

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

Owner's Manual

en

IP Cameras

GCI-K1627D	2 MP Full HD Indoor Dome IP Camera 3~10.5mm ICR IR 24 LED WDR
------------	---

GCI-K1627D.150.1.29.10.2014
© ASP AG



Content:			
1. Introduction	2	2. Video Compression	69
2. Important Safety Instructions	2	3. Video ROI	70
3. Package Contents	2	4. Video OCX Protocol	71
4. Installation	2	5. Video Frame Rate	72
1. Camera Overview	3	6. Video Mask	73
2. System Requirements	3	7. Audio (Audio and Bit Rate Settings)	74
3. Power Connection	4	11. Camera Settings	75
4. Ethernet Cable Connection	4	1. Exposure Setting	75
5. Alarm Application	4	2. White Balance Setting	76
6. How to open the Dome Camera	4	3. Picture Adjustment	77
5. Accessing the Camera	4	4. IR Function	77
6. Video Resolution Setup	9	5. Misc	78
7. Browser-based Viewer Introduction	9	6. Profile	79
8. Home Page	10	7. TV System Setup	81
9. System Related Settings	12	12. Logout	82
1. Host Name & System Time Setting	12	13. CMS Software Introduction	83
2. Security	13	14. Internet Security Settings	83
3. Network	24	15. GRUNDIG Viewer Download Procedure	86
4. DDNS	31	16. Install UPnP Components	88
5. Mail	32	17. Deleting the Existing GRUNDIG Viewer	91
6. FTP	33		
7. HTTP	34		
8. Events	35		
9. Storage Management (on Camera)	58		
10. Recording (on Camera)	60		
11. Schedule	61		
12. File Location (on PC)	61		
13. View Information	63		
14. Factory Default	64		
15. Software Version	65		
16. Software Upgrade	65		
17. Maintenance	66		
10. Streaming Settings	67		
1. Video Format	67		

1. Introduction

The Full HD Multiple Streaming Compact Dome IP Camera GCI-K1627D is a compact camera with an easy setup design. Moreover, 2 Megapixel Resolution is offered for providing high definition images. High Power PoE is supported to reduce complicated cabling without sacrificing performance. Quad Streams Compression (H.264 Baseline / Main / High Profile + MJPEG) is supported for efficient bandwidth and storage management. For dark environments, the cameras have incorporated the WDR, 3DNR and Day/Night ICR technologies to capture clear images in lowlight conditions.

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:



IP Camera



Self-Tapping Screw
(x3)



Plastic Screw
Anchors
(x3)



Power Terminal
Block



DC Jack Cable



Quick Guide



CD

4. Installation

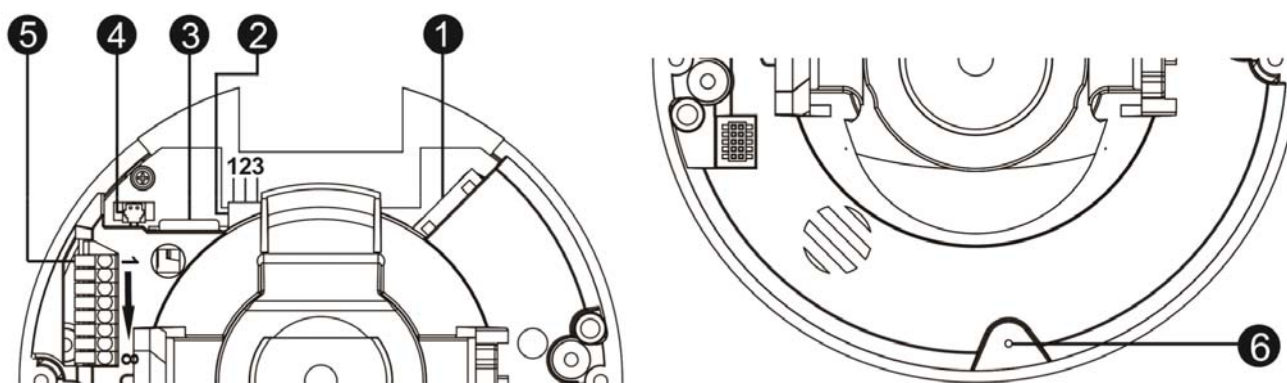
Do not install the product in a location subject to high temperature (over 50°C), low temperature (below -10°C), or high humidity. Doing so may cause fire or electric shock. Keep out of direct sunlight and heat radiation sources. This may cause fire. Avoid aiming the camera directly towards extremely 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 Overview



No.	Connector	Pin	Definition	Remarks
1	RJ-45	-	For network and PoE connections	
2	Power (DC 12V / AC 24V)	1	DC 12V	Power Connection
		2	Reserved	
		3	DC 12V GND	
3	microSD Card Slot	-	Insert the microSD card into the card slot to store videos and snapshots. Do not remove the microSD card when the camera is powered on.	
4	BNC*	-	For analogue video output	
5	Alarm & Audio I/O	1	Alarm In -	Alarm Connection
		2	Alarm In +	
		3	Alarm Out -	
		4	Alarm Out +	
		5	Audio Out L	Audio Out
		6	Audio Out R	
		7	GND	
		8	Audio In	
6	Default Button	-	Press the button for at least 20 seconds with one finger to restore the system.	

[*] Optional

NOTE: It is not recommended to record with the microSD card for 24/7 continuously as it may not be able to support long term continuous data reading/writing. Please contact the manufacturer of the microSD card for information regarding the reliability and the life expectancy.

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 / Windows 8

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

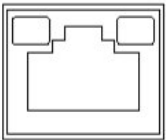
Please refer to section 4.1. Camera Overview for power wiring. Additionally, if using PoE, make sure Power Sourcing Equipment (PSE) is in use in the network.

4.4. Ethernet Cable Connection

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

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

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



Green Link Light indicates good network connection.

Orange Activity Light flashes for network activity indication.

4.5. Alarm Application

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

Please refer section 4.1. Camera Overview for details of the alarm connection.

4.6. How to open the Dome Camera

If you would like to open the dome camera to get access to the connectors, please make sure to push the metal base down and then slide it to the side. The metal base should then slide out and you can take the dome cover off.

