

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

en

Owner's Manual

IP Cameras & Domes

GCI-K1526T

2 Megapixel Full HD CMOS Bullet IP Camera ICR IR 23 LED

GCI-K1526T.60.1.10.05.2012

© ASP AG



Content:			
1. Introduction	1	16. View Log File	54
2. Important Safety Instructions	2	17. View User Information	55
3. Package Contents	2	18. View Parameters	57
4. Installation	2	19. Factory Default	57
1. Camera´s Connectors	3	20. Software Version	58
2. System Requirements	5	21. Software Upgrade	59
3. Power Connection	5	22. Maintenance	60
4. Ethernet Cable Connection	5	10. Streaming Settings	61
5. Alarm Connection	5	1. Video Format	61
6. Ceiling/Wall Mounting	5	2. Video Compression	63
5. Accessing the Camera	6	3. Video OCX Protocol	64
6. Video Resolution Setup	11	4. Video Frame Rate	65
7. Browser-based Viewer Introduction	14	5. Video Mask	66
8. Home Page	15	6. Audio (Audio and Bit Rate Settings)	67
9. System Related Settings	17	11. Camera Settings	68
1. Host Name & System Time Setting	17	1. Exposure Setting	68
2. Security	18	2. White Balance Setting	69
3. Network	27	3. Picture Adjustment	70
4. DDNS	33	4. Backlight Setting	70
5. Mail	34	5. Digital Zoom Setting	70
6. FTP	35	6. IR Function	71
7. HTTP	36	7. WDR Function	71
8. Application (Alarm Settings)	37	8. Noise Reduction	71
9. Motion Detection	42	9. TV System Setup	72
10. Network Failure Detection	46	12. Logout	72
11. Tampering	47	13. CMS Software Introduction	73
12. Storage Management (on Camera)	49	14. Internet Security Settings	73
13. Recording (on Camera)	52	15. GRUNDIG Viewer Download Procedure	76
14. File Location (on PC)	53	16. Install UPnP Components	78
15. Iris Adjustment	54	17. Deleting the Existing GRUNDIG Viewer	81

1. Introduction

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

With a sophisticated mechanical design and cable management, this Full HD IR Bullet IP Camera is easily installed and aesthetic.

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 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.

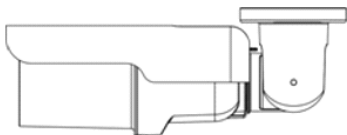
If any unusual smells or smoke comes out of the unit, stop using the product. In this case, immediately disconnect the power source and contact the service center. Continued use in such a condition may cause fire or electric shock.

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.)

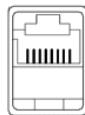
To prevent fire or electric shock, do not expose the inside of this device to rain or moisture.

3. Package Contents

These parts are included:



**Camera
(Cable included)**



**RJ-45 socket-to-socket
adapter**



**Self Tapping
Screws (x4)**



**Plastic Screw
Anchors (x4)**



Desiccant



**M4 Inner Hex
Wrench**



**Quick Guide &
Desiccant Guide**



CD

4. Installation

Do not install the 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. This may cause fire. Avoid aiming the camera directly towards extremely bright objects such as the sun, as this may damage the image sensor.

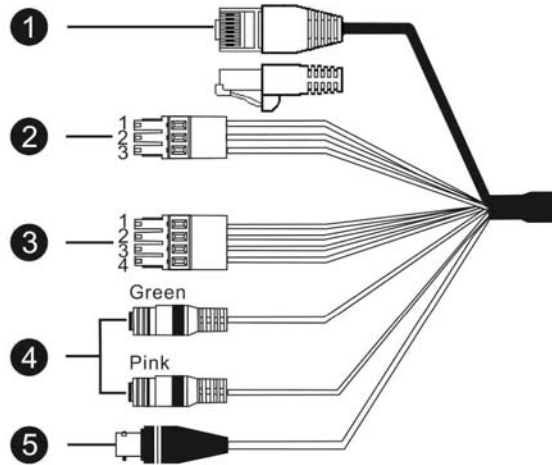
Do not install the unit in humid, dusty or sooty locations. Doing so may cause fire or electric shock. Install it in a place with good ventilation.

When installing the 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 the power off and then move or reinstall it.

4.1. Camera's Connectors

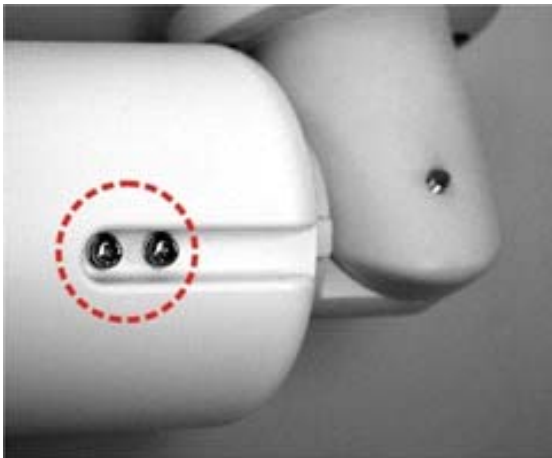
The IP Camera is equipped with an all-in-one cable for quick wiring. Definition for each connector will be given as follows.



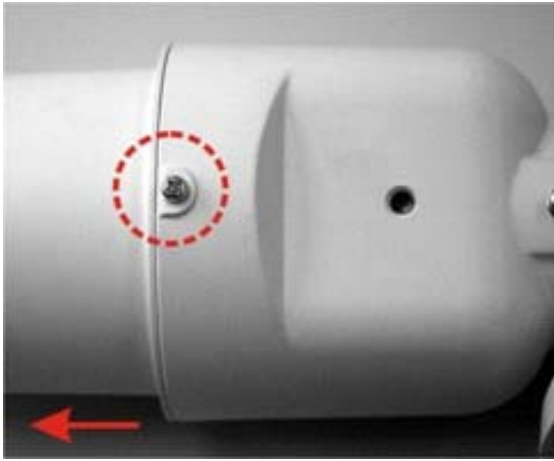
No	Cable	Pin	Definition	Remarks	
1	Network (with PoE)	-	RJ-45 connector		
2	Power (3-pin Terminal Block)	1	AC 24V-1	DC [-]	Power connection
		2	GND	Reserved	
		3	AC 24V-2	DC [+]	
3	Alarm (4-pin Terminal Block)	1	ALM_DI-	Alarm connection	
		2	ALM_DI+		
		3	ALM_DO-		
		4	ALM_DO+		
4	Audio I/O	Pink	Line In/ Mic In	Two-way audio transmission	
		Green	Line Out		
5	BNC	-	Analogue Video Output		

SD Card Slot / Reset Button:

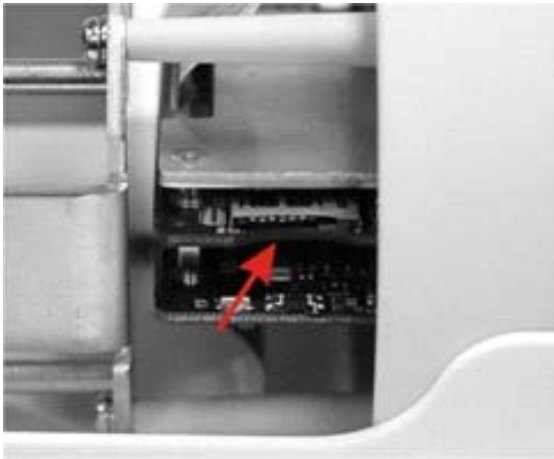
Follow the steps below to reach the SD Card Slot, Reboot Button and Factory Default Button on the IP Camera:



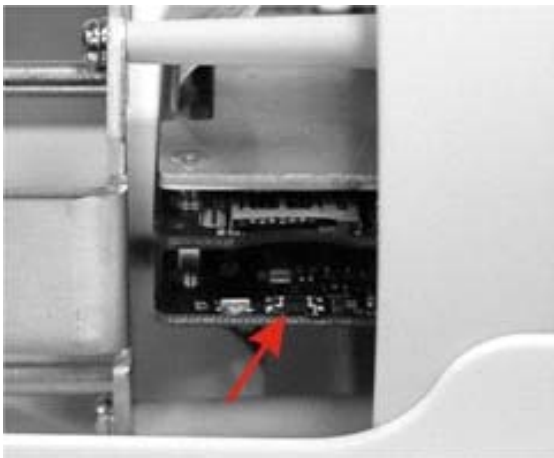
Step 1:
Unscrew the two screws on the Sunshield to remove it.



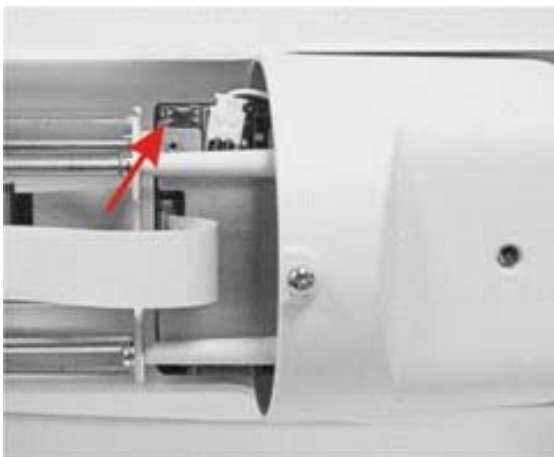
Step 2:
Unscrew the screw on the Camera Housing and remove the Front Housing.



SD Card Slot



Factory Default Button



Reboot Button

NOTE: Before installing the camera, please refer to the Desiccant User Guide in the package of the camera for instructions how to place the Desiccant in the Camera to prevent moisture from condensing on the IP Camera's Glass Cover.

4.2. System Requirements

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

Personal Computer :

- 1.) Intel Pentium M, 2.16 GHz or Intel Core 2 Duo, 2.0 GHz
- 2.) 2 GB RAM or more

Operating System :

Windows XP / Windows VISTA / Windows 7

Web Browser :

Microsoft Internet Explorer 6.0 or later
Firefox
Chrome
Safari

Network Card :

10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation

Viewer :

ActiveX control plug-in for Microsoft IE

4.3. Power Connection

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

4.4. Ethernet Cable Connection

Use of Category 5 Ethernet cable is recommended for network connection; to have best transmission quality, cable length shall not exceed 100 meters. Connect one end of the Ethernet cable to the RJ45 connector of the IP Camera, and the other end of the cable to the network switch or PC. Connect the camera network cable and the network cable from the switch to the RJ45 socket-socket adapter.

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

4.5. Alarm Connection

The camera is equipped with one alarm input and one relay output for alarm application.

Please refer to the label on the alarm terminal block and connect the alarm wiring accordingly.

4.6. Ceiling/Wall Mounting

The IR Bullet IP Camera can be installed directly on a wall or ceiling with the integrated 2-axis adjustable Bracket Mount. Please note that the wall or ceiling must have enough strength to support the IP Camera.

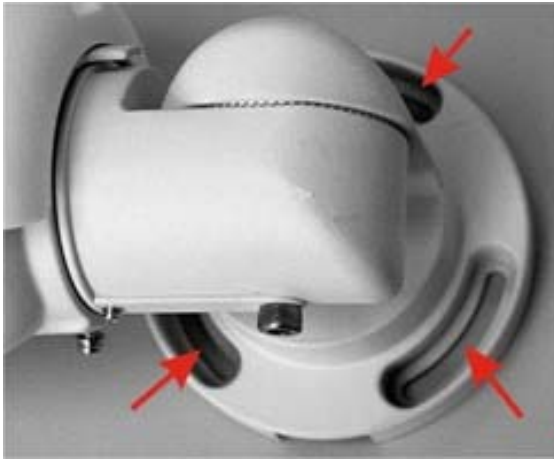
Follow the steps below to install the IP Camera:

Step 1:

Take the IP Bullet Camera out of its package.

Step 2:

Connect the Power/Ethernet/Alarm/Audio wires from the ceiling or wall to the corresponding connectors of the camera's All-in-one Cable.



Step 3:
 Fix the IP Camera's Bracket on the ceiling/wall with three supplied self tapping screws. Please consider the required end position of the camera. The self tapping screws should be affixed in a distance of 120° to ensure maximum flexibility of the bracket's position.



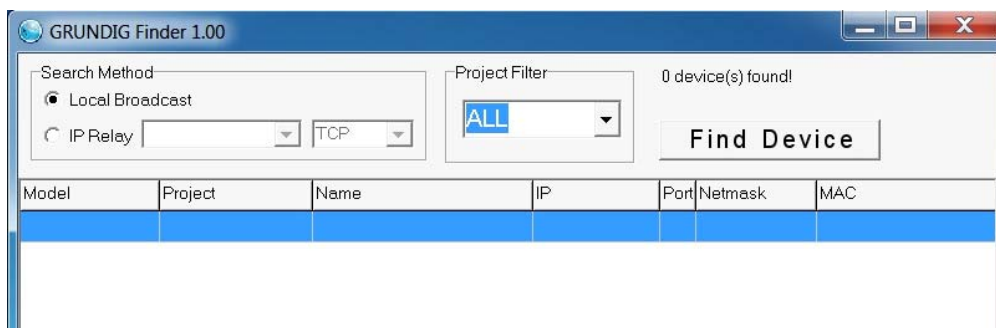
Step 4:
 Use the supplied Inner Hex Wrench to loosen the hex bolt on the side of the Bracket Mount to adjust the position of the IP Camera.

5. Accessing the Camera

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

GRUNDIG Finder Software Setup :

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

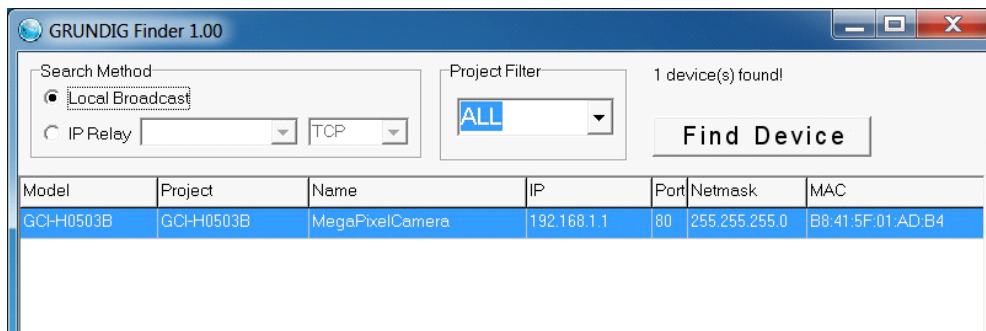


Step 2: The security alert window will pop up. Click “Unblock” to continue.

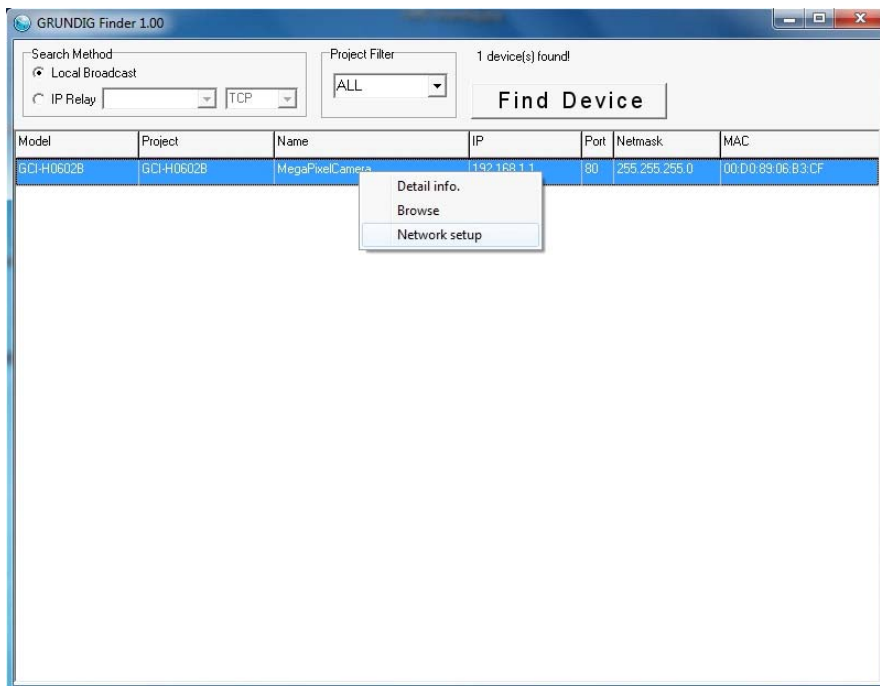


Device Search :

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



Step 4: Double-click or right-click and select “Browse” to access the camera 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 login to the IP Dome Camera.



The default login ID and password for the Administrator are:

Login ID: admin
Password: 1234

NOTE: ID and password are case sensitive.

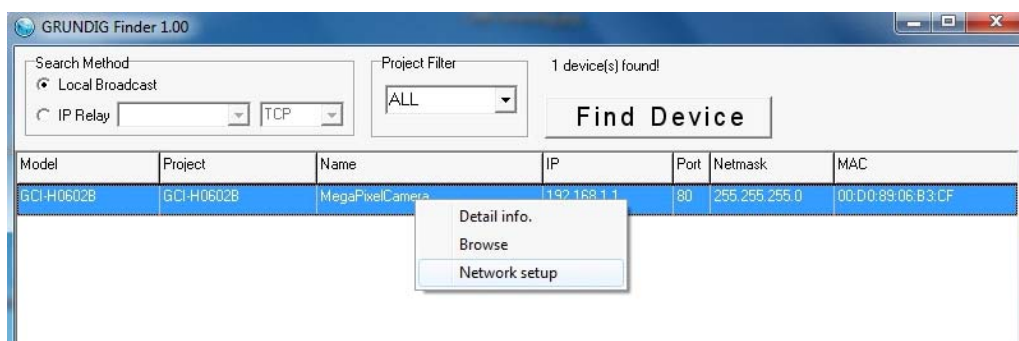
It is strongly advised to alter the administrator's password due to security concerns. Please refer to section 9.2. Security for further details.

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

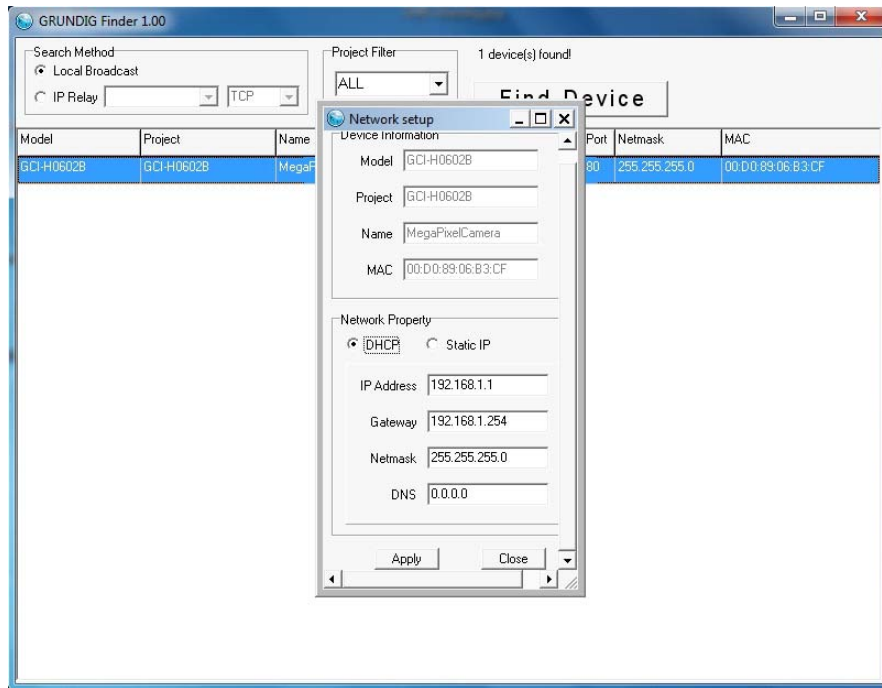
Example of changing the network property of the IP Camera :

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

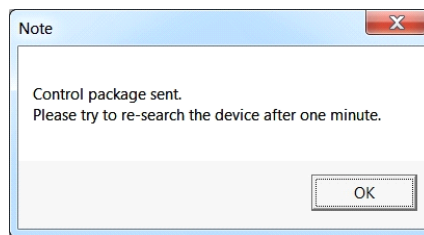
Step 1: In the finding device list, click on the IP Camera of which you would like to change the network property. Right-click on the selected item, and select "Network Setup". Meanwhile, record the IP Camera's MAC address for future identification.



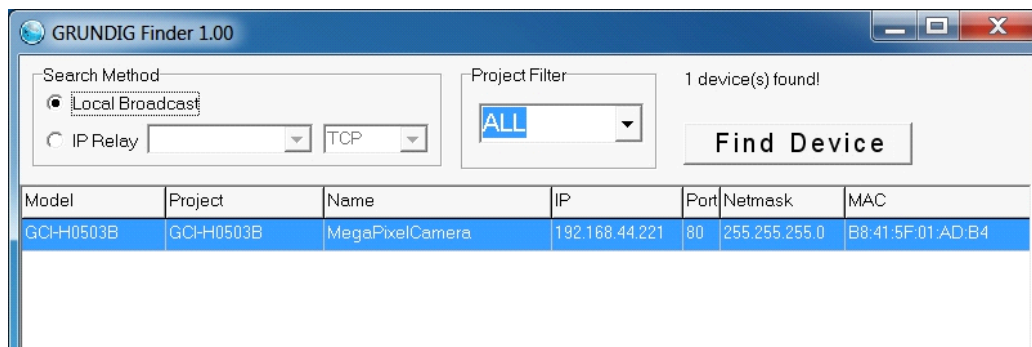
Step 2: The “Network Setup” page will come out. Select “DHCP,” and click on the “Apply” button at the bottom of the page.



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



Step 4: Click on the “Find Device” button to search all the devices. Then select the IP Camera with the correct MAC address. After double-clicking on the IP Camera, the login window will appear.



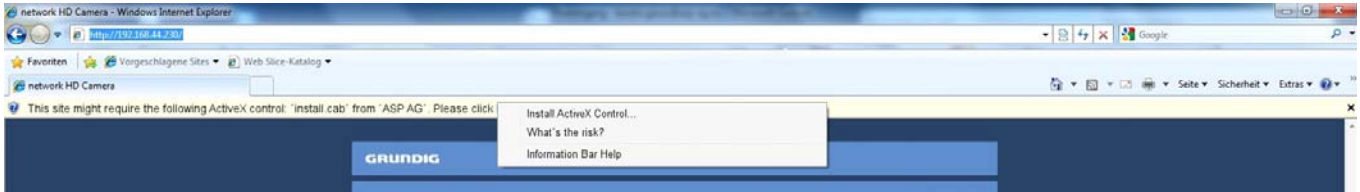
Step 5: Enter User name and Password to access the IP Camera.

Installing the GRUNDIG Viewer Software Online :

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

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.

