 Mbps Ethernet/ PoE
DC 12V IN	-	Power Input
RS-485	1	D+
	2	D-
	3	ISO GND
Alarm I/O	4	GND
	5	IN+
	6	OUT-
	7	OUT+

Please follow the procedure below for power, video and Ethernet connections of the Video Server.



Step 1:

Connect an analogue camera to the Video Server's BNC connector. To do this, please refer to section 4.1. Connections (Front Panel).

Step 2:

Connect the power adaptor to the Video Server's DC Jack. To do this, please refer to section 4.1. Connections (Rear Panel).

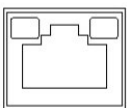
Step 3:

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 an Ethernet cable to the RJ-45 connector in the Video Server, and the other end of the cable to the network switch or PC.

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

Green Link Light indicates good network connection.

Orange Activity Light flashes for network activity indication.



4.2. System Requirements

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

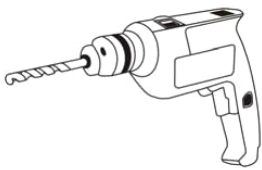
Web Browser :
Microsoft Internet Explorer 6.0 or later
Firefox
Chrome
Safari

Network Card :
10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation

Viewer :
ActiveX control plug-in for Microsoft IE

4.3. Ceiling/Wall Mounting

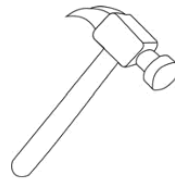
Installation Tools:



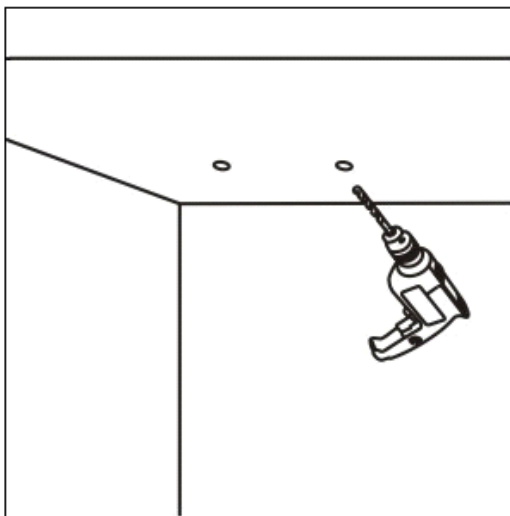
Power Drill



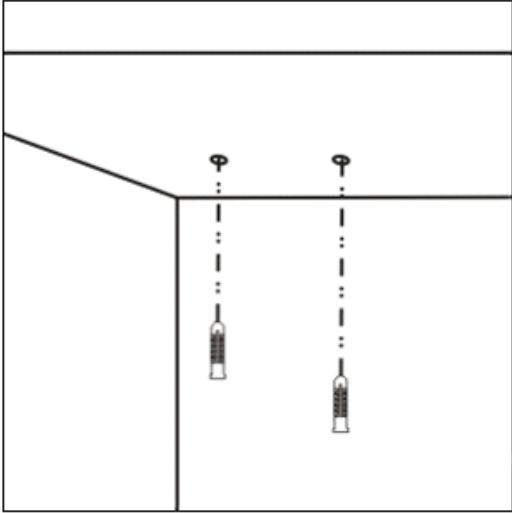
M4 Phillips-Head
Screwdriver



Hammer

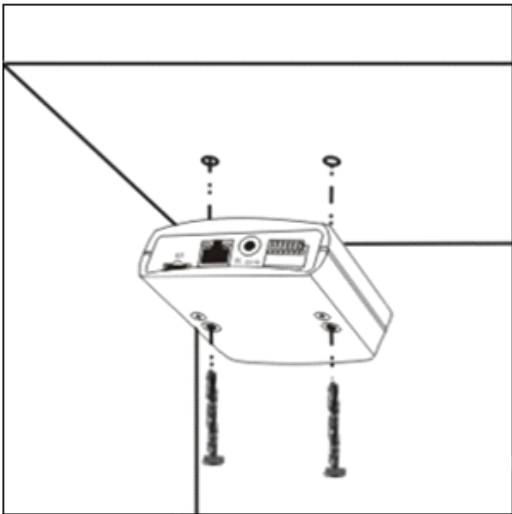


STEP 1:
Use a power drill to drill two holes in the ceiling or wall for the two M4 plastic anchors.



STEP 2:

Use a hammer to install two M4 plastic anchors.



STEP 3:

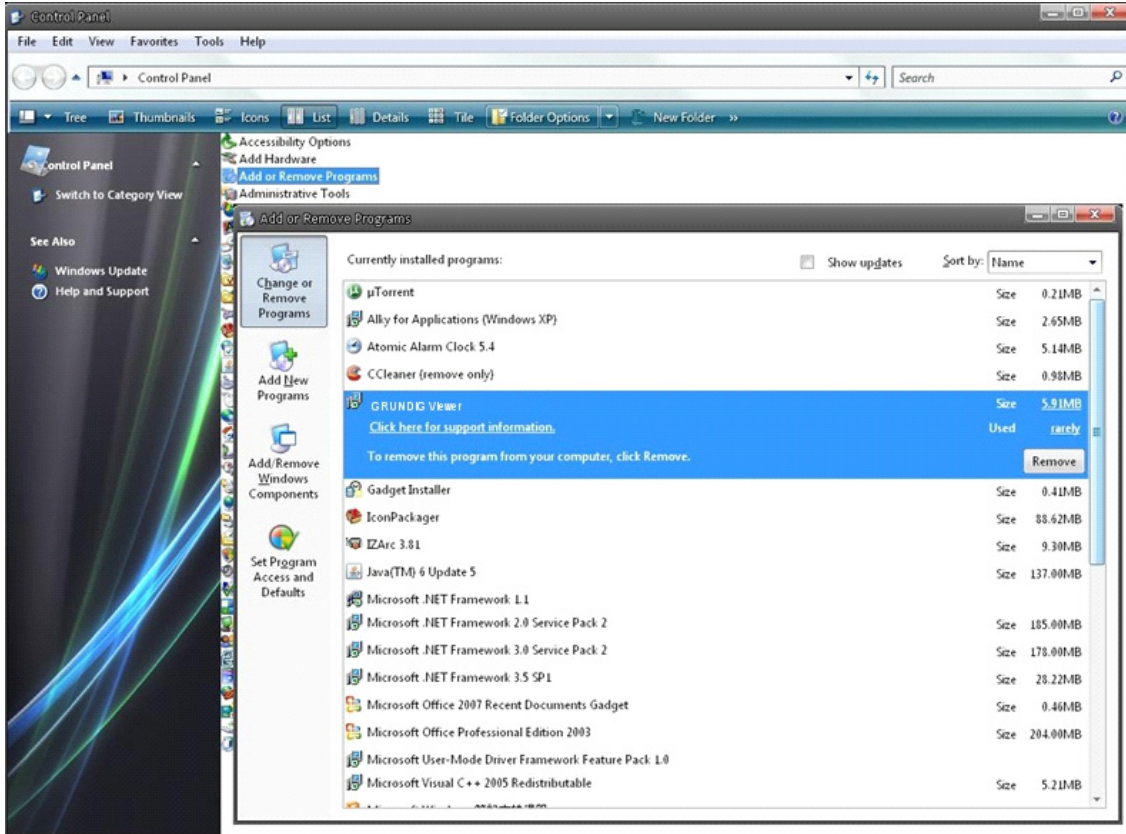
Install the video server on the ceiling by using a screwdriver to tighten the two M4 pan head self-tapping screws in the plastic anchors.

5. Deleting the Existing GRUNDIG Viewer

Users who have installed the GRUNDIG Viewer for 1.3 Megapixel Series IP Cameras on the PC need to delete the existing GRUNDIG Viewer first from the PC before accessing the Video Server.

Deleting the GRUNDIG Viewer :

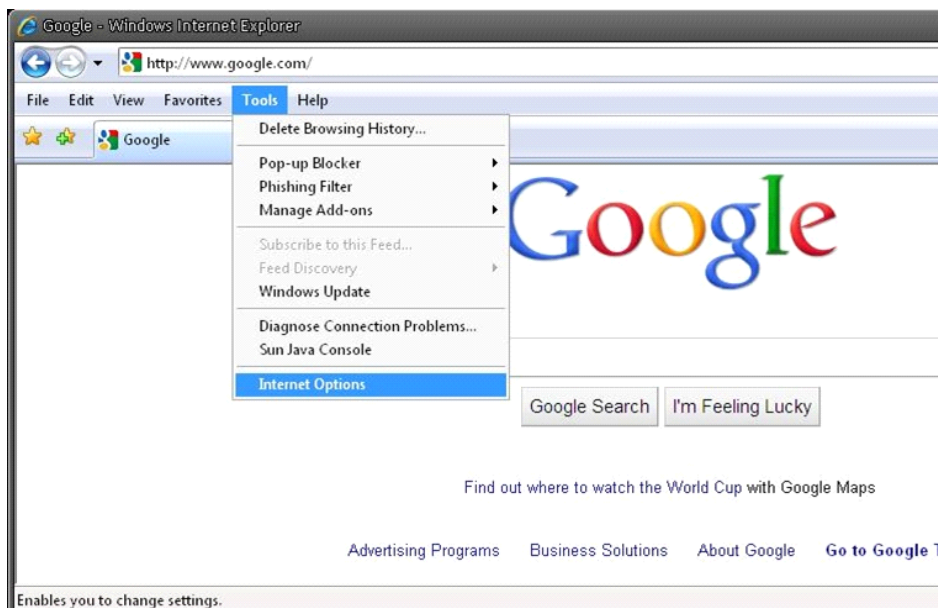
Click on “Control Panel”, and then click on “Add or Remove Programs”. In the “Currently installed programs” list, select “GRUNDIG Viewer” and click the button “Remove” to uninstall the existing GRUNDIG Viewer as shown in the figure below.



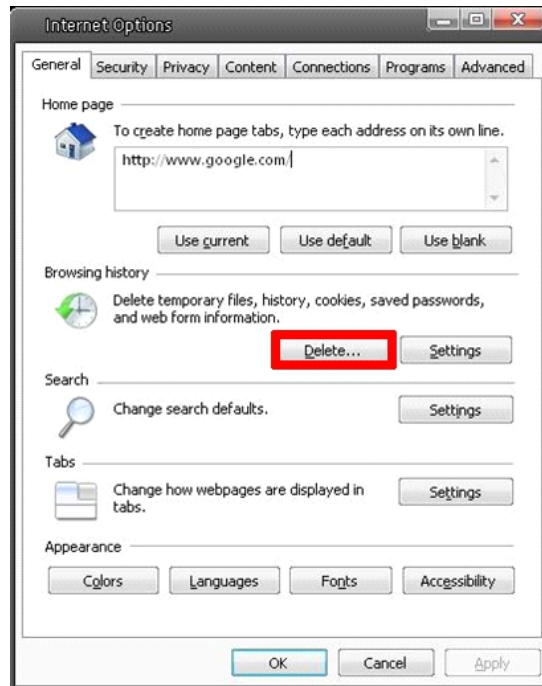
Deleting Temporary Internet Files :

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”.



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



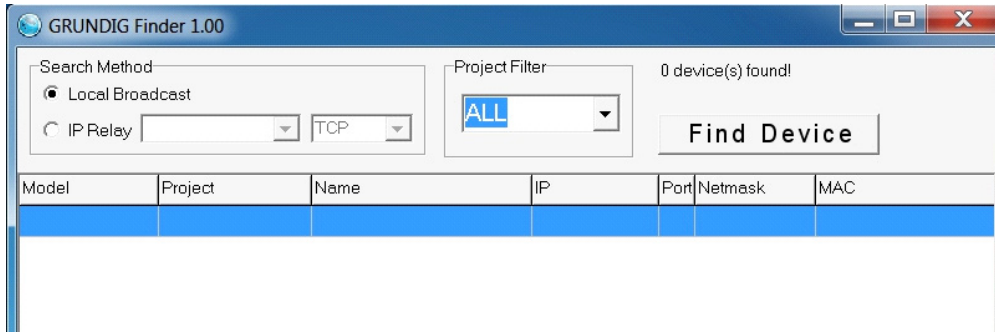
6. Accessing the Video Server

For initial access to the Video Server, users can search through the installer program: GRUNDIG Finder.exe, that can be found on the supplied CD.

GRUNDIG Finder Software Setup :

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



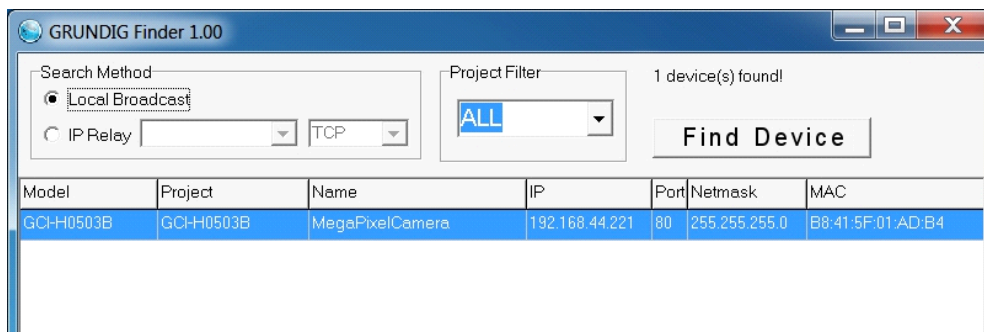


Step 2: The security alert window will pop up. Click “Unblock” to continue.



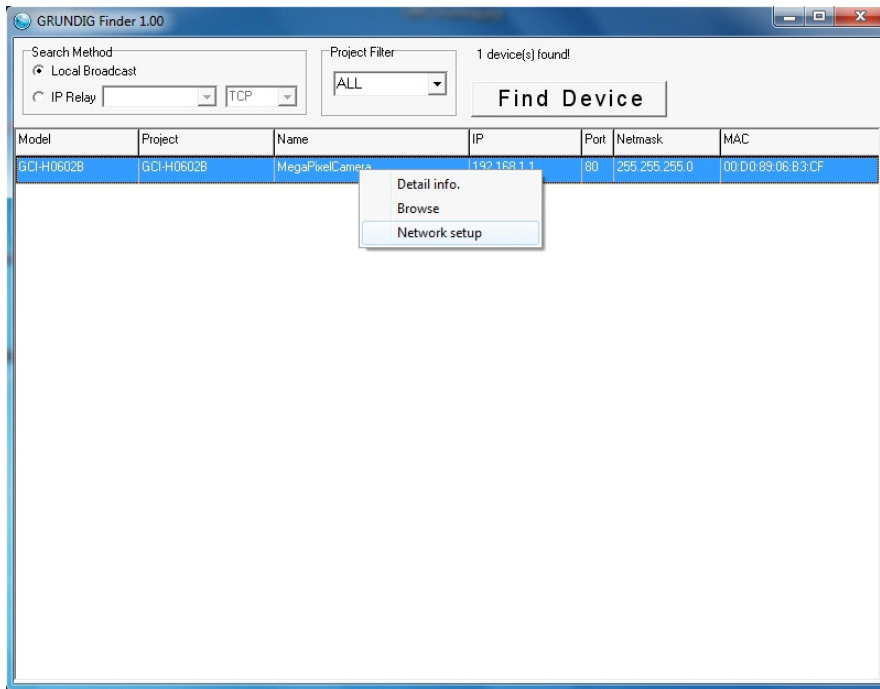
Device Search:

Step 3:
Click on “Find Device” again, afterwards all found IP devices will be listed in the page, as shown in the figure below. The Video Server’s default IP address is: 192.168.1.1.



Step 4:

Double-click or right-click and select "Browse" to access the Video Server directly via the web browser.



Step 5:

Then the dialogue box for entering the default user name and password (as shown below) will appear for logging in to the Video Server.



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 to alter the administrator's password due to security concerns. Please refer to section 9.2. Security for further details.

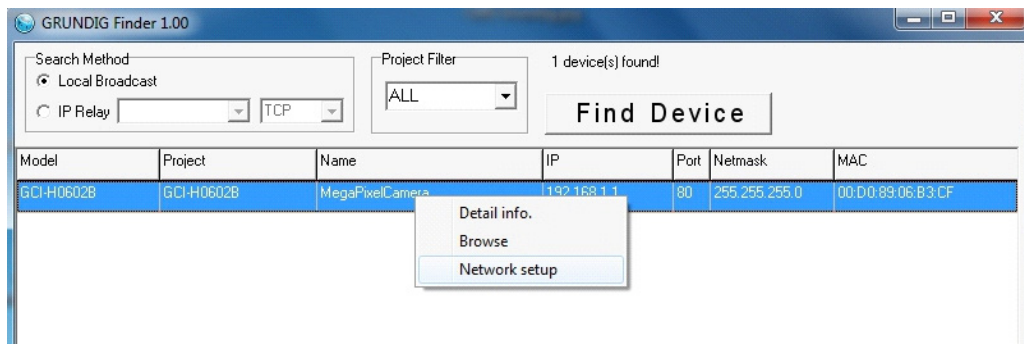
Additionally, users can change the Video Server's network property, either to DHCP or to Static IP, directly in the device finding list. Please refer to the following section for changing the Video Server's network property.

Example of Changing the Video Server's Network Property :

Users can directly change a Video Server's network property, e.g. from static IP to DHCP, in the finding device list. The procedure to change the Video Server's network property is explained below:

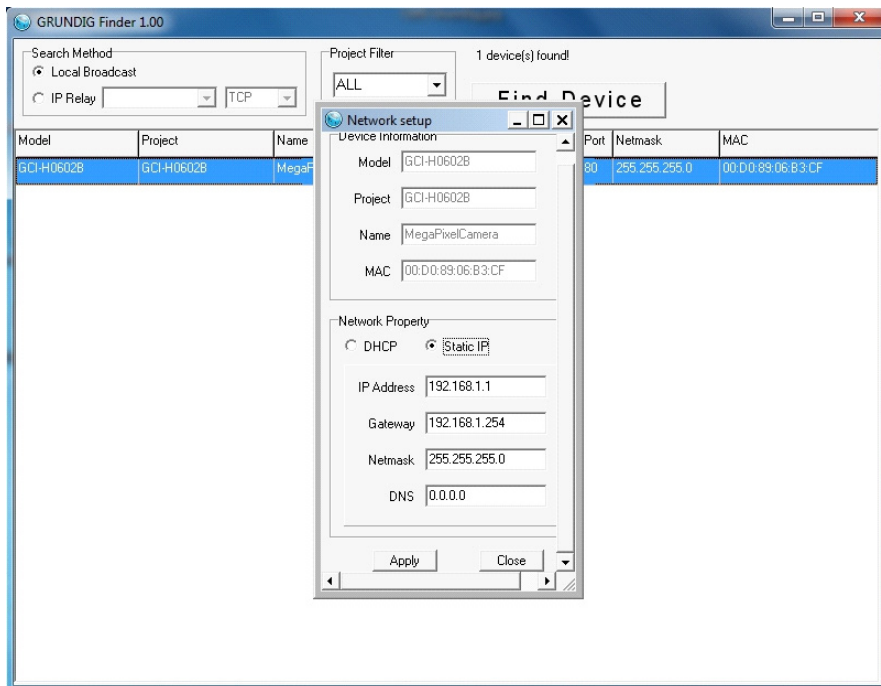
Step 1:

In the finding device list, click on the Video Server of which you would like to change the network property. Right-click on the selected item and select "Network Setup." Meanwhile, record the Video Server's MAC address for future identification.



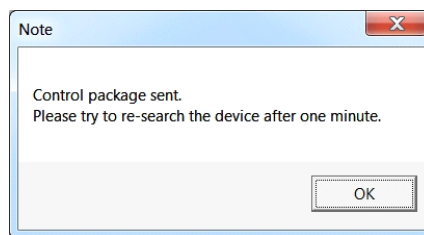
Step 2:

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



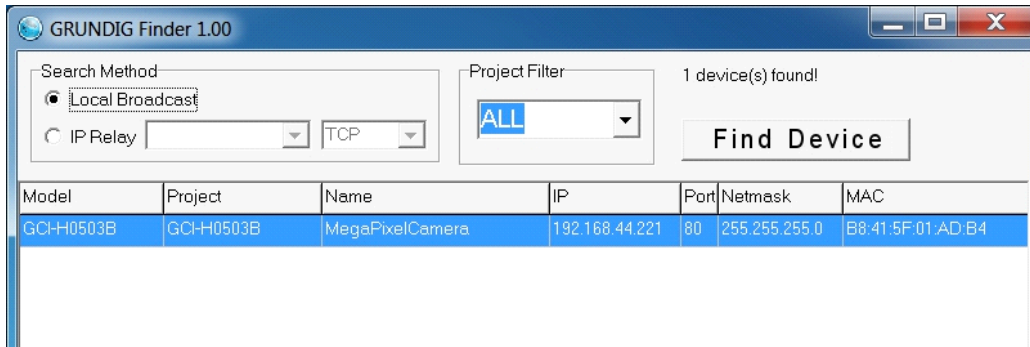
Step 3:

Click on "OK" in the Note of setting the change. Wait for one minute to re-search the Video Server.



Step 4:

Click on the “Find Device” button to search all the devices. Then select the Video Server with the correct MAC address. After double-clicking on the Video Server, the login window will appear.



Step 5:

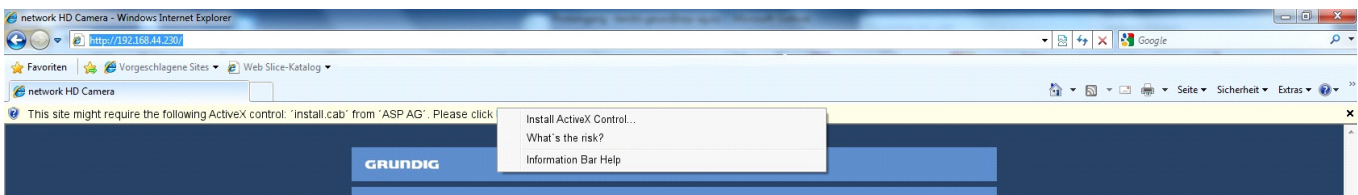
Enter User name and Password to access the Video Server.

Installing the GRUNDIG Viewer Software Online:

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

If the Web browser does not 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.