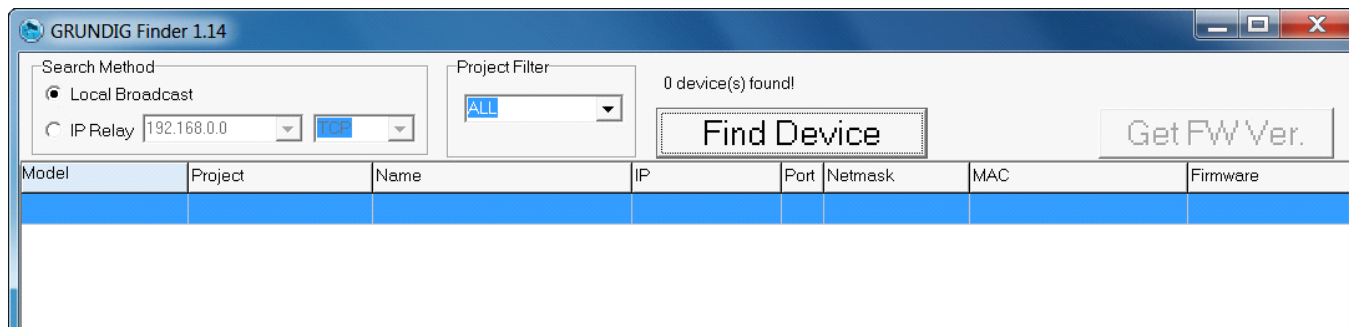
5. Accessing the Camera

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.



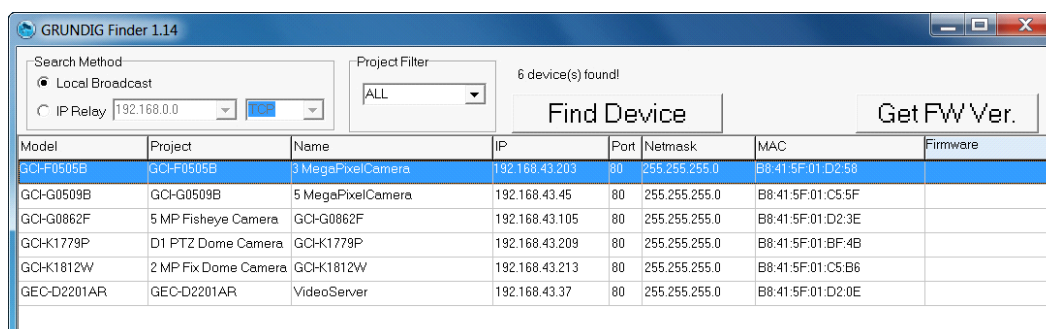


Step 2: The security alert window will pop up. Click "Unblock" to continue.

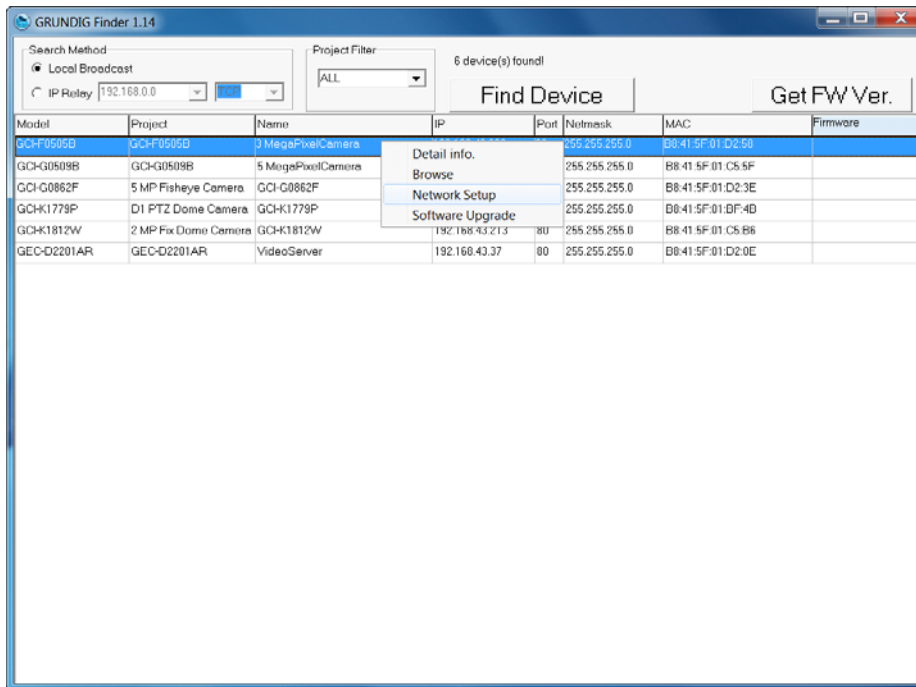


Device Search :

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.

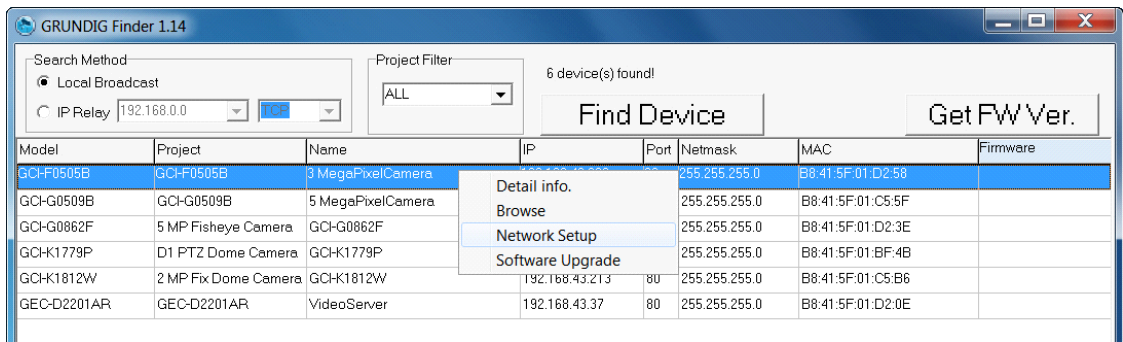
It is strongly advised to alter the administrator’s password due to security concerns. Please refer to section 9.2. Security for further details.