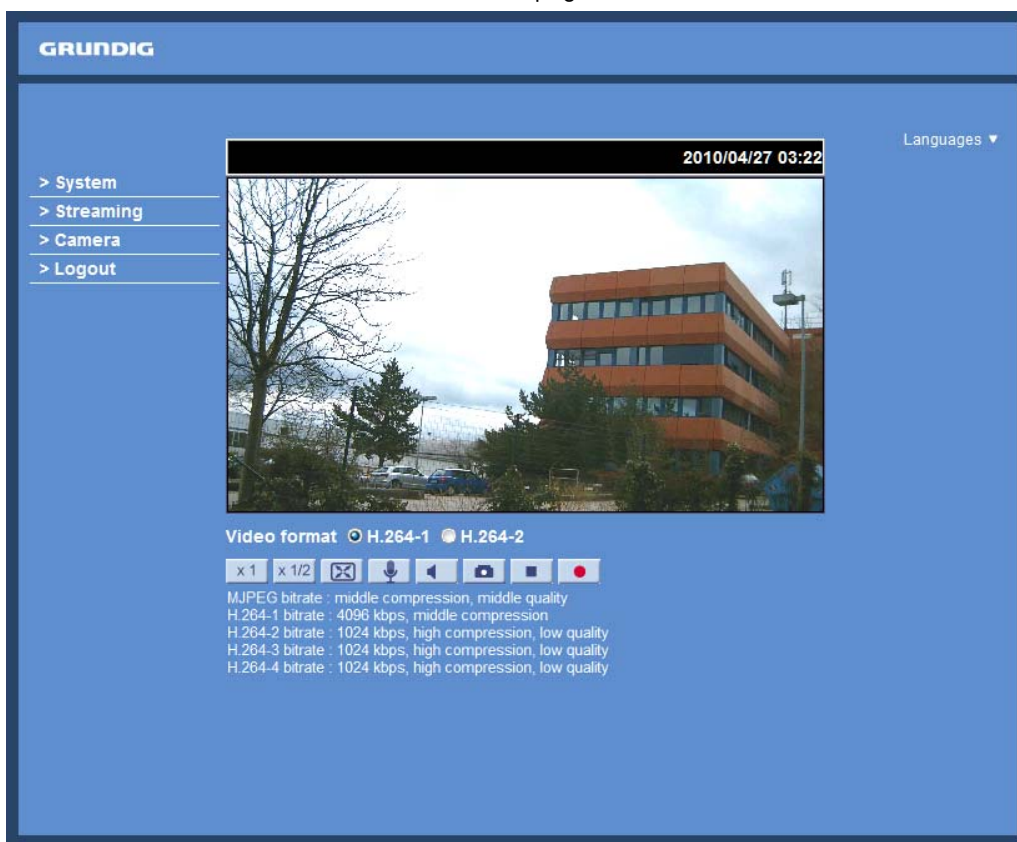


Then the security warning window will pop up. Click "Install" to carry on with the software installation.

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.

NOTE: If the Live Video Pane on the Home Page cannot be shown to the users who have installed the GRUNDIG Viewer on the PC previously, please refer to the procedure in chapter 17. Delete the Existing GRUNDIG Viewer.

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



Administrator/User Privileges :

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

Image and Focus Adjustment :

Adjust zoom and focus of the lens as necessary to produce a clear image. To set the correct angle of view and focus, you can use the BNC output on the camera. For this, please connect a PAL monitor to the BNC output.

6. Video Resolution Setup

The users can set up the Video Resolution on the Video Format page of the user-friendly browser-based configuration interface. The page "Video Format" can be found in the IP camera menu under the path: Streaming > Video Format.

Under the Video Resolution section in the menu page "Video Format", please select your preferred resolution setting:

H.264 + H.264		
H.264-1	H.264-2	BNC SUPPORT
1920 x 1080 (13fps)	1920 x 1080 (13fps)	√
	1280 x 1024 (25fps)	-
	1280 x 720 (25fps)	-
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
1920 x 1080 (25fps)	720 x 576 (25fps)*	√
	640 x 480 (25fps)	√
	352 x 288 (25 fps)	√
1280 x 1024 (25fps)	1280 x 1024 (13fps)	√
	1280 x 720 (25fps)	-
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1280 x 720 (25fps)	1280 x 720 (25fps)	√
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1024 x 768 (25fps)	1024 x 768 (25fps)	√
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
800 x 600 (25fps)	800 x 600 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
720 x 576 (25fps)	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
640 x 480 (25fps)	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
352 x 288 (25fps)	352 x 288 (25fps)	-

H.264 ⇄ MJPEG		
H.264	MJPEG	BNC SUPPORT
1920 x 1080 (13fps)	1920 x 1080 (13fps)	✓
	1280 x 1024 (25fps)	-
	1280 x 720 (25fps)	-
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
1920 x 1080 (25fps)	720 x 576 (25fps)	✓
	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
1280 x 1024 (25fps)	1280 x 1024 (13fps)	✓
	1280 x 720 (25fps)	-
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	✓
	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
1280 x 720 (25fps)	1280 x 720 (25fps)	✓
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	✓
	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
1024 x 768 (25fps)	1024 x 768 (25fps)	✓
	800 x 600 (25fps)	-
	720 x 576 (25fps)	✓
	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
800 x 600 (25fps)	800 x 600 (25fps)	✓
	720 x 576 (25fps)	✓
	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
720 x 576 (25fps)	720 x 576 (25fps)	✓
	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
640 x 480 (25fps)	640 x 480 (25fps)	✓
	352 x 288 (25fps)	✓
352 x 288 (25fps)	352 x 288 (25fps)	-

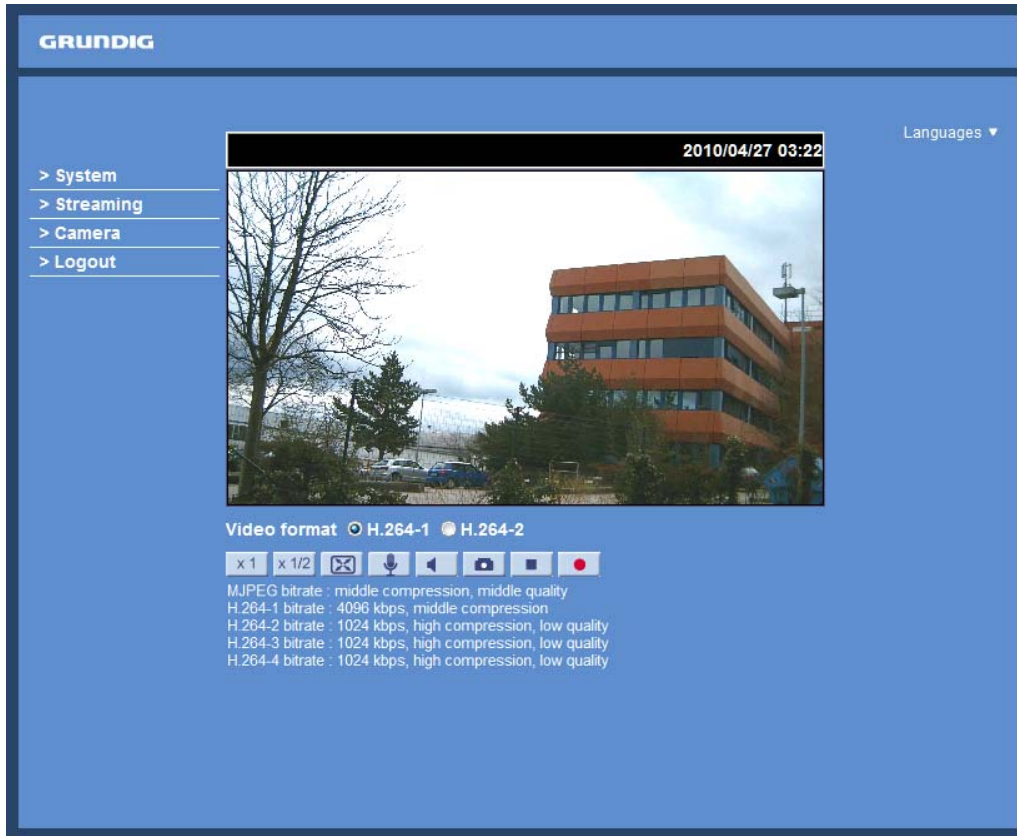
MJPEG Only	
MJPEG	BNC SUPPORT
1920 x 1080 (25fps)	✓
1280 x 1024 (25fps)	✓
1280 x 720 (25fps)	✓
1024 x 768 (25fps)	✓
800 x 600 (25fps)	✓
720 x 576 (25fps)	✓
640 x 480 (25fps)	✓
352 x 288 (25fps)	-
H.264 Only	
H.264	BNC SUPPORT
1920 x 1080 (25fps) Low Latency	✓
1920 x 1080 (25fps)	✓
1280 x 1024 (25fps)	✓
1280 x 720 (25fps)	✓
1024 x 768 (25fps)	✓
800 x 600 (25fps)	✓
720 x 576 (25fps)	✓
640 x 480 (25fps)	✓
352 x 288 (25fps)	-

(*) Default

For more streaming combinations with several streams, please refer to "Streaming" > "Video Format" in the camera menu.

7. Browser-based Viewer Introduction

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



There are four tabs on the left (System, Streaming, Camera 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. Further details will be interpreted in chapter 10. Streaming Settings.

Camera setting :

Users can adjust various camera parameters. Further details will be interpreted in chapter 11. Camera Settings.

Logout :

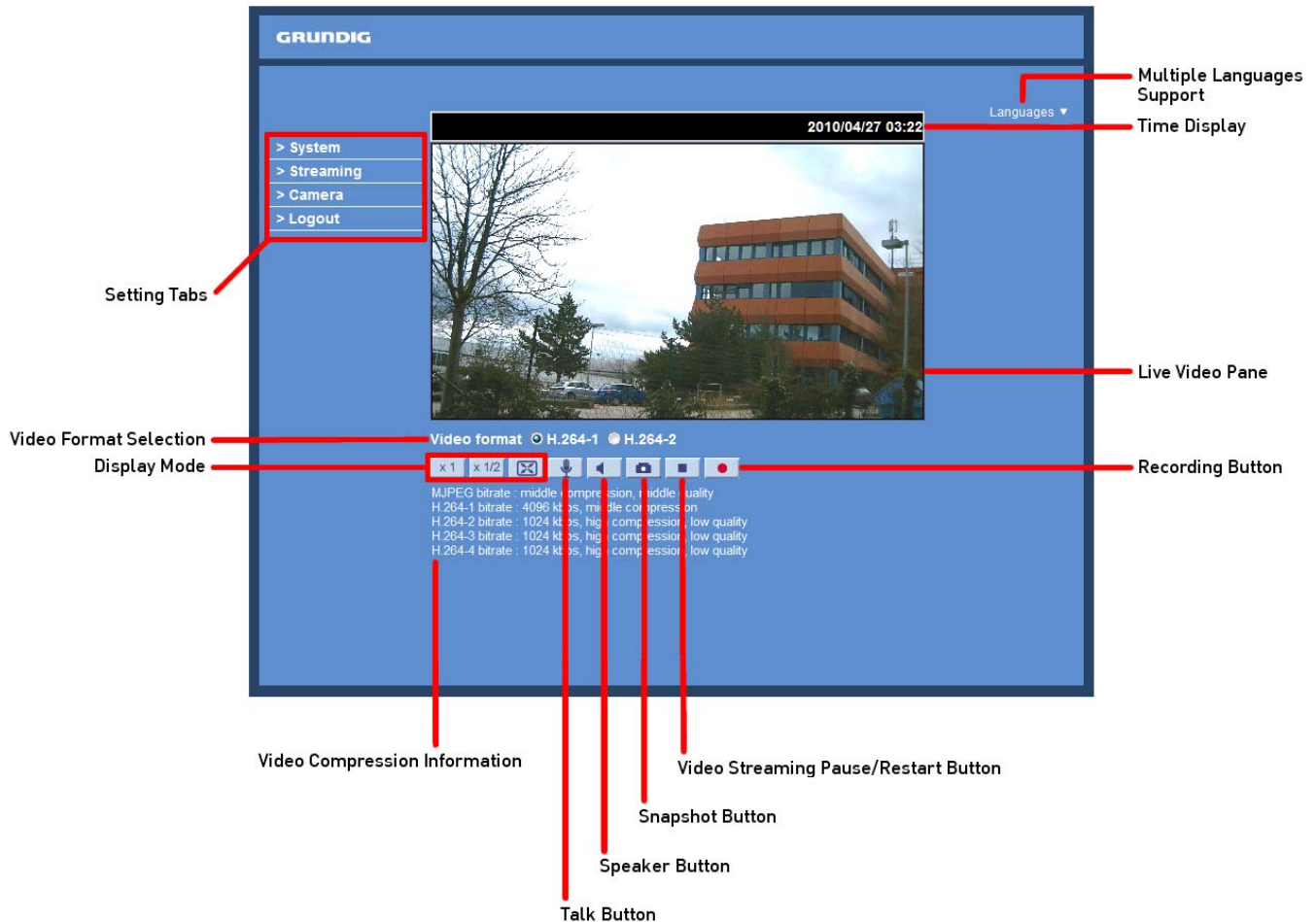
Click on this tab to re-login to the IP Camera with another user name and password. Further details will be interpreted in chapter 12. Logout.

Languages :

Please choose one of the supported languages (German, English, French, Italian or Russian).

8. Home Page

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



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 9.14. 'File Location (on PC)' 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 camera 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" page. The default storage location for the recordings is: C:/. See section 9.14. 'File Location (on PC)' 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.

Multiple Languages Support :

Multiple languages are supported for the viewer window interface.

NOTE:

The following functions are not available for the Browsers Firefox, Chrome, Safari and Opera: Full Screen Mode, Audio talk/listen, Snapshot, Playback and Recording.

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.

The screenshot displays the Grundig System configuration page. On the left is a navigation menu with categories: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and Back. The main content area is titled 'System' and contains the following settings:

- Host name:** MegaPixelCamera
- Time zone:** GMT+00:00 Gambia, Liberia, Morocco, England
- Enable daylight saving time:** (unchecked).
 - Time offset: 01:00:00
 - Start date: Jan 1st Sun Start time: 00:00:00
 - End date: Jan 1st Sun End time: 00:00:00
- Sync with computer time:** (checked).
 - PC date: 2012/04/26 [yyyy/mm/dd]
 - PC time: 13:13:45 [hh:mm:ss]
- Manual:** (checked).
 - Date: 2010/04/01 [yyyy/mm/dd]
 - Time: 00:00:00 [hh:mm:ss]
- Sync with NTP server:** (unchecked).
 - NTP server: 0.0.0.0 [host name or IP address]
 - Update interval: Every hour

A 'Save' button is located at the bottom of the configuration area.

9.1. Host Name & System Time Setting

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

This screenshot is identical to the one above, showing the Grundig System configuration page with the same navigation menu and settings for Host name, Time zone, Daylight saving time, Sync with computer time, Manual, and Sync with NTP server.

Host Name :

The name is for camera identification (max. 30 characters). If the alarm function (see section 9.8. 'Application (Alarm Settings)') 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 alternative way to synchronise your camera's clock with a NTP server. Please specify the server you wish to synchronise the camera 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. On the left is a navigation menu with categories: > System, Security, Network, and View information. The 'Security' category is expanded, showing sub-items: User, HTTPS, IP Filter, and IEEE 802.1X. The 'User' sub-item is selected. The main content area is titled 'Security' and contains three sections: 'Admin password' with two password input fields and a 'Save' button; 'Add user' with 'User name' and 'User password' input fields, and checkboxes for 'I/O access', 'Camera control', 'Talk', and 'Listen', with an 'Add' button; and 'Manage user' with a 'User name' dropdown menu (currently showing '-- no user --') and 'Delete' and 'Edit' buttons.

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.

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

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 the video when accessing the camera.

- Camera control:

This item allows the specified User to change the camera's parameters on the Camera Setting page.

- Talk/Listen:

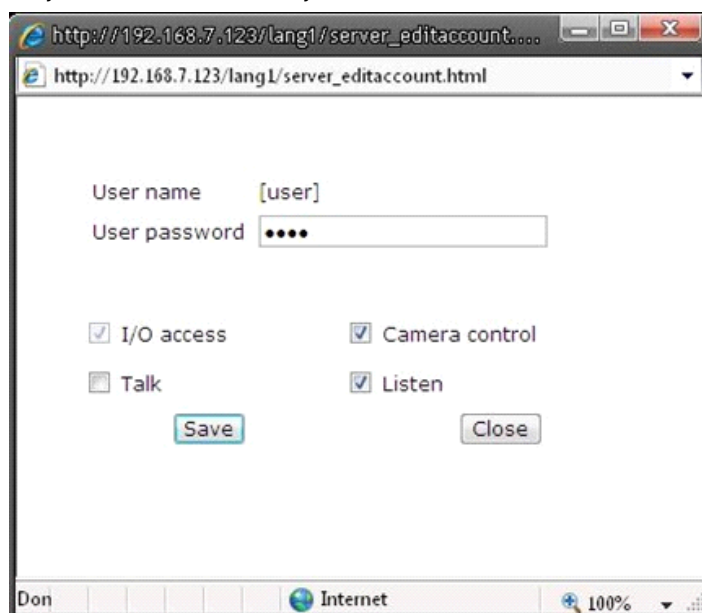
Talk and Listen functions allow the appointed user on the local site (PC site) to communicate, for instance, with the administrator on the remote site.

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.

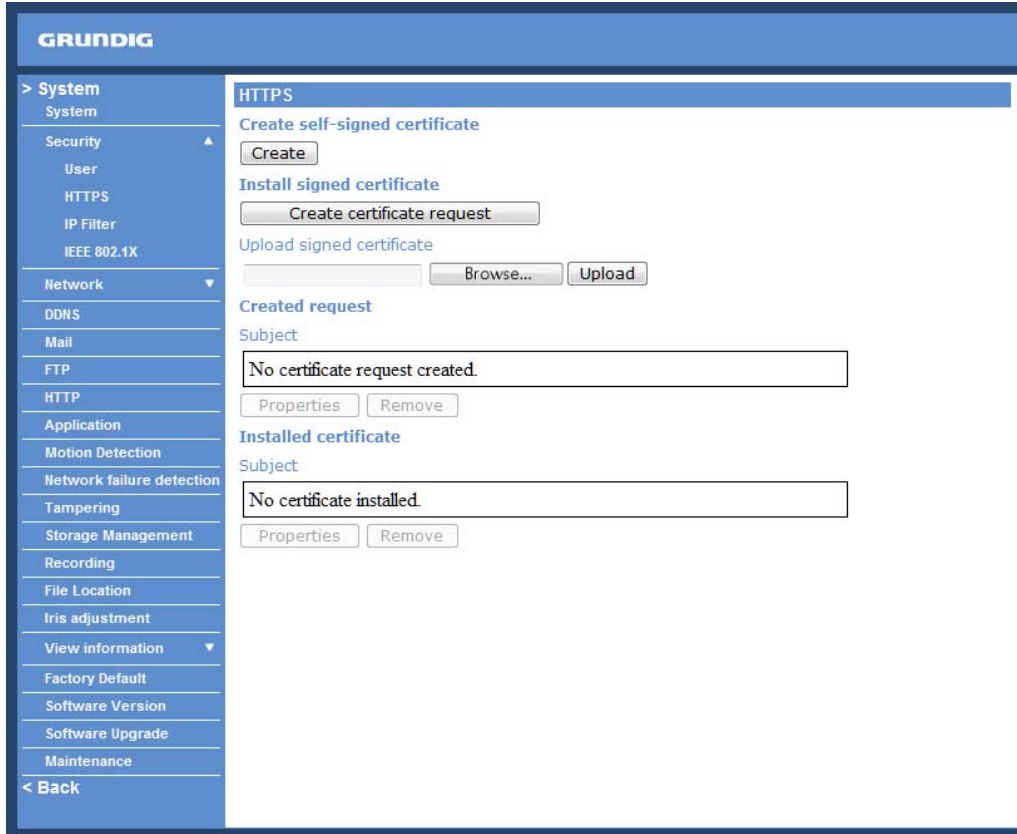
NOTE: It is required to enter the User password and to select the functions that will be open to the user. When finished, click <Save> to modify the account authority.



<HTTPS> :

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

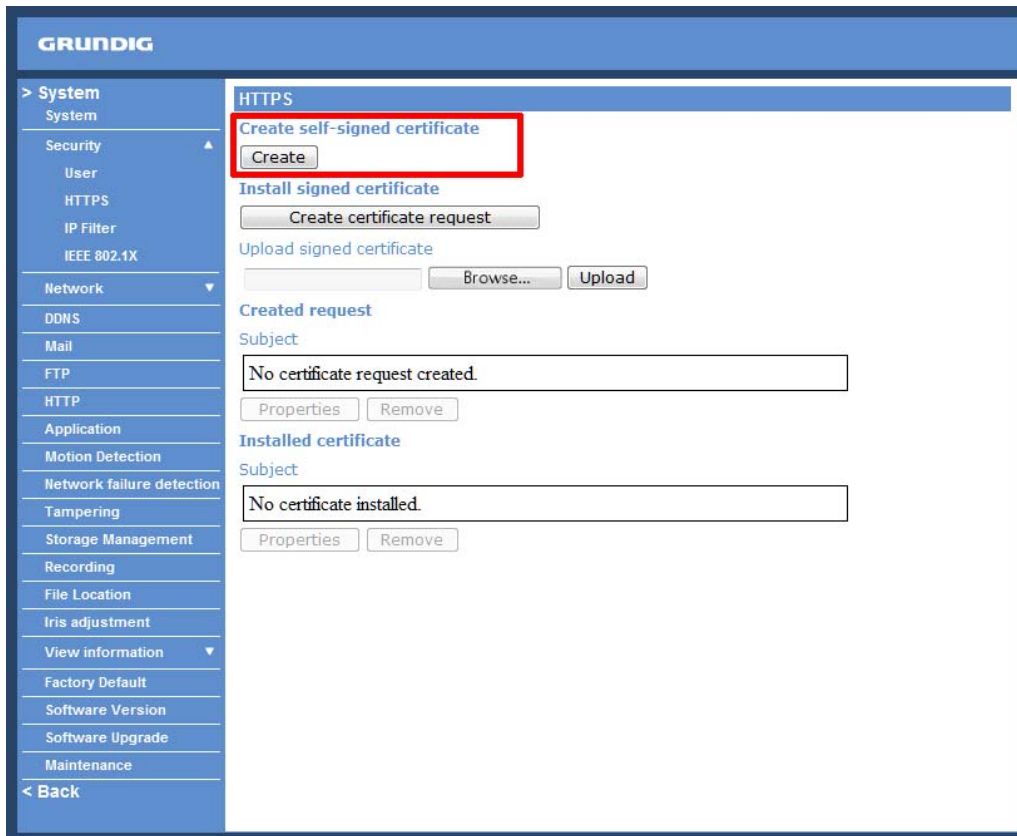
After clicking on the <HTTPS> tab, the HTTPS setting page will be shown as in the figure below.



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

Create self-signed certificate :

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

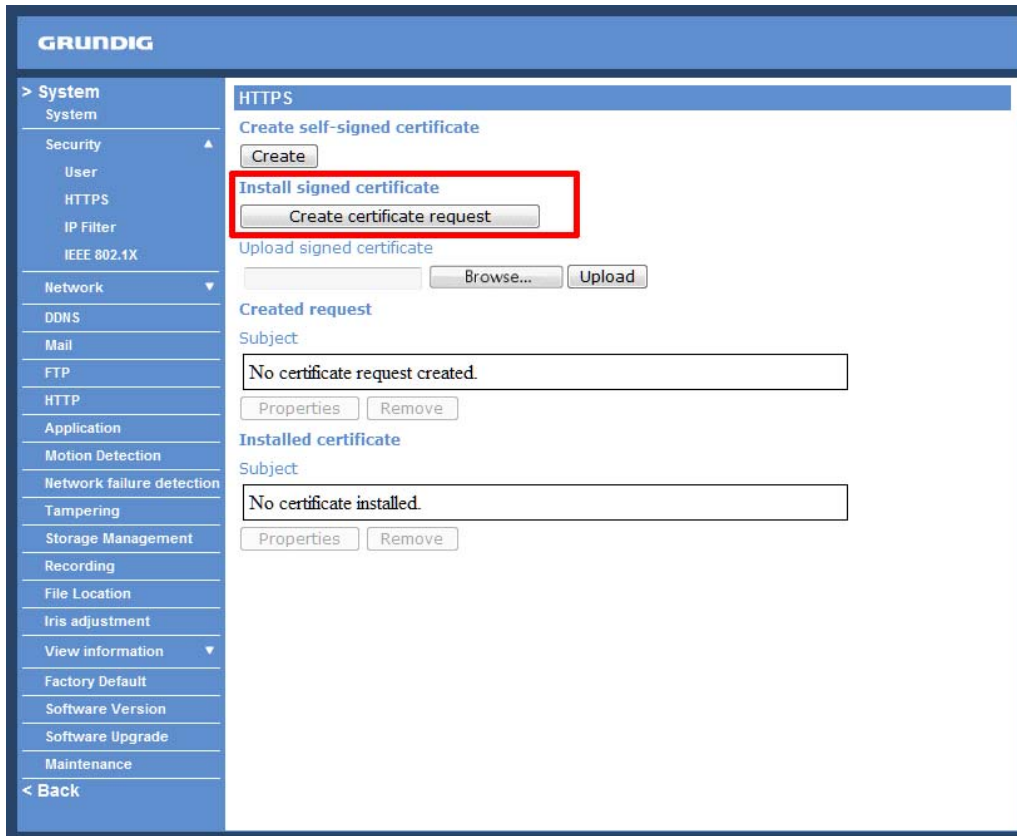


Click on the <Create> button under “Create self-signed certificate” and provide the requested information to install a self-signed certificate for the IP Camera. Please refer to the last part of this section: “Provide the Certificate Information” for more details.