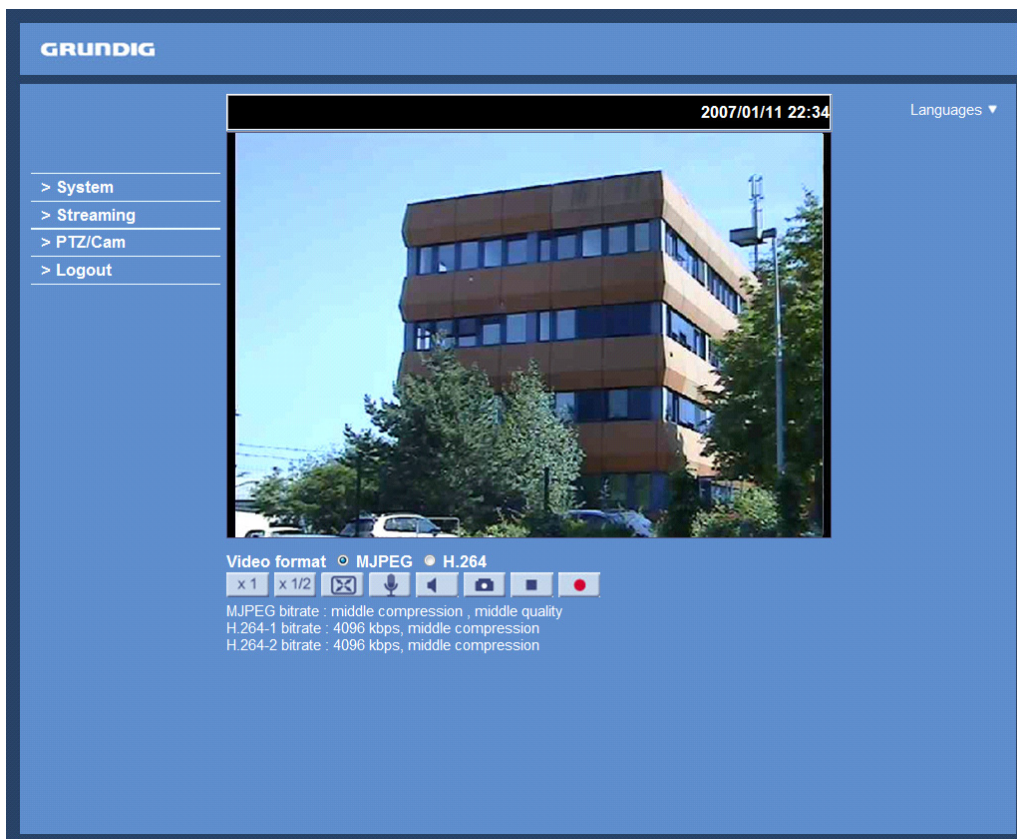
The Information Bar (just below the URL bar) may come out and ask for permission to install the ActiveX Control for displaying video in browser (see the picture below). Right-click on the Information Bar and select “Install ActiveX Control...” to allow the installation.



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

Click on “Finish” to close the GRUNDIG Viewer window when download is finished. For detailed software download procedure, please refer to chapter 15. GRUNDIG Viewer Download Procedure.

Once logged in to the Video Server, users will see the Home page as shown below:



Administrator/User Privileges :

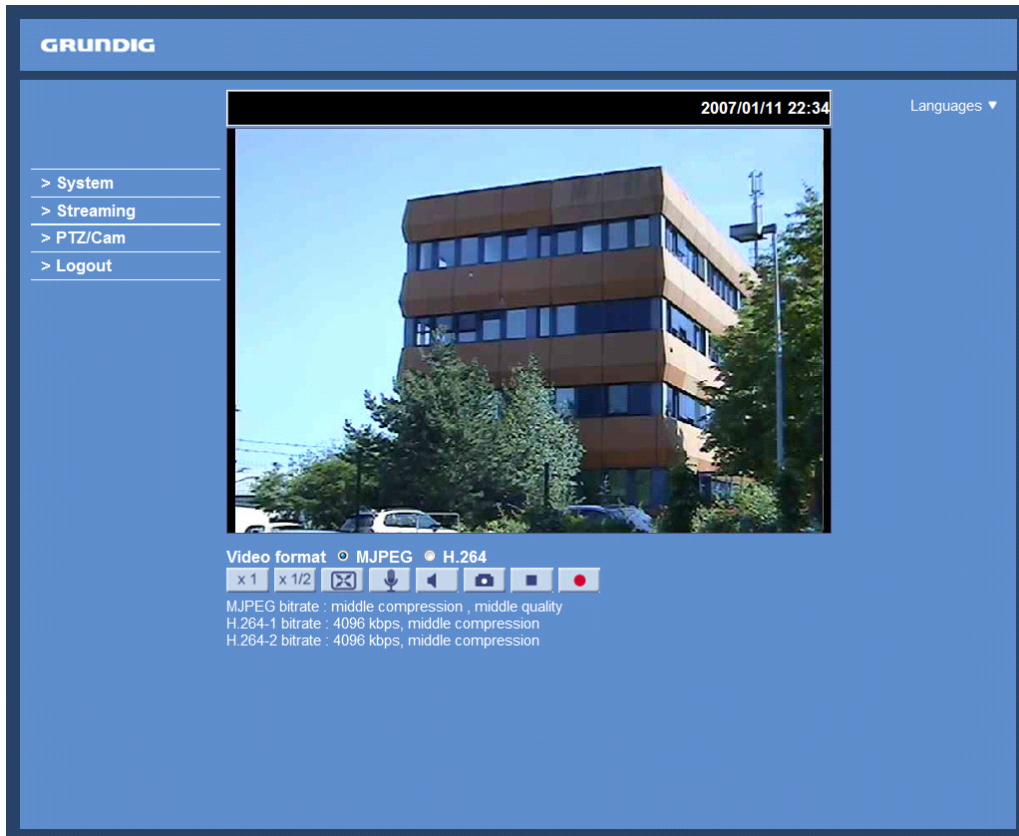
“Administrator” represents the person who can configure the Video Server and who authorises users to have access to the Video Server; “User” refers to someone who has access to the Video Server with limited authority, i.e. to enter the Home and Video Server setting pages.

Image and Focus Adjustment :

The image appears on the Home page when the Video Server was successfully accessed. Adjust zoom and focus as necessary to produce a clear image.

7. Browser-based Viewer Introduction

The picture below shows the main page of the Video Server's user interface.



There are four tabs on the left (System, Streaming, PTZ/Cam and Logout) and one tab on the right (Languages).

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.

Streaming setting :

The Administrator can configure a specific video resolution, video compression mode, video protocol, audio transmission mode, etc. in this page.

PTZ/Cam setting :

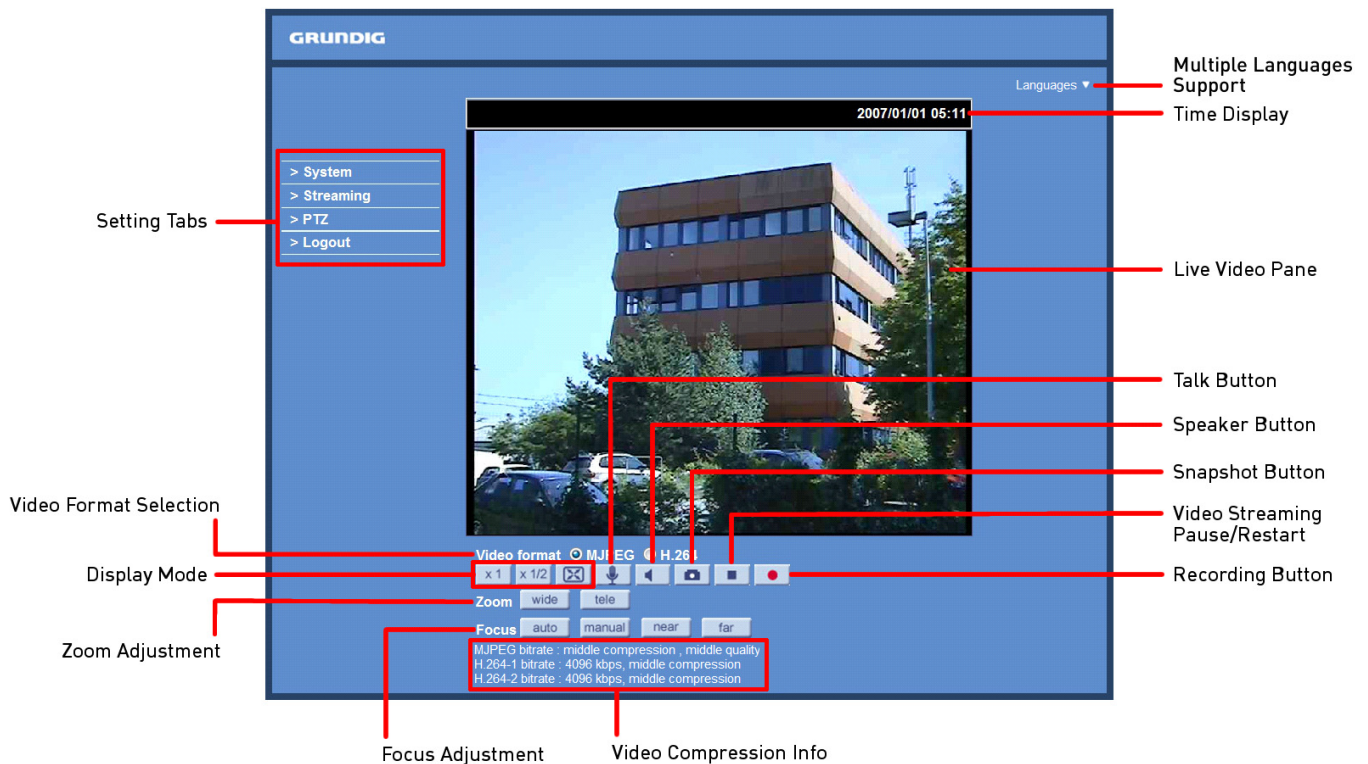
Users can access the Camera's OSD menu via the OSD Menu Control in the "PTZ/Cam" page.

Logout :

Click on this tab to re-login to the Video Server with another user name and password.

8. Home Page

In the Home page, there are several function buttons that are specified below.



Please note that all the function buttons will be visible after you selected "PTZ Camera" under System > Camera Control.

Display Mode (Screen Size Adjustment) :

The display size of the image can be adjusted to x1/2 and full screen.

Talk button (on/off) :

Talk function allows the local site to talk to the remote site. Click on this button to switch it 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) :

Click on the Speaker button to mute/activate the audio.

Snapshot button :

After clicking this button, the JPEG snapshots will be automatically 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 the Windows 7 operating system on their PC 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 please 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 Video Server as usual (as an administrator or user).

Video Streaming Pause/Restart button (pause/restart) :

If you click on the stop button to disable video streaming, the live video will be displayed as black. click on the restart button to show the live video again.

Recording button (on/off) :

When you click on this button, 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 recordings is: C:/. See section 9.13. File Location for further details.

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

Pan/Tilt Control :

Users can implement pan/tilt control by first moving the cursor to the live video pane; then left-click, hold the click and drag the pointer in any direction.

NOTE: You can access the PTZ Control only after you selected "PTZ Camera" under System > Camera Control.

Optical/Digital Zoom Control :

In Normal View display mode, users can implement zoom in/out by clicking in the zoom setting bar and adjusting the zoom manually or by clicking on the "Wide" / "Tele" buttons. In Full Screen mode, users can rotate the mouse wheel to zoom in/out on the image. When the camera reaches the limit of its optical range, it will automatically switch to digital zoom.

Zoom Adjustment :

Click on the buttons wide/ tele to control zoom in/out.

Zoom Adjustment :

Click on the buttons wide/ tele to control zoom in/out.

Focus Adjustment :

- Auto Focus:

Click on the "auto" button to enable AF mode. In this mode, the camera will keep in focus automatically and continuously regardless of zoom changes or any view changes.

- Manual Focus:

After clicking on the "Manual" button, users can adjust the focus manually via the "Near" and "Far" buttons.

Multiple Languages Support :

Multiple languages are supported for the viewer window interface.

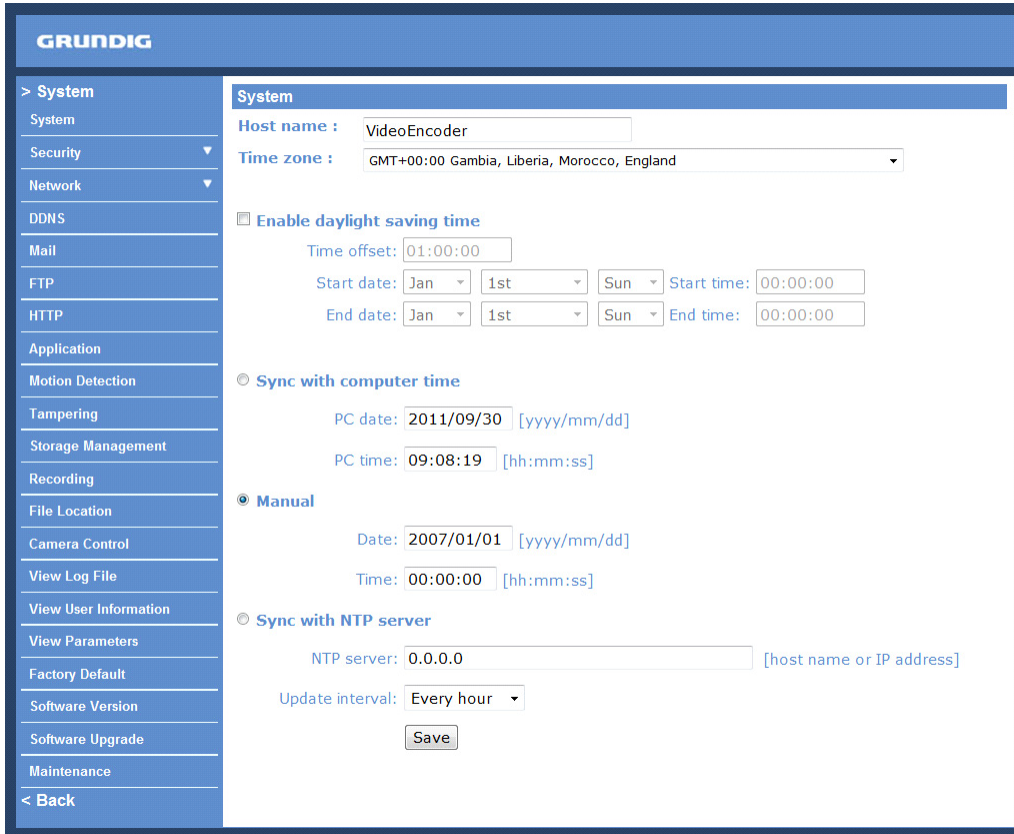
9. System Related Settings

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.

9.1. Host Name & System Time Setting

Click on the first category <System> in the left column; the page is shown below.



Host Name :

The name is for Video Server identification (max. 30 characters). If the 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 be displayed 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 the 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 :

After selecting this item, the video date and time display will be synchronised with the PC.

Manual :

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

Sync with NTP Server :

Network Time Protocol (NTP) is an alternate way to synchronise your Video Server’s clock with a NTP server. Please specify the server you wish to synchronise the Video Server with 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.

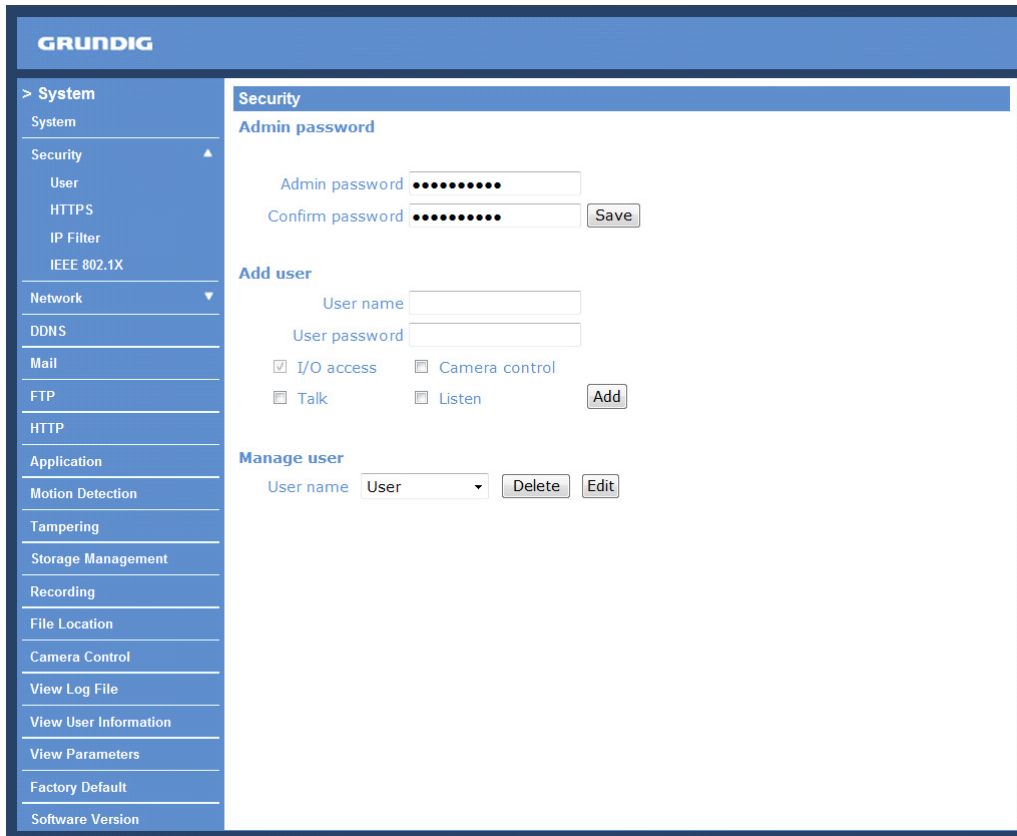
NOTE: Click on < Save > to confirm the new setting.

9.2. Security

When you click on the category <Security>, there will be a drop-down menu with several tabs including <User>, <HTTPS>, <IP Filter>, and <IEEE 802.1X>.

<User> :

When you click on the <User> tab under the category <Security>, the <User> page will be shown as in the picture below.



The screenshot shows the Grundig web interface for user management. On the left is a navigation menu with categories: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Tampering, Storage Management, Recording, File Location, Camera Control, View Log File, View User Information, View Parameters, Factory Default, and Software Version. The 'Security' category is expanded, showing sub-items: Admin password, Add user, and Manage user. The 'Admin password' section has two password input fields (masked with dots) and a 'Save' button. The 'Add user' section has fields for 'User name' and 'User password', and checkboxes for 'I/O access', 'Camera control', 'Talk', and 'Listen', with an 'Add' button. The 'Manage user' section shows a dropdown menu for 'User name' (currently set to 'User') and 'Delete' and 'Edit' buttons.

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 in the new user 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 "Camera control", "Talk" and "Listen" can be assigned.

- I/O access:

This item supports fundamental functions that enable users to view video when accessing the Video Server.

- Camera control:

This item allows the appointed user to change the Video Server's parameters on the Video Server Setting page.

- Talk/Listen:

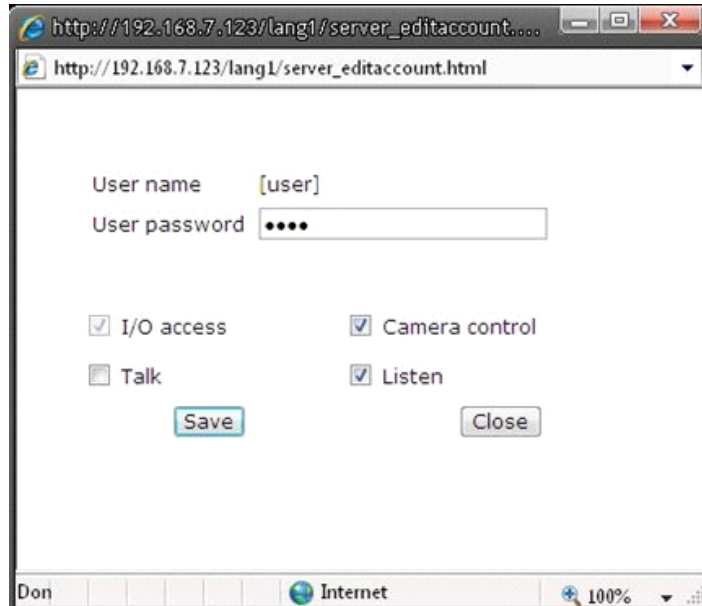
Talk and Listen functions allow the appointed user on the local site (PC site) to communicate, for instance, with the administrator on the remote site.

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.

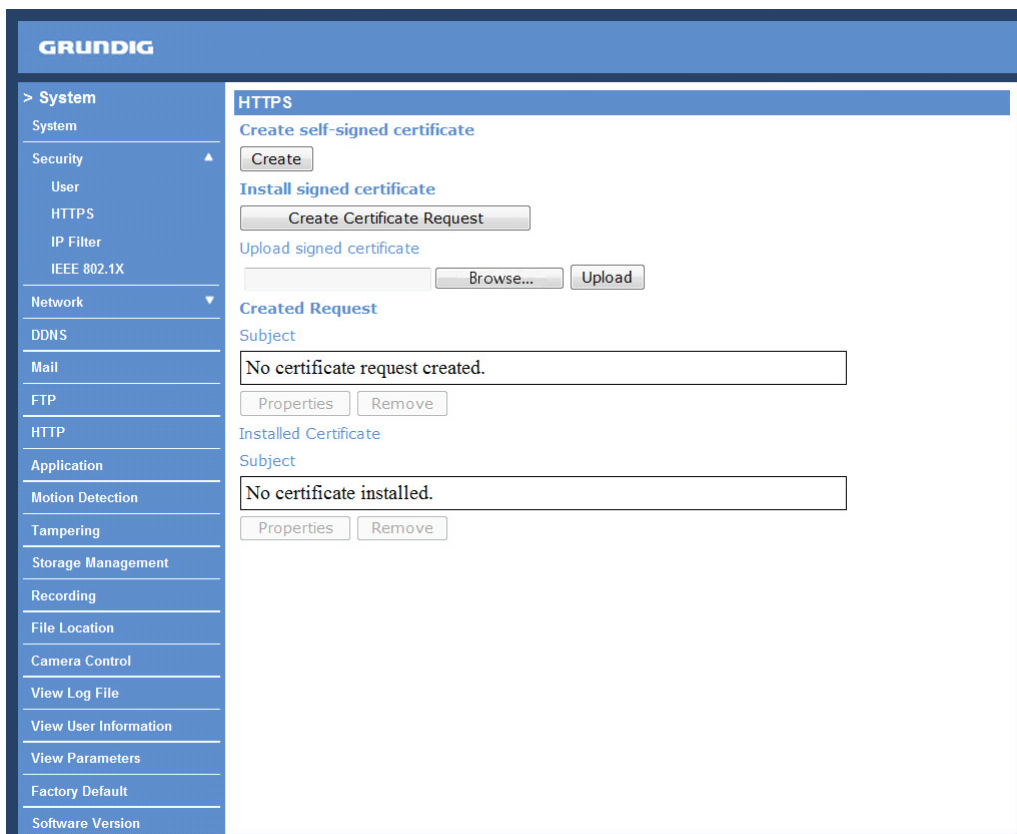
To edit a user, pull down the user list and select a user name. Click <Edit> to edit the user's password and privileges.

NOTE: It is required to enter the User password and to select the functions that will be open to the user. When finished, click <Save> to modify the account authority.