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.

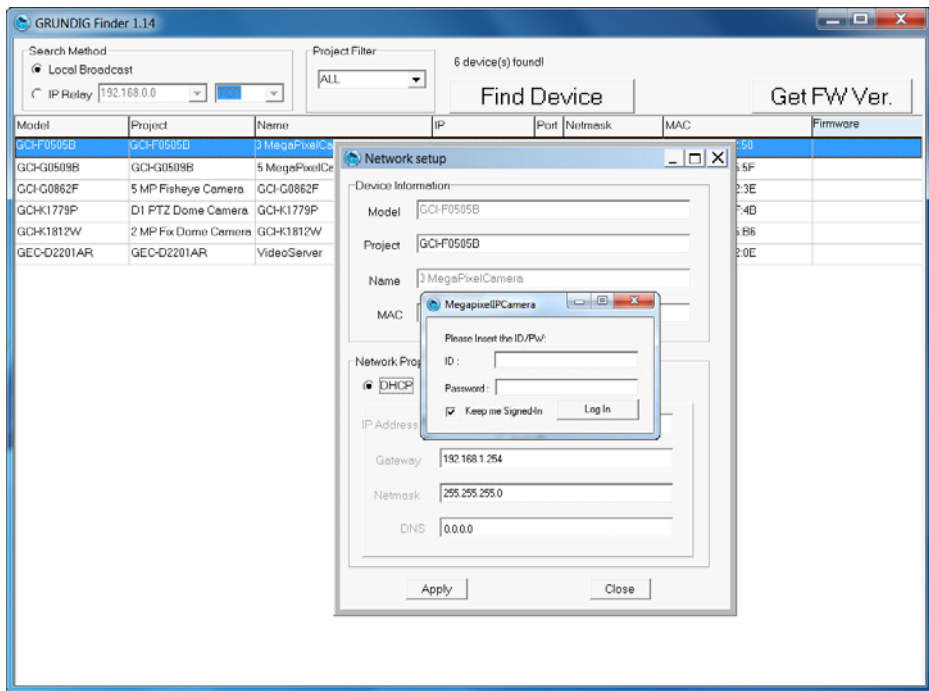
Example of changing the network property of the IP Camera :

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:

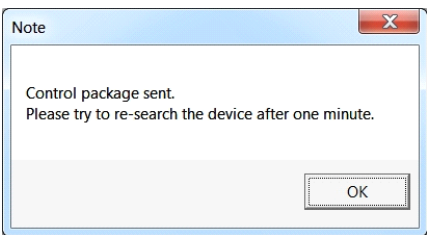
Step 1: In the finding device list, click on the IP Camera of which you would like to change the network property. Right-click on the selected item, and select “Network Setup”. Meanwhile, record the IP Camera’s MAC address for future identification.



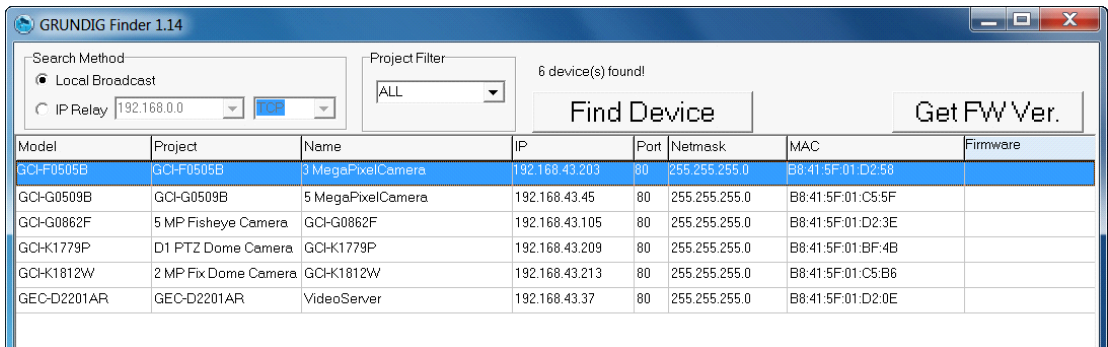
Step 2: The “Network Setup” page will come out. Select “DHCP,” and click on the “Apply” button at the bottom of the page.



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.



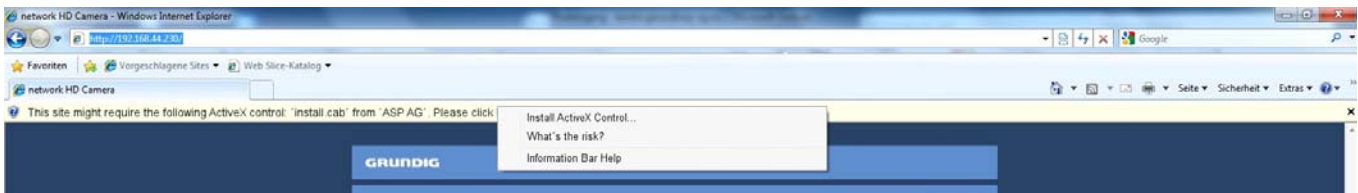
Step 5: Enter User name and Password to access the IP Camera.

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.