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

Install signed certificate :

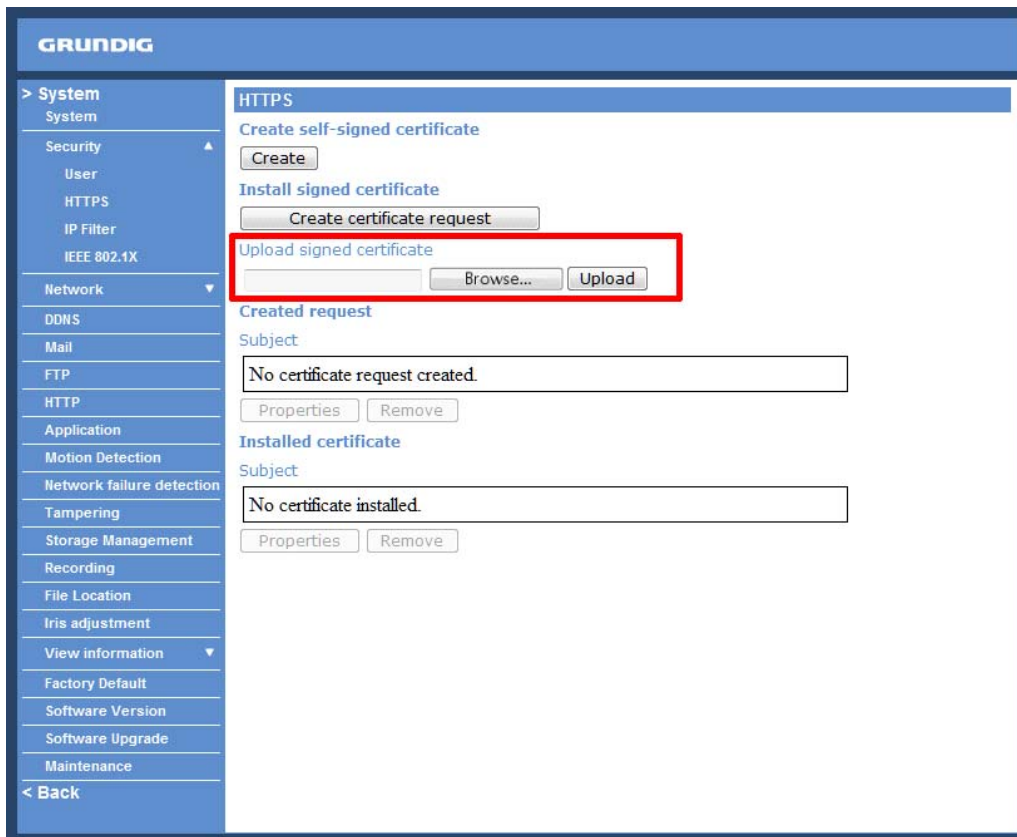
Click on the "Create Certificate Request" button to create and submit a certificate request in order to obtain a signed certificate from the CA (Certificate Authority).



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

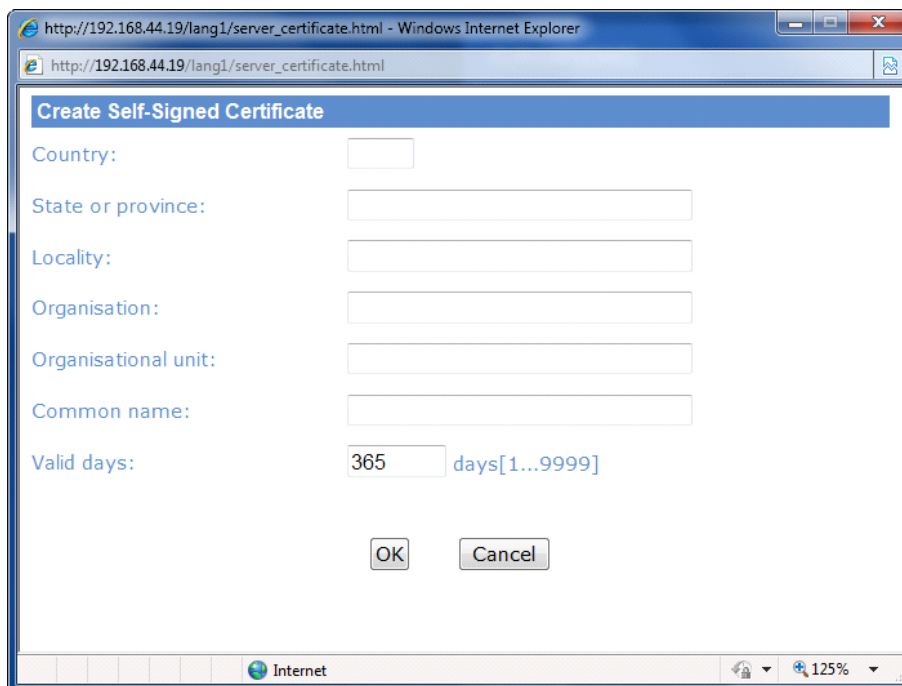
When the request is complete, the subject of the Created Request will be shown in the field. Click "Properties" below the Subject field, copy the PEM-formatted request and send it to your selected CA.

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



Provide the Certificate Information :

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



The image shows a screenshot of a web browser window titled "http://192.168.44.19/lang1/server_createrequest.html - Windows Internet Explorer". The browser's address bar also displays "http://192.168.44.19/lang1/server_createrequest.html". The main content area features a form titled "Create Certificate Request" with a blue header. The form contains six text input fields, each with a label to its left: "Country:", "State or province:", "Locality:", "Organisation:", "Organisational unit:", and "Common name:". Below the input fields are two buttons: "OK" and "Cancel". 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).

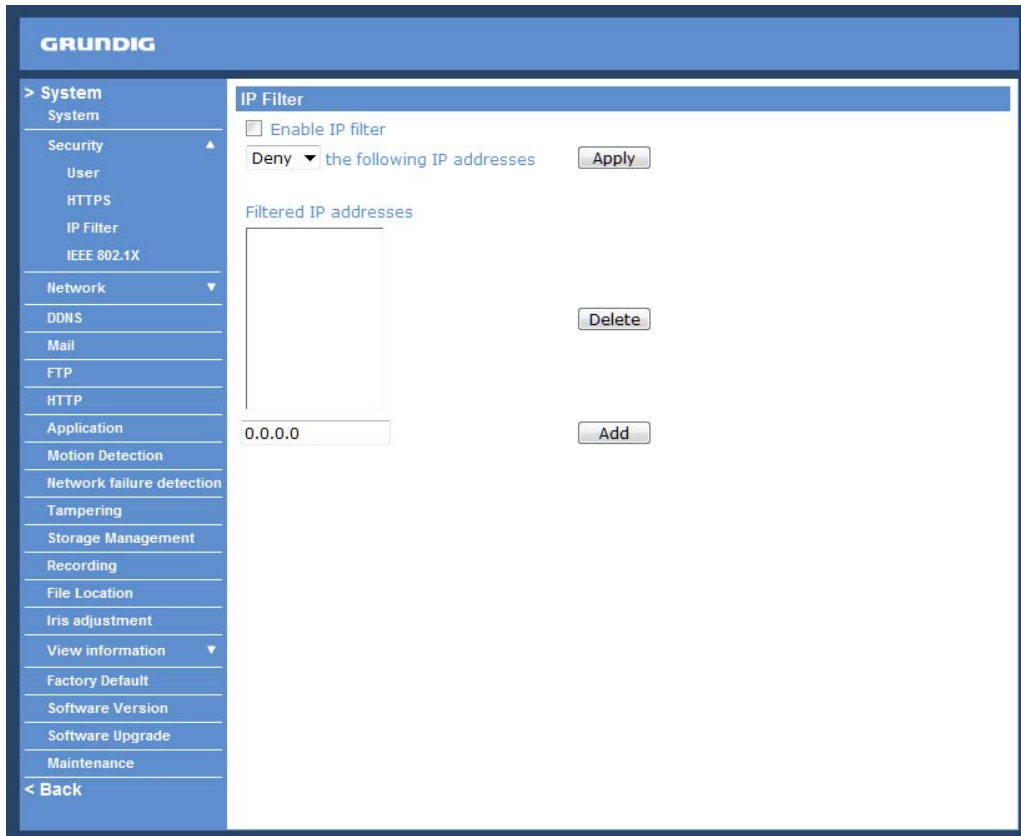
- Valid days (Self-signed Certificate Only):

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 IP Camera can be restricted by denying/allowing specific IP addresses.



General :

- Enable IP Filter:

Check the box to enable the IP Filter function. Once enabled, access to the IP Camera 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 IP Camera 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.

The screenshot shows the Grundig web interface for configuring IEEE 802.1X/EAP-TLS. The left sidebar contains a navigation menu with categories: System (System, Security, User, HTTPS, IP Filter, IEEE 802.1X), Network (DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View Information), and other options like Factory Default, Software Version, Software Upgrade, and Maintenance. The main content area is titled 'IEEE 802.1X/EAP-TLS' and includes sections for 'CA certificate', 'Client certificate', 'Private key', and 'Settings'. Each section has a 'Browse...' button and an 'Upload' button. The 'Settings' section includes an 'Identity' field with 'admin' entered, a 'Private key password' field with masked characters, and a checkbox for 'Enable IEEE 802.1X'. A 'Save' button is located at the bottom right of the settings area.

CA Certificate :

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

Client Certificate/Private Key :

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

Settings :

- Identity:

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

- Private Key Password:

Enter the password (maximum 16 characters) for your user 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

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

The screenshot shows the Grundig web interface for network configuration. The left sidebar contains a menu with categories: System, Security, Network (expanded), DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and Back. The main content area is titled 'Network' and has a 'General' sub-tab. Under 'General', there are three radio button options: 'Get IP address automatically', 'Use fixed IP address' (selected), and 'Use PPPoE'. The 'Use fixed IP address' section includes input fields for IP address (192.168.1.1), Subnet mask (255.255.255.0), Default gateway (0.0.0.0), Primary DNS (0.0.0.0), and Secondary DNS (0.0.0.0). The 'Use PPPoE' section includes input fields for User name and Password, and a 'Save' button. Below this is the 'Advanced' section with input fields for Web server port (80), RTSP port (554), MJPEG over HTTP port (8008), and HTTPS port (443), with a 'Save' button. At the bottom is the 'IPv6 address configuration' section with a checkbox for 'Enable IPv6' and an 'Address' input field with a 'Save' button.

<Basic> :

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

This screenshot is identical to the one above, showing the Grundig Network configuration page. The 'General' tab is selected, and the 'Use fixed IP address' option is chosen. The configuration fields for IP address, subnet mask, gateway, and DNS are visible, along with the advanced port settings and IPv6 configuration options.

Get IP address automatically (DHCP):

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

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

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

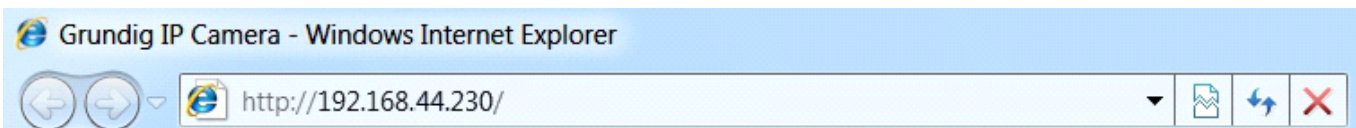
NOTE: Please make a record of the IP Camera's MAC address, which can be found on the label of the camera, for identification in the future.

Use a fixed IP address :

To set up 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. 192.168.44.230; then go to Default Gateway (explained later) and type in the appropriate setting, e.g. 192.168.44.1. Click on "Save" to confirm the new setting.

The screenshot shows the Grundig web interface for network configuration. The left sidebar contains a menu with options like System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and Back. The main content area is titled 'Network' and has a 'General' section. In the 'General' section, the 'Use fixed IP address' radio button is selected. The 'IP address' field is set to 192.168.44.230, the 'Subnet mask' is 255.255.255.0, and the 'Default gateway' is 192.168.44.1. There are also fields for Primary DNS (0.0.0.0) and Secondary DNS (0.0.0.0). 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. At the bottom is the 'IPv6 address configuration' section with an 'Enable IPv6' checkbox and an 'Address' field with a 'Save' button.

When using a static IP address to login to the IP Camera, users can access it either through the "GRUNDIG Finder" software (see 6. Accessing the Camera) or input the IP address in the URL bar and click on "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, all users must be informed about the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the IP Camera which has the IP address "192.168.0.100" from 80 to 8080, the users 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.

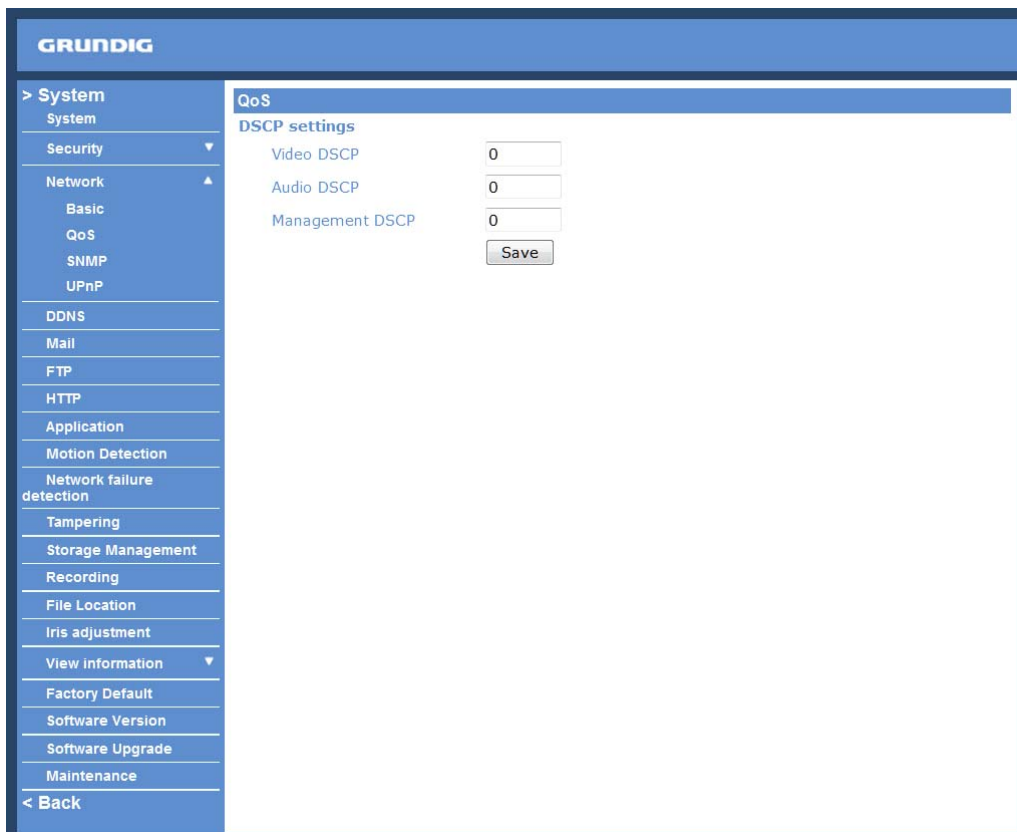
NOTE: Be aware to assign a different port number for each separate service mentioned above.

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 IP Camera 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 IP Cameras 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 IP Camera can be monitored and managed remotely by the network management system.

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 IP Camera to send messages to a management system about important events or status changes.

- Enable Traps:

Check the box to activate trap reporting.

- Trap address:

Enter the IP address of the management server.

- Trap community:

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

Trap option :

- Warm start:

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

Click the "Save" button to complete the setting.

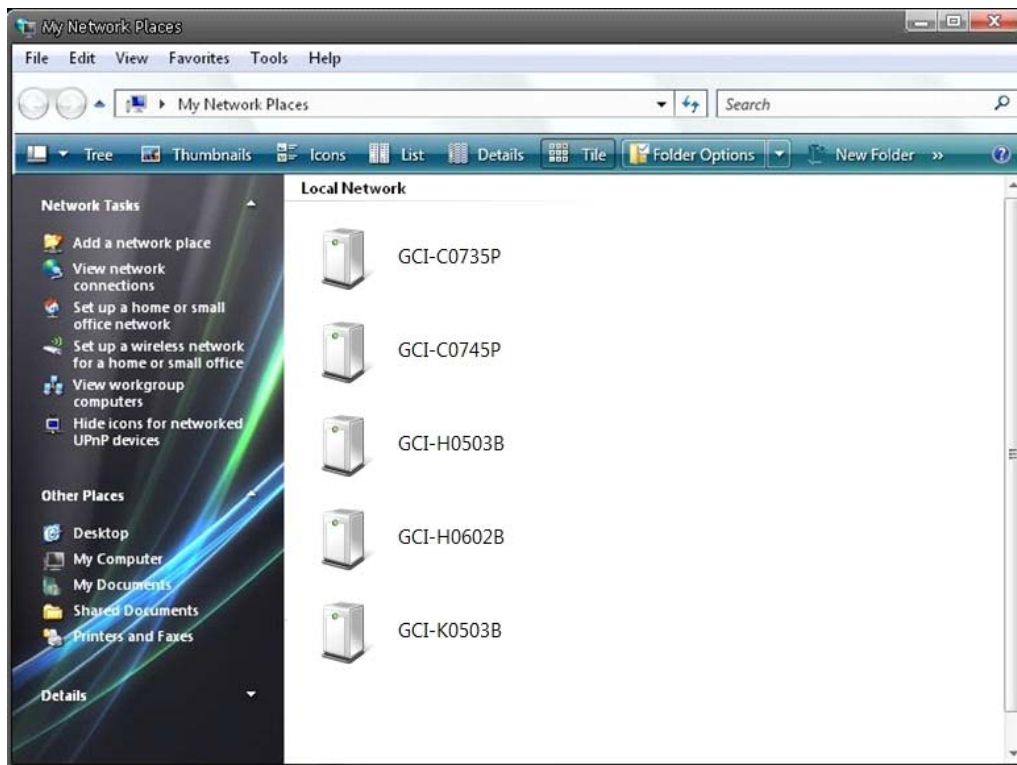
<UPnP> :

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, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and < Back. 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 'GCI-K1526T' and a 'Save' button.

UPnP Setting :

- Enable UPnP:

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



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

- Enable UPnP port forwarding:

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

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

- Friendly name:

Set the name of the IP Camera for identification.

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 contains 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 set up the sending of 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:

The screenshot shows the Grundig Mail configuration interface. The left sidebar contains a navigation menu with the following items: > System, System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View Information, Factory Default, Software Version, Software Upgrade, Maintenance, and < Back. The main content area is titled 'Mail' and 'SMTP'. It features two sets of configuration fields: '1st SMTP (mail) server' and '2nd SMTP (mail) server'. Each set includes fields for server, port (pre-filled with '25'), account name, password, and recipient email address. There are also checkboxes for '1st SMTP SSL' and '2nd SMTP SSL'. A 'Sender email address' field is at the bottom. A 'Save' button is located at the bottom right of the form area.

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.

The screenshot shows the Grundig FTP configuration interface. The left sidebar contains a menu with the following items: > System, System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and < Back. The main content area is titled 'FTP' and contains the following fields:

- 1st FTP server: [Text input field]
- 1st FTP server port: [Text input field with value '21']
- 1st FTP user name: [Text input field]
- 1st FTP password: [Text input field]
- 1st FTP remote folder: [Text input field]
- 1st FTP passive mode
- 2nd FTP server: [Text input field]
- 2nd FTP server port: [Text input field with value '21']
- 2nd FTP user name: [Text input field]
- 2nd FTP password: [Text input field]
- 2nd FTP remote folder: [Text input field]
- 2nd FTP passive mode

A 'Save' button is located at the bottom right of the form area.

9.7. HTTP

A HTTP Notification server can listen for notification messages from IP Cameras by triggered events. The HTTP setting page is shown below. Enter the HTTP details, which include the server name (for instance, http://192.168.1.1/admin.php), 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.

The screenshot shows the Grundig web interface for configuring HTTP notifications. The left sidebar contains a menu with the following items: > System, System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and < Back. The main content area is titled 'HTTP' and contains the following fields: 1st HTTP server, 1st HTTP user name, 1st HTTP password, 2nd HTTP server, 2nd HTTP user name, and 2nd HTTP password. A 'Save' button is located at the bottom right of the form area.

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

9.8. Application (Alarm Settings)

The IP Camera is equipped with one alarm input and one relay output for cooperation with the alarm system to catch event images. Please refer to the alarm pin definition below to connect alarm devices to the IP Camera if needed. The alarm configuration page is also shown below.

The screenshot shows the 'Application' settings page for a Grundig IP camera. The left sidebar contains a navigation menu with categories like System, Security, Network, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, and Maintenance. The main content area is titled 'Application' and includes the following sections:

- Alarm Switch:** Radio buttons for 'Off' (selected) and 'On'.
- Alarm Type:** Radio buttons for 'Normal close' and 'Normal open' (selected).
- Alarm Output:** Radio buttons for 'Output high' (selected) and 'Output low'.
- Triggered Action:** A list of actions with checkboxes: 'Enable alarm output' (checked), 'Send message by FTP', 'Upload image by FTP', 'Send HTTP notification', 'IR cut filter' (unchecked), 'Send message by E-Mail', 'Upload image by E-Mail', and 'Record stream to sd card'. There is also a dropdown menu for 'IR cut filter' set to 'on'.
- File Name:** A text input field for 'File name' (containing 'image.jpg'), radio buttons for 'Add date/time suffix' (selected), 'Add sequence number suffix (no maximum value)', 'Add sequence number suffix up to [0] and then start over', and 'Overwrite', and a 'Save' button.

Alarm Pin Definition :

Please refer to the label on the alarm terminal block and connect the alarm wiring accordingly.

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.

- IR Cut Filter:

If you select this item, the camera's IR cut filter (ICR) will be removed (on) or blocked (off) when the alarm input is triggered.

NOTE: The IR Function (Refer to IR Function) cannot be set to <Auto> mode when this trigger action is enabled.