<HTTPS> :

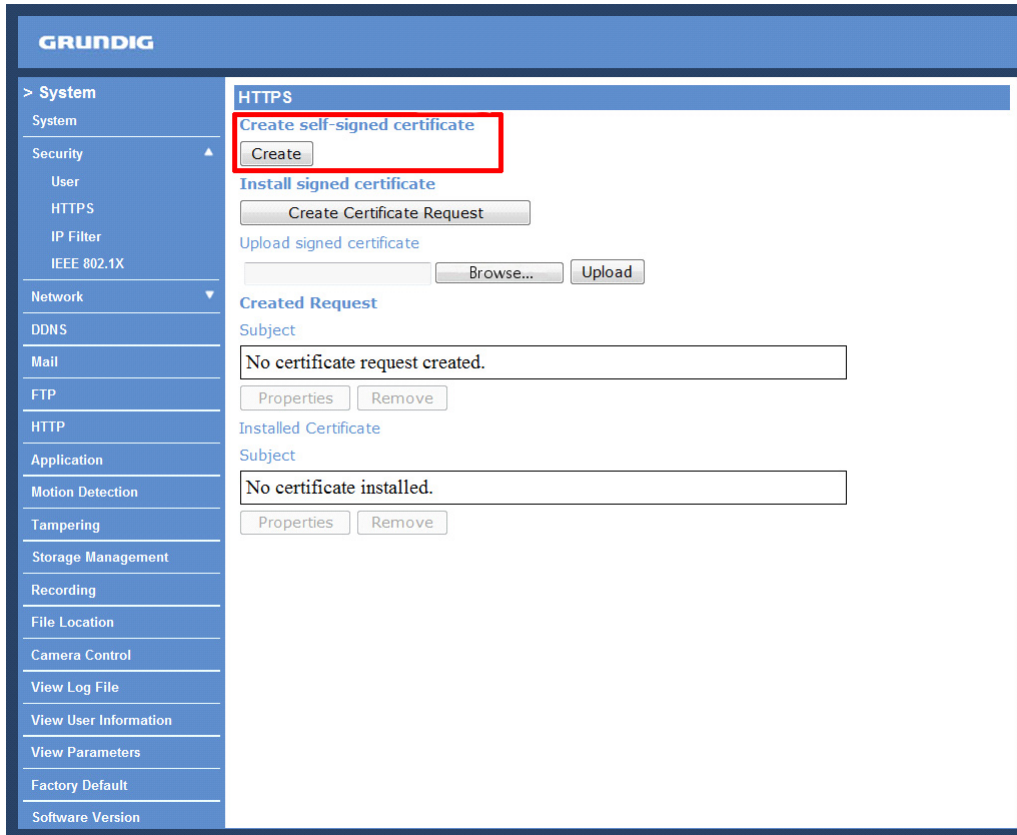
<HTTPS> allows secure connections between the Video Server and the web browser using the <Secure Socket Layer (SSL)> or the <Transport Layer Security (TLS)>, which prevent others from snooping on your Video Server settings or Username/Password. It is required to install a self-signed certificate or a CA-signed certificate for implementation of <HTTPS>.



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

Create self-signed certificate :

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



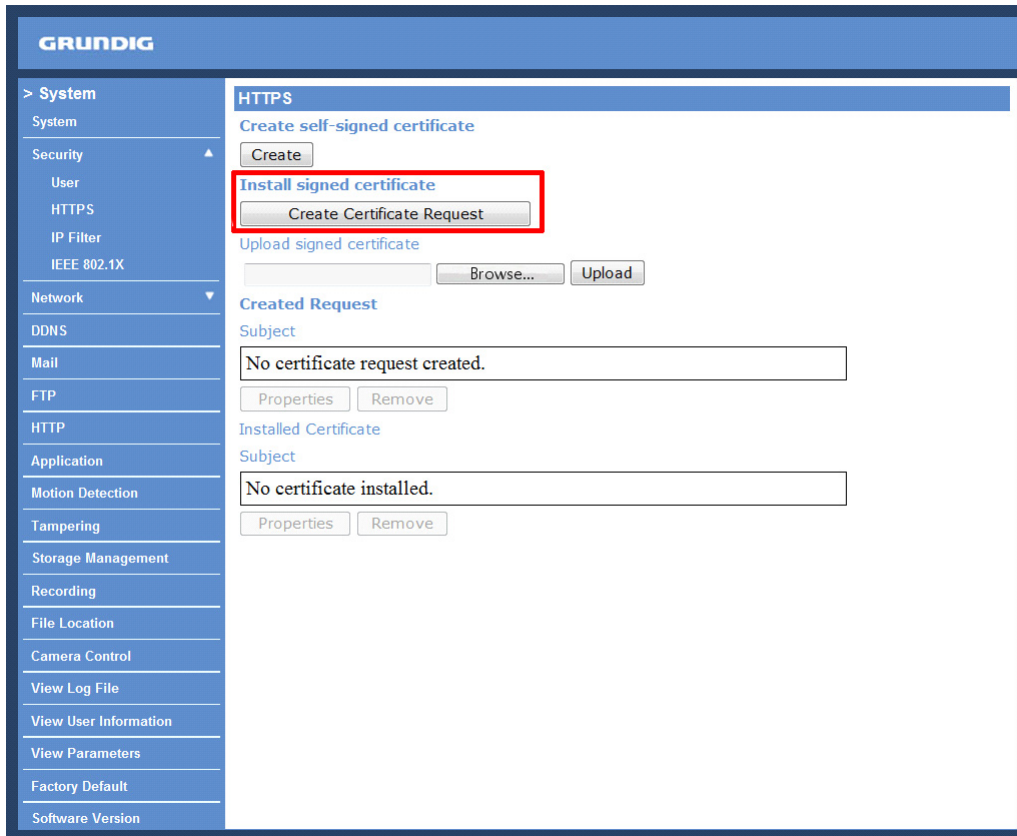
Click on the <Create> button under “Create self-signed certificate” and provide the requested information to install a self-signed certificate for the Video Server. Please refer to the last part of this section: “Provide the Certificate Information” for more details.

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 section “Provide the Certificate Information” for more details.

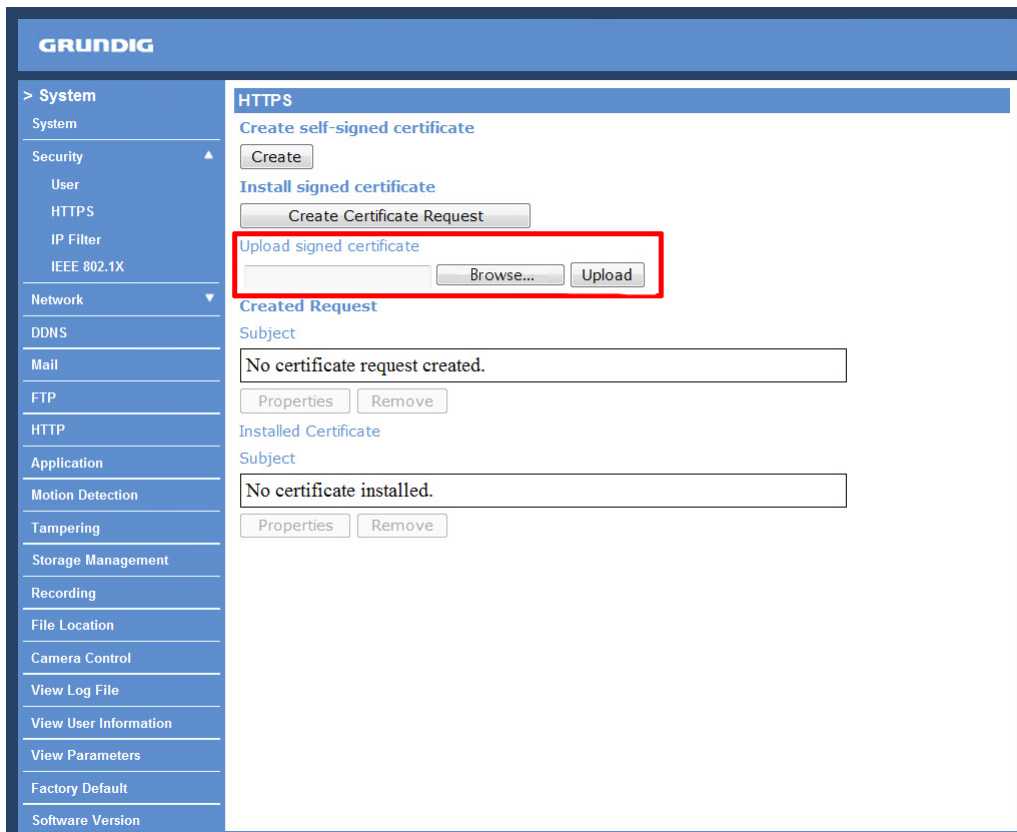
Install signed certificate :

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



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

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



Provide the Certificate Information :

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

The screenshot shows a web browser window titled "http://192.168.44.19/lang1/server_certificate.html - Windows Internet Explorer". The address bar shows "http://192.168.44.19/lang1/server_certificate.html". The main content area displays a form titled "Create Self-Signed Certificate" with the following fields:

- Country:
- State or province:
- Locality:
- Organisation:
- Organisational unit:
- Common name:
- Valid days: days[1...9999]

At the bottom of the form are "OK" and "Cancel" buttons. The browser's status bar at the bottom shows "Internet" and a zoom level of "125%".

- 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).

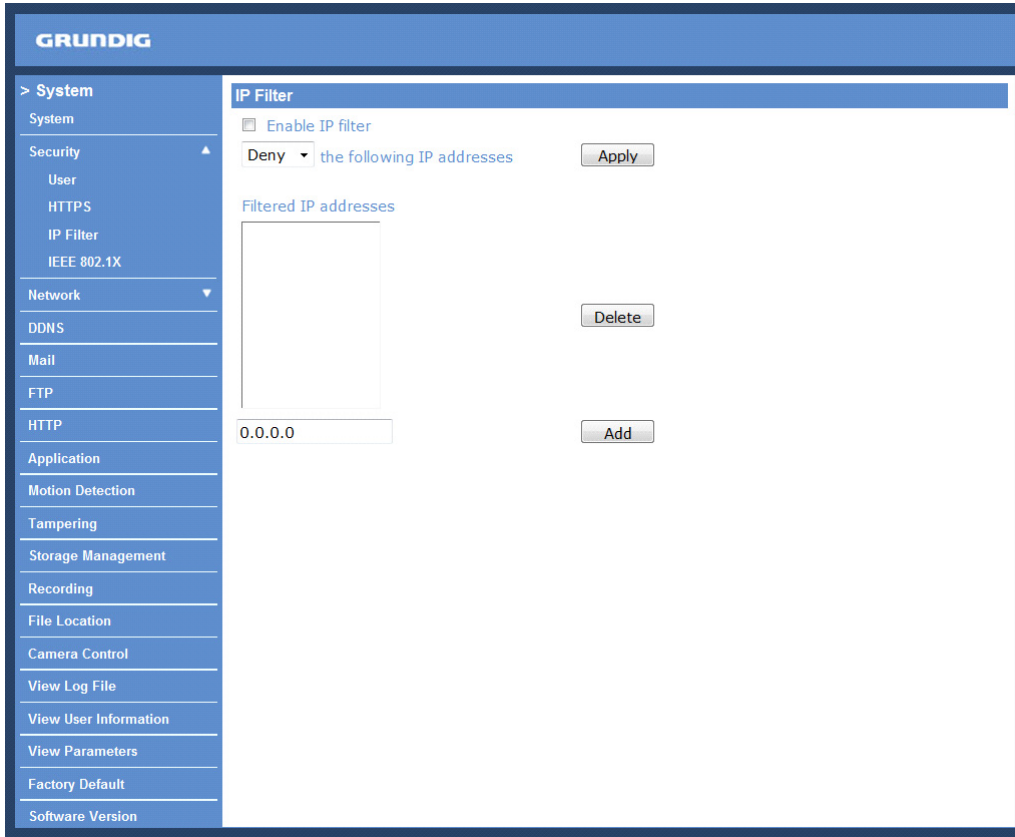
- Valid days (Self-signed Certificate Only):

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 Video Server can be restricted by denying/allowing specific IP addresses.



General :

- Enable IP Filter:

Check the box to enable the IP Filter function. Once enabled, access to the Video Server will be allowed/denied for the listed IP addresses (IPv4).

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

- Add/Delete IP Address:

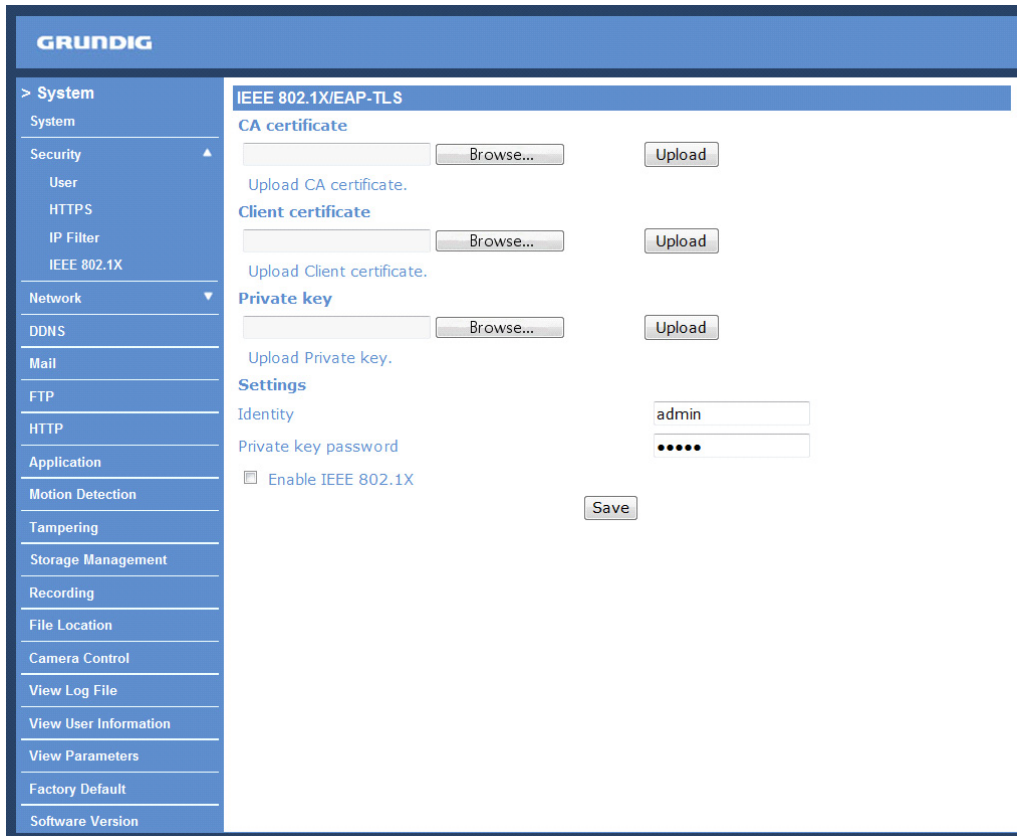
Input the IP address and click the <Add> button to add a new filtered address.

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 Video Server can access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). To do this, users need to contact the network administrator to receive certificates, user IDs and passwords.



CA Certificate :

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

Client Certificate/Private Key :

Upload the Client Certificate and Private Key for authenticating the Video Server 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 identification.

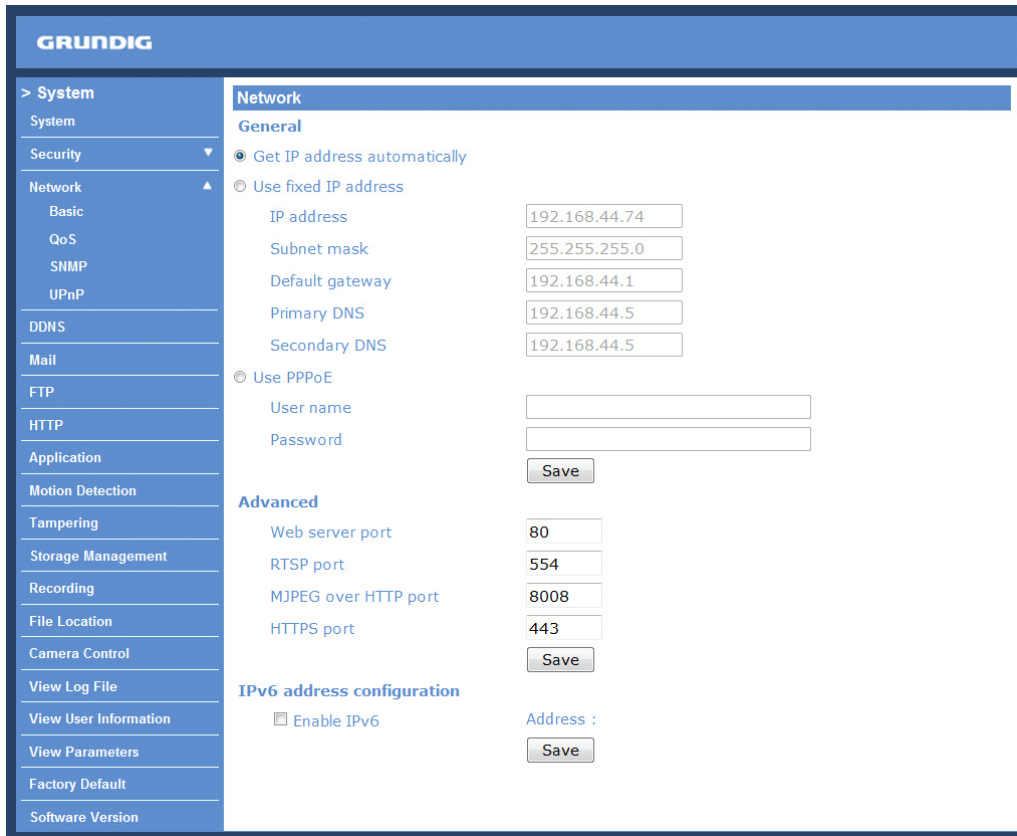
Enable IEEE 802.1X :

Check the box to enable IEEE 802.1X.

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

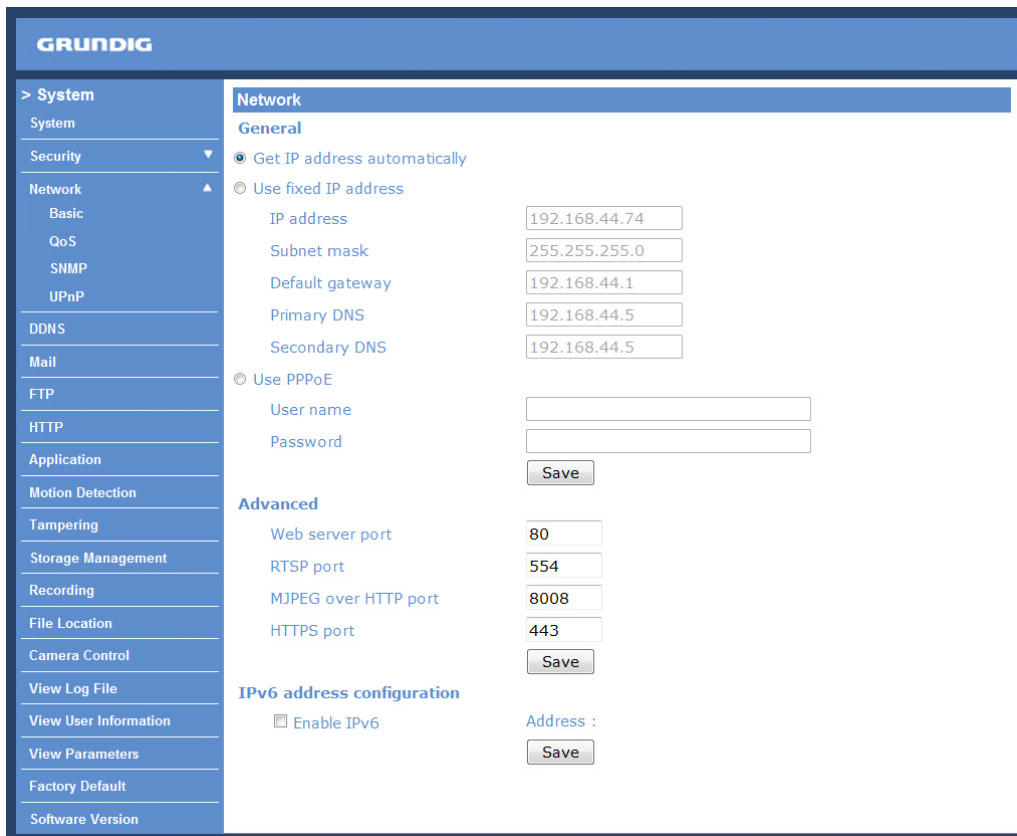
9.3. Network

After clicking on <Network> in the left column, the following page will display:



The screenshot shows the Grundig web interface for network configuration. The left sidebar contains a menu with categories: > System, System, Security, Network (expanded), DDNS, Mail, FTP, HTTP, Application, Motion Detection, Tampering, Storage Management, Recording, File Location, Camera Control, View Log File, View User Information, View Parameters, Factory Default, and Software Version. The main content area is titled 'Network' and has a 'General' tab selected. Under 'General', there are two radio button options: 'Get IP address automatically' (selected) and 'Use fixed IP address'. The 'Use fixed IP address' section includes input fields for IP address (192.168.44.74), Subnet mask (255.255.255.0), Default gateway (192.168.44.1), Primary DNS (192.168.44.5), and Secondary DNS (192.168.44.5). Below this is the 'Use PPPoE' section with fields for User name and Password, and a 'Save' button. The 'Advanced' section includes fields for Web server port (80), RTSP port (554), MJPEG over HTTP port (8008), and HTTPS port (443), with a 'Save' button. The 'IPv6 address configuration' section has a checkbox for 'Enable IPv6' and an 'Address' field with a 'Save' button.

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



This screenshot is identical to the one above, showing the Grundig Network configuration page. The 'Network' category in the left sidebar is expanded, and the 'Basic' sub-tab is selected. The configuration options and values are the same as in the previous screenshot.

<Basic> :

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

The screenshot displays the Grundig web interface for network configuration. On the left is a sidebar menu with the following items: > System, System, Security, Network (expanded), Basic, QoS, SNMP, UPnP, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Tampering, Storage Management, Recording, File Location, Camera Control, View Log File, View User Information, View Parameters, Factory Default, and Software Version. The main content area is titled 'Network' and contains the following sections:

- General:** Radio buttons for 'Get IP address automatically' (selected) and 'Use fixed IP address'. Below are input fields for IP address (192.168.44.74), Subnet mask (255.255.255.0), Default gateway (192.168.44.1), Primary DNS (192.168.44.5), and Secondary DNS (192.168.44.5).
- Use PPPoE:** Radio button for 'Use PPPoE'. Below are input fields for User name and Password, and a 'Save' button.
- Advanced:** Fields for Web server port (80), RTSP port (554), MJPEG over HTTP port (8008), and HTTPS port (443), with a 'Save' button.
- IPv6 address configuration:** A checkbox for 'Enable IPv6' and an 'Address' field with a 'Save' button.