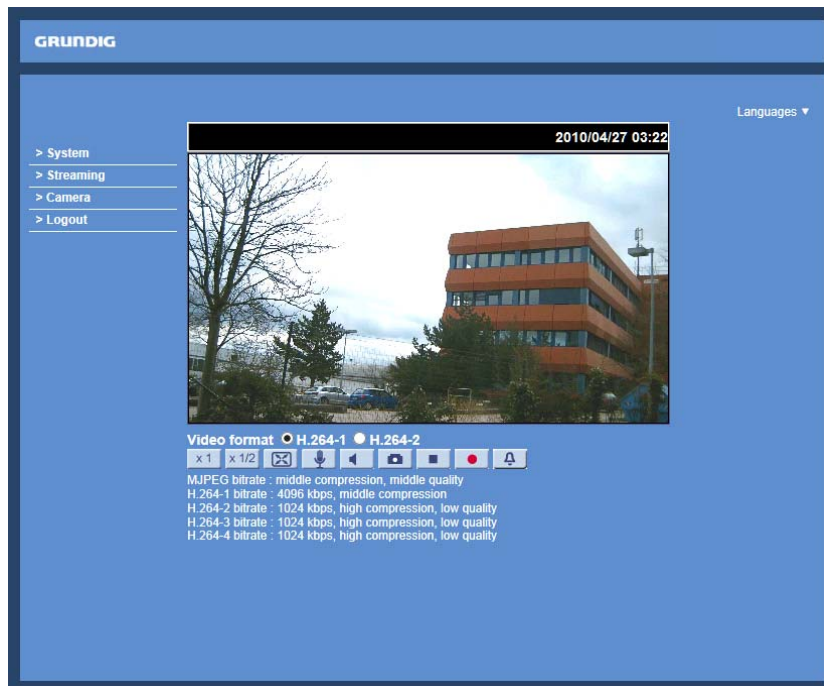


Then the security warning window will pop up. Click "Install" to carry on with the software installation.

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. Deleting 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

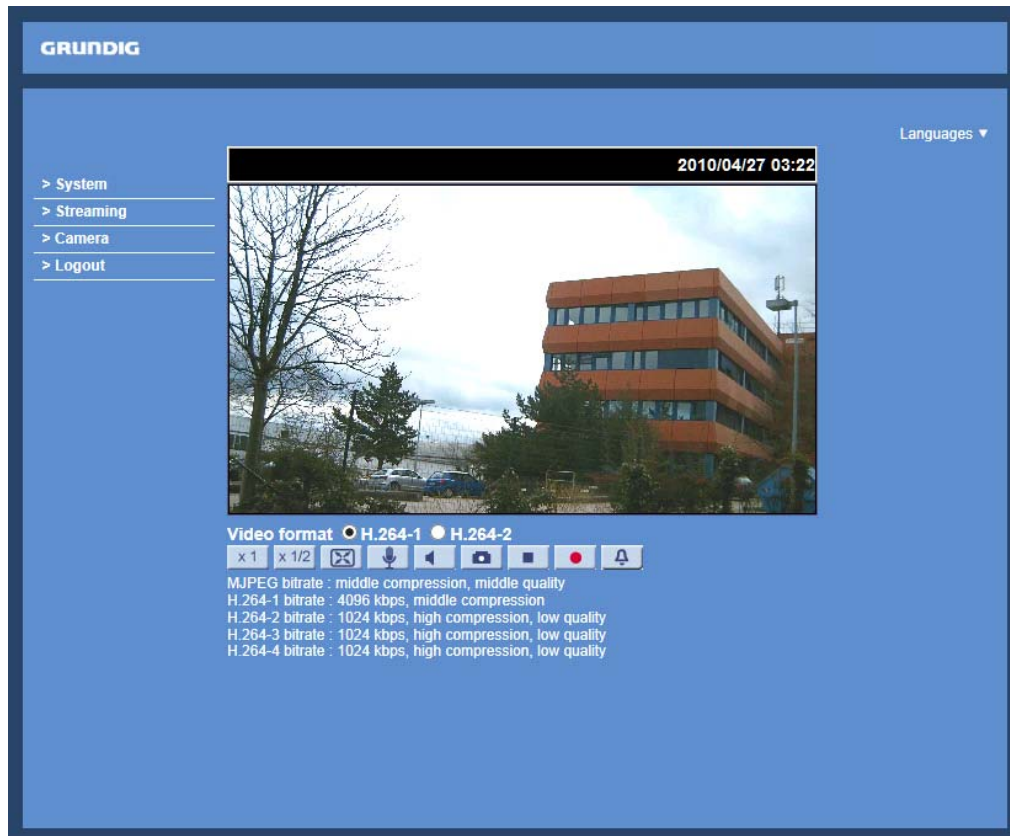
Users can set up the Video Resolution on the Video Format page of the user-friendly browser-based configuration interface. The page "Video Format" can be found in the IP camera menu under the path:

Streaming > Video Format.

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

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.

NOTE: This function is only open to the "User" who has been granted this privilege by the administrator.

Speaker Button (on/off) :

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

NOTE: This function is only open to the "User" who has been granted this privilege by the administrator.

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 9.12. 'File Location (on PC)' for further details.

NOTE: Users with the Windows 7 or Windows 8 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 9.12. 'File Location (on PC)' for further details.

NOTE: Users with the Windows 7 or Windows 8 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.

Manual Trigger Button :

Click on the <Manual Trigger > button to turn the manual trigger on or off.

Multiple Languages Support :

Multiple languages are supported for the viewer window interface.

9. System Related Settings

The picture below shows all categories under the “System” tab. Each category in the left column will be explained in the following sections.

NOTE: The “System” configuration page is only accessible by the Administrator.

The screenshot displays the Grundig System configuration interface. On the left is a navigation menu with categories: >System, System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File Location, 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:** 3 MP Fix Dome Camera
- Time zone:** GMT+00:00 Gambia, Liberia, Morocco, England
- Enable daylight saving time:** ☐ (unchecked). Sub-settings include Time offset (01:00:00), Start date (Jan 1st Sun), Start time (00:00:00), End date (Jan 1st Sun), and End time (00:00:00).
- Time format:** dd/mm/yyyy
- Sync with computer time:** ☐ (unchecked). Sub-settings include PC date (12/11/2014) and PC time (16:18:15).
- Manual:** ☒ (checked). Sub-settings include Date (01/04/2010) and Time (00:00:00).
- Sync with NTP server:** ☐ (unchecked). Sub-settings include NTP server (0.0.0.0) and 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. It displays the same navigation menu on the left and the same configuration options in the main area, including Host name, Time zone, Daylight saving time settings, Time format, and synchronization options (computer time, manual, and NTP server).

Host Name :

The name is for camera identification (max. 30 characters). If the alarm function (see section 9.8.1. '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.

Time format:

Choose a time format (yyyy/mm/dd or dd/mm/yyyy) from the drop-down menu.

The time format for "PC date" and "Date" under <Sync with Computer Time> and <Manual> will be changed according to the selected format.

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>.

Enable IEEE 802.1X :

Check the box to enable IEEE 802.1X.