- Send Alarm Message by FTP:

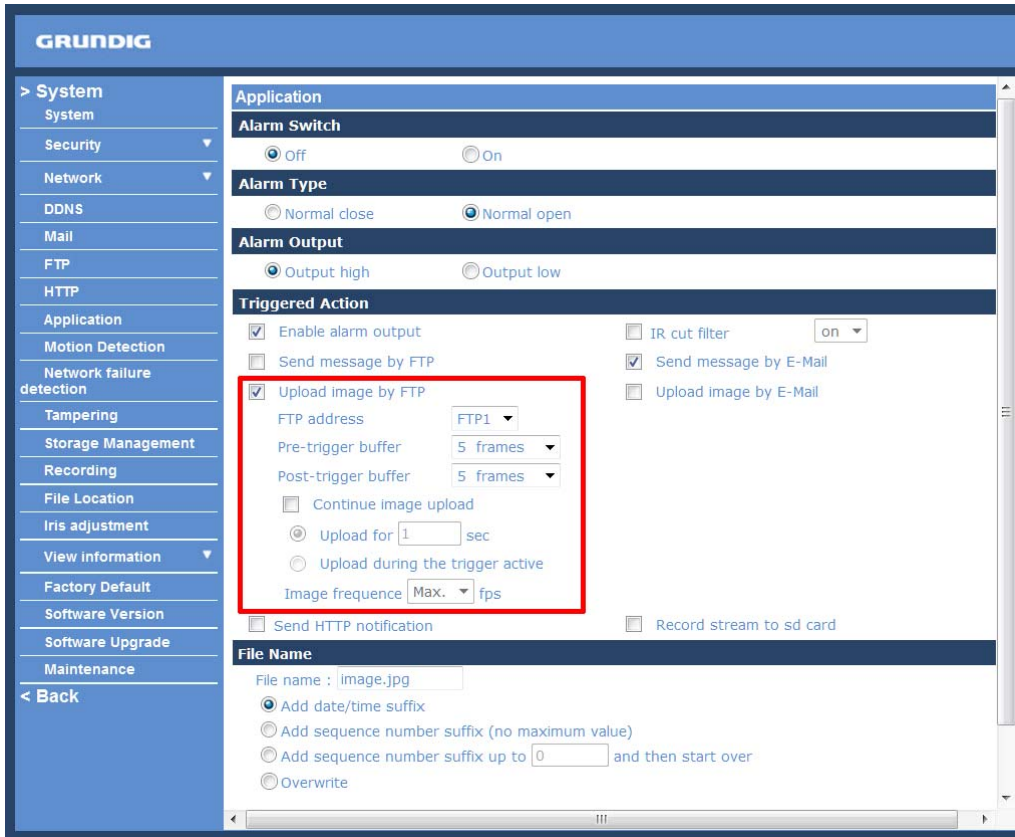
The Administrator can choose to send an alarm message by FTP when a motion is detected.

- Send Alarm Message by E-Mail:

The Administrator can choose to send an alarm message by E-Mail when an alarm is triggered.

- 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.



The <Pre-trigger buffer> recording function allows users to check what happened before the alarm. The pre-trigger buffer time range is from 1 to 20 frames.

On the other hand, the <Post-trigger buffer> is for uploading a certain amount of images after the alarm input is triggered. The post-trigger buffer time range is from 1 to 20 frames.

Check the box <Continue image upload> to upload the triggered images during a certain time or keep uploading until the trigger is off.

- Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to the FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds.

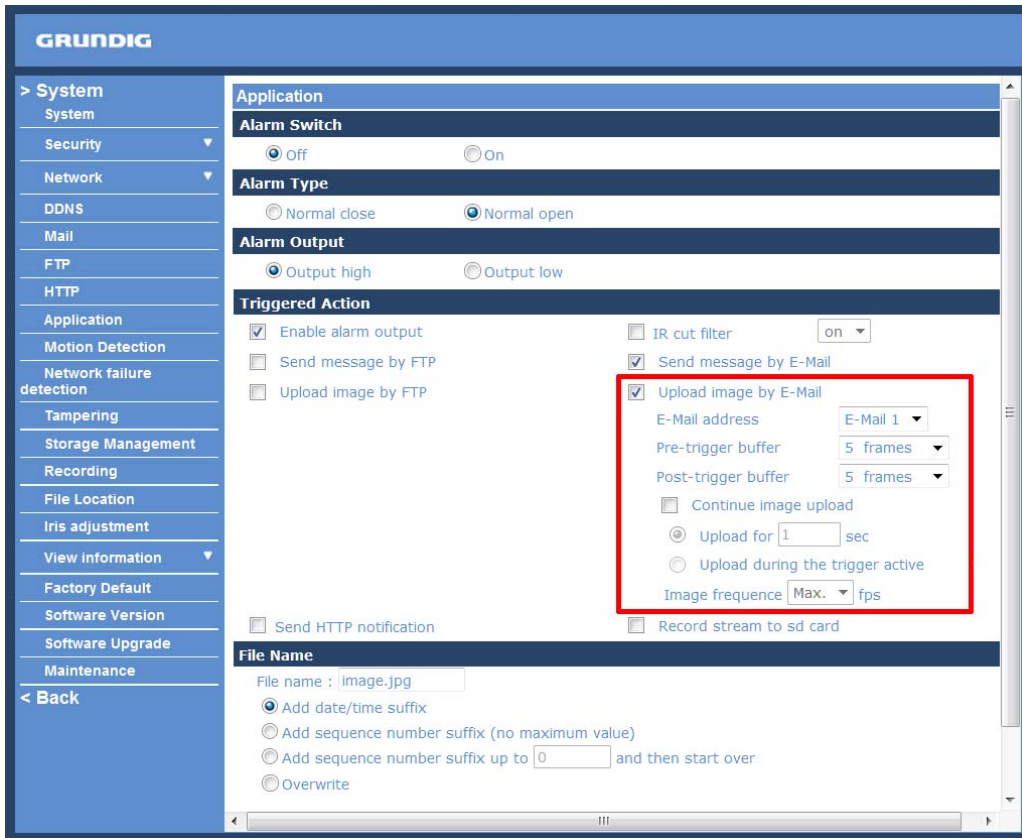
- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

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

- 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.



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 20 frames.

On the other hand, the <Post-trigger buffer> is for uploading a certain amount of images after the alarm input is triggered. The post-trigger buffer time range is from 1 to 20 frames.

Check the box <Continue image upload> to upload the triggered images during a certain time or keep uploading until the trigger is off.

- Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to the FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds.
- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

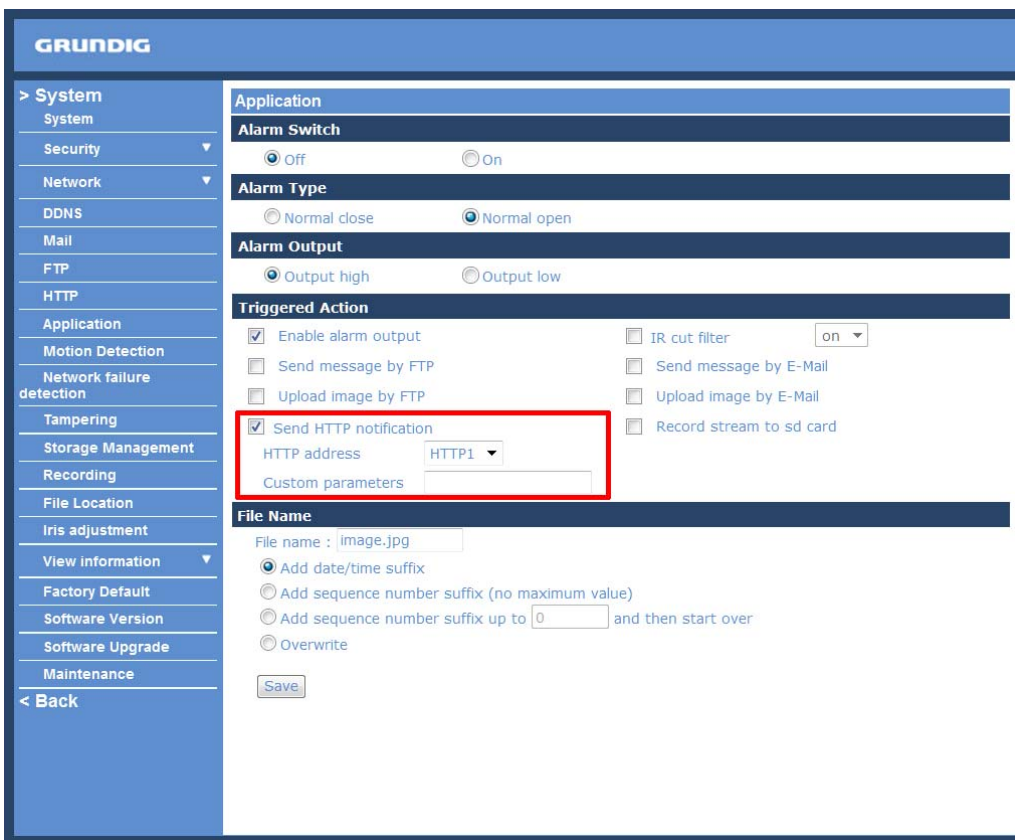
Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

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

- Send HTTP notification:

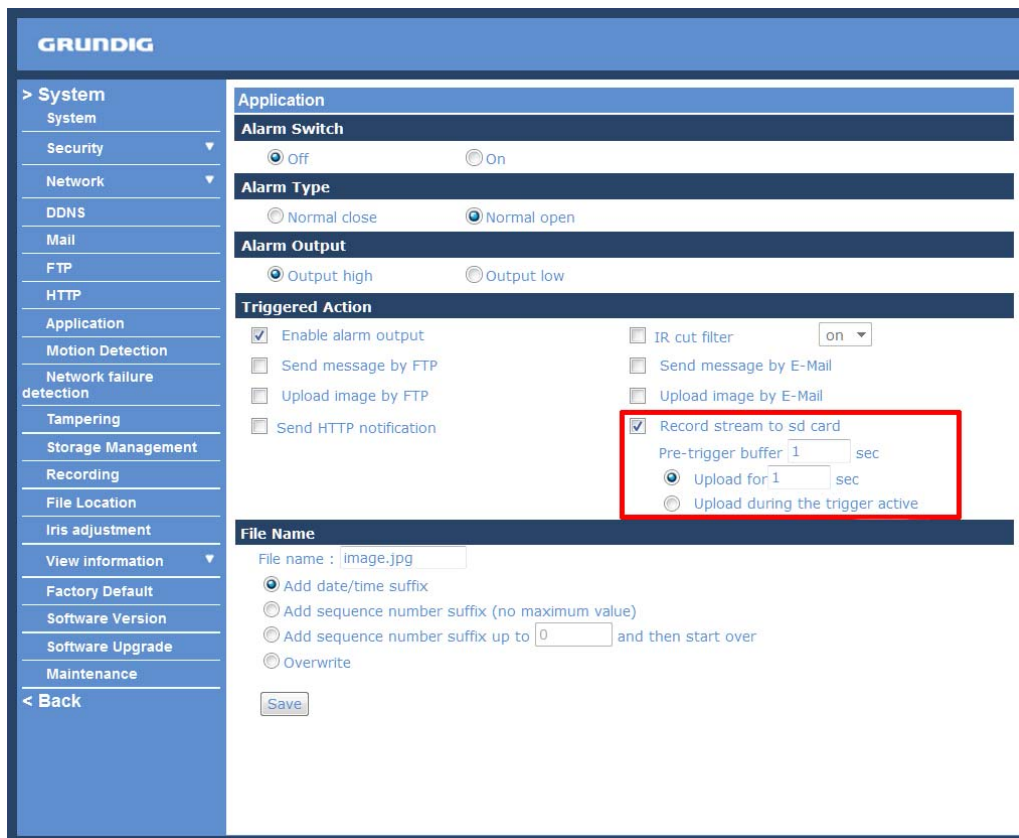
Check this item, select the destination HTTP address, and specify the parameters for event notifications when an <Alarm> is triggered. As soon as an alarm is triggered, the notification will be sent to the specified HTTP server.

For instance, if the custom parameter is set as "action=1&group=2", and the HTTP server's name is "http://192.168.1.200/admin.php", the notification will be sent to the HTTP server as "http://192.168.1.200/admin.php? Action=1&group=2" when an alarm is triggered.



- Record Stream to SD Card:

After selecting this item, the alarm-triggered recording will be saved on your Micro SD card.



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.

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:

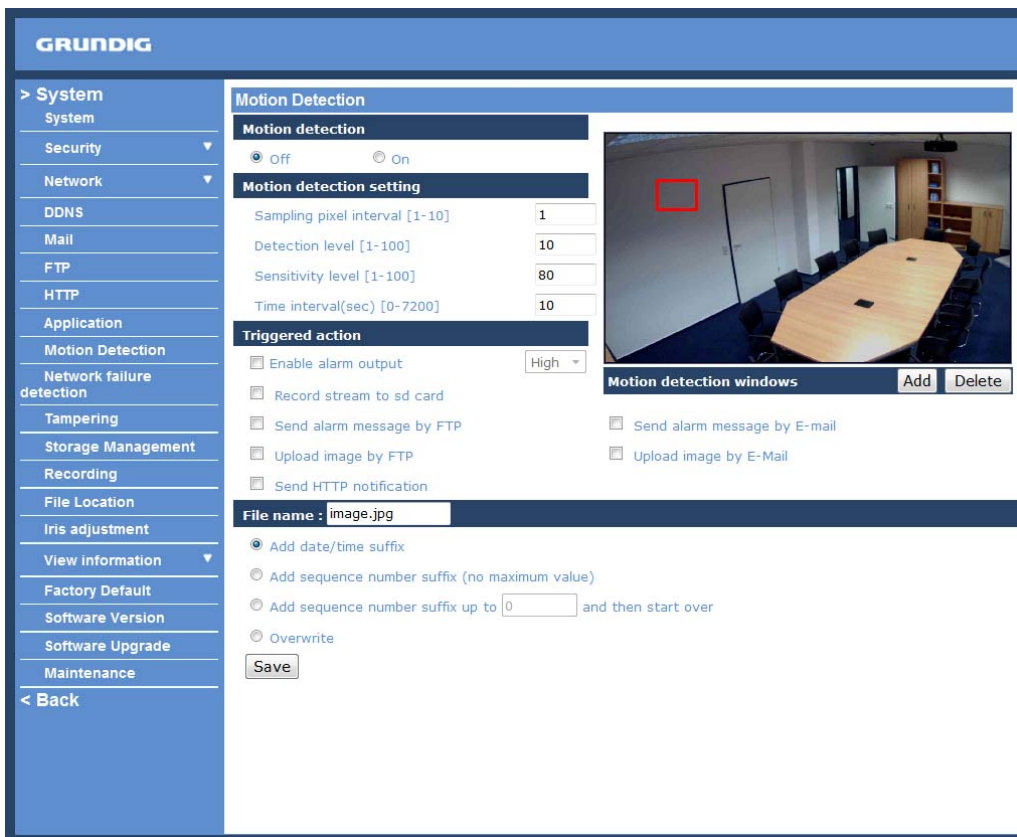
The original image in the FTP site will be overwritten with a static filename by the new uploaded file.

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

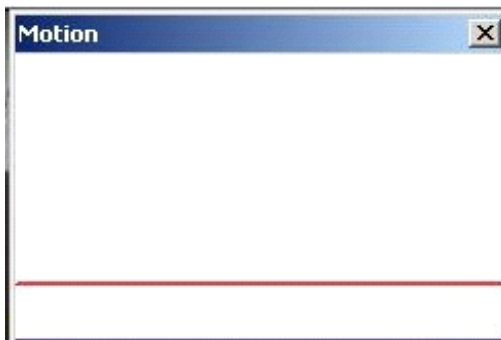
The Motion Detection function allows detecting suspicious motion and triggers alarms when motion volume in the detected area reaches/exceeds the determined sensitivity threshold value.



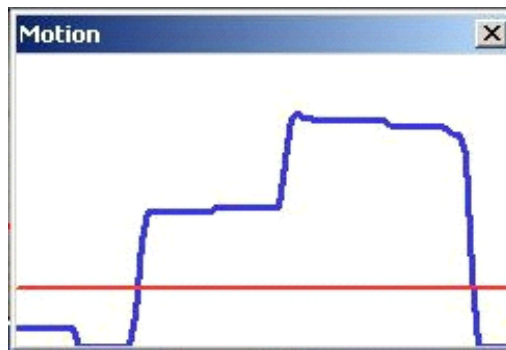
In the Motion Detection setting page a frame (Motion Detection Window) is displayed in the Live View Pane. The Motion Detection Window is for defining the motion detection area. To change the size of the Motion Detection Window, move the mouse cursor to the edge of the frame and draw it outward/inward.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



The detailed settings of Motion Detection are described as follows:

Motion Detection :

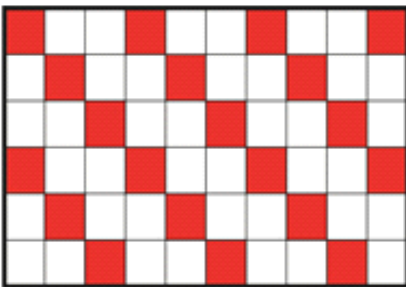
You will be able to turn the Motion Detection on/off in the System section "Motion Detection". The default setting is: Off.

Motion Detection Setting :

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

- Sampling pixel interval [1-10]:

The default value is 1. If the value is set as 3, it means that within the detection region, the system will take one sampling pixel for every 3 pixels by each row and each column (please refer to the figure below).



- 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) :

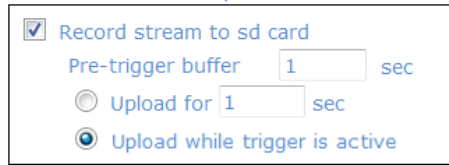
The Administrator can specify alarm actions that will take place when the alarm is triggered. All options are listed as follows:

- 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.



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.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.13. 'Recording (on Camera)' for further details.

- Send Alarm Message by FTP:

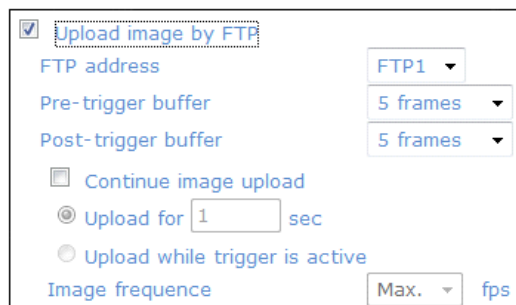
The Administrator can choose to send an alarm message by FTP when a motion is detected.

- Send Alarm Message by E-Mail:

The Administrator can choose to send an alarm message 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.



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 20 frames.

On the other hand, the <Post-trigger buffer> is for uploading a certain amount of images after the alarm input is triggered. The post-trigger buffer time range is from 1 to 20 frames.

Check the box <Continue image upload> to upload the triggered images during a certain time or keep uploading until the trigger is off.

- Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to the FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds.

- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

- 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.

Upload image by E-Mail
E-Mail address: E-Mail 1
Pre-trigger buffer: 5 frames
Post-trigger buffer: 5 frames
 Continue image upload
 Upload for 1 sec
 Upload while trigger is active
Image frequency: Max. fps

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 20 frames.

On the other hand, the <Post-trigger buffer> is for uploading a certain amount of images after the alarm input is triggered. The post-trigger buffer time range is from 1 to 20 frames.

Check the box <Continue image upload> to upload the triggered images during a certain time or keep uploading until the trigger is off.

- Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to the FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds.

- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

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

- Send HTTP notification:

Check this item, select the destination HTTP address, and specify the parameters for event notifications when <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://192.168.1.200/admin.php", the notification will be sent to the HTTP server as "http://192.168.1.200/admin.php? Action=1&group=2" when an alarm is triggered.

Send HTTP notification
HTTP address: HTTP1
Custom parameters: []

File Name :

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

Save :

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

9.10. Network Failure Detection

This function is used to detect network failure that might happen during camera operation.



Detection Switch :

Here you can turn the Network Failure Detection on and off.

Detection Type :

Here you can set an IP address that should be pinged in order to detect network failure. Please also set the interval (in minutes) for this ping.

Triggered Action (Multi-option) :

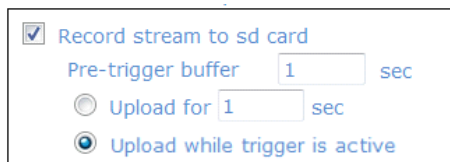
The Administrator can specify alarm actions that will take place when motion is detected. All options are listed as follows:

- Enable Alarm Output:

Check this item and select the predefined type of alarm output to enable alarm relay output when network failure 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 Network Failure is detected.



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.

- 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 FTP

FTP address: FTP1

Pre-trigger buffer: 5 frames

Post-trigger buffer: 5 frames

Continue image upload

Upload for 1 sec

Upload while trigger is active

Image frequency: Max. fps

NOTE: Please make sure that the local recording (with Micro SD/SDHC card) is activated so that this function can be implemented. See section 9.13. 'Recording (on Camera)' for further details.

- Send Alarm Message by FTP:

The Administrator can select whether to send an alarm message by FTP when Network Failure is detected.

- Send Alarm Message by E-Mail:

The Administrator can choose to send an alarm message by E-Mail when Network Failure is detected.

9.11. Tampering

The Tampering Alarm function helps the IP Camera against tampering 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).

GRUNDIG

> System

System

Security

Network

DDNS

Mail

FTP

HTTP

Application

Motion Detection

Network failure detection

Tampering

Storage Management

Recording

File Location

Iris adjustment

View information

Factory Default

Software Version

Software Upgrade

Maintenance

< Back

Tampering Alarm

Tampering Alarm

Off On

Tampering Duration

Minimum duration: 20 sec

Triggered Action

Enable alarm output: high

Record stream to sd card

Send message by FTP

Send message by E-Mail

Upload image by FTP

Upload image by E-Mail

Send HTTP notification

File Name

File name: image.jpg

Add date/time suffix

Add sequence number suffix (no maximum value)

Add sequence number suffix up to 0 and then start over

Overwrite

Save

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) :

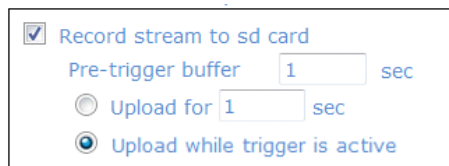
The Administrator can specify alarm actions that will take place when tampering is detected. All options are listed as follows:

- 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 Tampering is detected.



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.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.13. 'Recording (on Camera)' for further details.

- Send Alarm Message by FTP:

The Administrator can select whether to send an alarm message by FTP when Tampering is detected.

- Send Alarm Message by E-Mail:

The Administrator can choose to send an alarm message by E-Mail when Tampering is detected.

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 20 frames.

On the other hand, the <Post-trigger buffer> is for uploading a certain amount of images after the alarm input is triggered. The post-trigger buffer time range is from 1 to 20 frames.

Check the box <Continue image upload> to upload the triggered images during a certain time or keep uploading until the trigger is off.

- Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to the FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds.

- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

- 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.

Upload image by E-Mail
E-Mail address: E-Mail 1
Pre-trigger buffer: 5 frames
Post-trigger buffer: 5 frames
 Continue image upload
 Upload for 1 sec
 Upload while trigger is active
Image frequency: Max. fps

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 20 frames.

On the other hand, the <Post-trigger buffer> is for uploading a certain amount of images after the alarm input is triggered. The post-trigger buffer time range is from 1 to 20 frames.

Check the box <Continue image upload> to upload the triggered images during a certain time or keep uploading until the trigger is off.

- Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to the FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds.

- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

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

- Send HTTP notification:

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

For instance, if the custom parameter is set as "action=1&group=2", and the HTTP server's name is "http://192.168.1.200/admin.php", the notification will be sent to the HTTP server as "http://192.168.1.200/admin.php? Action=1&group=2" when an alarm is triggered.

Send HTTP notification
HTTP address: HTTP1
Custom parameters: []

File Name :

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

Save :

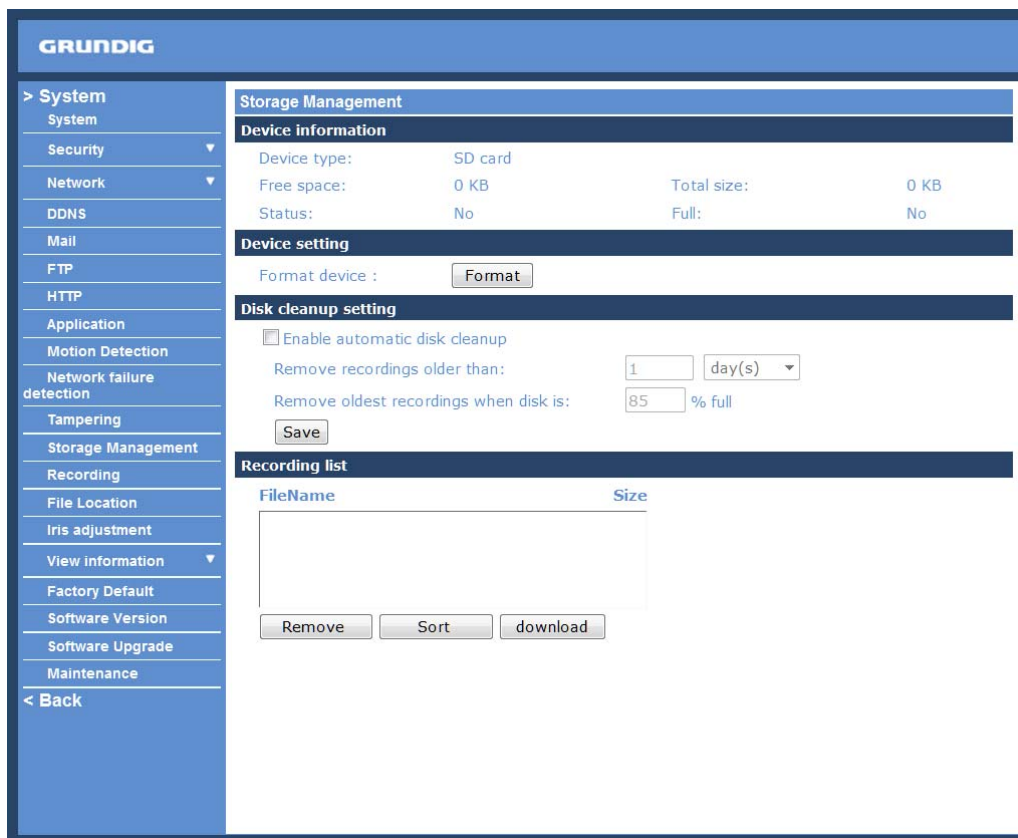
Click the Save button to save all the Tampering Alarm settings mentioned above.