Get IP address automatically [DHCP]:

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

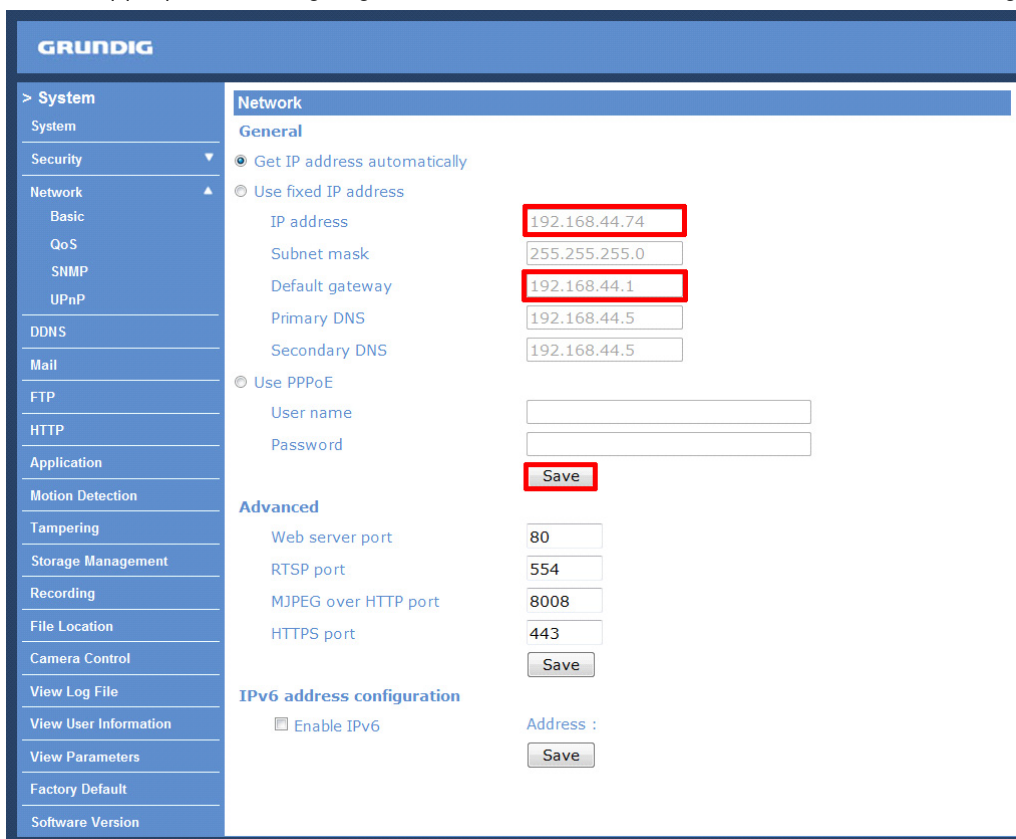
If "Get IP address automatically" is selected, after the Video Server restarts, users can search its IP address through the installer program: GRUNDIG Finder.exe that is on the supplied CD.

NOTE: The DHCP function can only be used if you have a DHCP server in the used network.

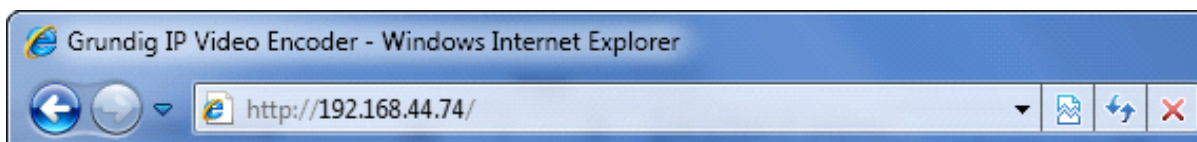
NOTE: Please make a record of the Video Server's MAC address, which can be found on the label of the Video Server, for identification in the future.

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. 192.168.44.106; then go to the Default Gateway (explained later) and type in the appropriate setting, e.g. 192.168.44.1. Press “Save” to confirm the new setting.



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



- IP address:

This is necessary for network identification.

- Subnet mask:

It is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

- Default gateway:

This is the gateway used to forward frames to destinations in different subnets. An invalid gateway setting will fail in 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 backs up the primary DNS.

Use PPPoE :

The PPPoE users need to enter the PPPoE Username and Password into the fields, and need to 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, users must be informed about the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Video Server whose IP address is 192.168.0.100 from 80 to 8080, the user must type in in the web browser "http://192.168.0.100:8080" instead of "http://192.168.0.100".

- RTSP port:

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

- MJPEG over HTTP port:

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

- HTTPS port:

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

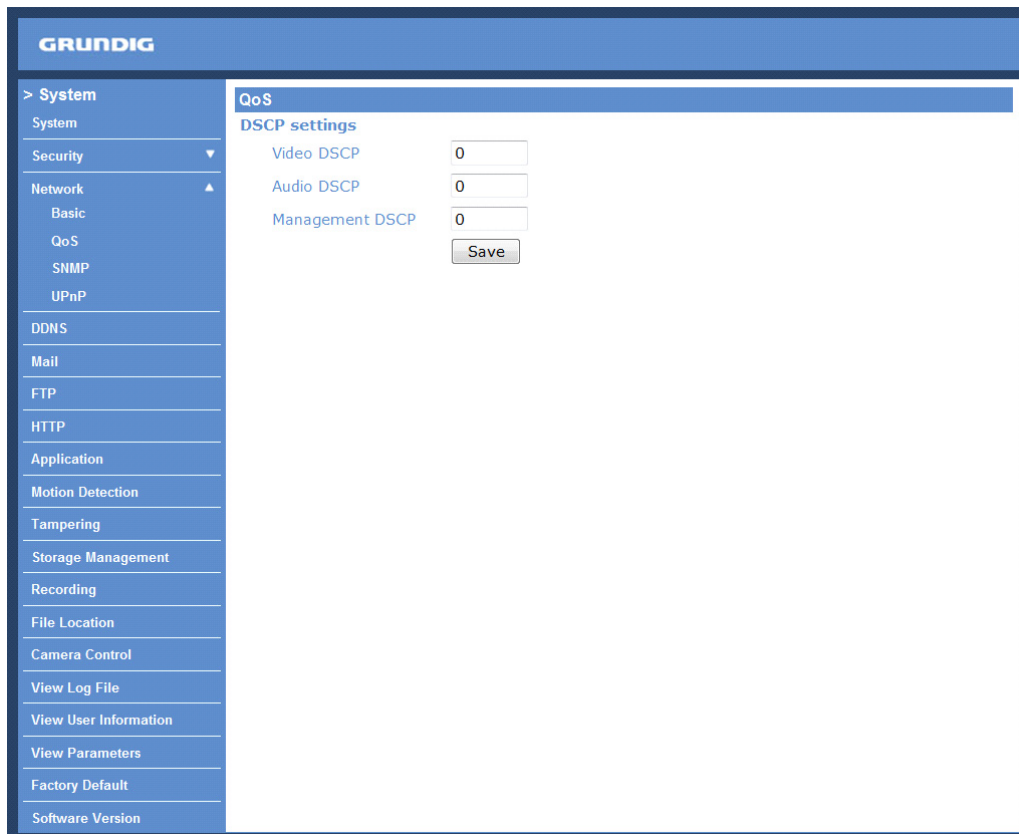
NOTE: Be aware to assign a different port number for each separate service mentioned above.

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 :

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

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

- Video DSCP:

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

- Audio DSCP:

This setting is only available for the Video Servers which support audio.

- Management DSCP:

This class consists of the 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 Video Server can be monitored and managed remotely by the network management system.

The screenshot shows the Grundig web interface for configuring SNMP settings. The left sidebar contains a navigation menu with categories like System, Security, Network, and Application. The main content area is titled 'SNMP Settings' and is divided into several sections. The 'SNMP v1/v2' section allows enabling SNMP v1 and v2, and setting read and write community names. The 'Traps for SNMP v1/v2' section allows enabling traps and setting a trap address and community. The 'Trap options' section includes a checkbox for 'Warm start'. A 'Save' button is located at the bottom left of the main content area.

SNMP v1/v2 :

- Enable SNMP:

Select the version of SNMP to use by checking the corresponding 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 Video Server 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 Video Server, performs a software reload.

Click the "Save" button to complete the setting.

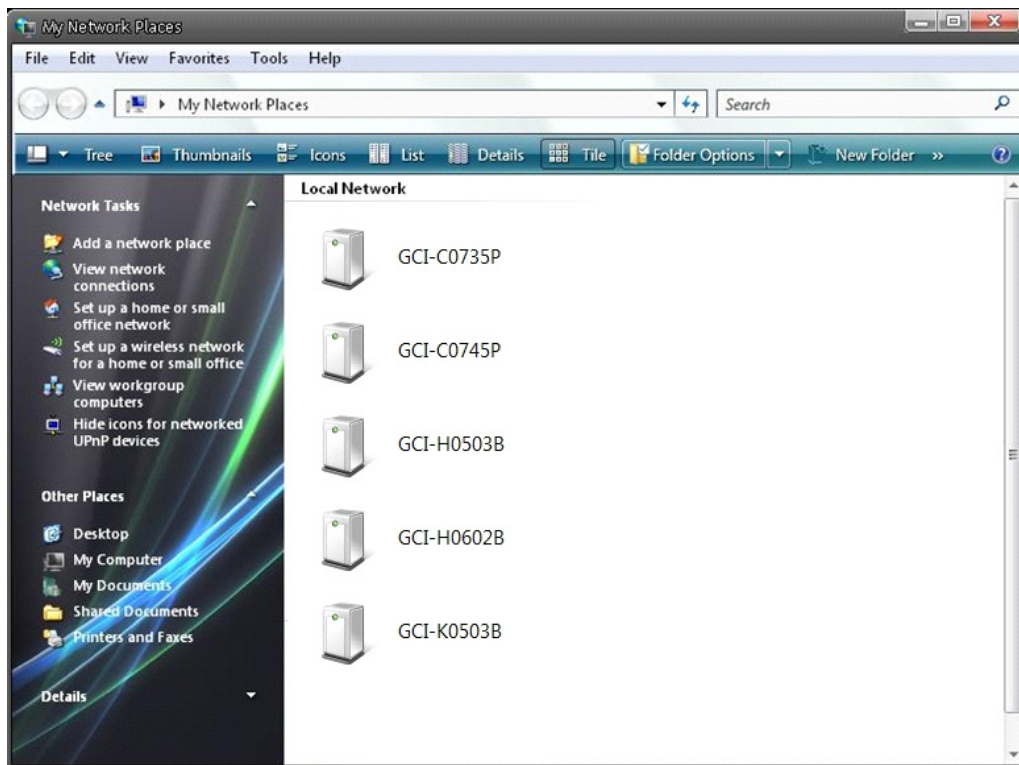
<UPnP> :

The screenshot shows the Grundig web interface for configuring UPnP settings. The interface has a blue header with the 'GRUNDIG' logo. On the left side, there is a navigation menu with the following items: > System, System, Security, Network, Basic, QoS, SNMP, UPnP, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Tampering, Storage Management, Recording, File Location, Camera Control, View Log File, View User Information, View Parameters, Factory Default, and Software Version. The main content area is titled 'UPnP' and 'UPnP setting'. It contains two checkboxes: 'Enable UPnP' (checked) and 'Enable UPnP port forwarding' (unchecked). Below these is a text input field for 'Friendly name' containing 'GEC-D2201AR' and a 'Save' button.

UPnP Setting :

- Enable UPnP:

When UPnP is enabled, whenever the Video Server is presented to LAN, the icon of the connected Video Server 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 UPnP port forwarding is enabled, the Video Server 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 Video Server for identity.

NOTE: The Default Friendly name is GEC-D2201AR.

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.

The screenshot shows the DDNS configuration interface. The left sidebar lists various system settings, with 'DDNS' selected. The main panel is titled 'DDNS' and includes the following elements:

- Dynamic DNS**: Use Dynamic DNS If You Want To Use Your DDNS Account.
- Enable DDNS
- Provider: DynDNS.org(Dynamic) (dropdown menu)
- Host name: [text input field]
- Username/E-mail: [text input field]
- Password/Key: [text input field]
- Save button

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 user name or e-mail required by the DDNS provider for authentication.

Password/Key :

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

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 from server to server. 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:

GRUNDIG	
> System	Mail
System	SMTP
Security	1st SMTP (mail) server
Network	1st SMTP (mail) server port 25
DDNS	1st SMTP account name
Mail	1st SMTP password
FTP	1st recipient email address
Application	2nd SMTP (mail) server
Motion Detection	2nd SMTP (mail) server port 25
Storage Management	2nd SMTP account name
Recording	2nd SMTP password
Camera Control	2nd recipient email address
File Location	Sender email address
View Log File	Save
View User Information	
View Parameters	
Factory Default	
Software Version	
Software Upgrade	
Maintenance	
< Back	

Two sets of SMTP can be configured. Each set includes the 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 the sending of 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, into the fields.

Click "Save" when the setting is finished.

GRUNDIG	
> System	FTP
System	FTP
Security	Built-in FTP server port: 21
Network	1st FTP server: [text box]
DDNS	1st FTP server port: 21
Mail	1st FTP user name: [text box]
FTP	1st FTP password: [text box]
Application	1st FTP remote folder: [text box]
Motion Detection	<input type="checkbox"/> 1st FTP passive mode
Storage Management	2nd FTP server: [text box]
Recording	2nd FTP server port: 21
Camera Control	2nd FTP user name: [text box]
File Location	2nd FTP password: [text box]
View Log File	2nd FTP remote folder: [text box]
View User Information	<input type="checkbox"/> 2nd FTP passive mode
View Parameters	[Save]
Factory Default	
Software Version	
Software Upgrade	
Maintenance	
< Back	

9.7. HTTP

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

Click "Save" when the setting is finished.

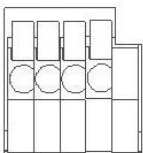


Please also refer to: 9.8. Application: Send HTTP notification / 9.9. Motion Detection for HTTP Notification settings.

9.8. Application (Alarm Settings)

The Video Server supports one set of alarm input and alarm output. Please make sure the alarm connections are properly wired before starting to configure alarm related settings on this "Application" page. Please refer to the pin definition table below for alarm system wiring.

PIN 4: GND
PIN 5: IN+
PIN 6: OUT-
PIN 7: OUT+



4 5 6 7 I/O

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 the 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:

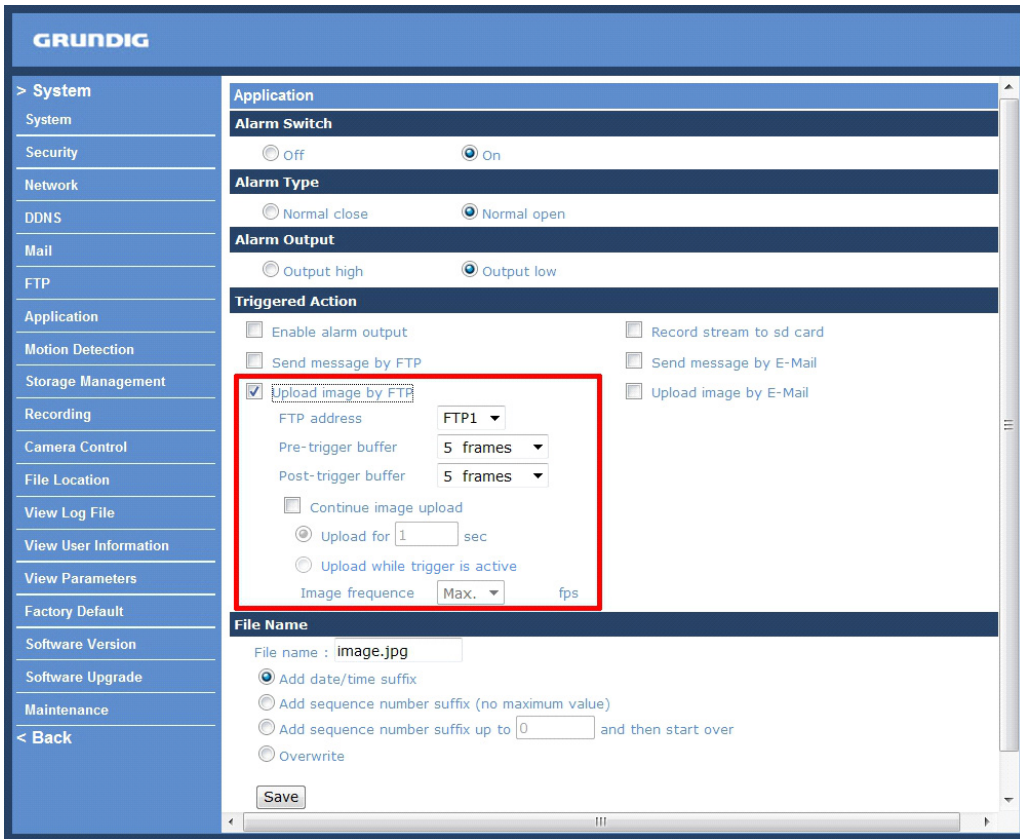
Select this item to enable alarm relay output.

- 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.

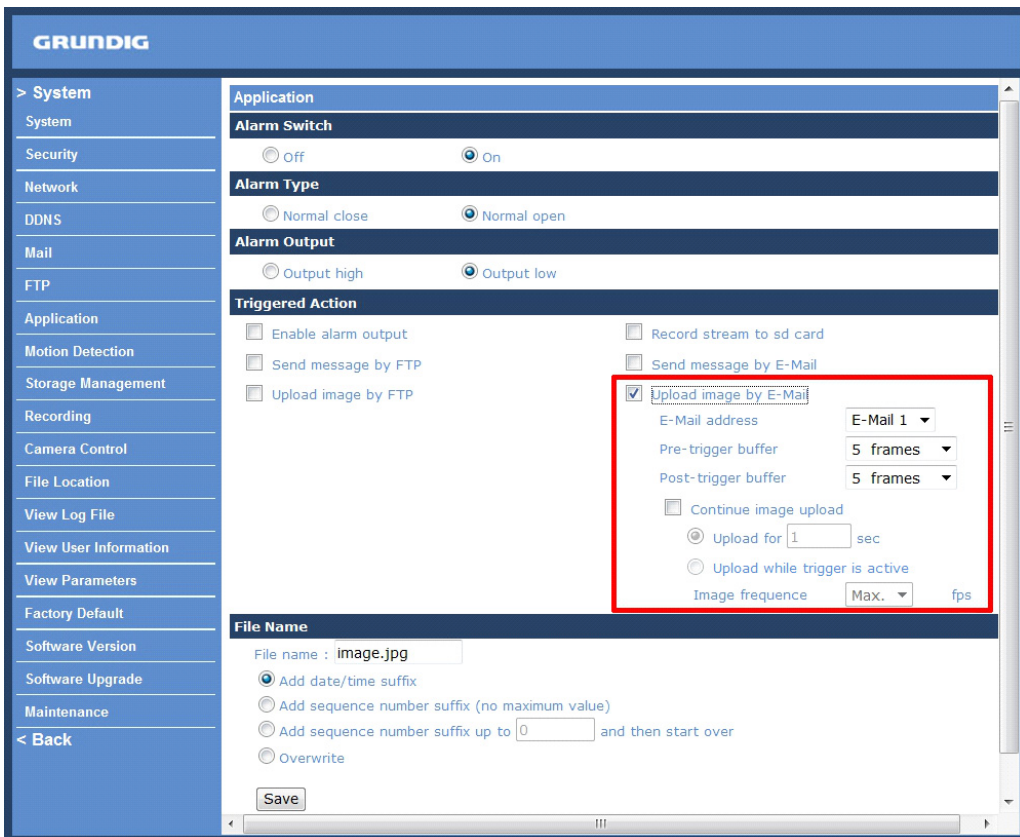
- Upload Image by FTP:

After selecting this item, 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.



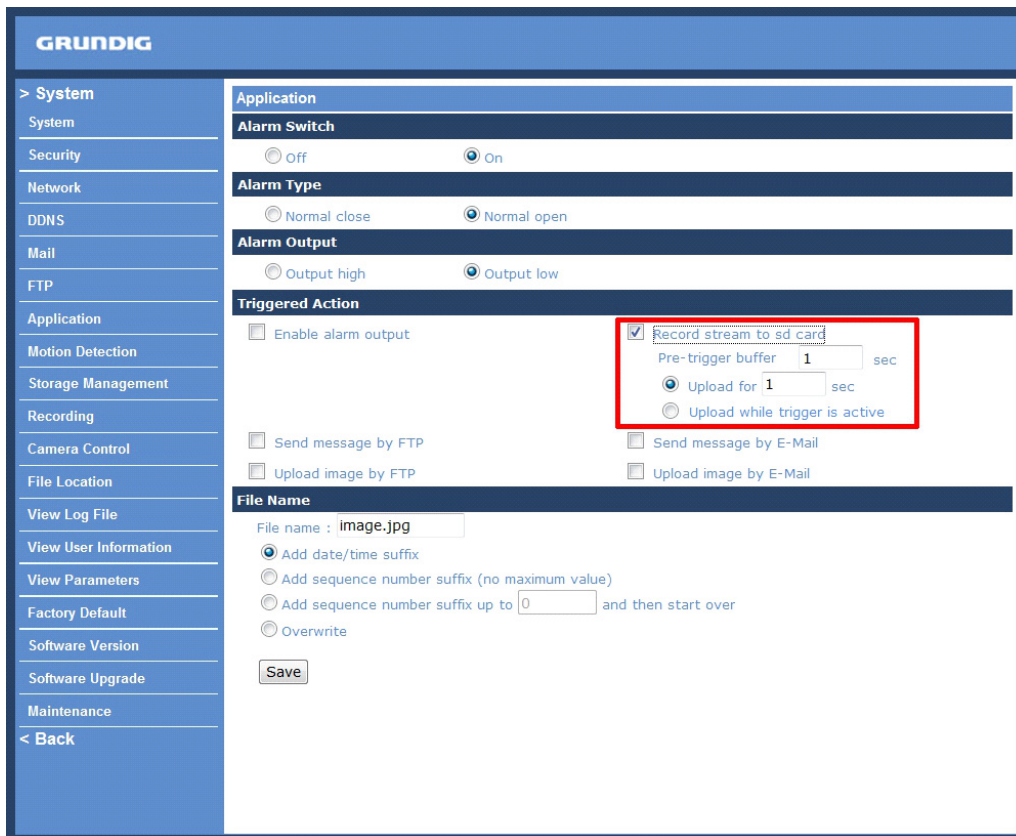
- Upload Image by E-Mail:

After selecting this item, 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.



- Record stream to SD Card:

When you check this item, the alarm-triggered recording will be stored on your 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.

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

The pre-trigger buffer recording function allows users to check what happened to trigger the alarm. The pre-trigger buffer time range is from 1 to 3 seconds.