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

9.2.1. User

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

Admin Password :

Change the administrator's password by putting in the new password in the "Admin password" and "Confirm password" 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:

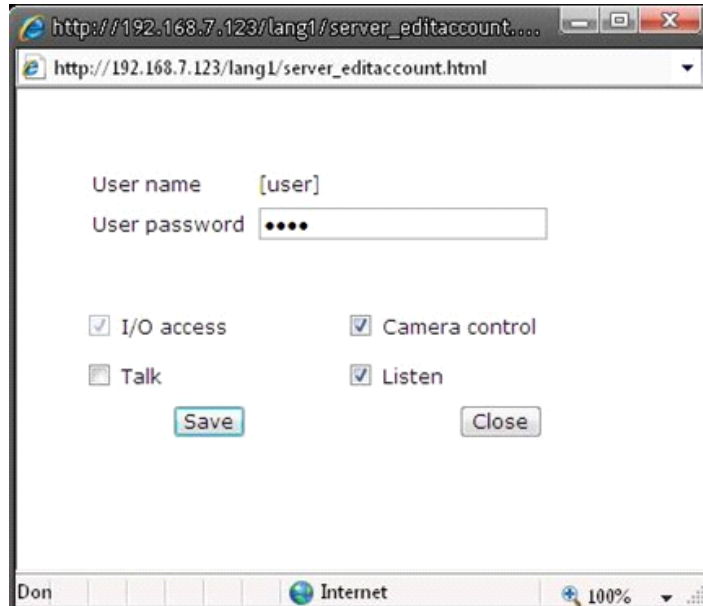
Talk and Listen functions allow the appointed user on the local site (PC site) to communicate, for instance, with the administrator on the remote site.

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.



Streaming Authentication Setting :

The Network Camera provides two types of security settings for an HTTP transaction: basic and digest. Please choose the one that meets your network security requirements.

- Disable: To inactivate the function.

- Basic: In this mode, the password is sent in plain text format and there can be potential risks of the password being intercepted.

- Digest: User credentials are encrypted using an MD5 algorithm and thus provide better protection against unauthorised accesses.

Click on the <Save> button to confirm the settings.

9.2.2. 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>.

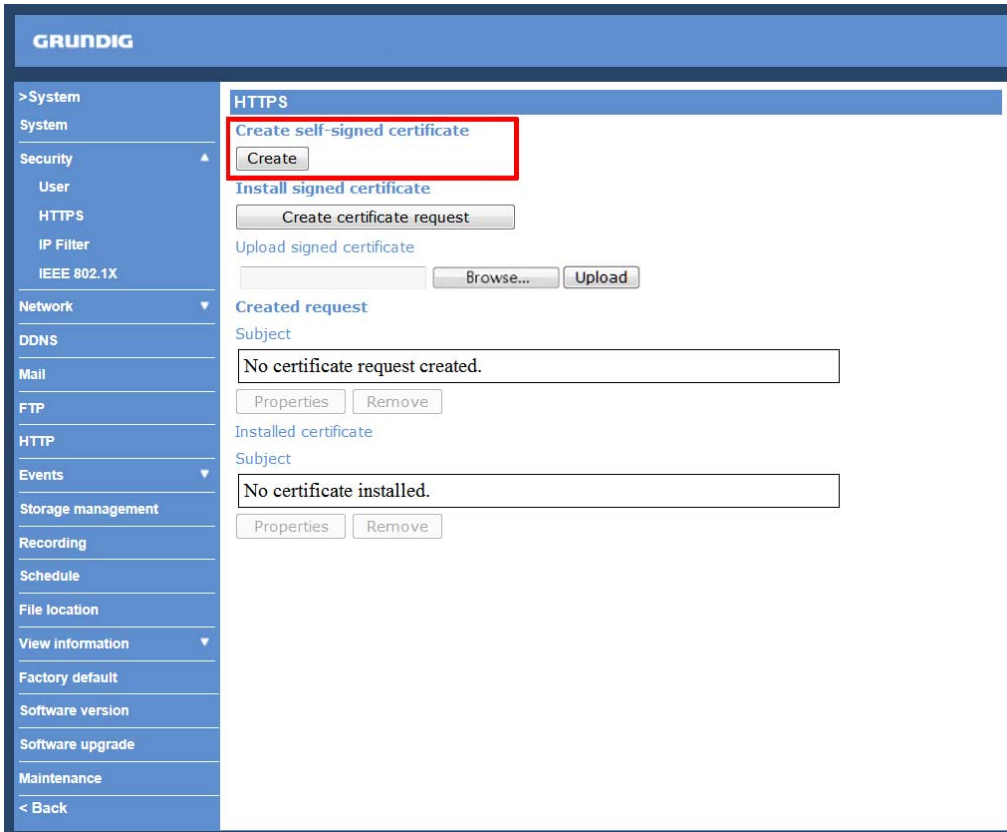
After clicking on the <HTTPS> tab, the HTTPS setting page will be shown as in the figure below.

The screenshot displays the Grundig web interface for HTTPS configuration. The left-hand navigation pane lists various system settings, with 'HTTPS' highlighted under the 'Security' category. The main panel, titled 'HTTPS', provides options for certificate management. It includes a 'Create self-signed certificate' section with a 'Create' button, an 'Install signed certificate' section with a 'Create certificate request' button, and an 'Upload signed certificate' section with a text field, a 'Browse...' button, and an 'Upload' button. Below these are two sections for managing certificates: 'Created request' and 'Installed certificate'. Each section shows a 'Subject' field with the message 'No certificate request created.' and 'No certificate installed.' respectively, and includes 'Properties' and 'Remove' buttons for each entry.

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.



The screenshot displays the Grundig web interface for configuring HTTPS. On the left is a navigation menu with categories like >System, Security, Network, and Events. The main content area is titled 'HTTPS' and contains the following elements:

- Create self-signed certificate:** A link highlighted with a red box, with a 'Create' button directly below it.
- Install signed certificate:** A section containing a 'Create certificate request' button and an 'Upload signed certificate' area with a 'Browse...' button and an 'Upload' button.
- Created request:** A section showing the status 'No certificate request created.' with 'Properties' and 'Remove' buttons.
- Installed certificate:** A section showing the status 'No certificate installed.' with 'Properties' and 'Remove' buttons.