9.12. Storage Management (on Camera)

Users can store local recordings on a Micro SD/SDHC card of up to 32 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 9.13. 'Recording (on Camera)') 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 device and was later transferred to another device 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 modus is set to "Always" and at the same time the event recording (when a motion detection or an alarm takes place) is also turned on, in this case, when an event occurs, the event will be recorded first, afterwards the camera will return to normal recording mode.

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

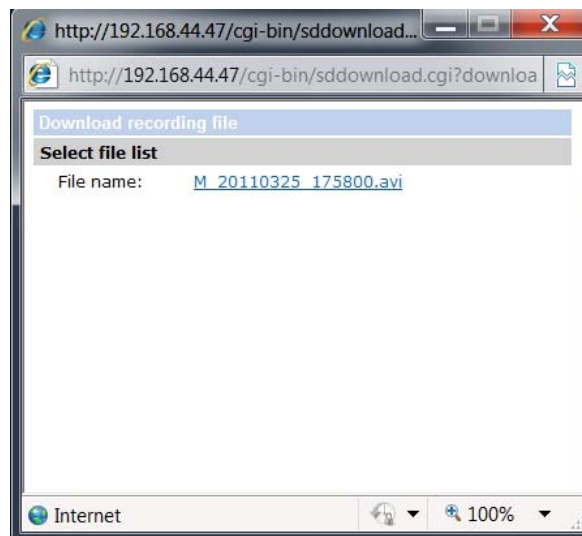
- Sort:

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

NOTE: The capital letters (A, M or R) appearing in the very beginning of a name denote the sort of the recording: A stands for Alarm, M stands for Motion and R stands for regular recording.

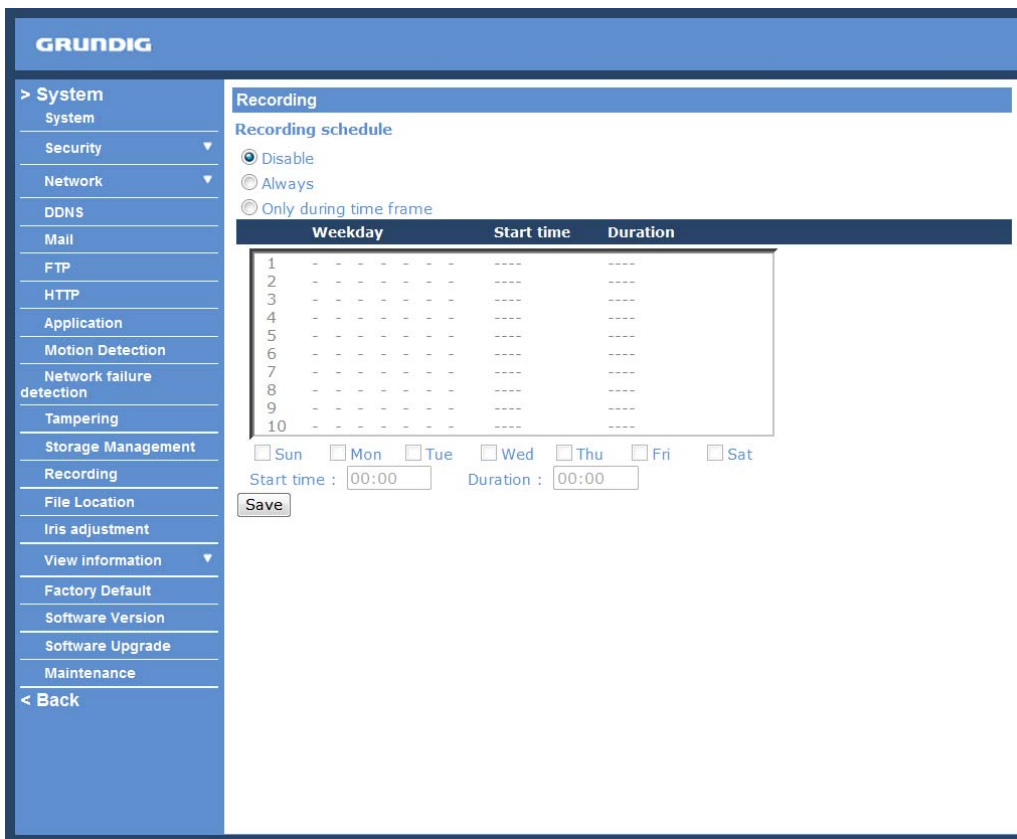
- Download:

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.



9.13. Recording (on Camera)

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



Activating Micro SD/SDHC Card Recording :

Two types of schedule mode are offered: "Always" and "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.

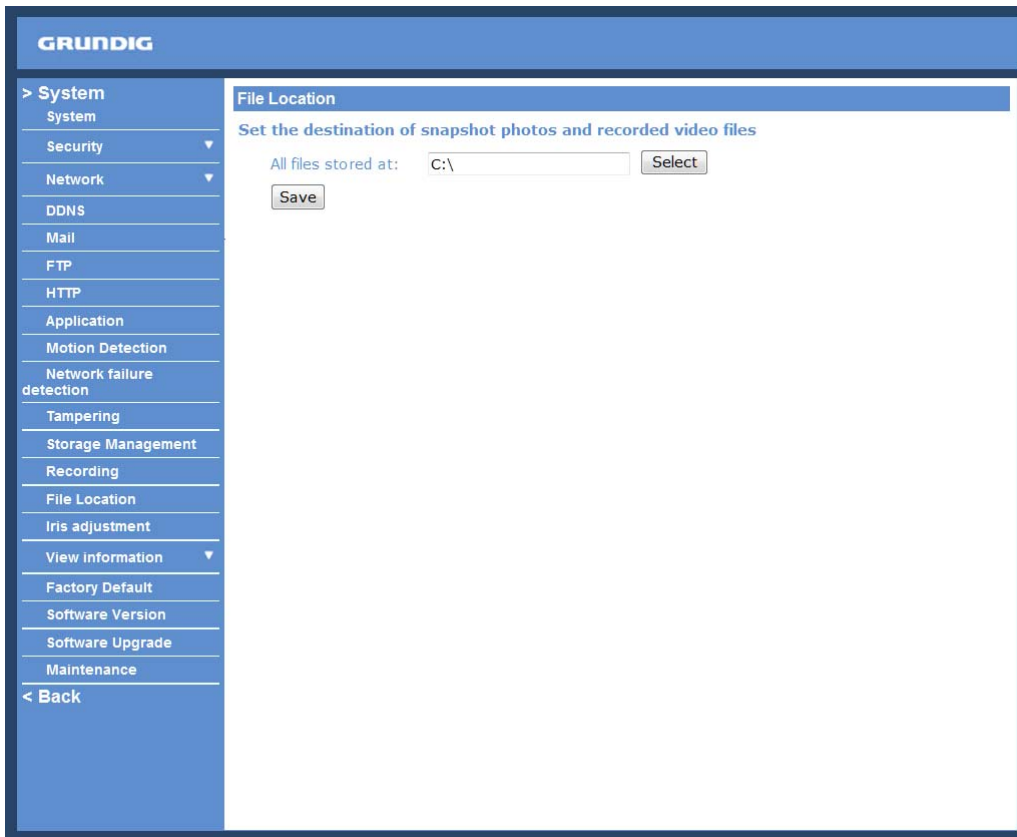
Terminating Micro SD/SDHC Card Recording :

Select "Disable" to terminate the recording function.

9.14. File Location (on PC)

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 designated location.

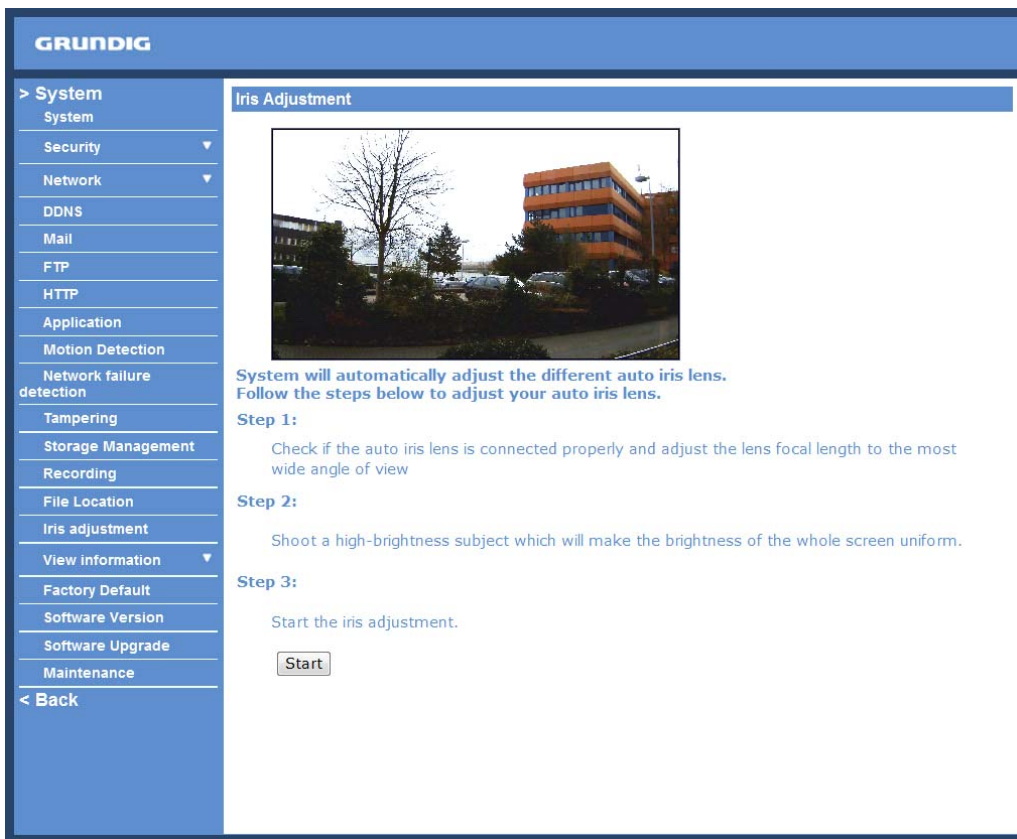
NOTE: Please make sure the selected file path contains valid characters such as letters and numbers.



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).

9.15. Iris Adjustment

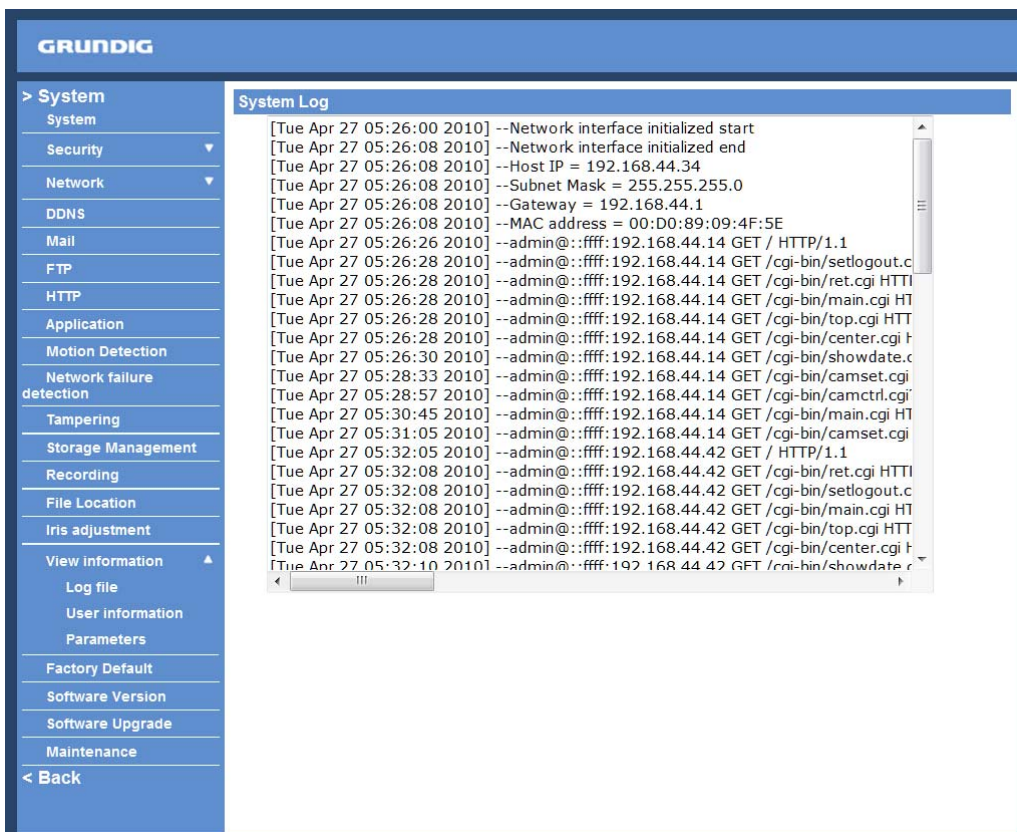
For users who use an auto-iris lens, when it is required to undertake an iris adjustment, please refer to the iris adjustment procedure in the sub-menu "Iris Adjustment" to adjust the iris.



The screenshot shows the Grundig web interface. On the left is a navigation menu with options like System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion Detection, Network failure detection, Tampering, Storage Management, Recording, File Location, Iris adjustment, View information, Factory Default, Software Version, Software Upgrade, Maintenance, and Back. The main content area is titled "Iris Adjustment" and features a photograph of a building. Below the photo, the text reads: "System will automatically adjust the different auto iris lens. Follow the steps below to adjust your auto iris lens." The steps are: Step 1: Check if the auto iris lens is connected properly and adjust the lens focal length to the most wide angle of view. Step 2: Shoot a high-brightness subject which will make the brightness of the whole screen uniform. Step 3: Start the iris adjustment. A "Start" button is visible at the bottom of the steps.

9.16. 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 shows the Grundig web interface with the "System Log" menu item selected. The log content is displayed in a scrollable window. The log entries include: [Tue Apr 27 05:26:00 2010] --Network interface initialized start, [Tue Apr 27 05:26:08 2010] --Network interface initialized end, [Tue Apr 27 05:26:08 2010] --Host IP = 192.168.44.34, [Tue Apr 27 05:26:08 2010] --Subnet Mask = 255.255.255.0, [Tue Apr 27 05:26:08 2010] --Gateway = 192.168.44.1, [Tue Apr 27 05:26:08 2010] --MAC address = 00:D0:89:09:4F:5E, [Tue Apr 27 05:26:26 2010] --admin@:ffff:192.168.44.14 GET / HTTP/1.1, [Tue Apr 27 05:26:28 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/setlogout.c, [Tue Apr 27 05:26:28 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/ret.cgi HTTP, [Tue Apr 27 05:26:28 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/main.cgi HT, [Tue Apr 27 05:26:28 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/top.cgi HTT, [Tue Apr 27 05:26:28 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/center.cgi f, [Tue Apr 27 05:26:30 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/showdate.c, [Tue Apr 27 05:28:33 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/camset.cgi, [Tue Apr 27 05:28:57 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/camctrl.cgi, [Tue Apr 27 05:30:45 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/main.cgi HT, [Tue Apr 27 05:31:05 2010] --admin@:ffff:192.168.44.14 GET /cgi-bin/camset.cgi, [Tue Apr 27 05:32:05 2010] --admin@:ffff:192.168.44.42 GET / HTTP/1.1, [Tue Apr 27 05:32:08 2010] --admin@:ffff:192.168.44.42 GET /cgi-bin/ret.cgi HTTP, [Tue Apr 27 05:32:08 2010] --admin@:ffff:192.168.44.42 GET /cgi-bin/setlogout.c, [Tue Apr 27 05:32:08 2010] --admin@:ffff:192.168.44.42 GET /cgi-bin/main.cgi HT, [Tue Apr 27 05:32:08 2010] --admin@:ffff:192.168.44.42 GET /cgi-bin/top.cgi HTT, [Tue Apr 27 05:32:08 2010] --admin@:ffff:192.168.44.42 GET /cgi-bin/center.cgi f, [Tue Apr 27 05:32:10 2010] --admin@:ffff:192.168.44.42 GET /cgi-bin/showdate.c

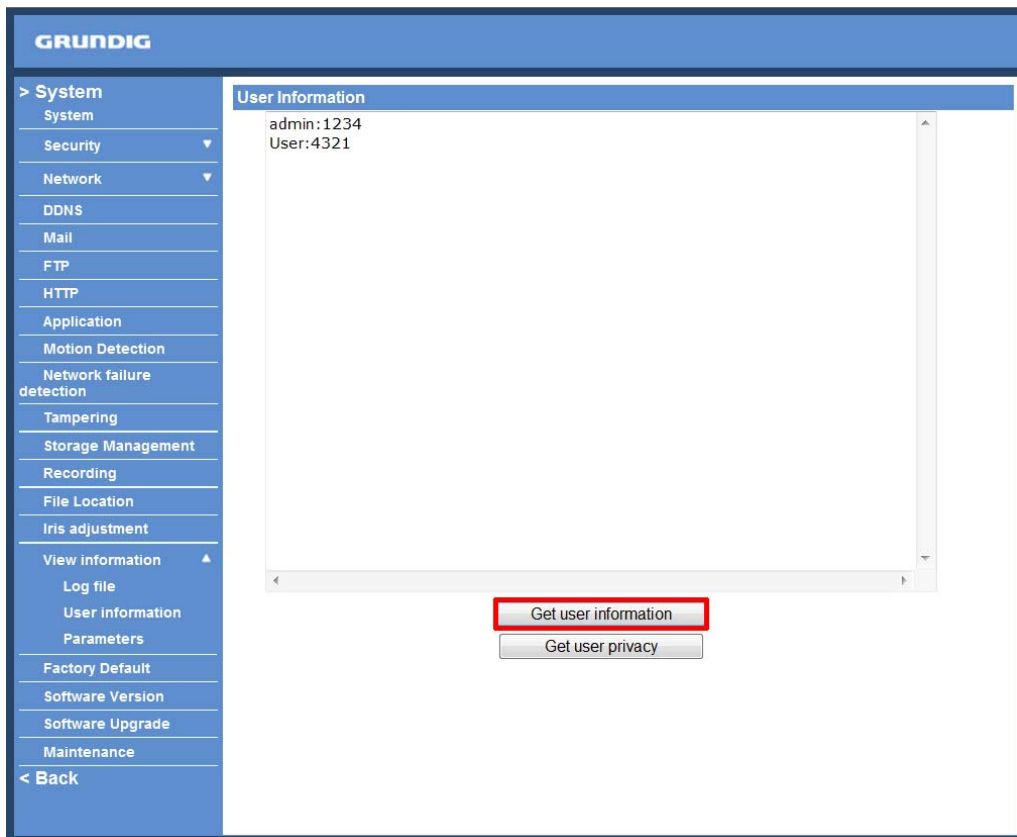
9.17. View User Information

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

View User Login Information :

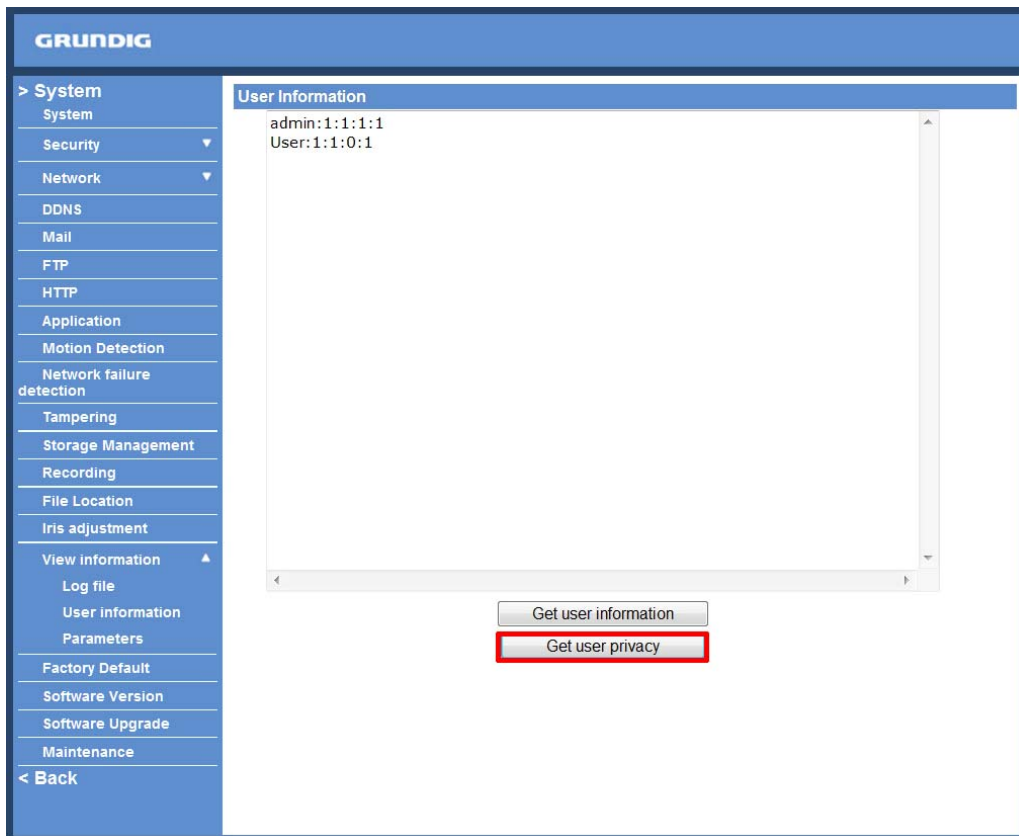
All the users in the network will be listed in the "User Information" zone, as shown below. The picture below shows: User: 4321