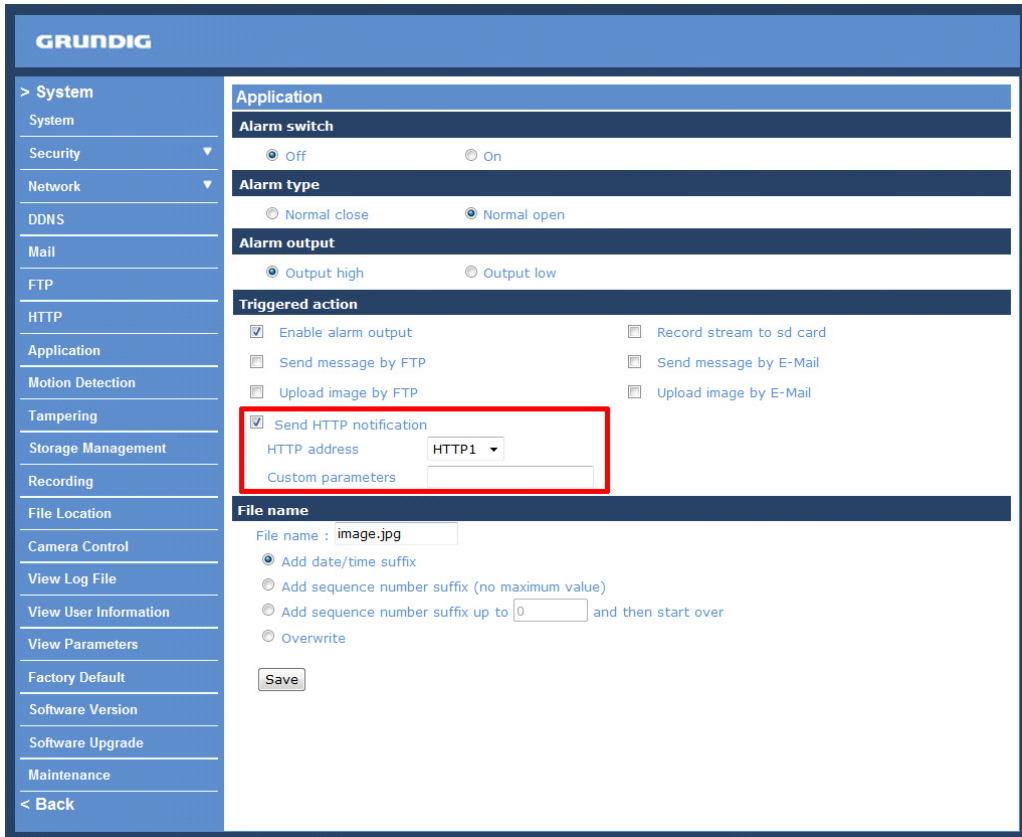
Select <Upload for __ sec> to set the recording duration after the alarm is triggered. The setting range is from 1 to 99999 seconds.

Select <Upload while trigger is active> to record the triggered video until the trigger is turned off.

- Send HTTP notification:

Check this item, select the destination HTTP address, and specify the parameters for event notifications when an <Alarm> is triggered. As soon as an alarm is triggered, the notification will be sent to the specified HTTP server.

For instance, if the custom parameter is set as "action=1&group=2", and the HTTP server's name is "http://192.168.0.1/admin.php", the notification will be sent to the HTTP server as "http://192.168.0.1/admin.php?action=1&group=2" when an alarm is triggered.



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: imageXXXXXX.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:

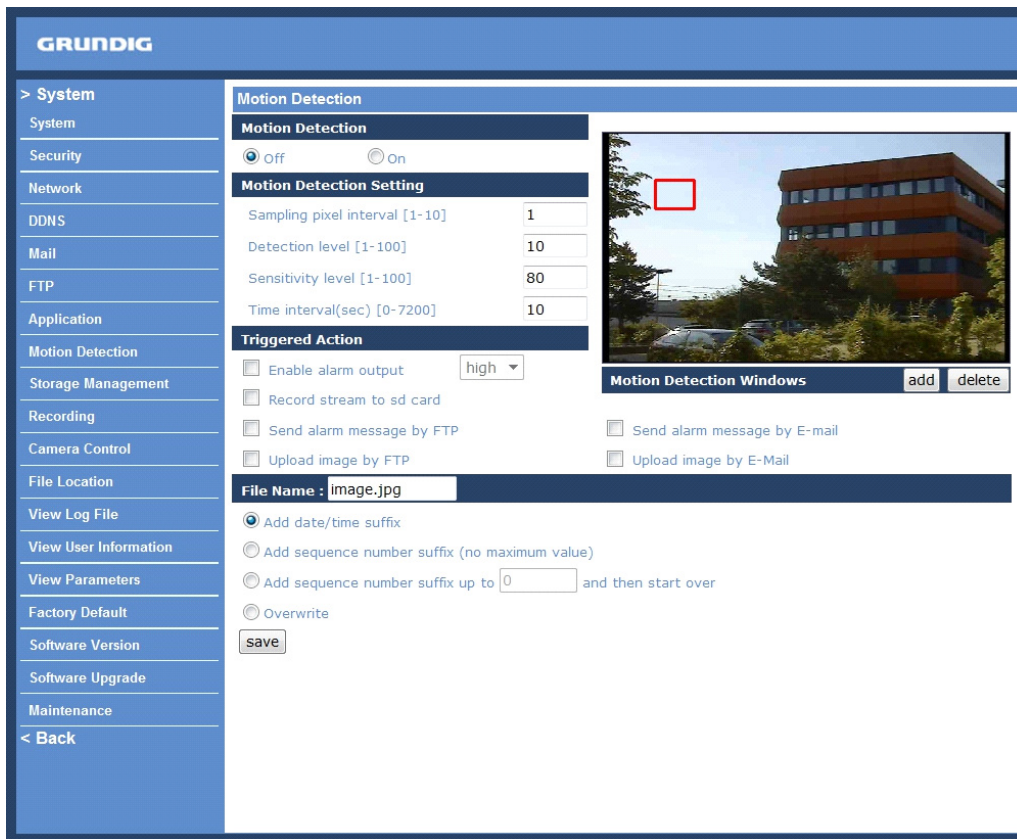
The original image in the FTP site will be overwritten with a static filename by the new uploaded file.

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

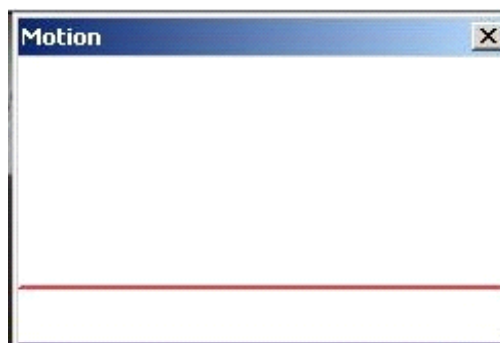
The Motion Detection function allows detecting suspicious motion and triggers alarms when motion volume in the detected area reaches/exceeds the determined sensitivity threshold value.



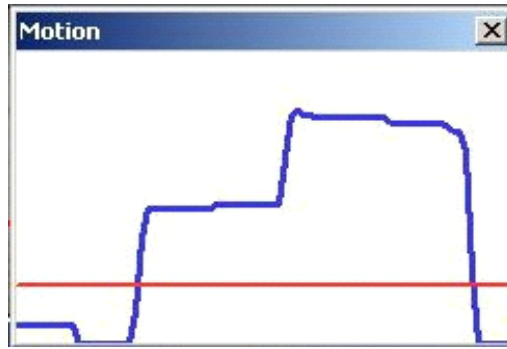
In the Motion Detection setting page a frame (Motion Detection Window) is displayed in the Live View Pane. The Motion Detection Window is for defining the motion detection area. To change the size of the Motion Detection Window, move the mouse cursor to the edge of the frame and draw it outward/inward.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

Up to 10 Motion Detection Windows can be set. click on the "Add" button under the Live View Pane to add a Motion Detection Window. To delete 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, a pop-up window (Motion) with motion indication will be shown.



When a 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 the Motion Detection on/off 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 the detection 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 the detection 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 this item and select the predefined type of alarm output to enable alarm relay output when motion is detected.

- Record stream to SD Card:

When you select this item, the Motion Detection recording will be stored on your Micro SD/SDHC card when motion is detected.

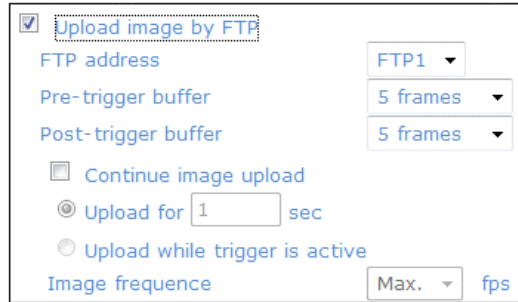
NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.12. Recording for further details.

- 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.

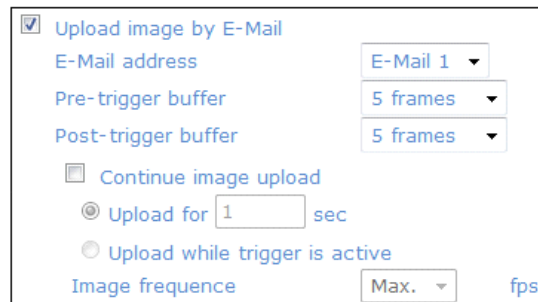
- Upload Image by FTP:

After selecting this item, 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 E-Mail:

After selecting this item, 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.



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

The pre-trigger buffer recording function allows users to check what happened to trigger the alarm. The pre-trigger buffer time range is from 1 to 3 seconds.

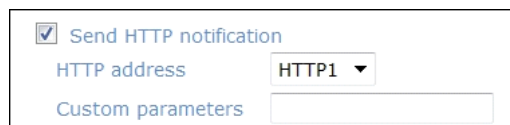
Select <Upload for __ sec> to set the recording duration after the alarm is triggered. The setting range is from 1 to 99999 seconds.

Select <Upload while trigger is active> to record the triggered video until the trigger is turned off.

- 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.

For instance, if the custom parameter is set as "action=1&group=2", and the HTTP server's name is "http://192.168.0.1/admin.php", the notification will be sent to the HTTP server as "http://192.168.0.1/admin.php?action=1&group=2" when an alarm is triggered.



File Name :

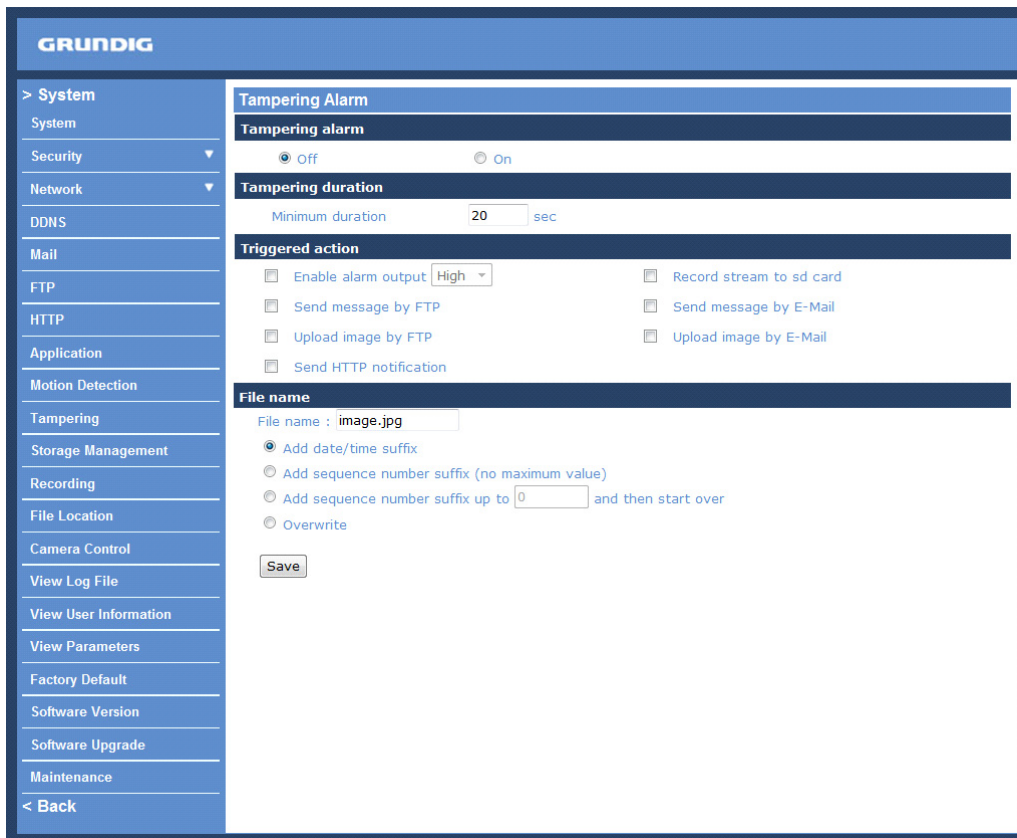
The uploaded image's filename format can be set in this section. Please select the one that meets your requirements (please see the section "File Name" in 9.8. Application).

Save :

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

9.10. Tampering

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



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

Tampering Alarm :

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

Tampering Duration :

The Minimum Tampering Duration is the time the video analysis will need to determine whether any camera tampering has occurred. Defining the Minimum Duration can also be interpreted as defining the Tampering threshold; longer duration represents a higher threshold. The 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:

When you check this item, the alarm-triggered recording will be stored on your Micro SD/SDHC card when an alarm was triggered.

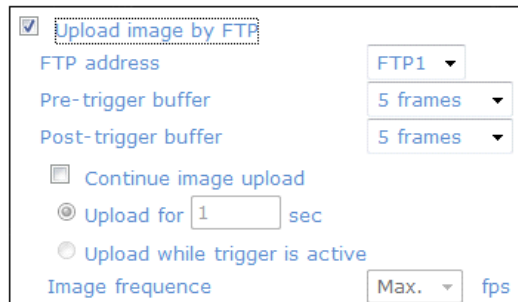
NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.12. Recording for further details.

- 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.

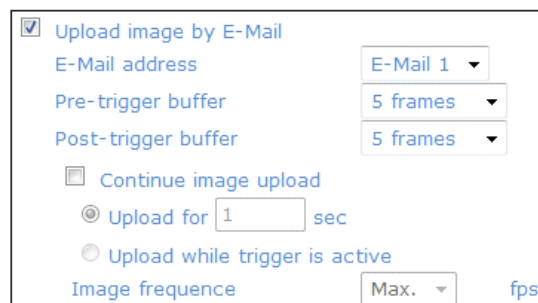
- Upload Image by FTP:

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



- Upload Image by E-Mail:

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



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

The pre-trigger buffer recording function allows users to check what happened to trigger the alarm. The pre-trigger buffer time range is from 1 to 3 seconds.

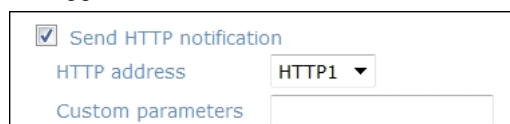
Select <Upload for __ sec> to set the recording duration after the alarm is triggered. The setting range is from 1 to 99999 seconds.

Select <Upload while trigger is active> to record the triggered video until the trigger is turned off.

- 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.

For instance, if the custom parameter is set as "action=1&group=2", and the HTTP server's name is "http://192.168.0.1/admin.php", the notification will be sent to the HTTP server as "http://192.168.0.1/admin.php?action=1&group=2" when an alarm is triggered.



File Name :

The uploaded image's filename format can be set in this section. Please select the one that meets your requirements (please see the section "File Name" in 9.8. Application).

Save :

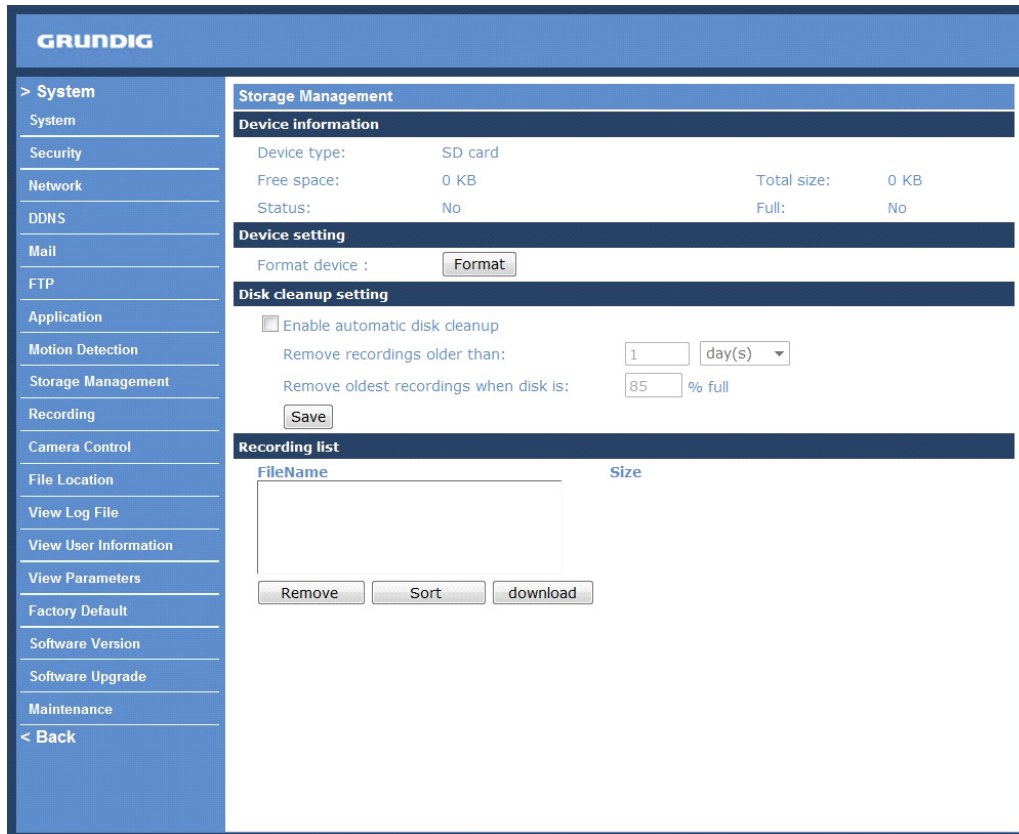
Click the Save button to save all the Tampering Alarm settings mentioned above.

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 product and was later transferred to another product with a different software platform.



Device Information :

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

Device Setting :

Click on the “Format” button to format the memory card.

Disk Cleanup Setting :

Users can enable an automatic recordings cleanup by checking this item and 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 mode 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 Video Server 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 event recording, the product will return to regular recording mode.

Recording list	
FileName	Size
M_20110325_175641.avi	1114 K
M_20110325_175800.avi	14855 K
M_20110325_175824.avi	9901 K
M_20110325_180018.avi	16938 K
M_20110325_180047.avi	16904 K

Remove Sort Download

- Remove:

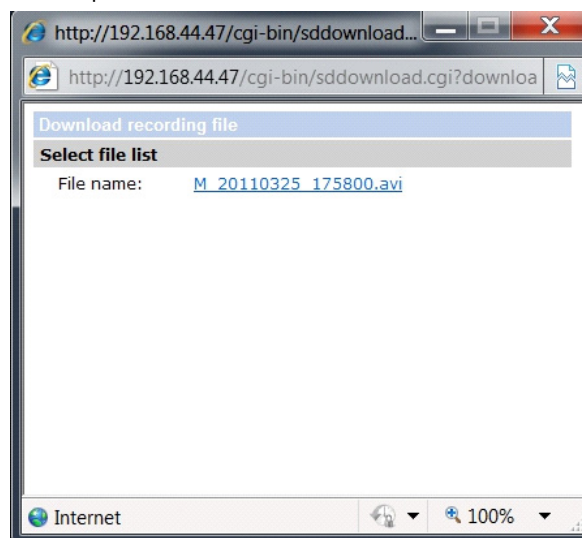
To remove a file, select the file first, and then click on the "Remove" button.

- Sort:

When you click on the "Sort" button, the files in the Recording list will be listed in name and date order.

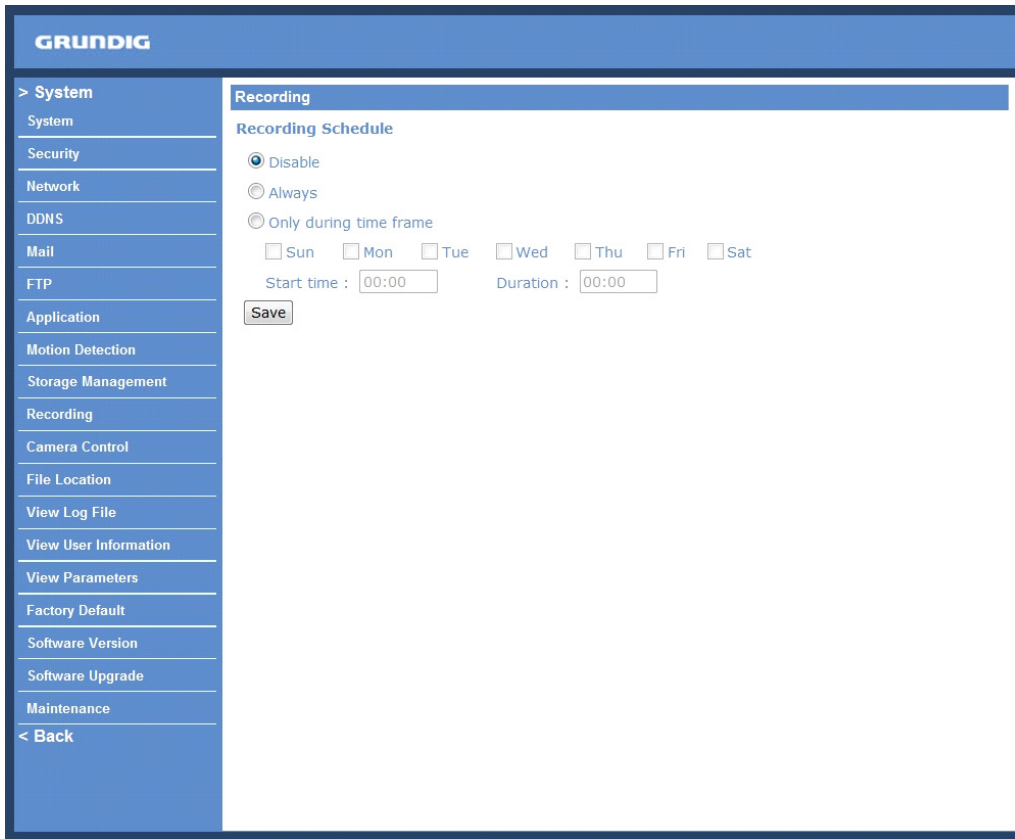
- Download:

To open/download a video clip, select the file first, and then click on the "Download" button underneath 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.



9.12. Recording

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



The screenshot shows the GRUNDIG web interface for configuring recording settings. On the left is a navigation menu with the following items: > System, System, Security, Network, DDNS, Mail, FTP, Application, Motion Detection, Storage Management, Recording, Camera Control, File Location, View Log File, View User Information, View Parameters, Factory Default, Software Version, Software Upgrade, Maintenance, and < Back. The main content area is titled 'Recording' and contains a 'Recording Schedule' section. It features three radio button options: 'Disable' (selected), 'Always', and 'Only during time frame'. Below these are checkboxes for each day of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. There are also input fields for 'Start time' and 'Duration', both currently set to '00:00'. A 'Save' button is located at the bottom left of the configuration area.

Activating Micro SD/SDHC Card Recording :

Two types of schedule mode are offered: "Always" and "Only during time frame". You can set up the time frame according to your requirements or you can choose "Always" to allow the Micro SD/SDHC Card Recording to be activated all the time.