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 :

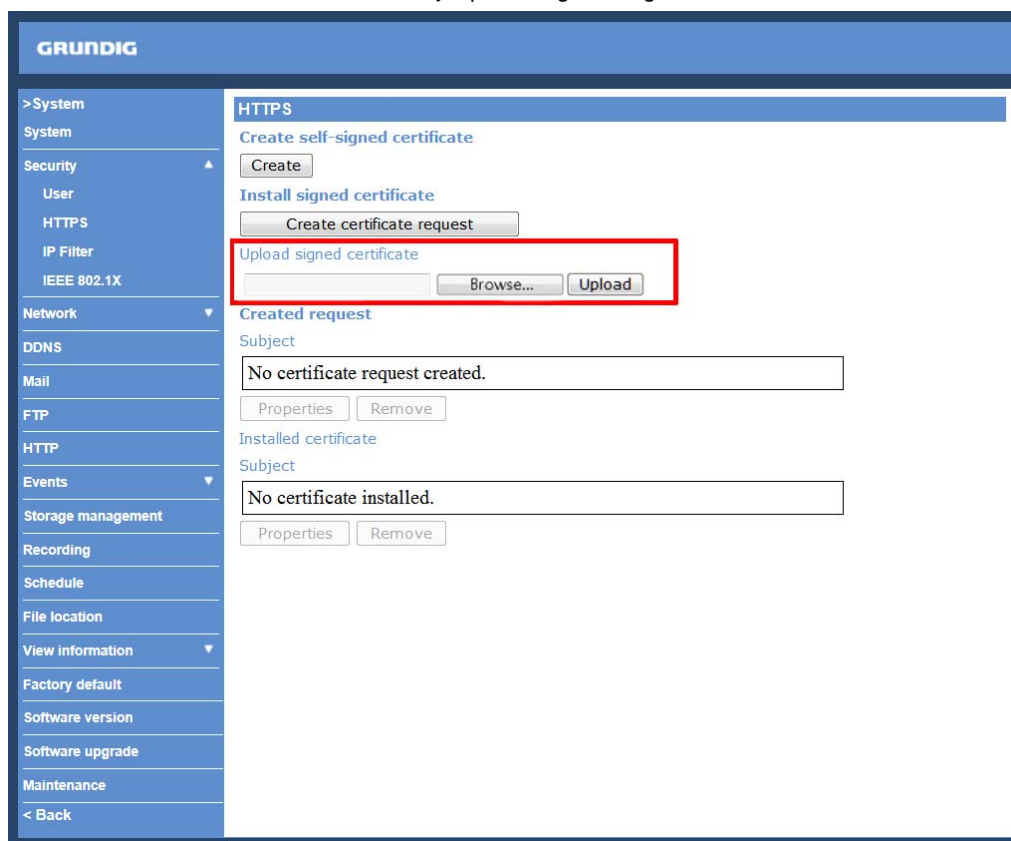
Click on the “Create Certificate Request” button to create and submit a certificate request in order to obtain a signed certificate from the CA (Certificate Authority).

The screenshot shows the GRUNDIG web interface. On the left is a navigation menu with categories like >System, Security, Network, and Events. The 'HTTPS' option is selected. The main content area is titled 'HTTPS' and contains several sections: 'Create self-signed certificate' with a 'Create' button; 'Install signed certificate' with a 'Create certificate request' button (highlighted by a red rectangle); 'Upload signed certificate' with a text input, 'Browse...' button, and 'Upload' button; 'Created request' with a 'Subject' field containing 'No certificate request created.' and 'Properties'/'Remove' buttons; and 'Installed certificate' with a 'Subject' field containing 'No certificate installed.' and 'Properties'/'Remove' buttons.

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:

http://192.168.44.19/lang1/server_certificate.html - Windows Internet Explorer

http://192.168.44.19/lang1/server_certificate.html

Create Self-Signed Certificate

Country:

State or province:

Locality:

Organisation:

Organisational unit:

Common name:

Valid days: days[1...9999]

OK Cancel

Internet 125%

The screenshot shows a web browser window titled "http://192.168.44.19/lang1/server_createrequest.html - Windows Internet Explorer". The address bar also shows "http://192.168.44.19/lang1/server_createrequest.html". The main content area has a blue header bar with the text "Create Certificate Request". Below the header, there are six text input fields with labels: "Country:", "State or province:", "Locality:", "Organisation:", "Organisational unit:", and "Common name:". At the bottom of the form, there 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).

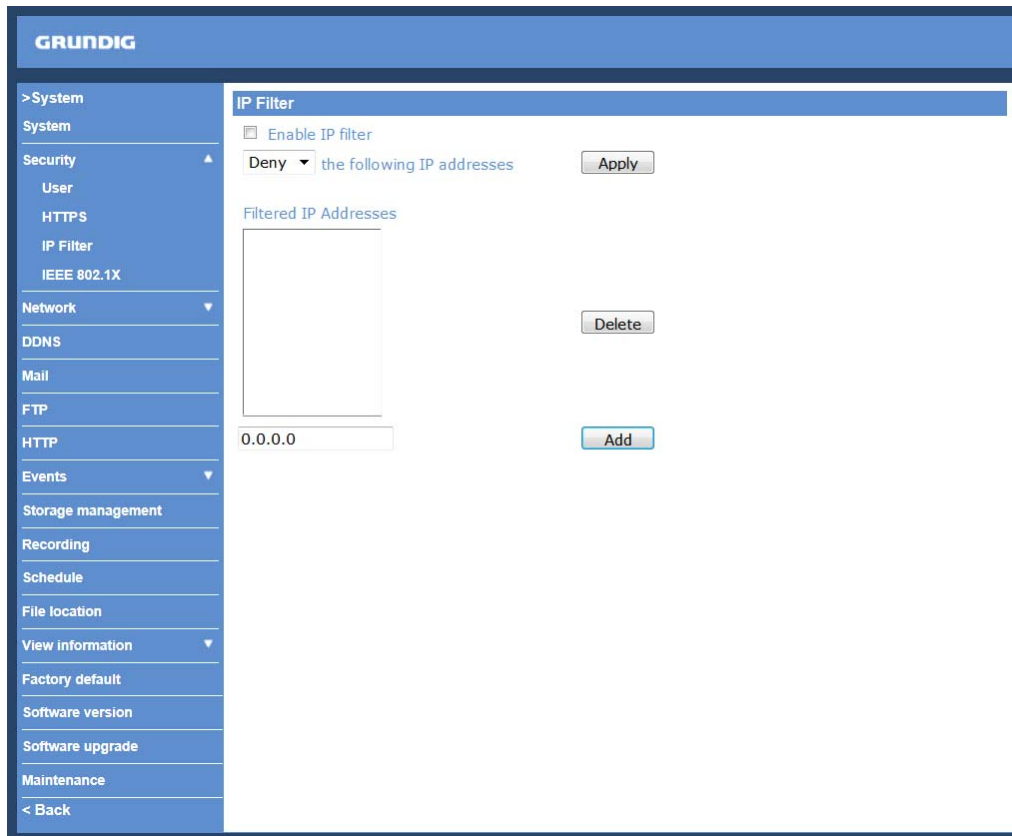
- Valid days (Self-signed Certificate Only):