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

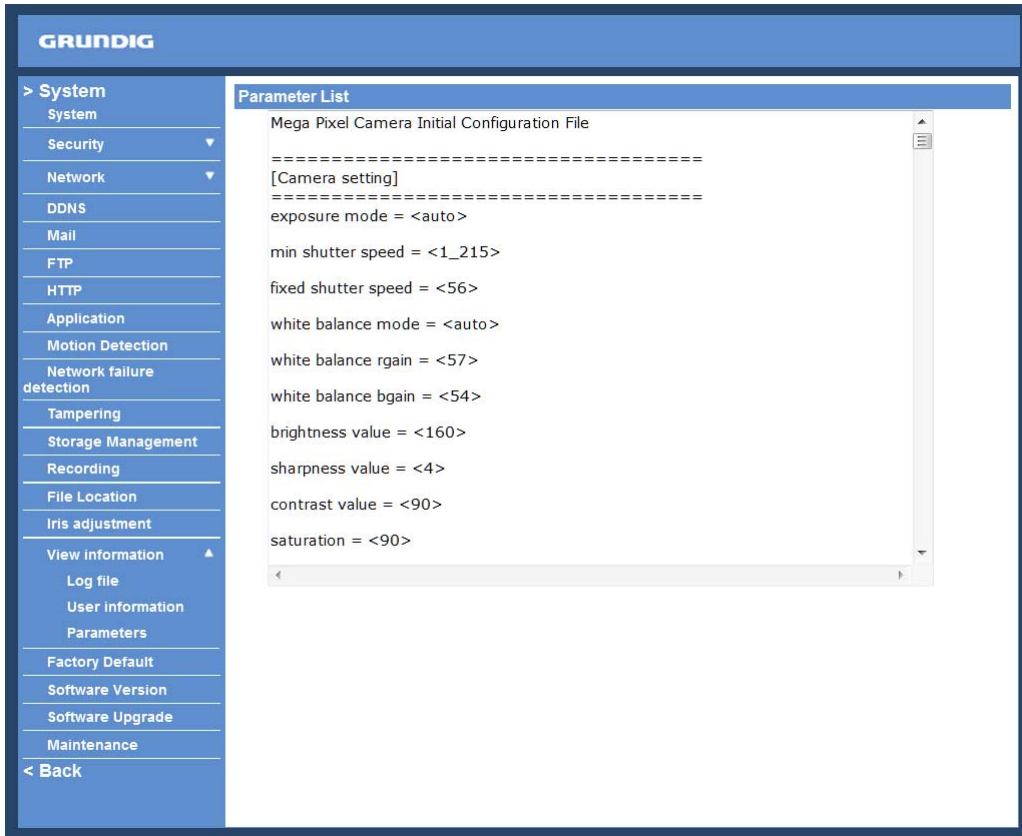
1:1:0:1 = I/O access : Camera control : Talk : Listen (see 9.2. Security)

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



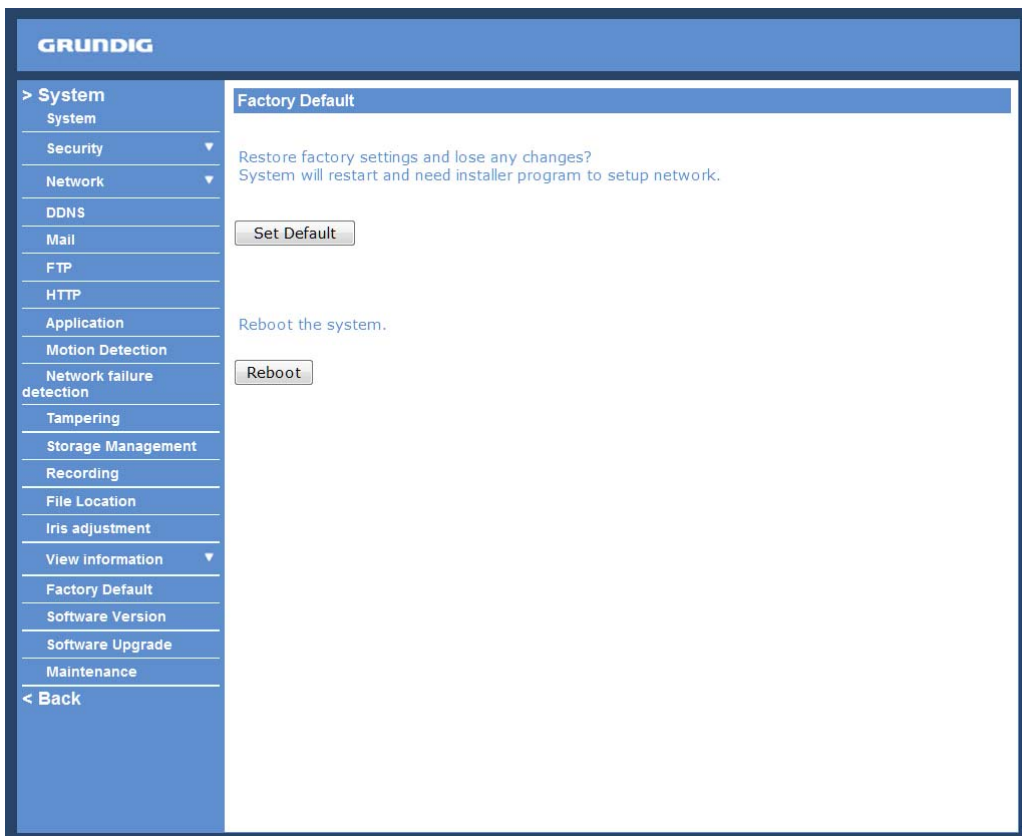
9.18. View Parameters

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



9.19. Factory Default

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



Set Default :

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

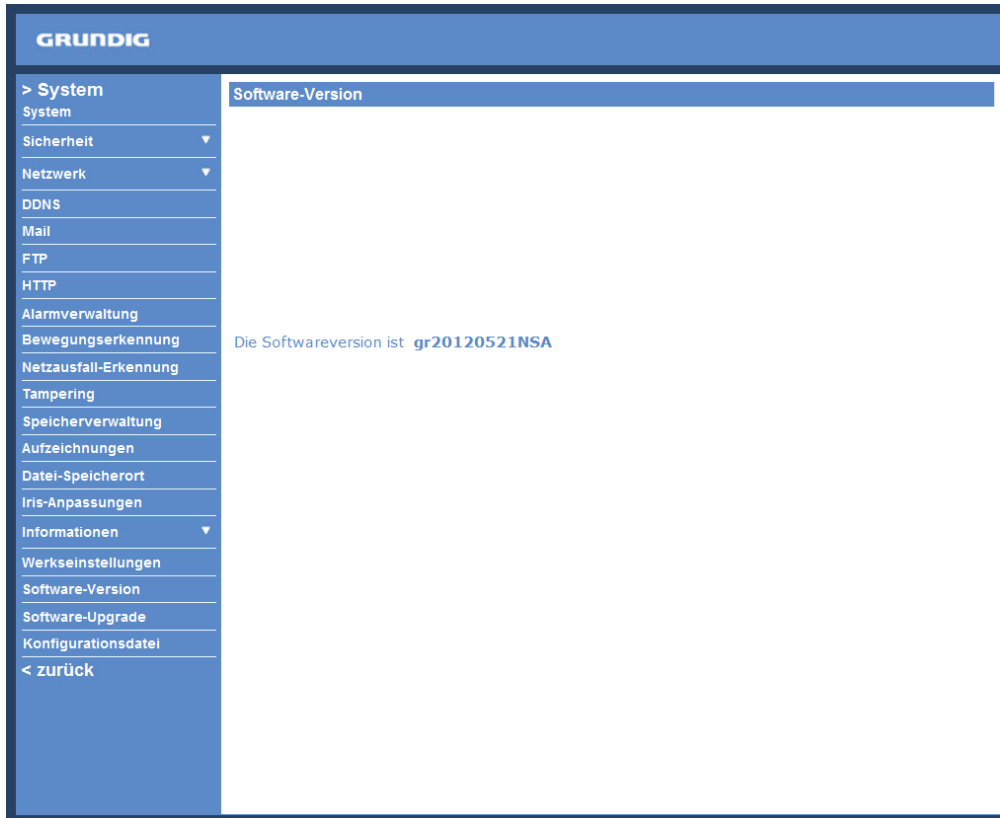
NOTE: The IP address will also be restored to default (192.168.1.1).

Reboot :

When you click on the “Reboot” button, the system will restart without changing the current settings.

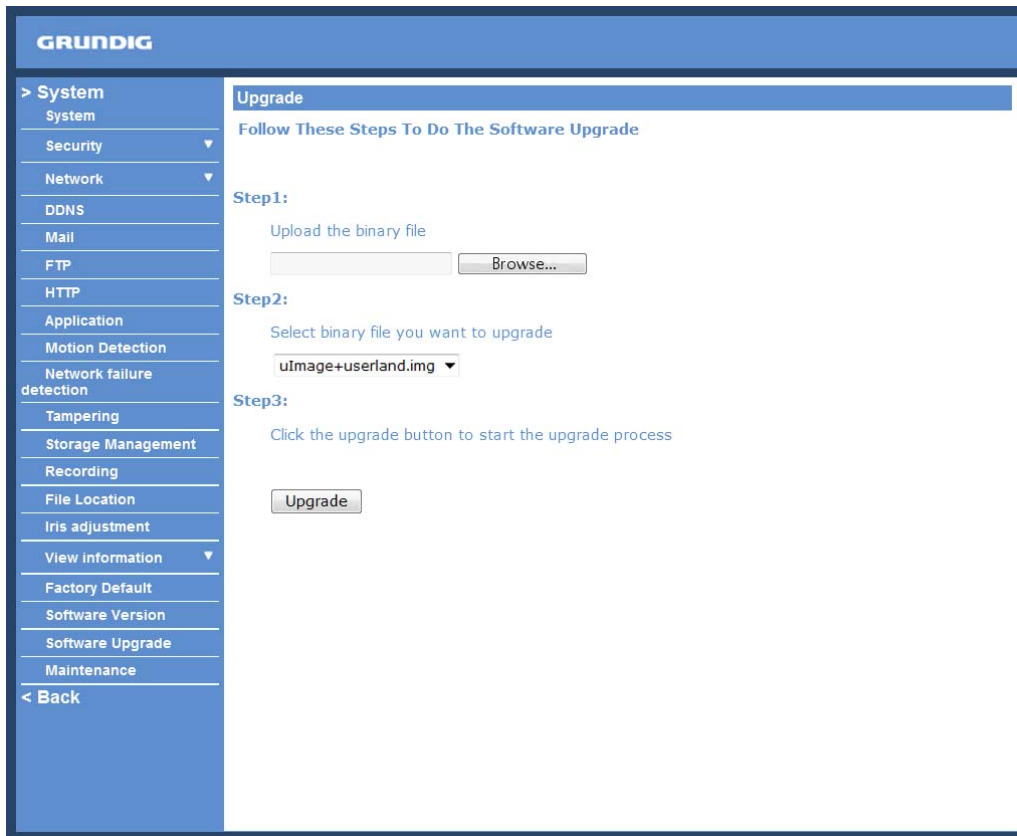
9.20. Software Version

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



9.21. Software Upgrade

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



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 on “Browse” and select the following binary file to be uploaded: ulmage+userland.

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 “ulmage+userland”.

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.

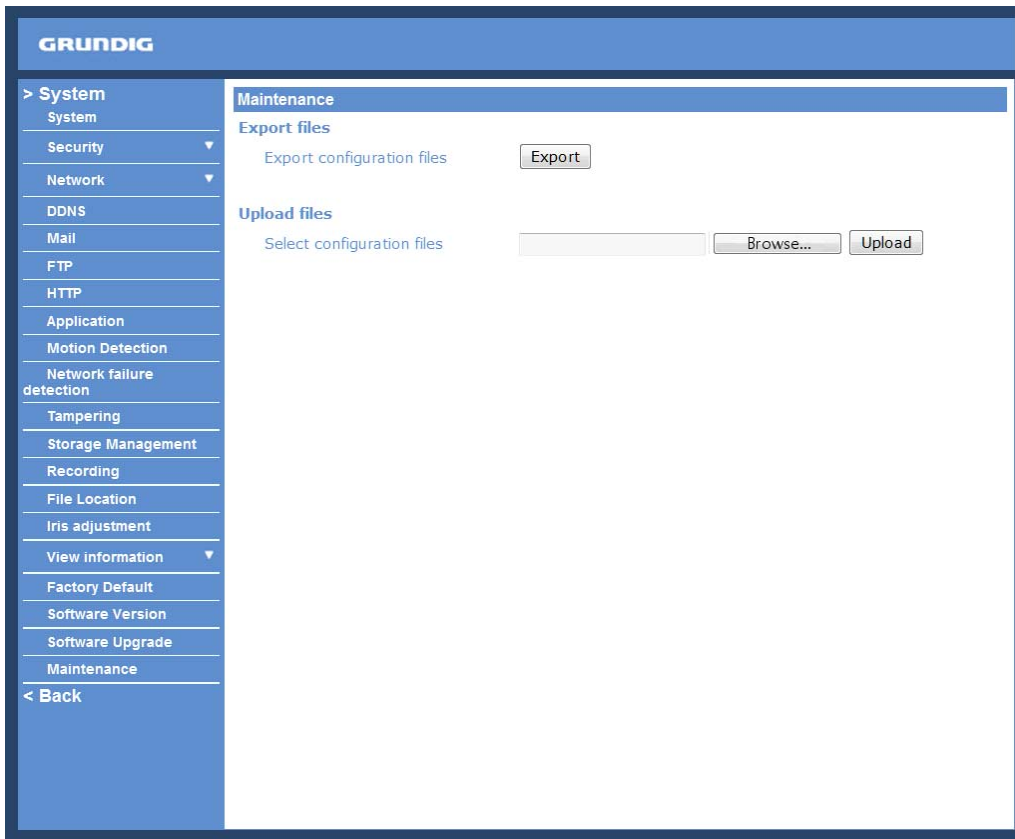
Step 4: Close the video browser.

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 the IP Camera, and then allow the automatic download of the GRUNDIG Viewer.

9.22. Maintenance

Users can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the IP Camera. This is especially convenient if you want to have the same configuration for multiple cameras.



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

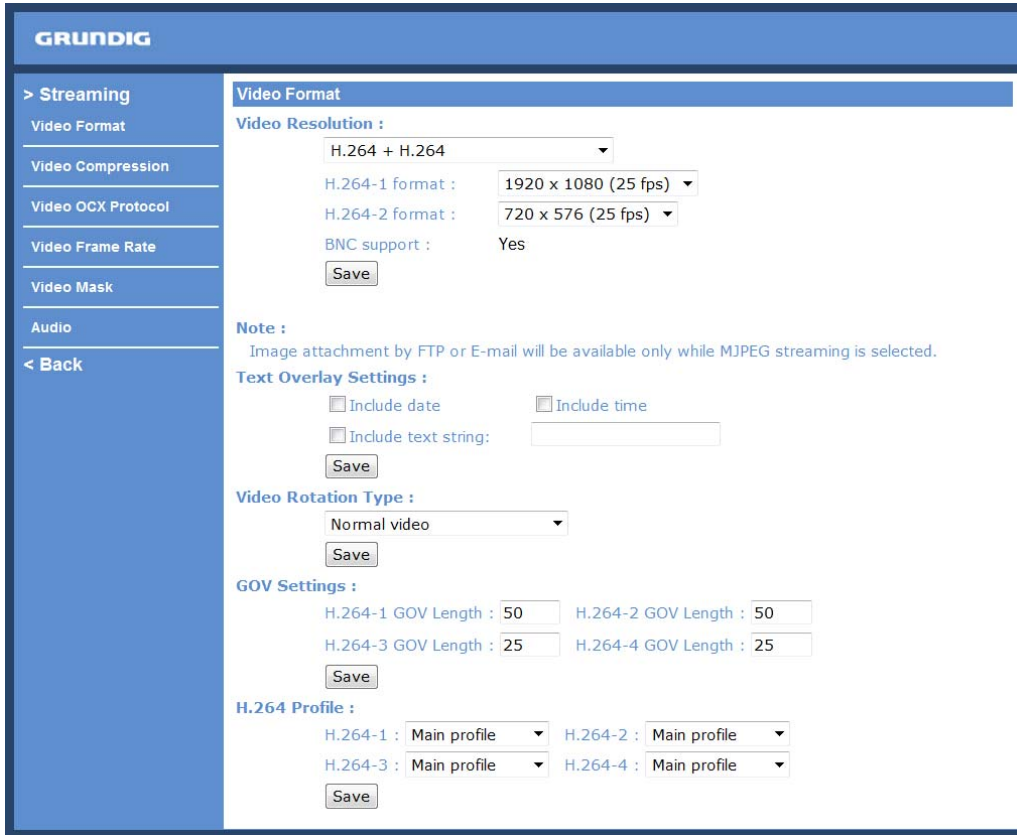
NOTE: The cameras need to have the same software version to upload the configuration file.

10. Streaming Settings

10.1. Video Format

Video Resolution :

Under the Video Resolution section, the available video resolution formats include MJPEG and H.264. Please refer to Chapter 6. Video Resolution Setup for combination details.



The screenshot shows the Grundig Streaming Settings interface. On the left is a navigation menu with options: > Streaming, Video Format, Video Compression, Video OCX Protocol, Video Frame Rate, Video Mask, Audio, and < Back. The main content area is titled 'Video Format' and contains the following settings:

- Video Resolution :** A dropdown menu set to 'H.264 + H.264'. Below it are two more dropdowns: 'H.264-1 format : 1920 x 1080 (25 fps)' and 'H.264-2 format : 720 x 576 (25 fps)'. A 'BNC support : Yes' label is present, followed by a 'Save' button.
- Note :** A text note stating 'Image attachment by FTP or E-mail will be available only while MJPEG streaming is selected.'
- Text Overlay Settings :** Three checkboxes: 'Include date', 'Include time', and 'Include text string:'. The 'Include text string' checkbox is followed by an empty text input field. A 'Save' button is below.
- Video Rotation Type :** A dropdown menu set to 'Normal video', followed by a 'Save' button.
- GOV Settings :** Four input fields for GOV Length: 'H.264-1 GOV Length : 50', 'H.264-2 GOV Length : 50', 'H.264-3 GOV Length : 25', and 'H.264-4 GOV Length : 25'. A 'Save' button is below.
- H.264 Profile :** Four dropdown menus for profiles: 'H.264-1 : Main profile', 'H.264-2 : Main profile', 'H.264-3 : Main profile', and 'H.264-4 : Main profile'. A 'Save' button is below.

Click on "Save" to confirm the setting.

Text Overlay Settings :

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

Click "Save" to confirm the Text Overlay setting.

Video Rotation Type :

Users can change the video display type if necessary. The selectable video rotation types include Normal video, Flip video, Mirror video, 90 degree counter-/clockwise and 180 degree rotation. Differences between these types are illustrated below.

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



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



The following are descriptions of different video rotation types.

- Flip video:

If you select <Flip video>, the image will be rotated horizontally.

- Mirror video:

If you select <Mirror video>, the image will be rotated vertically.

- 90 degree counter-/clockwise:

Selecting <90 degree counter-/clockwise> will inverse the image 90° counter-/clockwise. The image will only be shown with the right proportions in "Fullscreen View". Click on the Fullscreen Button (third button from the left) on the main page to enlarge the image and double-click to go back to "Normal View".

- 180 degree rotation:

Selecting the <180 Degree rotation> will inverse the image 180° counter-/clockwise.

Click “Save” to confirm the setting.

GOV Settings :

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

This camera provides three H.264 streaming formats to meet the requirements from viewing devices, the surveillance system, and the network condition of the application and installation environment.

H.264 Baseline profile: Standard Efficiency Encoding Format

H.264 Main profile: Good Efficiency Encoding Format

H.264 High profile: High Efficiency Encoding Format

10.2. Video Compression

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

MJPEG compression setting (MJPEG Q (Quality) factor):

A higher value implies higher bit rates and a higher visual quality. The default setting is 35; the setting range is from 1 to 70.

Click "Save" to confirm the setting.

H.264-1 / H.264-2 / H.264-3 / H.264-4 bit rate:

The default setting of H.264-1 is 4096 kbps and of H.264-2/H.264-3/H.264-4 is 1024 kbps. The setting range for H.264-1 is from 64 to 8192 kbps and for H.264-2/H.264-3/H.264-4 it is from 64 to 2048 kbps.

Click "Save" to confirm the setting.

The screenshot shows the Grundig Video Compression settings page. On the left is a navigation menu with options: > Streaming, Video Format, Video Compression (selected), Video OCX Protocol, Video Frame Rate, Video Mask, Audio, and < Back. The main content area is titled 'Video Compression' and contains several 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 : 1024 kbit/s [Save]
- H.264-3 Compression setting :** H264-3 bit rate : 1024 kbit/s [Save]
- H.264-4 Compression setting :** H264-4 bit rate : 1024 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, enable H.264-3 CBR mode, enable H.264-4 CBR mode [Save]

Compression information setting :

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

Click "Save" to confirm the setting.

CBR mode setting :

The CBR (Constant Bit Rate) mode can become the preferred bit rate mode if the available bandwidth 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.

10.3. Video OCX Protocol

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

Video OCX protocol 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

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

The screenshot displays the Grundig web interface for video settings. On the left is a blue sidebar with a menu: '> Streaming', 'Video Format', 'Video Compression', 'Video OCX Protocol', 'Video Frame Rate' (highlighted), 'Video Mask', 'Audio', and '< Back'. The main content area has a blue header 'Video Frame Rate'. Below it are five sections, each with a title and a text input field containing '25', followed by a 'Save' button:

- MJPEG Frame Rate Setting:** MJPEG frame rate : 25 [Save]
- H.264-1 Frame Rate Setting:** H.264-1 frame rate : 25 [Save]
- H.264-2 Frame Rate Setting:** H.264-2 frame rate : 25 [Save]
- H.264-3 Frame Rate Setting:** H.264-3 frame rate : 25 [Save]
- H.264-4 Frame Rate Setting:** H.264-4 frame rate : 25 [Save]

MJPEG / H.264-1 / H.264-2 / H.264-3 / H.264-4 Frame Rate:

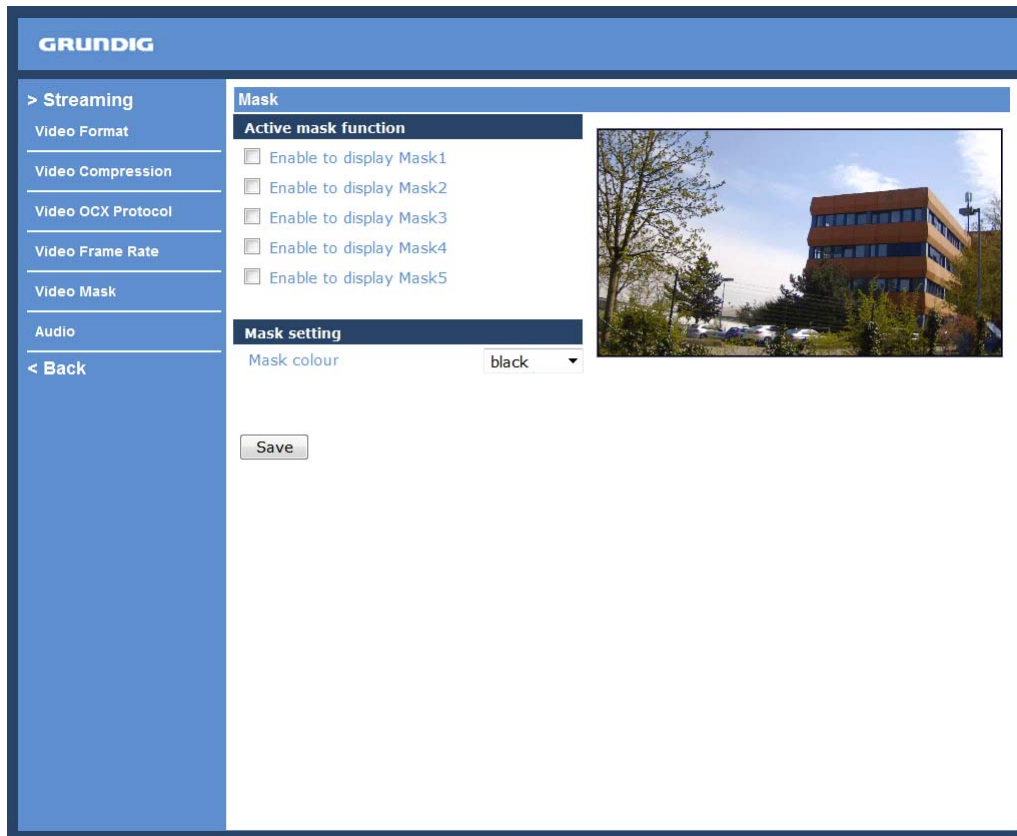
The default setting of MJPEG/H.264-1/H.264-2/H.264-3/H.264-4 Frame Rate is 25 fps. The setting range is from 1 to 25.

Click on <Save> to confirm the setting.

NOTE: A lower frame rate will decrease video smoothness.