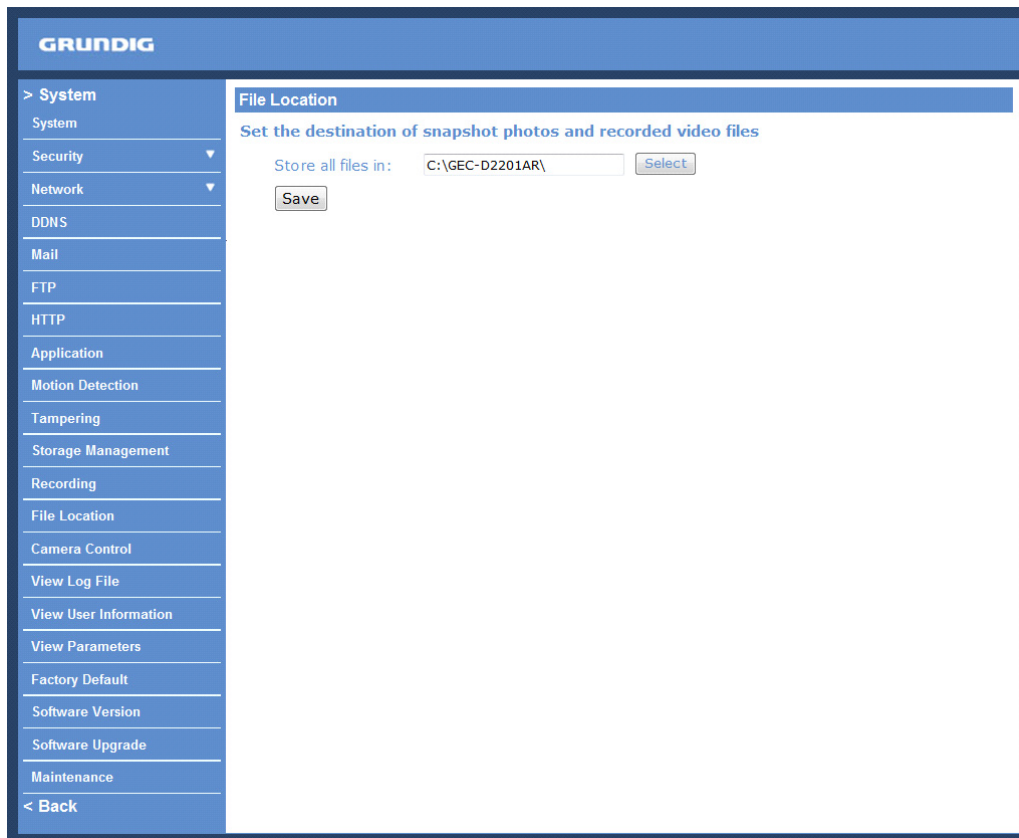
Please click on the "Save" button to confirm the schedule mode.

Terminating Micro SD/SDHC Card Recording :

Select "Disable" to terminate the recording function.

9.13. File Location

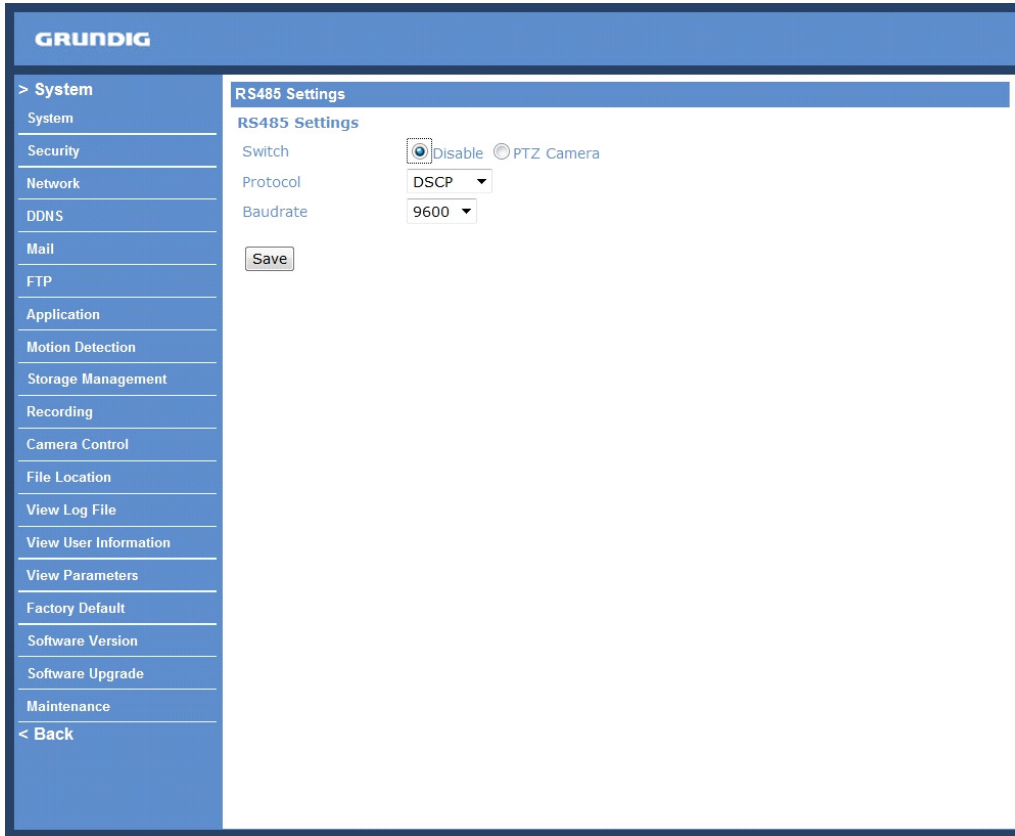
Users can specify a storage location for the snapshots and the live video recording. The default setting is: C:\. Once the setting is confirmed, click on "Save," and all the snapshots and recordings will be saved in the designate location.



NOTE: Users with the Windows 7 operating system on their PC 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 please 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. Camera Control

Users can enable the RS-485 Interface to control the analogue camera that is connected to the Video Server.



Activating Camera Control :

Select "PTZ Camera" and choose the Protocol and Baud rate that fits the connected analogue camera setting from the drop-down menu. Please click on the "Save" button for confirming the settings.

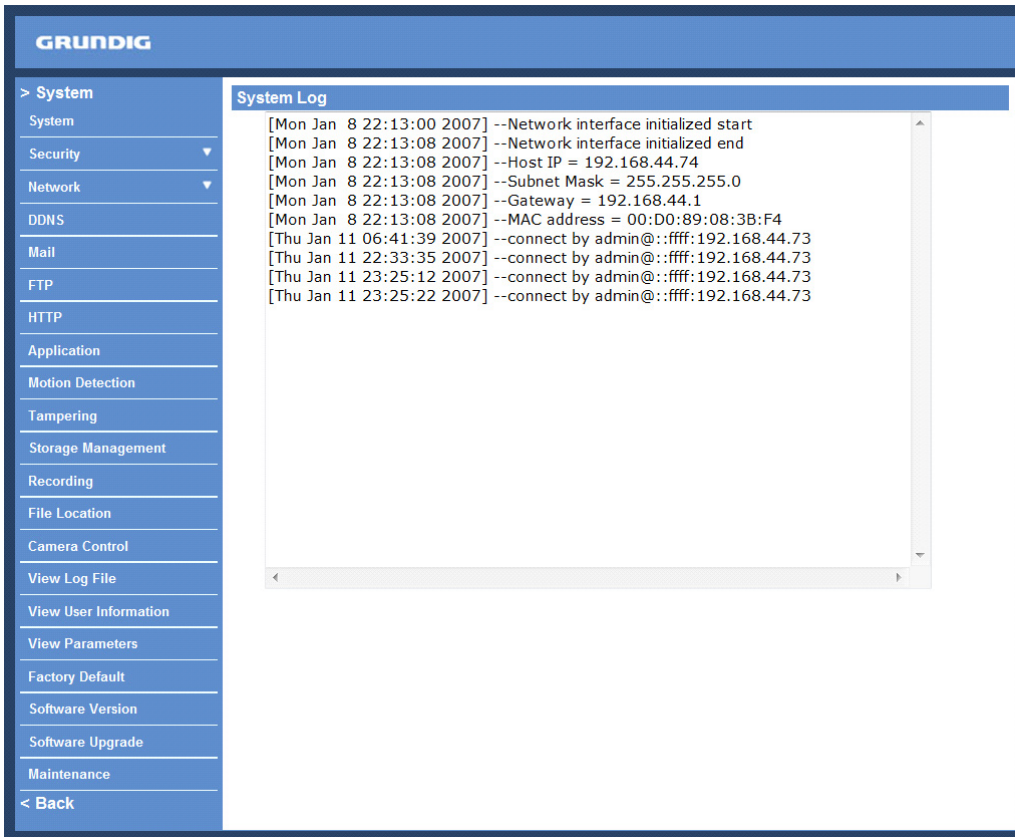
Please refer to 11. PTZ Settings for further camera control directions.

Terminating Camera Control :

Select "Disable" to terminate the camera control.

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.



The screenshot displays the Grundig web interface. On the left is a navigation menu with the following items: > System, System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Tampering, Storage Management, Recording, File Location, Camera Control, View Log File, View User Information, View Parameters, Factory Default, Software Version, Software Upgrade, Maintenance, and < Back. The 'View Log File' option is highlighted. The main content area is titled 'System Log' and contains the following log entries:

```
[Mon Jan 8 22:13:00 2007] --Network interface initialized start
[Mon Jan 8 22:13:08 2007] --Network interface initialized end
[Mon Jan 8 22:13:08 2007] --Host IP = 192.168.44.74
[Mon Jan 8 22:13:08 2007] --Subnet Mask = 255.255.255.0
[Mon Jan 8 22:13:08 2007] --Gateway = 192.168.44.1
[Mon Jan 8 22:13:08 2007] --MAC address = 00:D0:89:08:3B:F4
[Thu Jan 11 06:41:39 2007] --connect by admin@::ffff:192.168.44.73
[Thu Jan 11 22:33:35 2007] --connect by admin@::ffff:192.168.44.73
[Thu Jan 11 23:25:12 2007] --connect by admin@::ffff:192.168.44.73
[Thu Jan 11 23:25:22 2007] --connect by admin@::ffff:192.168.44.73
```

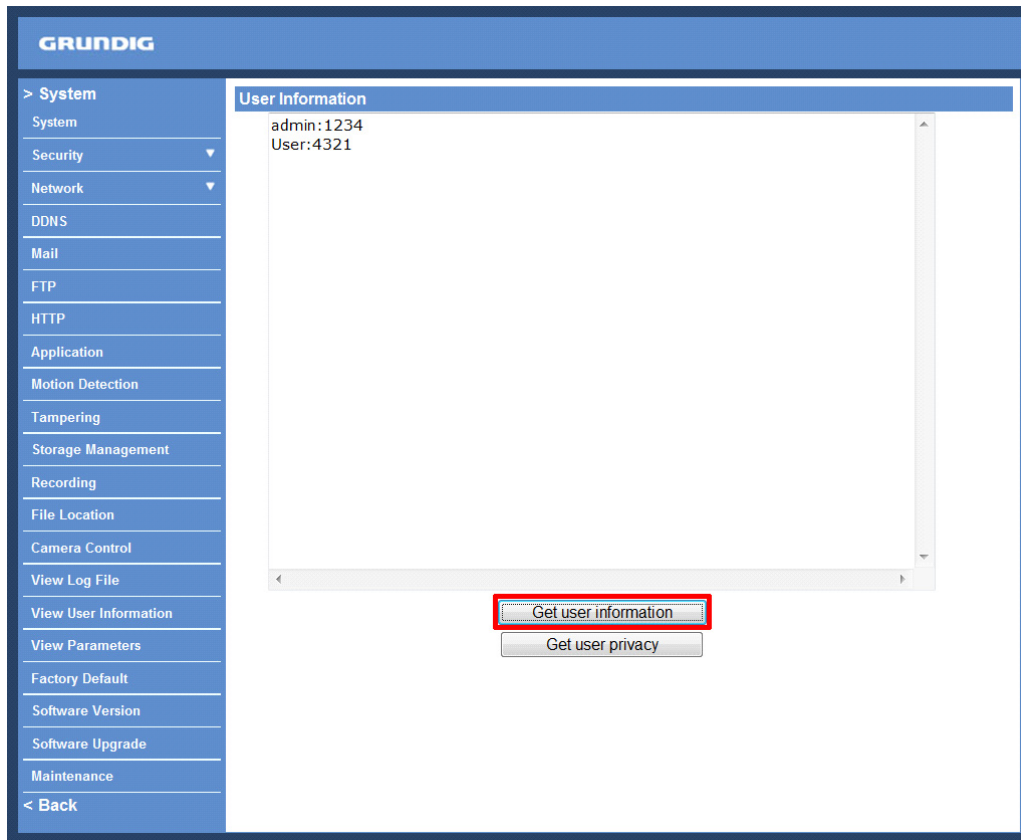
9.16. View User Information

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

View User Login Information :

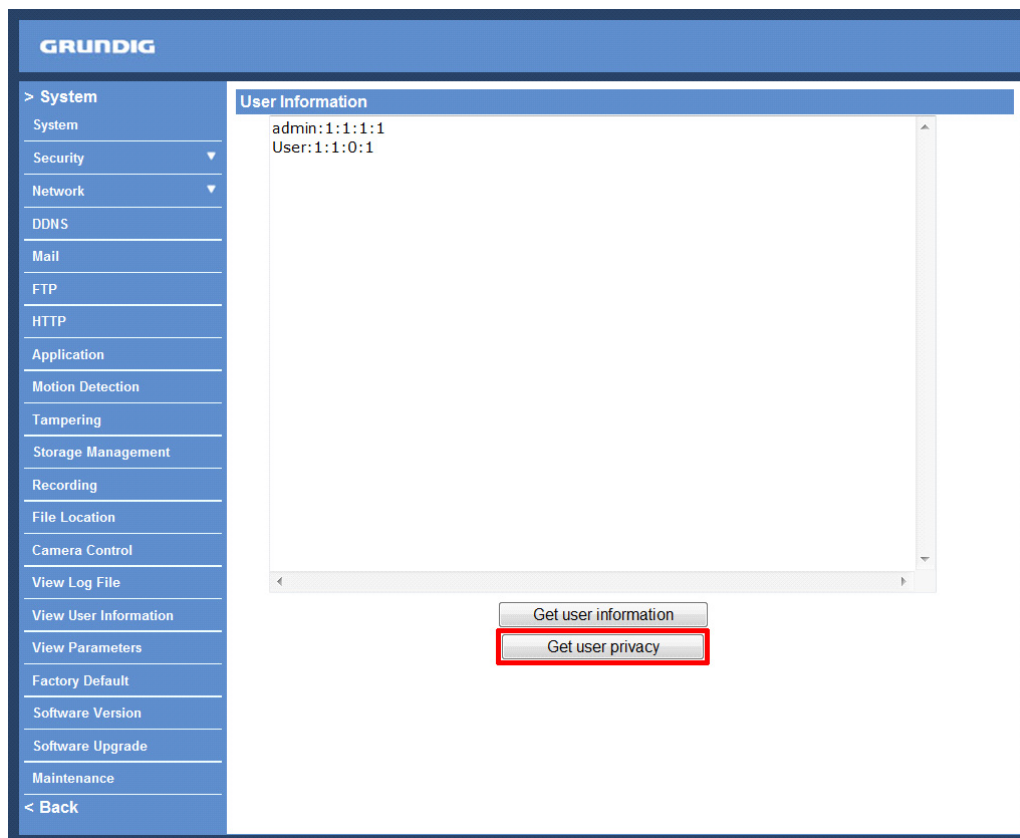
All the users in the network will be listed in the "User Information" zone, as shown below. The picture below shows: User: 4321

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



View User Privilege :

If you click on "Get user privacy" at the bottom of the page, the Administrator will be able to view each user's privileges.



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

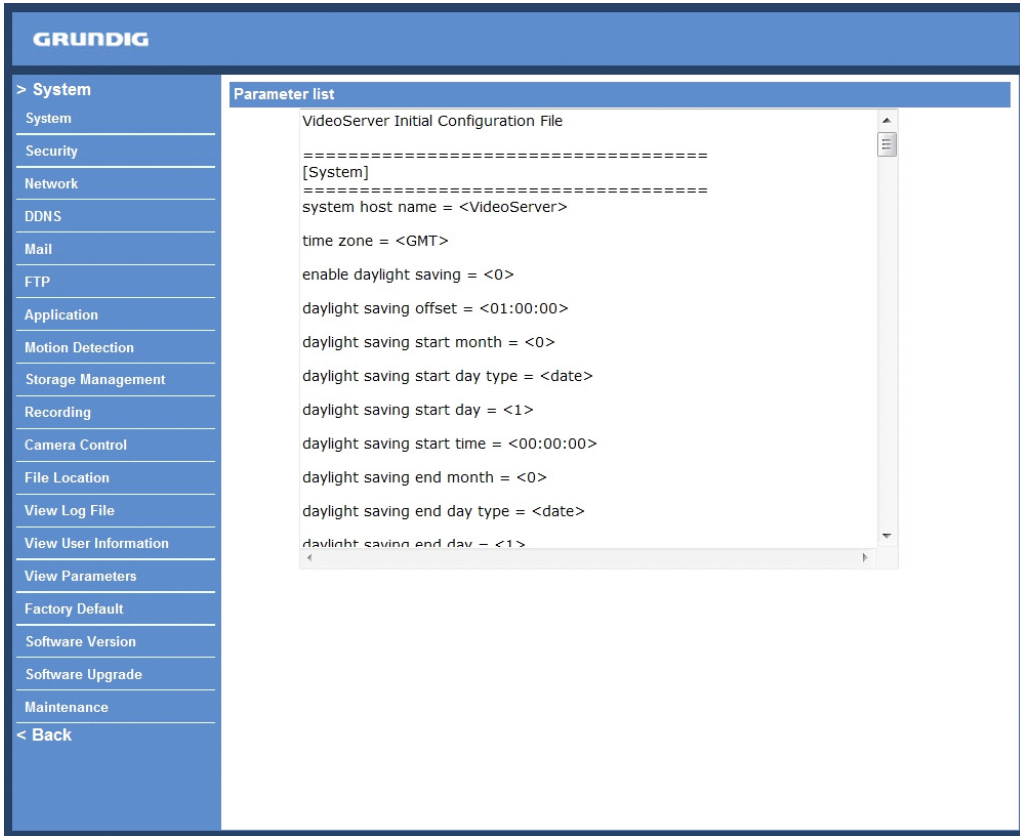
1:1:0:1 = I/O access : Camera control : Talk : Listen (see 9.2. Security)

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



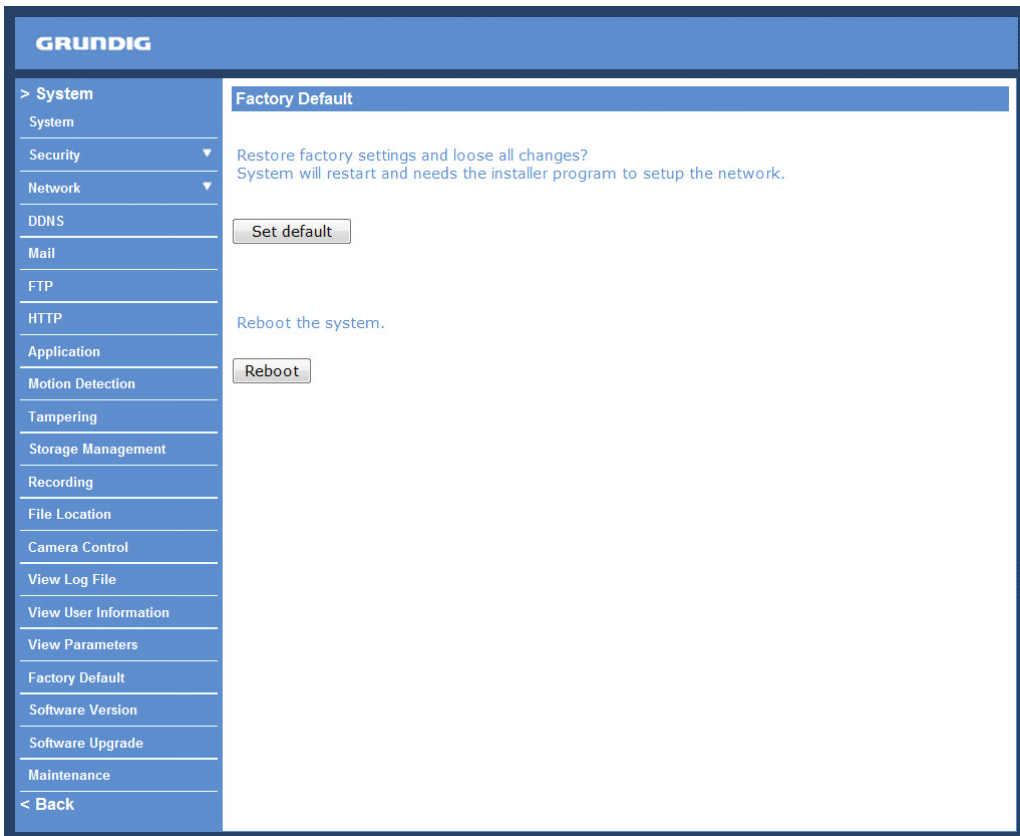
9.17. View Parameters

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



9.18. Factory Default

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



Set Default :

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

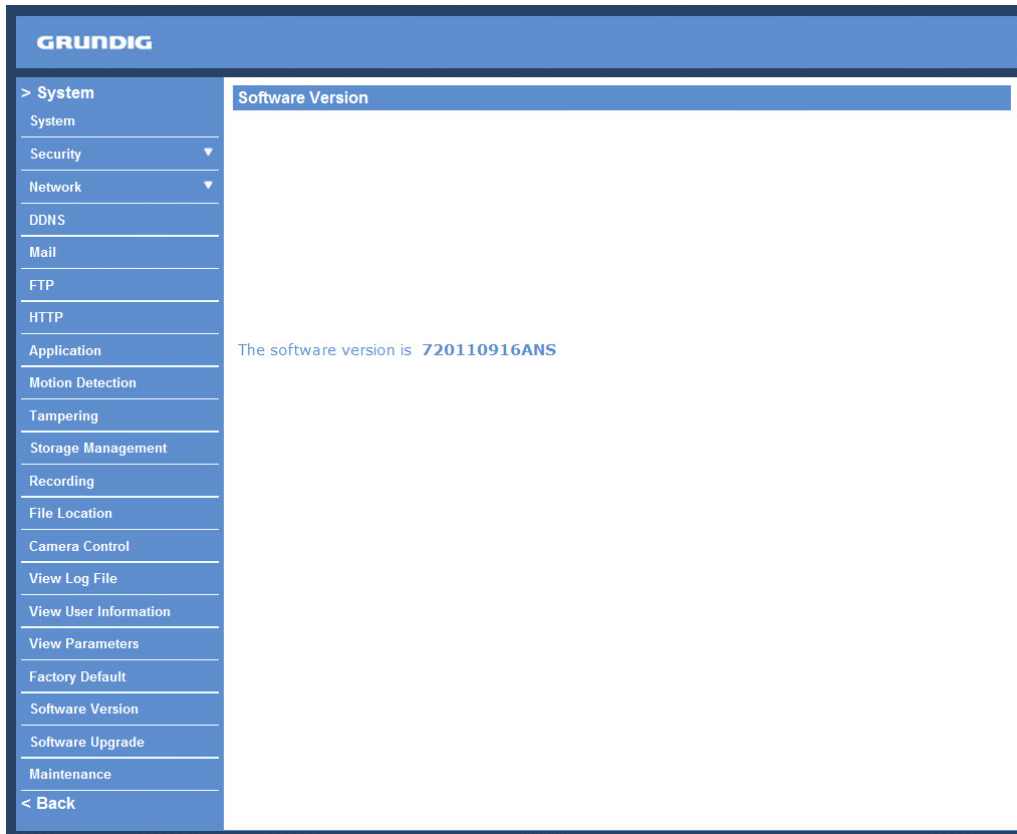
NOTE: The IP address will also be restored to default (192.168.1.1).