Enter the period in days (1~9999) to indicate the valid period of the certificate.

Click "OK" to save the Certificate Information after completing.

9.2.3. 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.

In addition, to filter a group of IP addresses, enter an address in the blank space followed by a slash and a number ranging from 1 to 31, e.g. 192.168.2.81/30. The number after the slash can define how many IP addresses will be filtered. For details, please refer to the following example.

Example: Filtering a group of consecutive IP addresses

The steps below show what will be filtered when 192.168.2.81/30 is entered.

Step 1: Convert 192.168.2.81 to binary numbers. The binary numbers for the decimal number 192.168.2.81 are: 11000000.10101000.00000010.01010001.

(For conversion, you can use the calculator of Windows. For Windows XP and Windows Vista, click <View> on the calculator and click <Scientific>. For Windows 7 and Windows 8, click <View> on the calculator and click <Programmer>. Then select first <Dec> and enter the decimal number, for example "2", and select <Bin> to calculate the according binary number. You will receive "10". In the example above, 6 zeros were added before the number 10 because every binary number must consist of 8 digits.)

The number "30" after the slash is referring to the first 30 digits of the binary numbers.

Step 2: Convert a few IP addresses before and after 192.168.2.81 to binary numbers. Then compare their first 30 digits to the binary numbers of 192.168.2.81.

a. Convert 192.168.2.80 to binary numbers. The binary numbers are 11000000.10101000.00000010.01010000. The first 30 digits are the same with the binary numbers of 192.168.2.81, thus 192.168.2.80 will be filtered.

b. Convert 192.168.2.79 to binary numbers. The binary numbers are 11000000.10101000.00000010.01001111. The first 30 digits are different with the binary numbers of 192.168.2.81, thus 192.168.2.79 will not be filtered. This also means the IP addresses before 192.168.2.79 will not be filtered. Therefore, users can stop converting the IP addresses before 192.168.2.79 to binary numbers.

c. Repeat the same procedure in "a" with the IP addresses after 192.168.2.81. Stop when the situation explained in "b" happens. Namely, the 30th digit of the binary numbers of IP address 192.168.2.84 is different, and will not be filtered.

As a result, the IP addresses 192.168.2.80 to 192.168.2.83 will be filtered when entering 192.168.2.81/30. But IP addresses 192.168.79 and 192.168.84 will not be filtered when entering 192.168.2.81/30.

9.2.4. 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 lists various system settings, with 'IEEE 802.1X' selected. The main content area is titled 'IEEE 802.1X/EAP-TLS' and contains the following sections:

- CA certificate:** Includes a text input field, a 'Browse...' button, and an 'Upload' button. Below it, the text 'Uploads CA Certificate.' is displayed.
- Client certificate:** Includes a text input field, a 'Browse...' button, and an 'Upload' button. Below it, the text 'Uploads Client Certificate' is displayed.
- Private key:** Includes a text input field, a 'Browse...' button, and an 'Upload' button. Below it, the text 'Uploads Private Key.' is displayed.
- Settings:** Includes a text input field for 'Identity' (containing 'admin'), a text input field for 'Private key password' (masked with dots), and a checkbox labeled 'Enable IEEE 802.1X'. A 'Save' button is located at the bottom right of this section.

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.

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>.

GRUNDIG

>System
System
Security
Network
Basic
QoS
SNMP
UPnP
DDNS
Mail
FTP
HTTP
Events
Storage management
Recording
Schedule
File location
View information
Factory default
Software version
Software upgrade
Maintenance
< Back

Network

General

☒ Get IP address automatically

☐ Use fixed IP address

IP address192.168.1.1

Subnet mask255.255.255.0

Default gateway0.0.0.0

Primary DNS0.0.0.0

Secondary DNS0.0.0.0

☐ Use PPPoE

User name

Password

Save

Advanced

Web server port80

RTSP port554

MJPEG over HTTP port8008

HTTPS port443

Save

IPv6 address configuration

☐ Enable IPv6

Address :

Save

MAC address: B8:41:5F:09:07:91

9.3.1. 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.

GRUNDIG

>System
System
Security
Network
Basic
QoS
SNMP
UPnP
DDNS
Mail
FTP
HTTP
Events
Storage management
Recording
Schedule
File location
View information
Factory default
Software version
Software upgrade
Maintenance
< Back

Network

General

☒ Get IP address automatically

☐ Use fixed IP address

IP address192.168.1.1

Subnet mask255.255.255.0

Default gateway0.0.0.0

Primary DNS0.0.0.0

Secondary DNS0.0.0.0

☐ Use PPPoE

User name

Password

Save

Advanced

Web server port80

RTSP port554

MJPEG over HTTP port8008

HTTPS port443

Save

IPv6 address configuration

☐ Enable IPv6

Address :

Save

MAC address: B8:41:5F:09:07:91

Get IP address automatically (DHCP):

The camera's default setting is "Use fixed IP address". Please refer to the previous section 5. 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 :

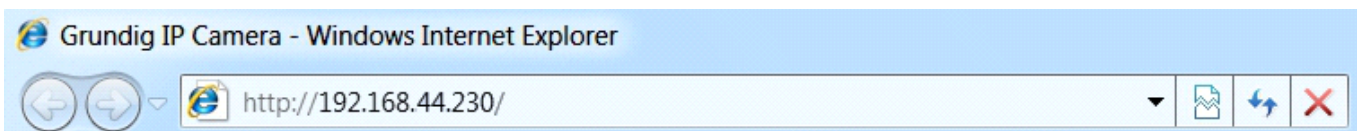
To set up a static IP address, select "Use fixed IP address" and move the cursor to the IP address blank (as indicated below) and insert the new IP address, e.g. 192.168.44.230; then go to Default Gateway (explained later) and type in the appropriate setting, e.g. 192.168.44.1.