10.5. Video Mask

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



Active Mask Function :

- Add a Mask:

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

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

- Cancel a mask:

If you uncheck the checkbox of the Video Mask that is meant to be deleted, the selected mask will disappear from the Live Video pane instantly.

Mask Setting :

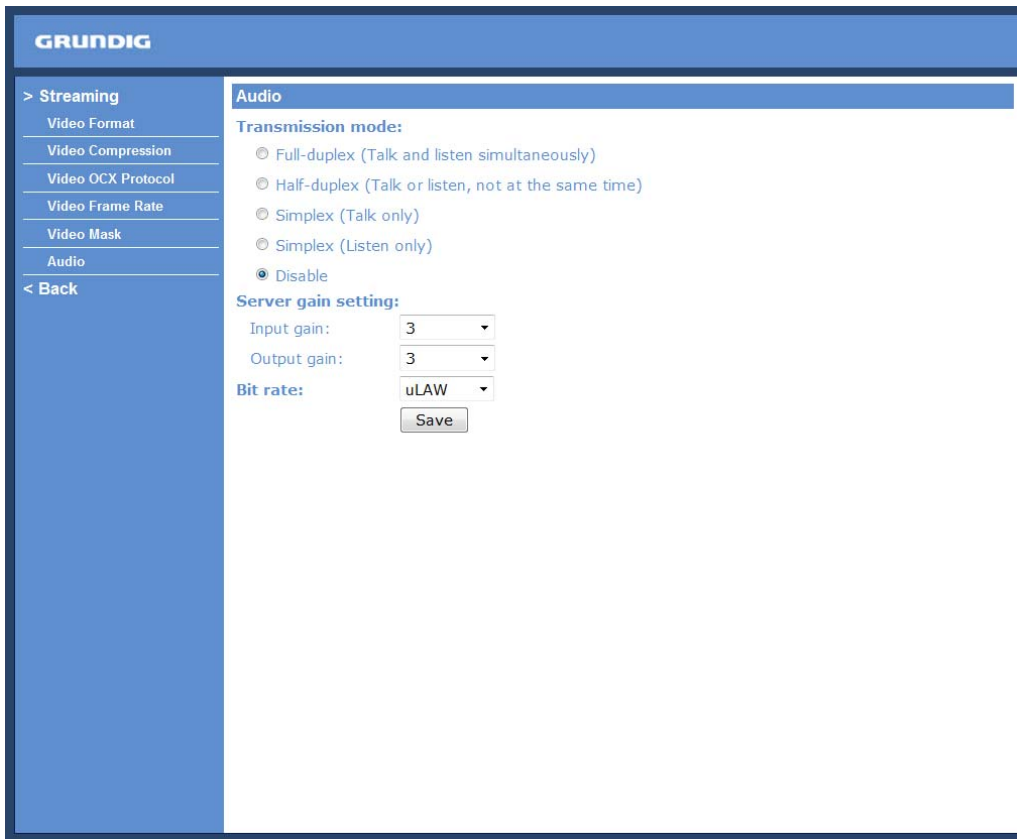
- Mask colour:

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

Click on "Save" to confirm the setting.

10.6. Audio (Audio and Bit Rate Settings)

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".

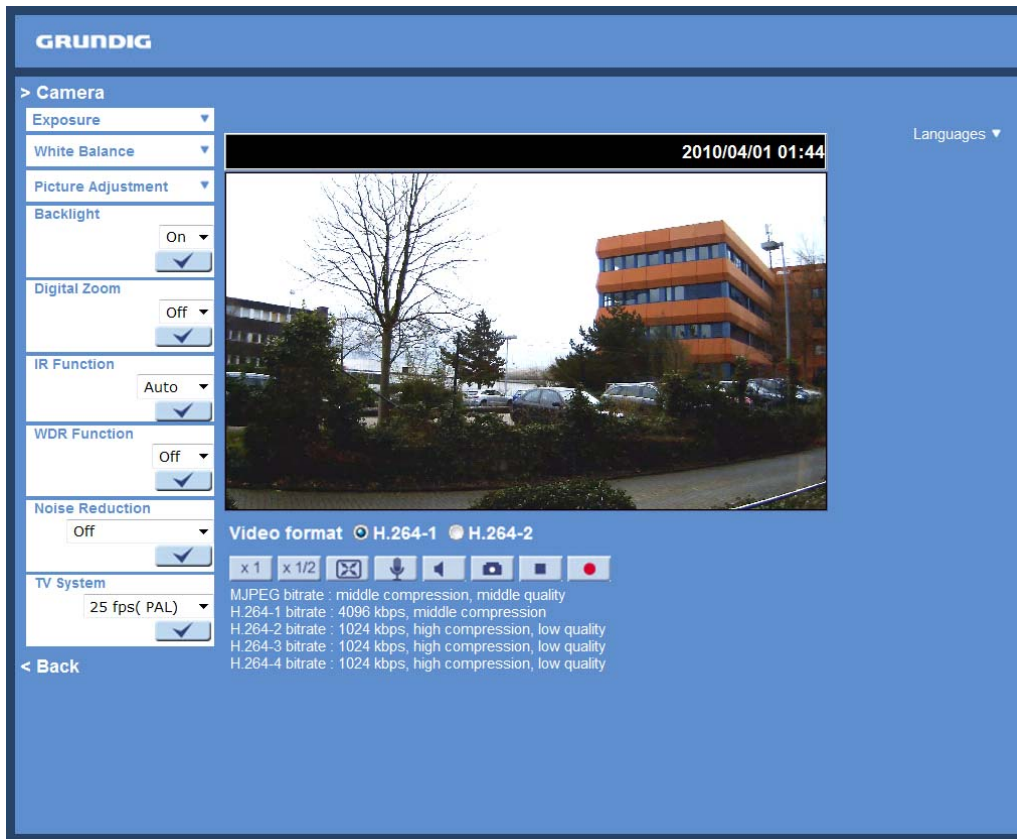
Bit Rate :

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.

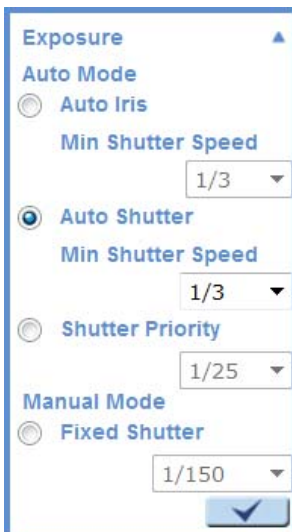
11. Camera Settings

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



11.1. Exposure Setting

Display of the Exposure pull-down menu:



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

Auto Mode :

- Auto Iris Mode:

In this mode, the exposure gives priority to the auto iris. The minimum shutter speed can be set from 1/1.5 to 1/25 sec. AGC (Auto Gain Control) will function automatically according to the light conditions of the subject.

- Auto Shutter Mode:

This function is used to control the shutter speed and to adjust the iris automatically according to the light intensity. It is also effective if a fixed iris lens is being used. The minimum shutter speed range is configurable from 1/1.5 to 1/425 sec.

- Shutter Priority Mode:

This function is to set the shutter speed to a specified speed. The range is configurable from 1/25 to 1/425 sec.

Manual Mode:

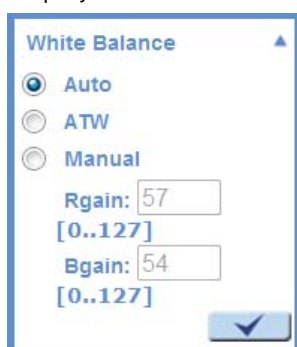
- Fixed Shutter Mode:

In this mode, a fixed shutter speed can be selected from the drop-down menu. The shutter speed range is from 1/10000 to 1/1.5 sec. With 18 options depending on the camera model. Users can choose a suitable shutter speed according to the environmental illumination.

Click on < ✓ > to confirm the new setting.

11.2. White Balance Setting

Display of the White Balance pull-down menu:



To display natural colours, the camera needs to know the reference colour temperature of the light source. Based on this reference colour temperature the camera will calculate the correct values for all colours. The camera can perform a measurement by itself or the user can set up the reference colour temperature manually. The scale unit of the colour temperature is Kelvin [K]. The following list shows the colour temperature of some light sources for reference.

Users can select one of the White Balance Control modes according to the operating environment.

Light Sources :

Cloudy Sky (Colour Temperature: 6,000 to 8,000 K)

Noon Sun and Clear Sky (Colour Temperature: 6,500 K)

Household Lighting (Colour Temperature: 2,500 to 3,000 K)

75-watt Bulb (Colour Temperature: 2,820 K)

Candle Flame (Colour Temperature: 1,200 to 1,500 K)

Auto Mode :

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

ATW Mode (Auto Tracking White Balance) :

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

Manual Mode :

In this mode, users can change the White Balance value manually. Users can select a number between 0 ~ 127 in the "R-Gain/B-Gain" item to gain the red/blue illuminant on the Live Video Pane.

Click on < ✓ > to confirm the new setting.

11.3. Picture Adjustment

Display of the Picture Adjustment pull-down menu:



Brightness:

The users can adjust the image's brightness by adjusting the item. Please select a number from the range of -12 to +13. To increase the video brightness, select a bigger number.

Click on < ✓ > to confirm the new setting.

Sharpness:

Increasing the sharpness level can make the image look sharper. Please select a number from the range of +0 to +15. This function especially enhances the object's edges.

Click on < ✓ > to confirm the new setting.

Contrast:

The camera image contrast level is adjustable. Please choose from a range of -6 to +19.

Click on < ✓ > to confirm the new setting.

Saturation:

The camera image saturation level is adjustable. Please select from a range of -6 to +19.

Click on < ✓ > to confirm the new setting.

Hue:

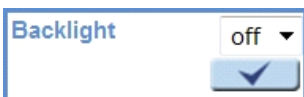
The camera image hue level is adjustable. Please select from a range of -12 to +13.

Click on < ✓ > to confirm the new setting.

11.4. Backlight Setting

Based on various lighting situations, users can turn the function of Backlight Compensation on or off to optimise the video quality. The default value of Backlight is: Off.

Click on < ✓ > to confirm the new setting.



11.5. Digital Zoom Setting

The camera's Digital Zoom is adjustable from x2 to x8.

Click on < ✓ > to confirm the new setting.



11.6. IR Function

With the IR cut filter, the Camera can still catch a clear image at night time or in low light conditions.



For these cameras the following IR function modes are provided:

Auto :

The camera switches automatically from Colour mode to Black & White mode and back without switching on the LEDs.

On :

The camera is always in B&W mode, the LEDs are always off.

Off :

The camera stays always in Colour mode.

Light Sensor Mode :

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

Light On Mode :

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

Light Off Mode :

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

Smart Mode:

The Smart Mode enhances the monochrome/night mode stability in ascenario where IR illumination is dominant. In this mode, when the external IR illuminator is turned on, the IR cut filter of the IP Camera will stay open (i.e. monochrome/night mode), preventing the camera from returning to colour/day mode when the IR illumination is dominant.

Additionally, the day/night IR switching mechanism will then depend on the ambient light level instead of the light sensor (Light sensor mode) on the IR LED module.

Click on < ✓ > to confirm the new setting.

11.7. WDR Function

The Wide Dynamic Range (WDR) function is for solving high contrast or changing light issues to improve the video display. The WDR is adjustable from Low, Mid to Hi. A higher level of WDR represents a wider dynamic range, so that the IP Camera can catch a greater scale of brightness.

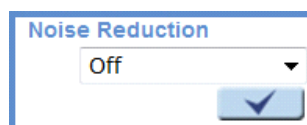
Click on < ✓ > to confirm the new setting.



11.8. Noise Reduction

The IP Camera provides multiple <Noise Reduction> options for delivering an optimised image quality especially in extra low-light conditions.

The different level options for 3D Noise Reduction (3DNR) include Low, Mid and Hi. A higher level of 3DNR generates relatively enhanced noise reduction.



The proprietary Smart Picture Quality (SPQ) video processing method can drastically minimise motion blur and reduce the noise especially in a low-light environment. The combination of SPQ and 3DNR at different levels further yields exceptional video performance in various conditions.

The Noise Reduction function is configurable with the following options:

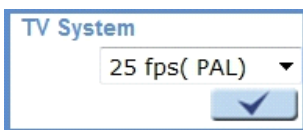
- 3DNR Low
- 3DNR Mid
- 3DNR Hi
- SPQ
- SPQ + 3DNR Low
- SPQ + 3DNR Mid
- SPQ + 3DNR Hi

Click on < ✓ > to confirm the new setting.

11.9. TV System Setup

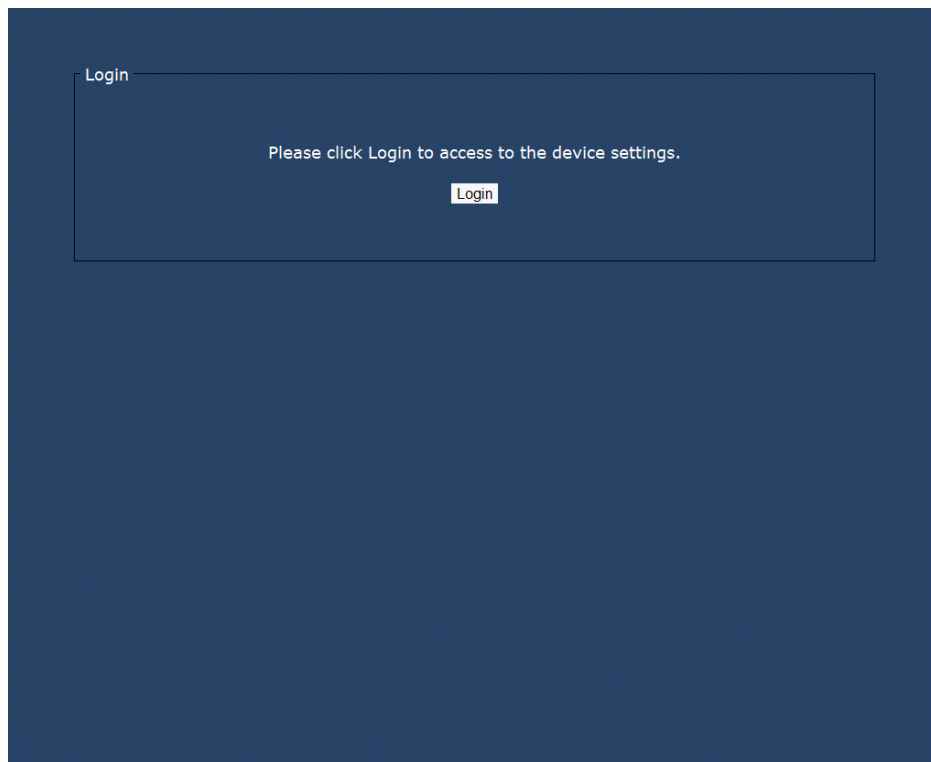
Select the video format that matches the present TV system.

Click on < ✓ > to confirm the new setting.



12. Logout

When you press the "Logout" tab at the top of the page, the login window will pop up. This permits login with another user name.



13. CMS Software Introduction

The Central Management System (CMS) software bundles IP cameras and analogue cameras that are connected to the network via the Video Server into one system. Offering powerful functionalities via intuitive interface, it is a centralised monitoring solution for your video surveillance equipments.

The GRUNDIG CMS Software gives the user access to monitor multiple IP Cameras and Video Servers, and allows the user to monitor simultaneously 16 sites per group (up to 10 groups) within several clicks.

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



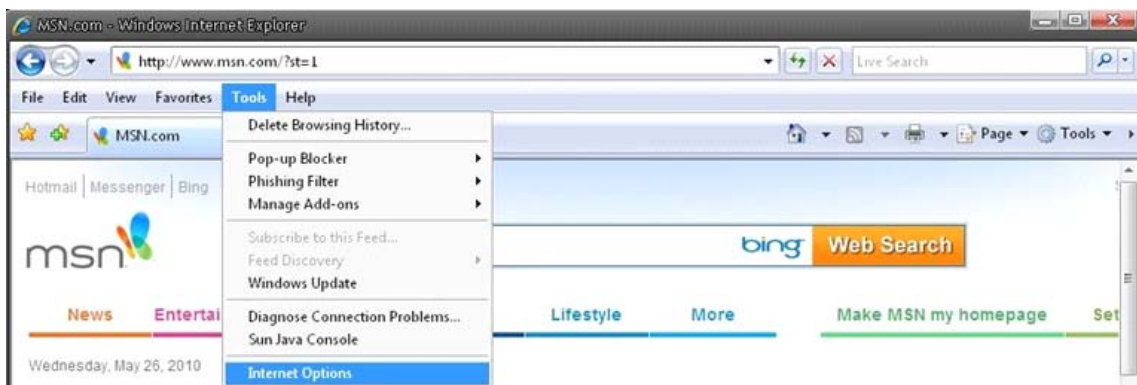
14. Internet Security Settings

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

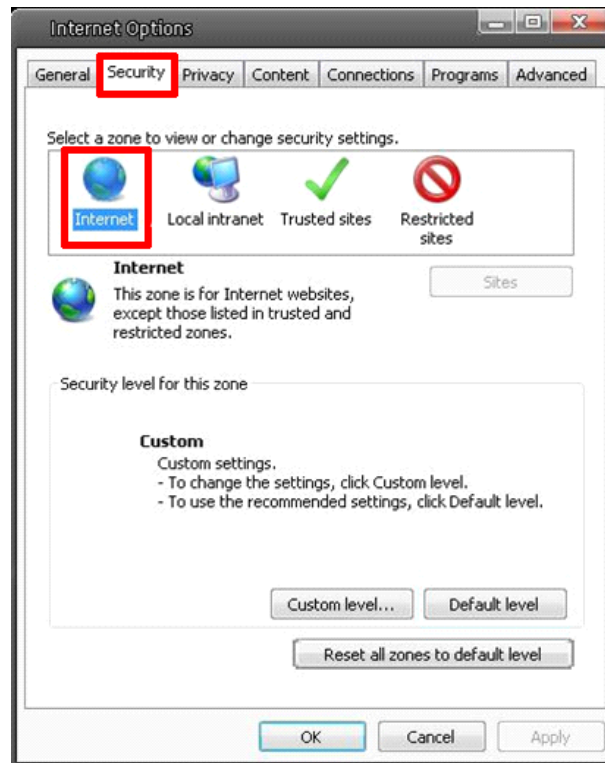
Internet Security Level : Default

Step 1: Start the Internet Explorer.

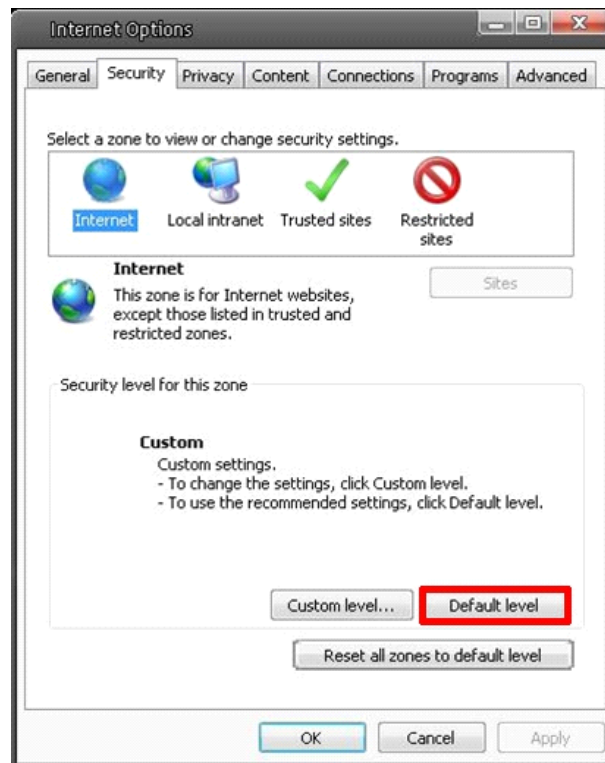
Step 2: Select <Tools> from the main menu of the browser. Then click on <Internet Options>.



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



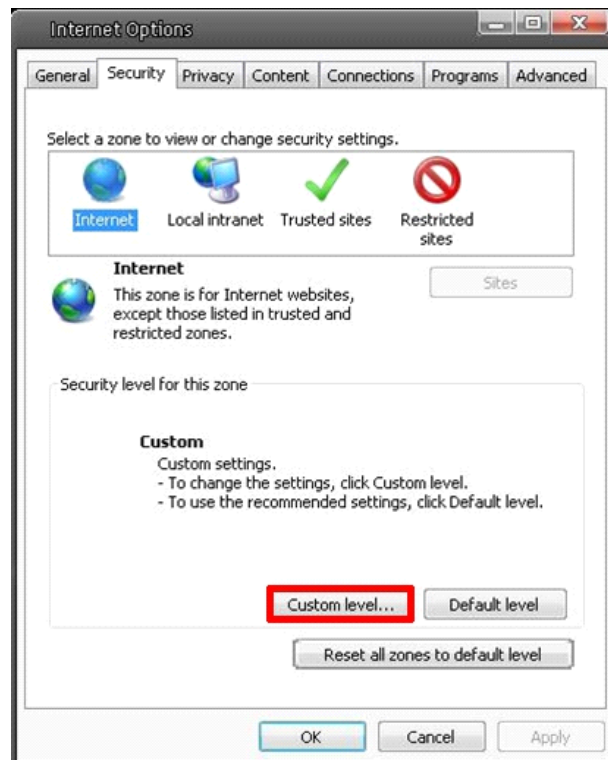
Step 4: Down the page, click on "Default level..." and then click "OK" to confirm the setting. Close the browser window, and open a new one later when accessing the IP Camera.



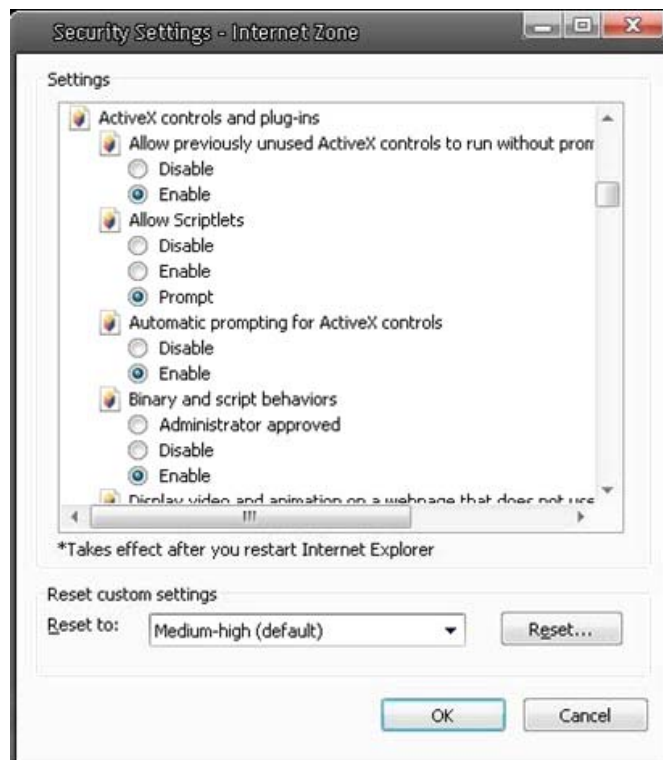
ActiveX Controls and Plug-in Settings :

Step 1~3: 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 on <OK> to accept the settings and to close the Security screen.