Reboot :

When you click on the “Reboot” button, 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.



9.20. Software Upgrade

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

The screenshot shows the GRUNDIG software upgrade interface. The page has a blue header with the GRUNDIG logo. On the left is a navigation menu with categories like System, Security, Network, etc. The main content area is titled 'Upgrade' and contains three steps: Step 1: Upload the binary file with a 'Browse...' button; Step 2: Select binary file you want to upgrade with a dropdown menu showing 'userland.jffs2'; Step 3: Click the upgrade button to start the upgrade process with an 'Upgrade' button.

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, in this case: 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: Click on “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 be displayed 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.

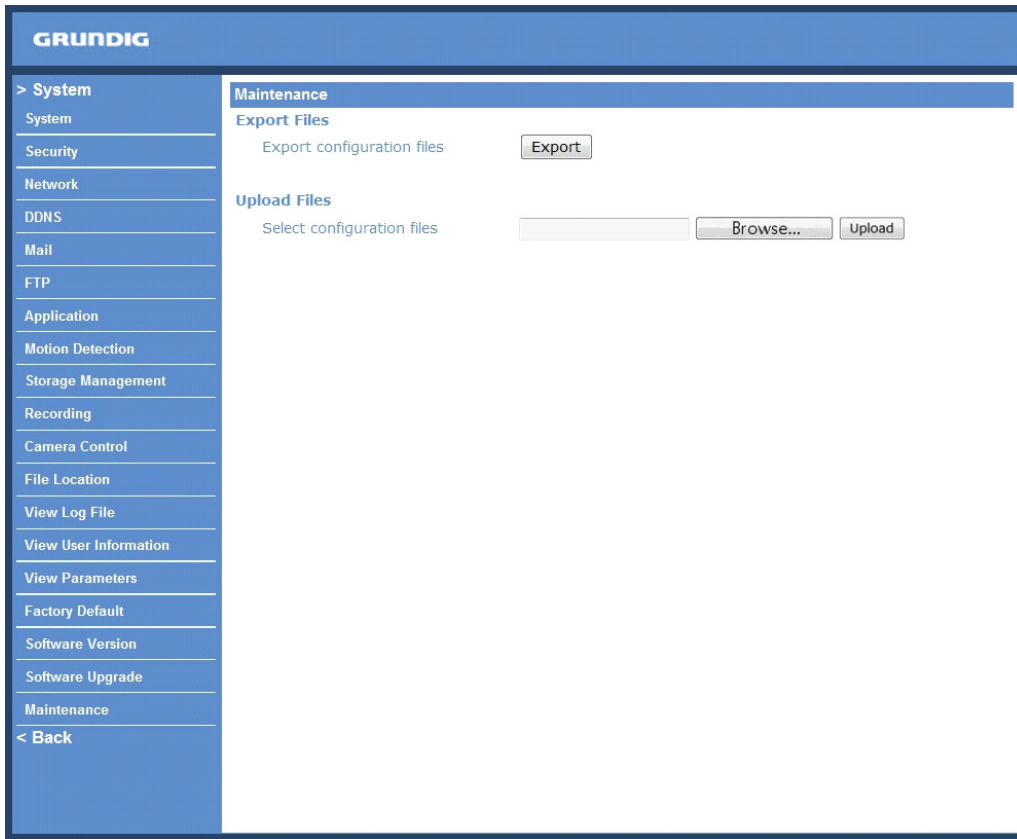
Step 4: Close the video browser.

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

Step 6: Open a new web browser, re-login to the Video Server, 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 Video Server.



Export:

Users can save the system settings by exporting the configuration file (.bin) to a specified location for future use. When you click on the "Export" button, the File Download window will pop up as shown below. Click "Save" and specify a desired location for saving the configuration file.

Upload:

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

10. Streaming Settings

After clicking on the tab "Streaming" on top of the page, the configurable video and audio items will be displayed in the left column. Here the Administrator can configure a specific video resolution, the video compression mode, video protocol, audio transmission mode, etc. These settings will be specified in detail in the following sections.

10.1. Video Format

The video format setting page is shown below:

The screenshot shows the Grundig Video Format configuration page. The left sidebar contains a navigation menu with the following items: > Streaming, Video Format (selected), Video Compression, Video OCX Protocol, Video Frame Rate, Audio, and < Back. The main content area is titled 'Video Format' and includes the following sections:

- Video resolution :** A dropdown menu is set to 'MJPEG + H.264'. Below it are two radio button options: 'MJPEG D1 (30fps) + H.264 D1 (30fps)' and 'MJPEG CIF (30fps) + H.264 D1 (30fps)'. A 'Save' button is located below these options.
- Note :** A note stating: 'Image attachment by FTP or E-mail will be available only while MJPEG streaming is selected.'
- Text overlay settings :** Three checkboxes are present: 'Include date', 'Include time', and 'Include text string'. The 'Include text string' checkbox is accompanied by an empty text input field. A 'Save' button is located below these options.
- Video deinterlace :** Three radio button options are listed: '3D deinterlacing', 'Intra field deinterlacing', and 'Inter field deinterlacing (off)'. A 'Save' button is located below these options.
- GOV settings :** Two input fields are shown: 'H.264-1 GOV length' and 'H.264-2 GOV length', both containing the value '25'. A 'Save' button is located below these fields.

Video Resolution :

The Video Server provides two sets of video dual streaming formats:

- H.264 D1 (30fps) + MJPEG D1 (30fps)
- H.264 D1 (30fps) + MJPEG CIF (30fps)
- H.264 D1 (30fps) + H.264 D1 (30fps)
- H.264 D1 (30fps) + H.264 CIF (30fps)

Click "Save" to confirm the Video Format setting.

Video Deinterlace :

The Video Server supports the deinterlacing function. Users can either choose to activate the deinterlacing function or disable the function by selecting a mode from the list as shown below:

- 3D Deinterlacing
- Intra Field Deinterlacing
- Inter Field Deinterlacing (off)

Click "Save" to confirm the Video Format 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. The setting range for the GOV length is from 2 to 64. The default setting of GOV is 30.

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.

The screenshot shows the Grundig Video Compression settings page. The left sidebar has a menu with the following items: > Streaming, Video Format, Video Compression, Video OCX Protocol, Video Frame Rate, Audio, and < Back. The main content area is titled 'Video Compression' and contains the following sections:

- 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]

MJPEG compression settings include:

- high compression, low bit rate, low quality
- middle compression, default
- low compression, high bit rate, high quality

H.264 compression settings include:

- highest compression, lowest quality
- middle compression
- low compression, highest quality, default

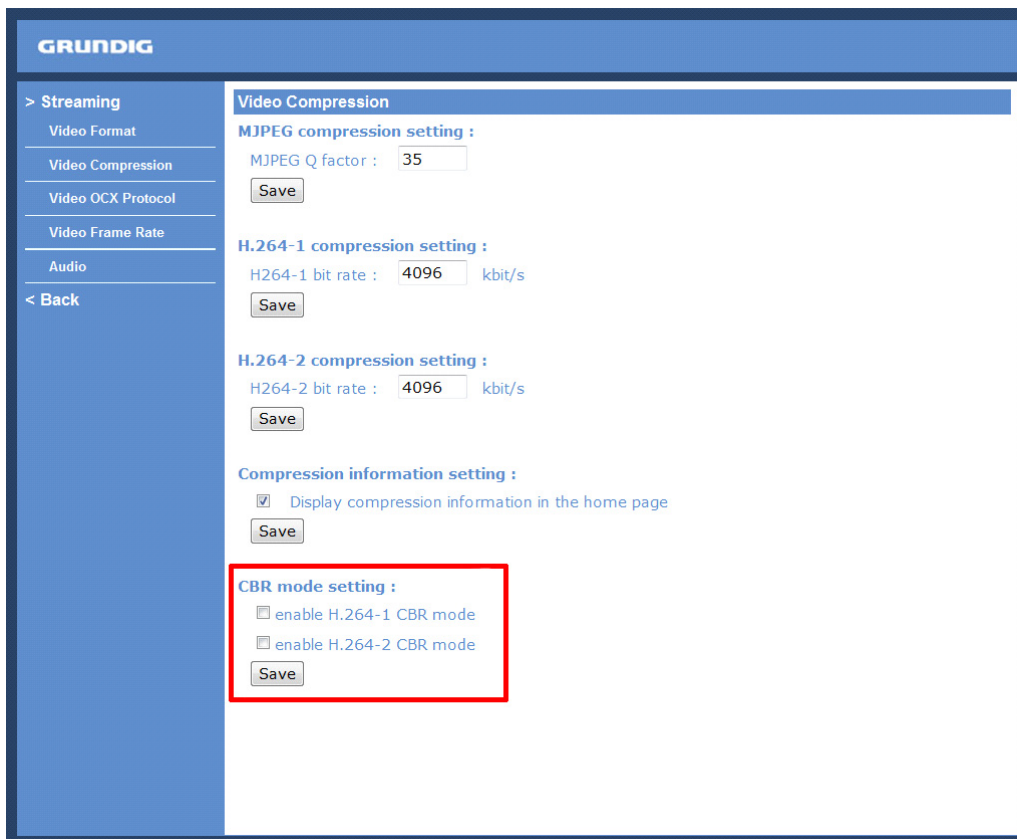
Users can also choose whether the compression information is to be displayed in the Home page.

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 on "Save" to confirm the setting.



GRUNDIG

> Streaming

- Video Format
- Video Compression
- Video OCX Protocol
- Video Frame Rate
- Audio

< Back

Video Compression

MJPEG compression setting :

MJPEG Q factor :

H.264-1 compression setting :

H264-1 bit rate : kbit/s

H.264-2 compression setting :

H264-2 bit rate : 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

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:

The screenshot shows the Grundig Video OCX Protocol configuration page. On the left is a blue sidebar with a menu: > Streaming, Video Format, Video Compression, Video OCX Protocol (highlighted), Video Frame Skip, Video Mask, Audio, and < Back. The main content area has a blue header 'GRUNDIG' and a sub-header 'Video OCX Protocol'. Below this is the 'Video OCX protocol setting' section with five radio button options: RTP over UDP (selected), RTP over RTSP(TCP), RTSP over HTTP, MJPEG over HTTP, and Multicast mode. Under the Multicast mode option, there are six input fields: 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), and Multicast TTL (1). A 'Save' button is located below the input fields. A 'Note' section at the bottom states: '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.

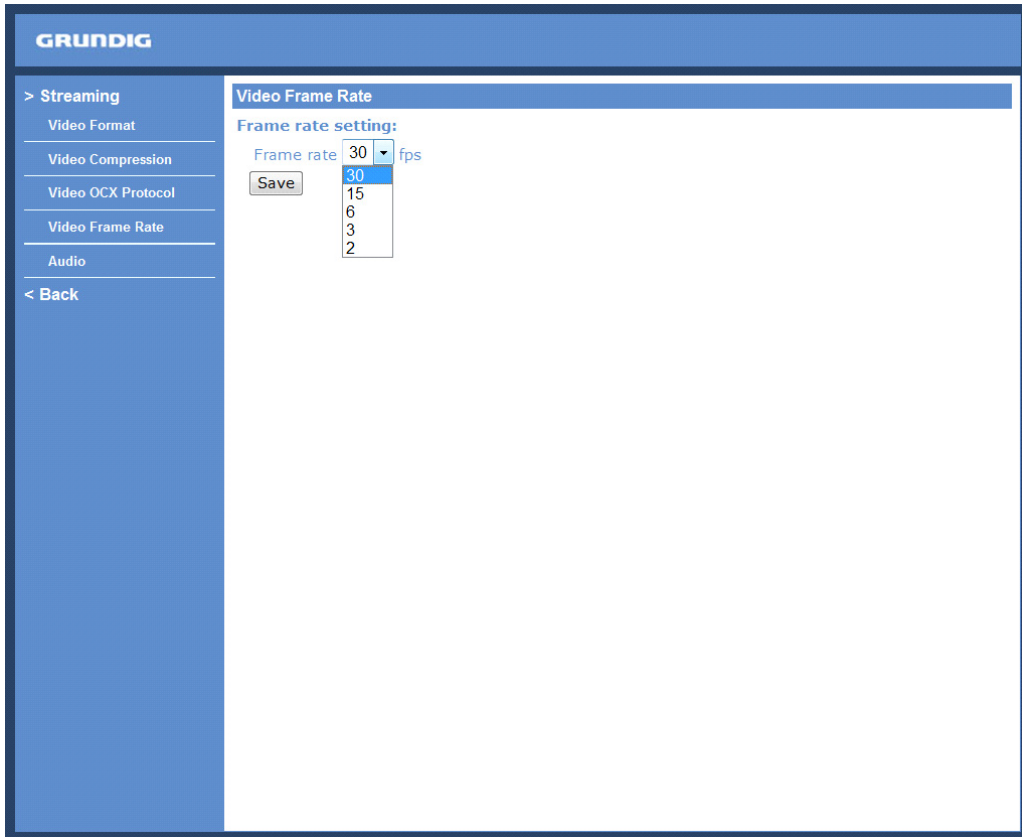
Click on "Save" to confirm the setting.

10.4. Video Frame Rate

The Frame rate options include:

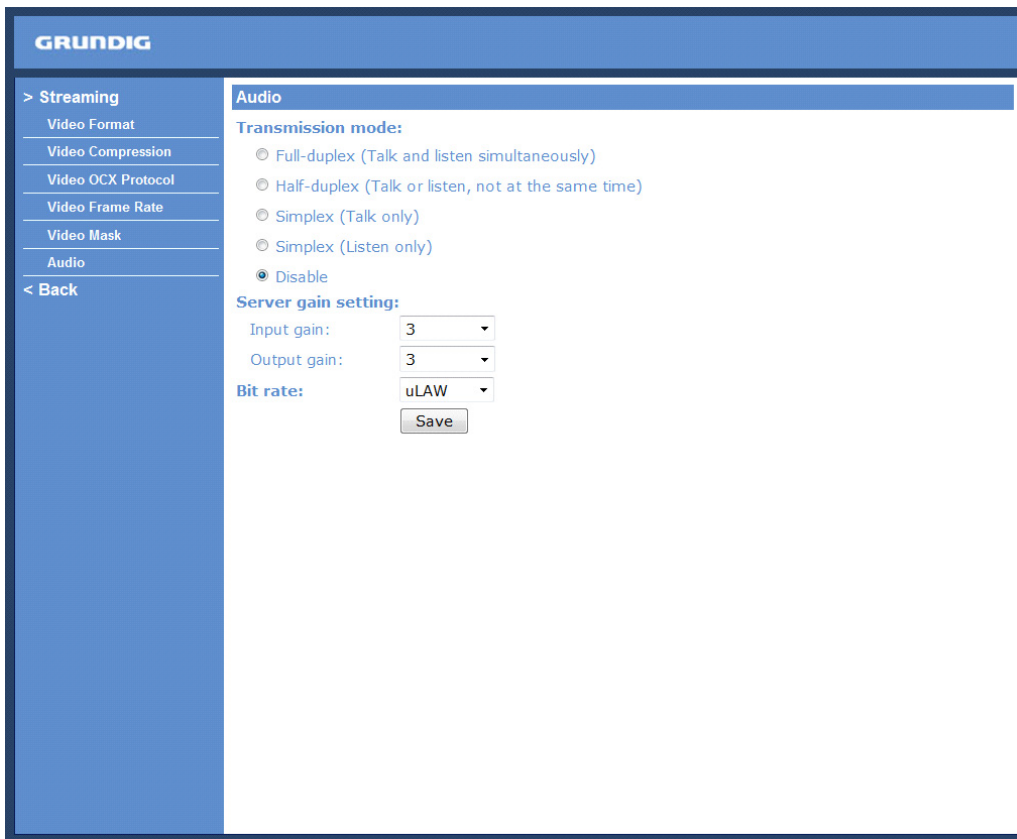
- 30 fps
- 15 fps
- 6 fps
- 3 fps
- 2 fps

Click "Save" to confirm the setting.



10.5. Audio

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



Transmission Mode :

- Full-duplex (Talk and Listen simultaneously):

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

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

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

- Simplex (Talk only):

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

- Simplex (Listen only):

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

- Disable:

Select this item to turn the audio transmission function off.

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 :

The selectable audio transmission bit rates 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 on "Save" to confirm the setting.

11. PTZ Settings

Under the "PTZ/Cam" category, users are allowed to control the connected camera, view the Camera OSD menu via the OSD manual control panel, and change the camera settings through the Camera OSD menu.

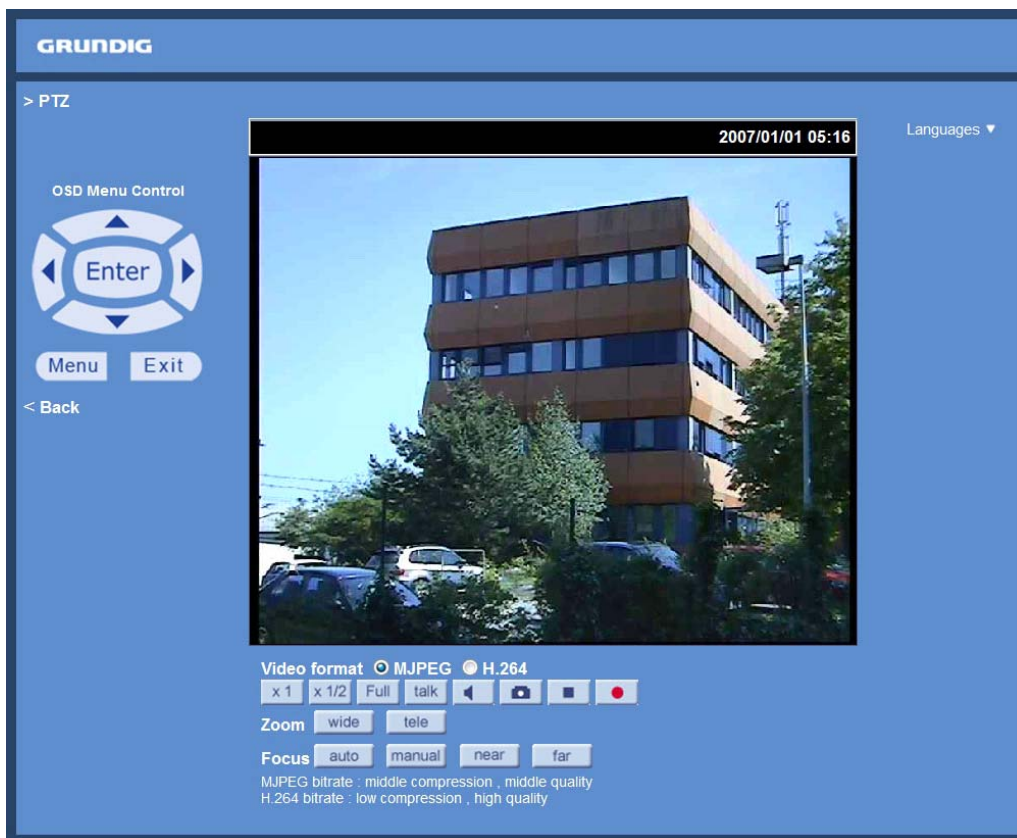
NOTE: Please make sure Camera Control Settings have been completed. You can access the PTZ Control only after you selected "PTZ Camera" under System > Camera Control. Please refer to 9.11. Camera Control.

To enter the OSD menu of the connected camera, click < Menu>. The Camera OSD menu will be shown in the live video pane.

MAIN PAGE 1	
LANGUAGE	ENGLISH
DEFAULT CAMERA	ON
BACKLIGHT	OFF
FOCUS	AUTO
AE MODE	ENTER
WBC MODE	AUTO
SETUP MENU 1	ENTER
SETUP MENU 2	ENTER

OSD Menu Control :

The detailed functions and parameter settings of your Swiftdome Camera can be set through the OSD (On Screen Display) menu with the OSD Menu Control.



To select the setup item, click on the direction buttons on the OSD Menu Control to move the OSD cursor in the OSD menu.

To setup an item, click on the direction buttons on the OSD Menu Control to move the OSD cursor in the OSD menu. For items with →, click the right/left direction icon on the OSD Menu Control to select them. For items with ↓, click the <Enter> icon on the OSD Menu Control to enter the sub menu. For items with →↓, users can click on the right/left direction icons to select the functions, and then click on the <Enter> icon on the OSD Menu Control to enter their sub menu.

For further detailed setup procedures, please refer to the user's manual of the analogue camera.

Display Mode (Screen Size Adjustment) :

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

Digital Zoom Control :

In full screen mode, users can implement digital PTZ by rotating the mouse wheel (for zoom in/out).

Talk button (on/off) :

The Talk function allows the local site to talk to the remote site. Click on this button to switch it to on/off. Please refer to section 9.2. Security: Add user >> Talk/Listen for further details. This function is only open to the "User" who has been granted this privilege by the Administrator.

Speaker button (on/off) :

Press the Speaker button to mute/activate the audio.

Snapshot button :

Press this button, and the JPEG snapshots will automatically be saved in the appointed place. The default place of saving snapshots is: C:\. To change the storage location, please refer to section 9.13. File Location for further details.

NOTE: Users with the Windows 7 operating system on their PC 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 please 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 Video Server as usual (as an administrator or user).

Video Streaming Pause/Restart button (stop/restart) :

If you click on the stop button to disable video streaming, the live video will be displayed as black. Click on the restart button to show the live video again.

Recording button (on/off) :

When you click on this button, the recordings from the Live View will be saved to the location specified in the "File Location" (snapshot) page; 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.

Pan/Tilt Control :

Users can implement pan/tilt control by first moving the cursor to the live video pane; then left-click, hold it and drag the pointer in any direction.

Zoom Adjustment :

Click on the buttons wide/ tele to control zoom in/out.

Zoom Adjustment :

Click on the buttons wide/ tele to control zoom in/out.

Focus Adjustment :

- Auto Focus (Continuous AF):

Click on the "auto" button to enable AF mode. In this mode, the camera will keep in focus automatically and continuously regardless of zoom changes or any view changes.

- Manual Focus:

After clicking on the "Manual" button, users can adjust the focus manually via the "Near" and "Far" buttons. The status will also be displayed above the screen as shown below.

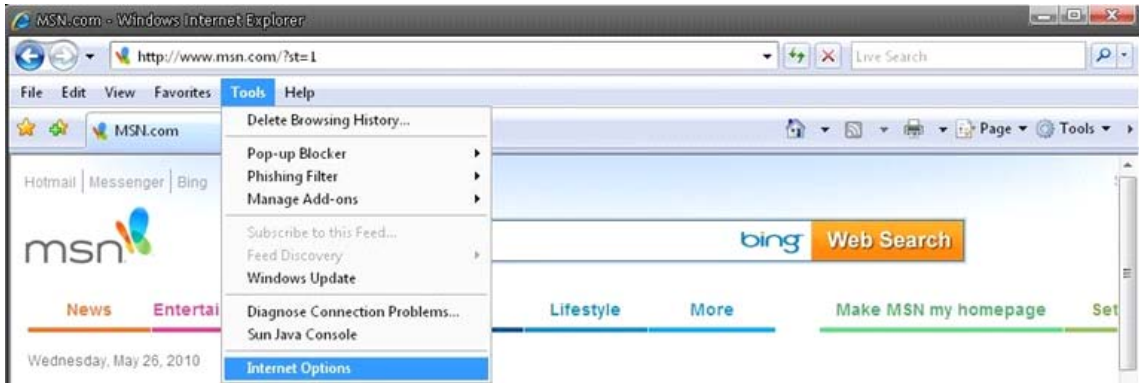
14. Internet Security Settings

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

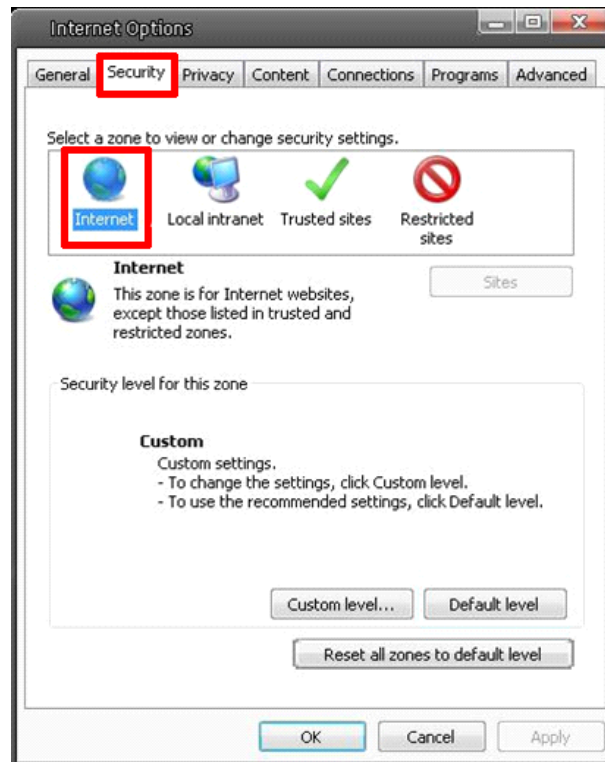
Internet Security Level : Default

Step 1: Start the Internet Explorer.

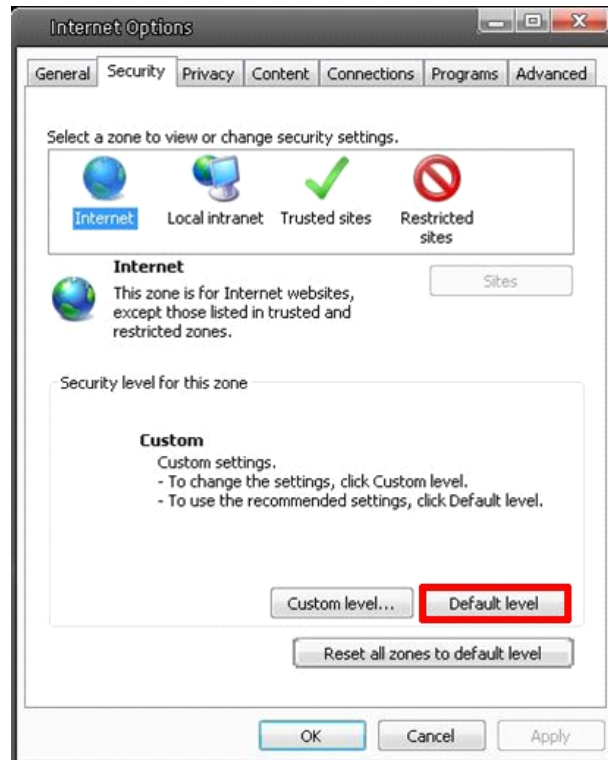
Step 2: Select <Tools> from the main menu of the browser. Then click on <Internet Options>.



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



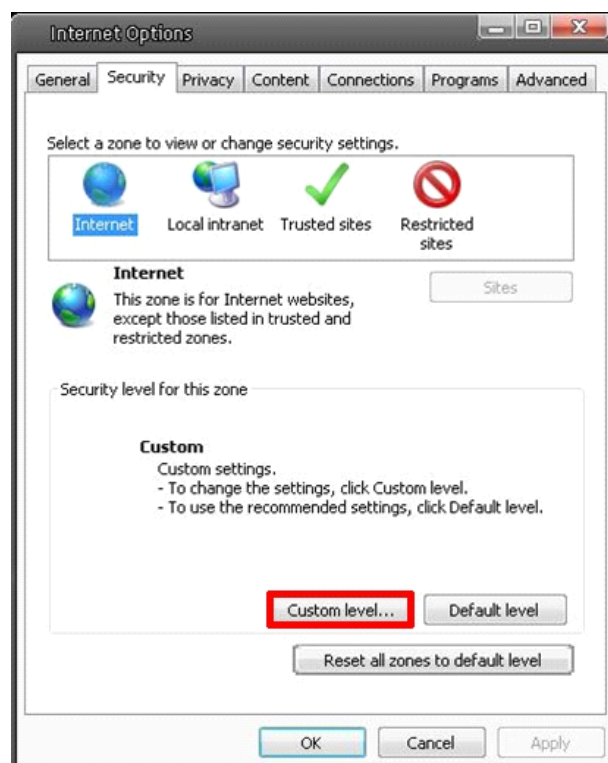
Step 4: Down the page, press “Default level...” (see the picture above) and click “OK” to confirm the setting. Close the browser window, and open a new one later when accessing the Video Server.



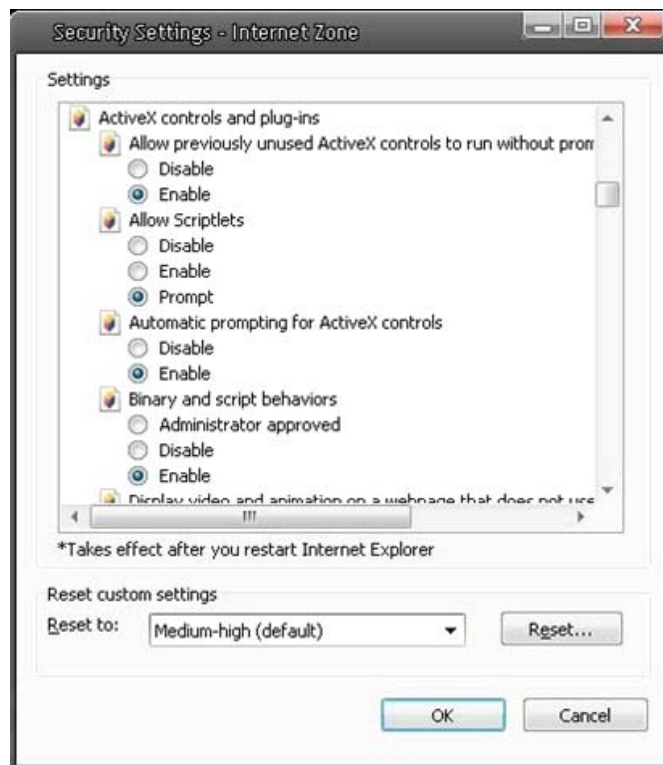
ActiveX Controls and Plug-in Settings :

Step 1~3: Please refer to the previous section above.

Step 4: Down the page, click on “Custom level...” (see the picture below) to change ActiveX controls and plug-in settings.



The Security Settings screen is displayed as shown below:



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 open a new one later for accessing the Video Server.

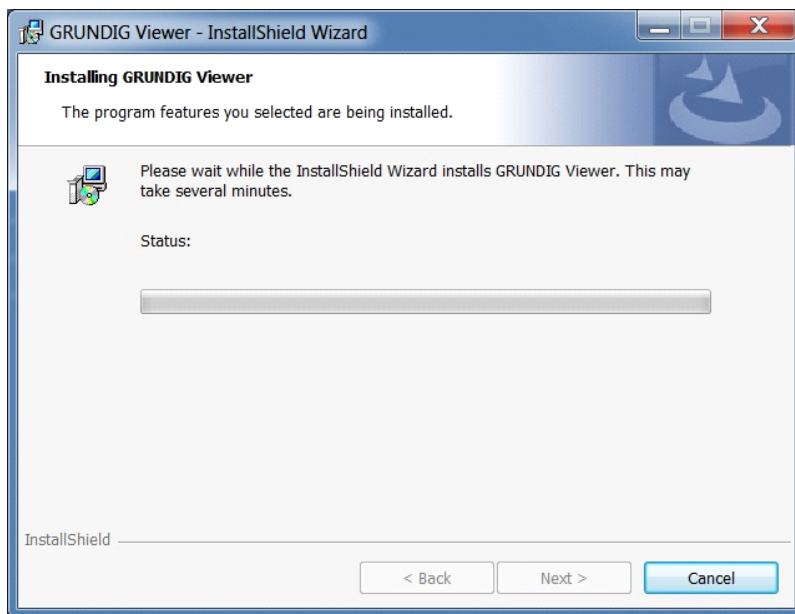
15. GRUNDIG Viewer Download Procedure

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

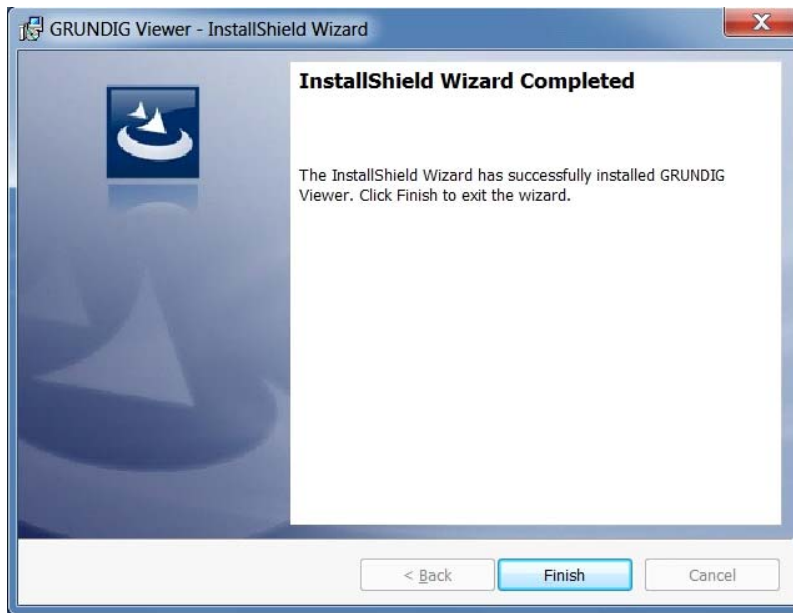
Step 1: In the GRUNDIG Viewer installation page, click “Next” to start the installation.



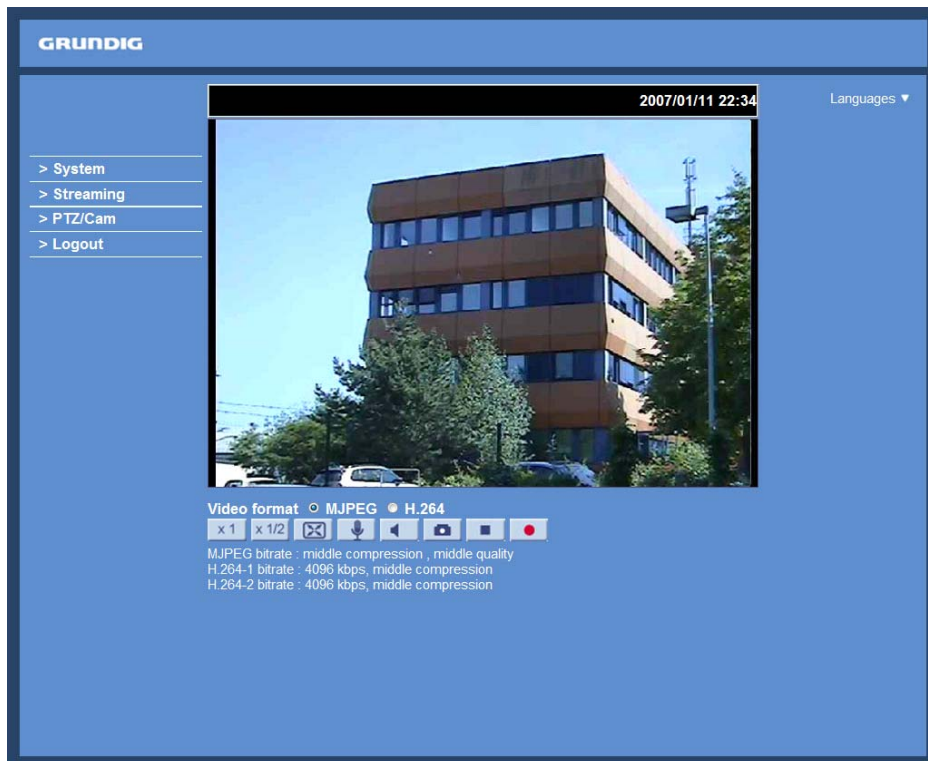
Step 2: Setup starts. Please wait for a while until the loading bar runs out.



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



Then, the Video Server's Home page will be displayed as follows:



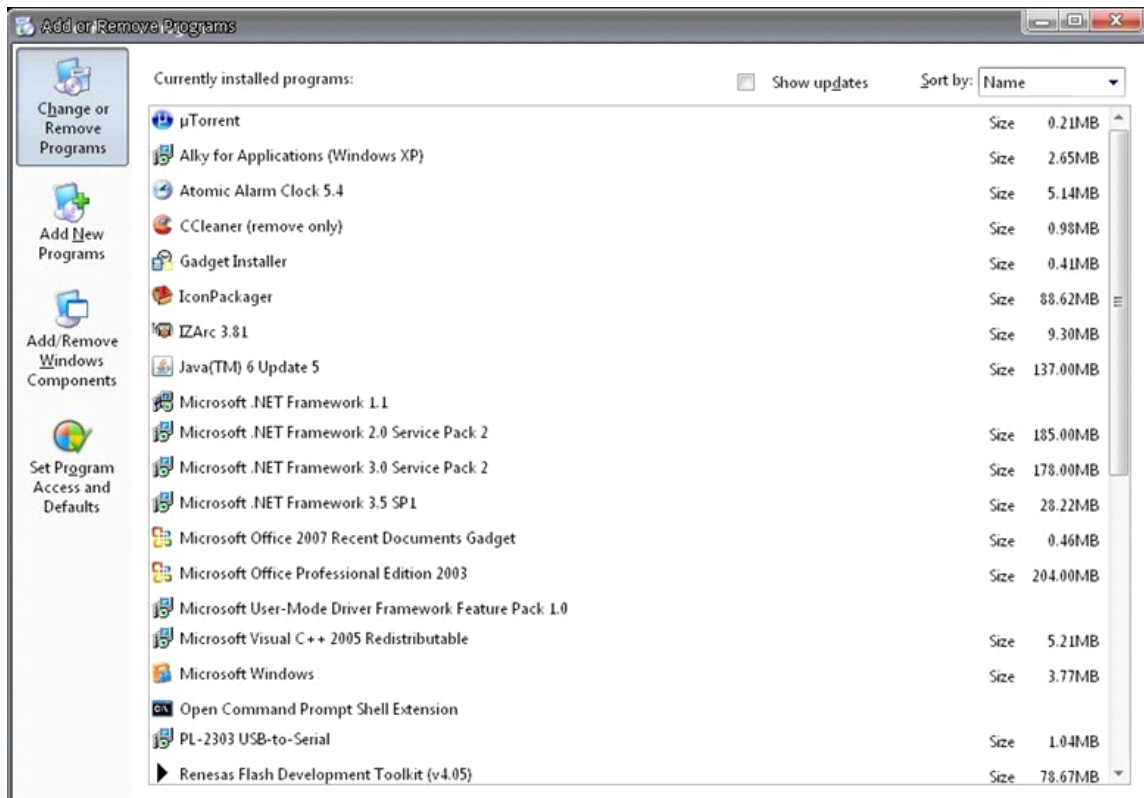
16. Install UPnP Components

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

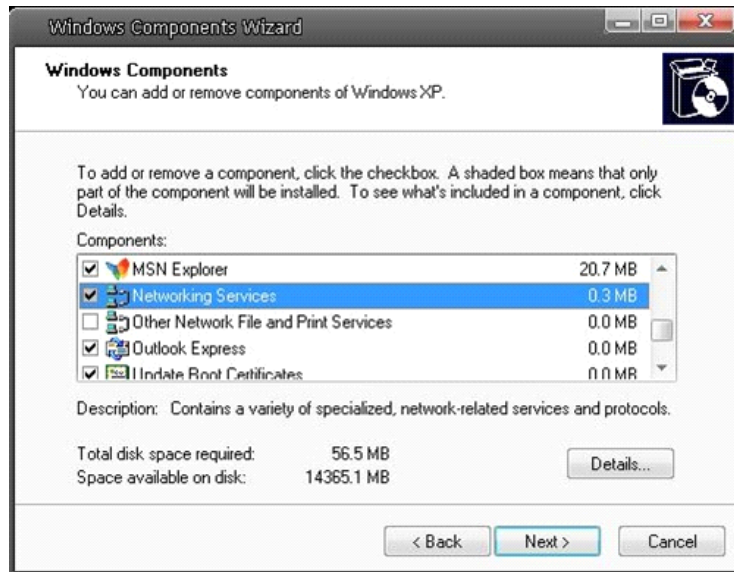
Step 1: Go to “Start”, click on “Control Panel”, and then double-click on “Add or Remove Programs”.



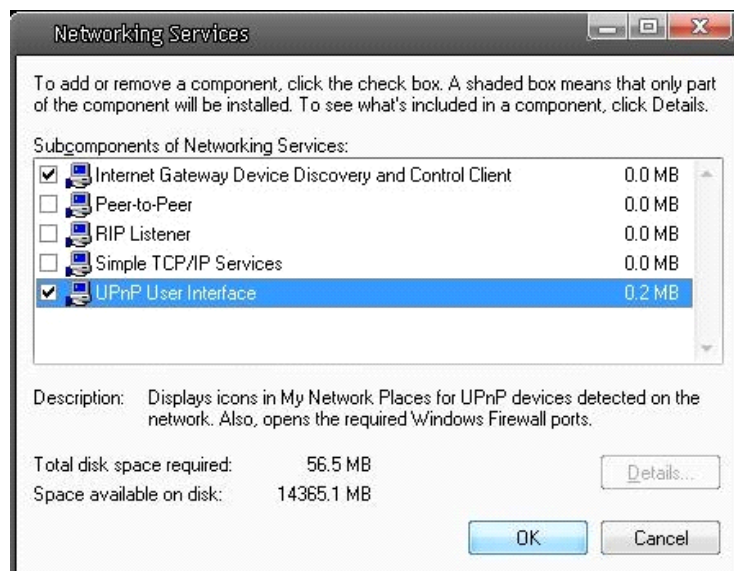
Step 2: Click on “Add/Remove Windows Components” in the Add or Remove Programs page.



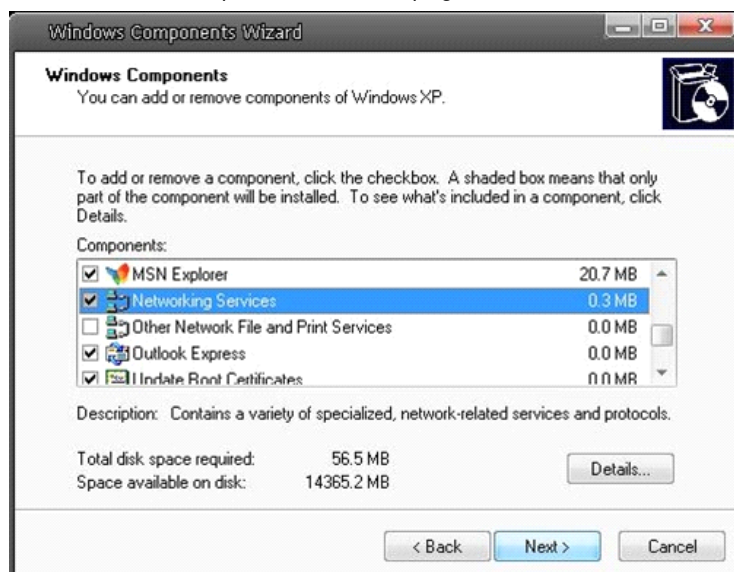
Step 3: Select "Networking Services" from the Components list in the Windows Components Wizard window, and then click on "Details".



Step 4: Select "UPnP User Interface" in the Networking Services' subcomponents list and then click on "OK".



Step 5: Click on "Next" in the Windows Components Wizard page.



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



Specifications GEC-D2201AR

Video Inputs	1 CH Composite, BNC
Video Outputs	1 CVBS, 1Vpp, BNC
Audio Inputs	1x 3.5mm jack
Audio Outputs	1x 3.5mm jack
Network	10/100 Base-T
Client OS	MS Windows XP / VISTA / 7 / Mac OS
Web Browser	MS Internet Explorer 6.0 (or higher), Firefox, Google Chrome, Safari
Video Compression	H.264, MJPEG
Video Resolution	D1 (720x576), CIF (352x288)
Alarm Inputs	1
Alarm Outputs	1
Alarm Event	Alarm Input, Motion Detection: Image transfer FTP, E-mail, recording on Micro SD-card *
Network Protocol	TCP/UDP/IP, HTTP, FTP, SMTP, ARP, ICMP, DHCP, Telnet, RTP/RTSP
Network Streaming	Dual H.264, simultaneously H.264+MJPEG
Audio Compression	G.726, G.711
Serial Interface(s)	RS-485
PTZ Control	Pan/Tilt/Zoom/Focus, Camera OSD
Software Upgrade	Firmware Upgrade by Web Browser
Login Access Level	up to 20 user, 1 Administrator
Recording	Micro SD memory slot for internal recording *
DDNS	Supporting Public DDNS servers *
Operating Temperature	-10°C ~ +50°C
Humidity	less than 90%
Supply Voltage	12 VDC / PoE
Power Consumption	4,2 W
Weight	0,2 kg
Dimensions (wxhxd)	137 x 99 x 28 mm