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

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

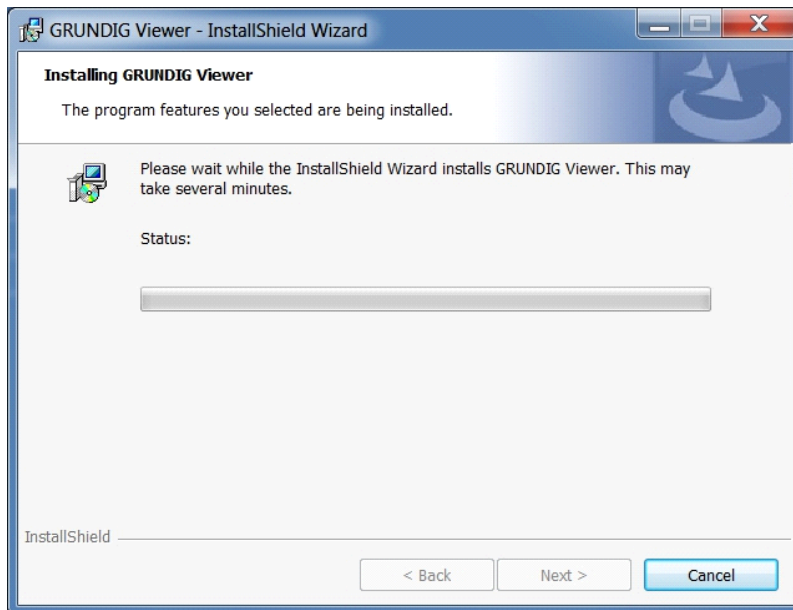
15. GRUNDIG Viewer Download Procedure

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

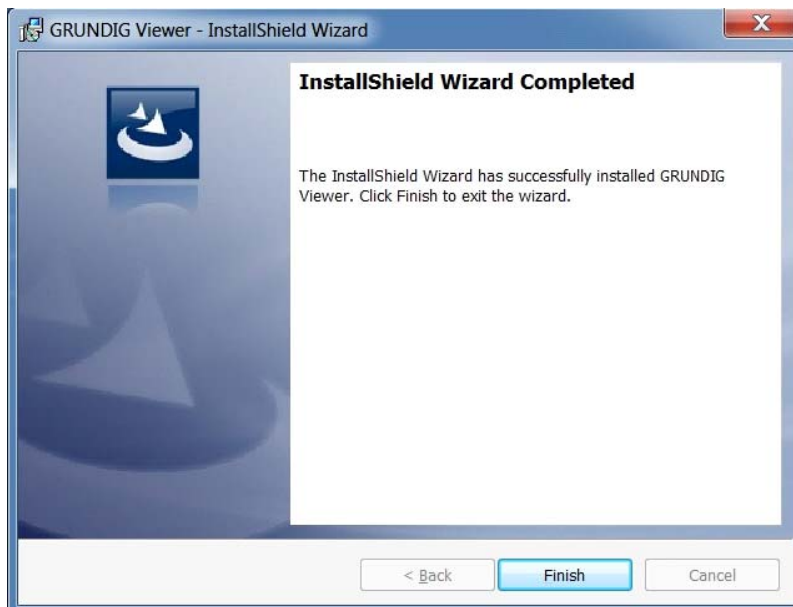
Step 1: In the GRUNDIG Viewer installation page, click “Next” to start the installation.



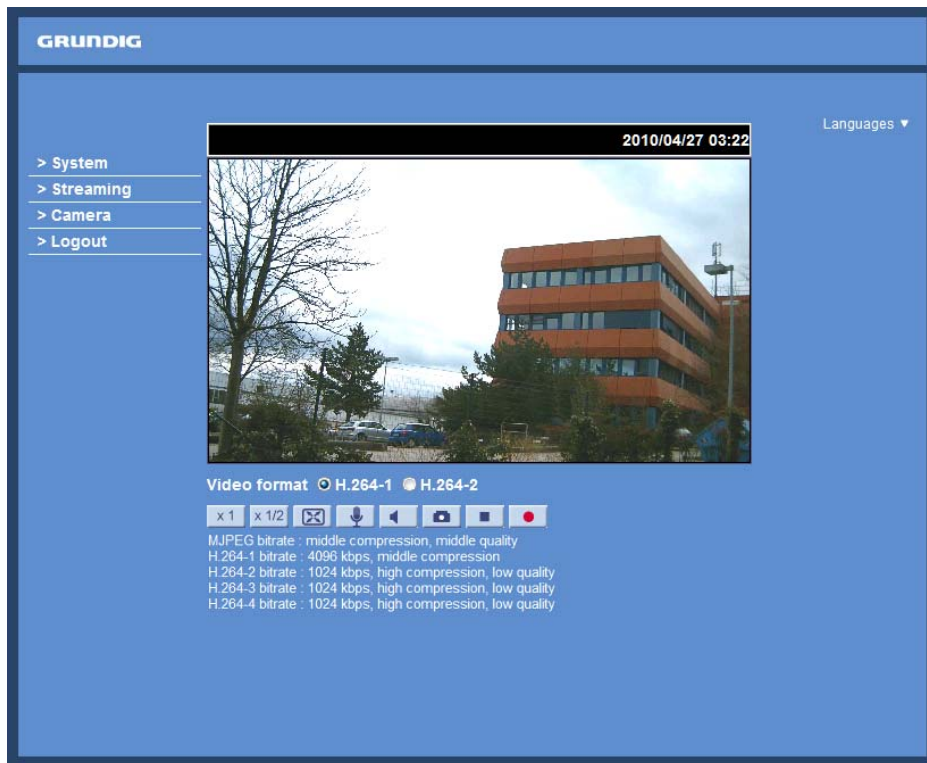
Step 2: Setup starts. Please wait for a while until the loading bar runs out.



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



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



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

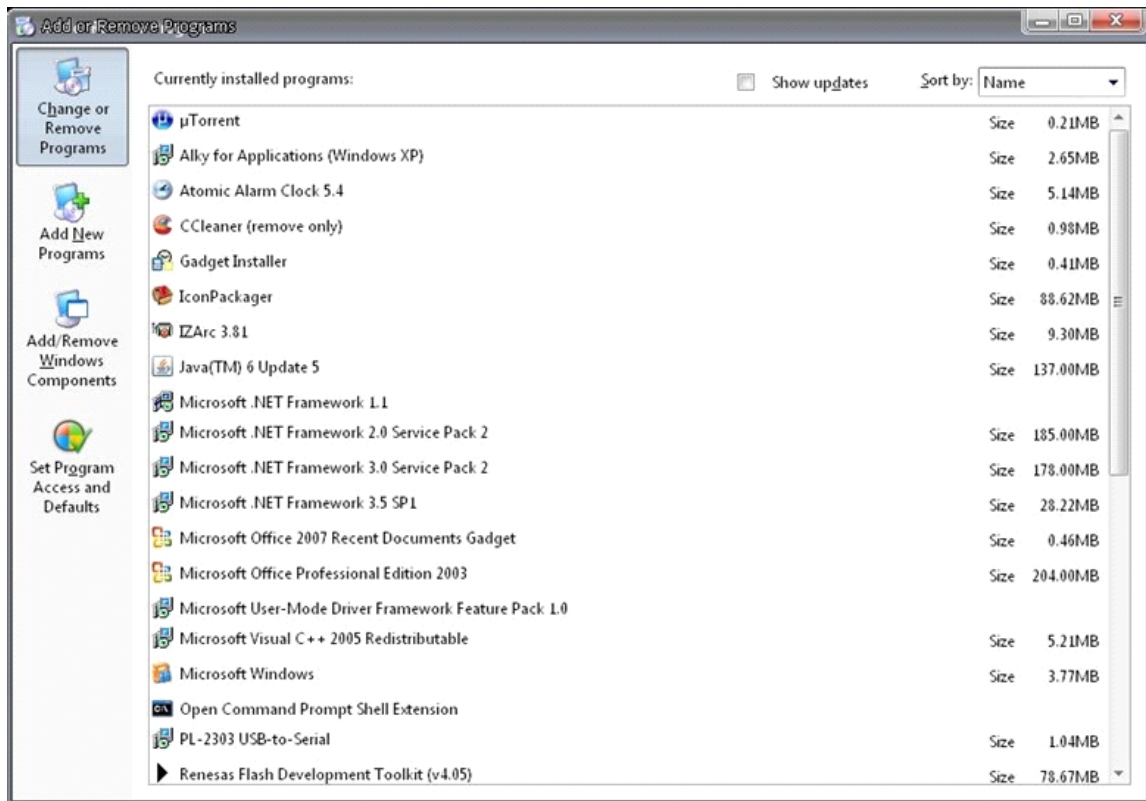
16. Install UPnP Components

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

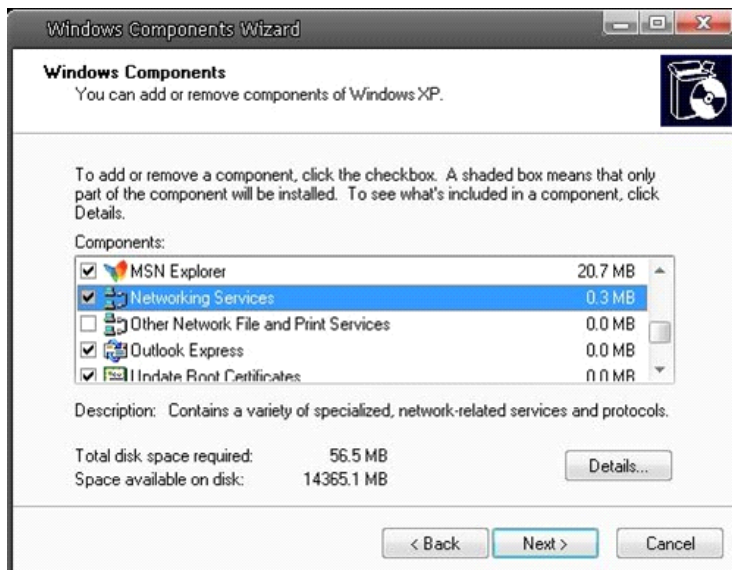
Step 1: Go to "Start", click on "Control Panel", and then double-click on "Add or Remove Programs".



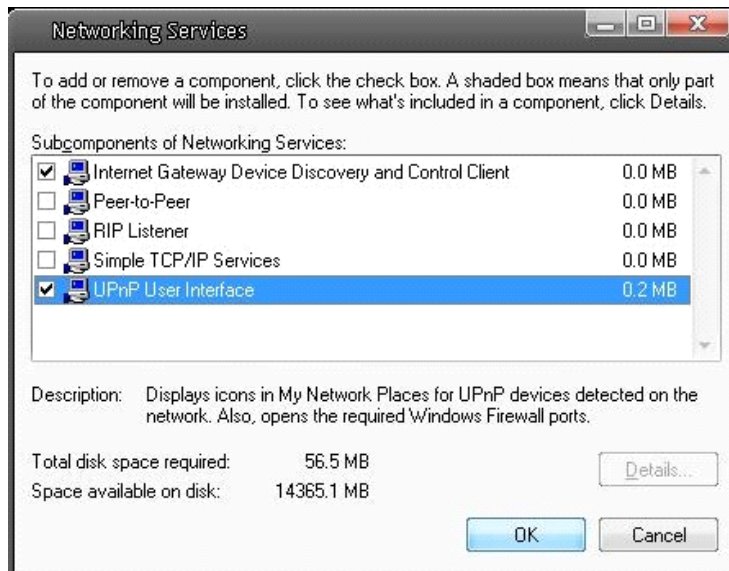
Step 2: Click on "Add/Remove Windows Components" in the Add or Remove Programs page.



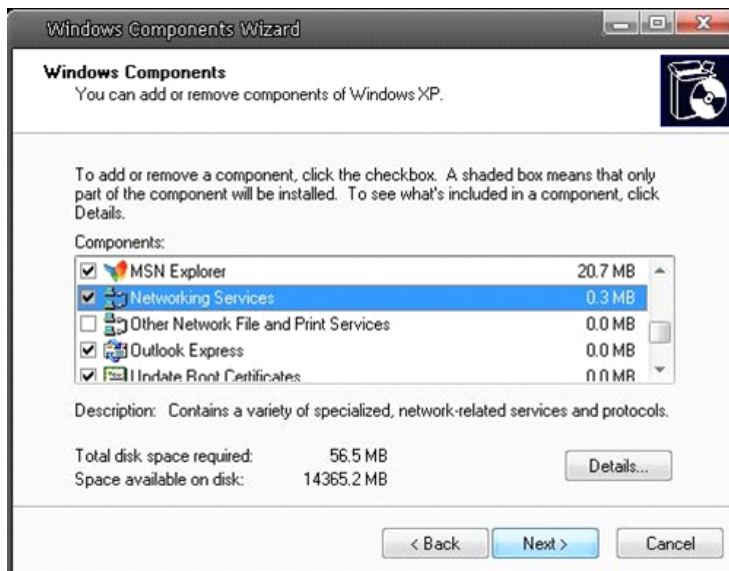
Step 3: Select "Networking Services" from the Components list in the Windows Components Wizard window, and then click on "Details".



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.

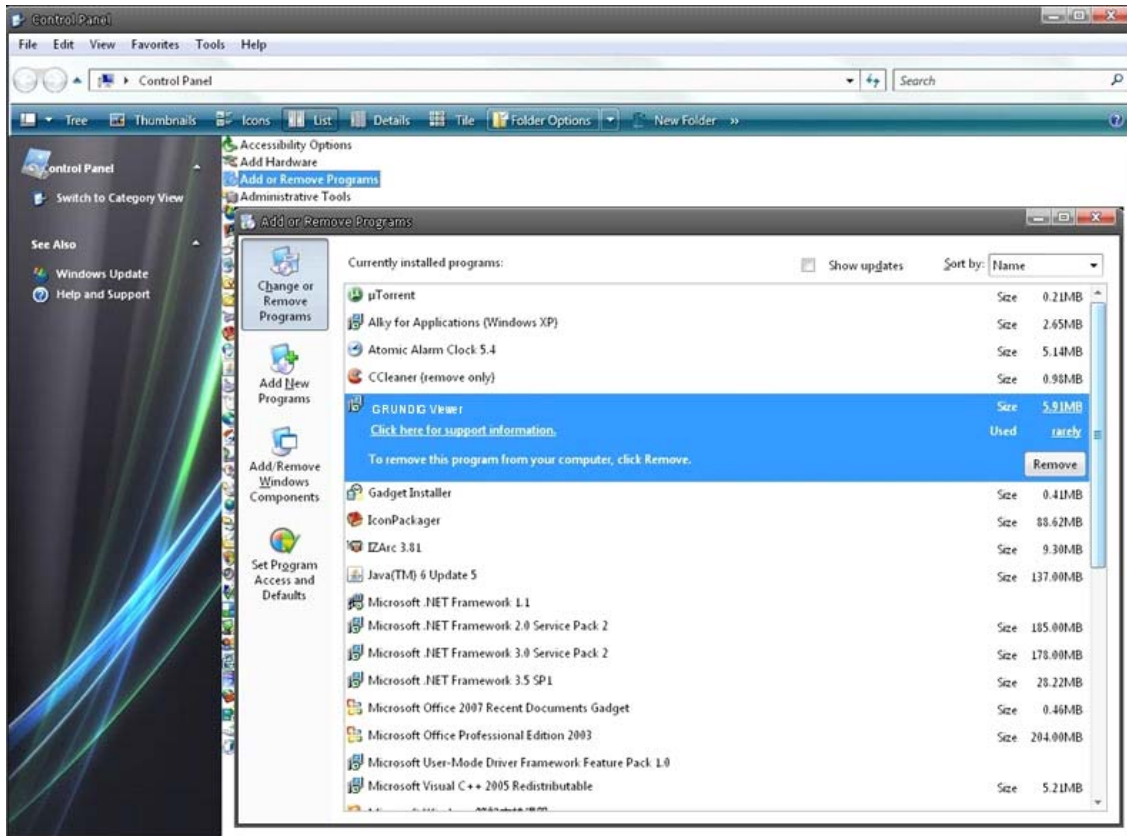


17. Deleting the Existing GRUNDIG Viewer

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 this IP Camera.

Deleting the GRUNDIG Viewer :

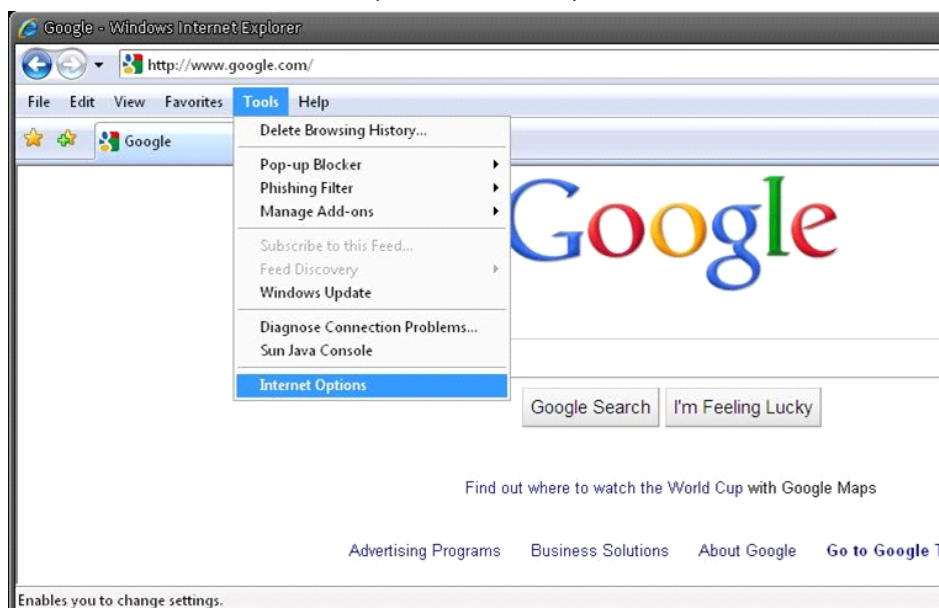
Click on “Control Panel”, and then click on “Add or Remove Programs”. In the “Currently installed programs” list, select “GRUNDIG Viewer” and click the button “Remove” to uninstall the existing GRUNDIG Viewer as shown in the figure below.



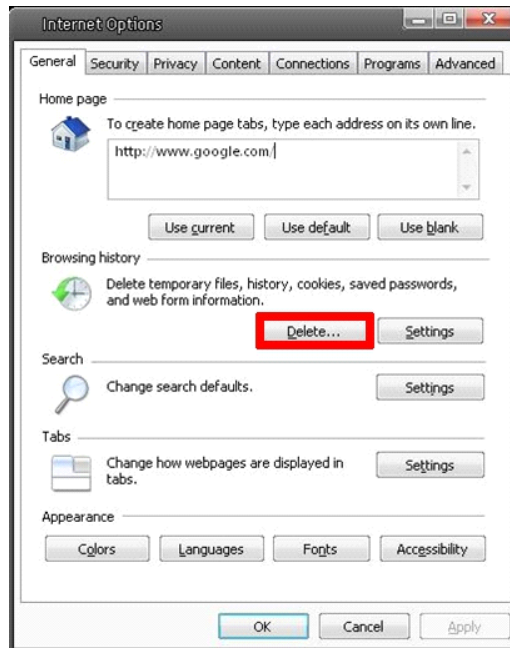
Deleting Temporary Internet Files :

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”.



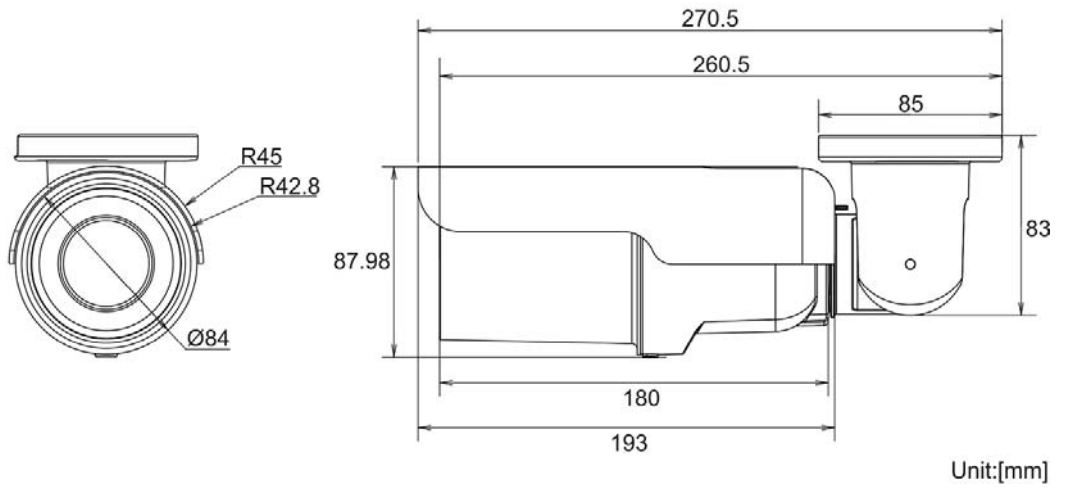
STEP 2: Click on "Delete" in the first pop-up window. Then tap "Delete Files" in the "Temporary Internet files" section in the next pop-up window.



Specifications GCI-K1526T

Image Sensor	1/2.7" CMOS Omnivision, 2 Megapixel
Pixels - Total	1920(H) x 1080(V)
Col/B&W	On/Off/Auto, IR-cut filter removable (ICR)
Sensitivity Colour	0.5 Lux@F1.4 (IRE50), 0.2 Lux@F1.4 (IRE30)
Sensitivity B&W	0.1 Lux@F1.4 (IRE50), 0.02 Lux@ F1.4 (IRE30)
Lens Drive Type	Auto iris (DC)
Lens Focal Length	3 ~ 9 mm
BLC	On/Off
WDR	High/Medium/Low
Digital Noise Reduction (DNR)	On/Off (Adaptive 3D + 2D)
Motion Detection	On/ Off/ Sensitivity/ Area setting
Tampering Alarm	On/Off
Privacy zones	5 zones, rectangle
White Balance	ATW, AWB, Manual
Digital Zoom	Yes
Shutter Speed	1 sec to 1/10,000 sec
Alarm Inputs	1
Alarm Outputs	1
Web Browser	MS Internet Explorer 6.0 (or higher), Firefox, Google Chrome, Safari
Number of Clients	Up to 20 user
Video Compression	H.264, MJPEG
Video Resolution	Full HD 1080p/ SXGA/ HD 720p/ XGA/SVGA/ 4CIF/ VGA/ CIF
Video Streaming	Simultaneous: H.264 (1080p, 25fps) + MJPEG (D1, 25fps), H.264 (1080p, 25fps) + H.264 (4CIF, 25fps)
Network Protocol	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, DHCP, PPPoE, UPnP, SMTP, ICMP, IGMP, SNMP, IEEE802.1x, QoS, ONVIF
SD memory	supports up to 32 GB capacity of micro SD/SDHC memory
Alarm Event	Alarm Input, Motion Detection or Schedule: Image transfer or alarm message by FTP, Image transfer or alarm message by E-mail, recording on SD-card, enable alarm output and send HTTP notification
Audio Compression	G.726, G.711
Video Outputs	1Vpp, BNC
Input/Output sockets	Video Out(BNC), Power(3-Pin Term), RJ-45, Micro SD Card Slot, Alarm Terminal 4-Pin (Alarm In 2-Pin, Alarm Out 2-Pin), Audio (2 mini Jack 3.5mm)
Firmware Upgrade	Firmware upgrade by Web Browser
Configuration	Upload & Download configuration on remote PC
Protection Rating	IP66
Operating Temperature	-10°C ~ +50°C
Humidity	10 ~ 90% no condensation
Regulation	CE, FCC, RoHS Compliant
Supply Voltage	12 VDC / 24 VAC / PoE IEEE 802.3af
Power Consumption	8.9 (LED on) W
Weight	1 kg
Dimensions (wxhxd)	Ø 84 x 287 mm

Dimensions



EC Declaration of Conformity



GCI-K1526T 2 Megapixel Full HD CMOS Bullet IP Camera
ICR IR 23 LED

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

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

Applied harmonised standards and technical specifications:

EN 55022 CLASS A: 2006 + A1: 2007 (Class A)
EN 61000-3-2: 2006/A1: 2009, EN 61000-3-3: 2008,
AS/NZS CISPR 22: 2009 (Class A),
EN 50130-4: 1995 / A1: 1998 / A2: 2003,
IEC 61000-4-2: 2008, IEC 61000-4-3: 2010,
IEC 61000-4-4: 2010, IEC 61000-4-5: 2005,
IEC 61000-4-6: 2008, IEC 61000-4-11: 2004,
Mains Supply Voltage Variations

ASP AG

Lüttringhauser Str. 9
42897 Remscheid
Germany

Remscheid, 21.05.2012

Ludwig Bergschneider
CEO