Click on "Save" to confirm the new setting.

The screenshot shows the Grundig IP Camera web interface. On the left is a navigation menu with options like System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, Software version, Software upgrade, Maintenance, and < Back. The 'Network' section is expanded, showing 'General' and 'Advanced' tabs. Under 'General', the 'Get IP address automatically' option is selected, but the 'Use fixed IP address' option is also visible. 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 these are fields for User name and Password, and a 'Save' button. Under the 'Advanced' tab, there are 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, there is an 'IPv6 address configuration' section with a checkbox for 'Enable IPv6' and an 'Address' field, and a 'MAC address' field showing B8:41:5F:09:07:91.

When a note for system restart appears, click on <OK> and the system will restart. Wait for 15 seconds. The camera's IP address in the URL bar will be changed, and users have to login again.

When using a static IP address to login to the IP Camera, users can access it either through the "GRUNDIG Finder" software (see 5. 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 :

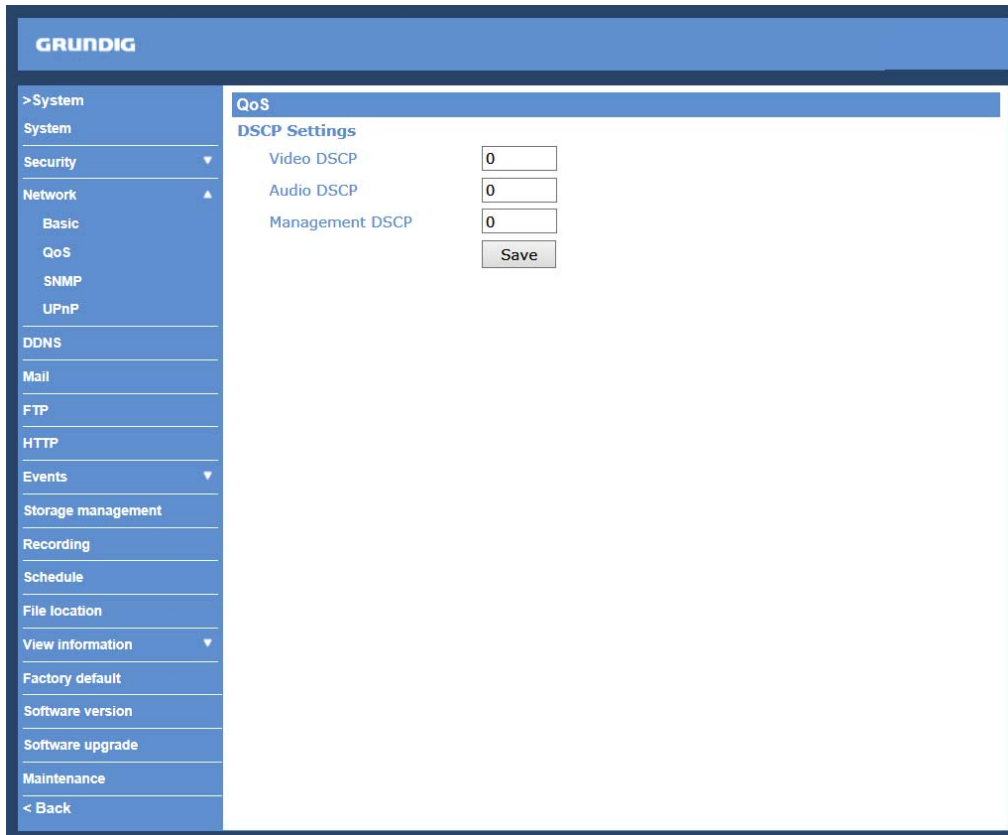
With IPv6 support, users can use the corresponding IPv6 address for browsing. Enable IPv6 by checking the box and click "Save" to complete the setting.

MAC address :

This is the MAC number of this camera.

9.3.2. QoS

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.



The screenshot shows the Grundig web interface. On the left is a navigation menu with categories: >System, System, Security, Network (expanded), DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, Software version, Software upgrade, Maintenance, and < Back. Under the 'Network' category, 'QoS' is selected. The main content area is titled 'QoS' and 'DSCP Settings'. It contains three input fields: 'Video DSCP' with value '0', 'Audio DSCP' with value '0', and 'Management DSCP' with value '0'. A 'Save' button is located below these fields.

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.

9.3.3. SNMP

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

The screenshot displays the Grundig web interface for configuring SNMP settings. The left sidebar lists various system settings, with 'SNMP' highlighted under the 'Network' category. The main panel, titled 'SNMP Settings', contains three primary sections: 'SNMP v1/v2', 'SNMP v3', and 'Traps for SNMP v1/v2/v3'. The 'SNMP v1/v2' section includes checkboxes for enabling v1 and v2, and text input fields for 'Read community' (default: public) and 'Write community' (default: private). The 'SNMP v3' section features a checkbox to enable v3, and fields for 'Security name', 'Authentication type' (MD5 selected), 'Authentication password', 'Encryption type' (DES selected), and 'Encryption password'. The 'Traps for SNMP v1/v2/v3' section has a checkbox to enable traps, and fields for 'Trap address' and 'Trap community' (default: public). A 'Trap option' section with a 'Warm start' checkbox is also present. A 'Save' button is positioned at the bottom of the configuration area.

SNMP v1/v2 :

- Enable SNMP:

Select the version of SNMP to use by checking the corresponding box.

- Read Community:

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

- Write Community:

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

SNMP v3 :

This option contains cryptographic security, a higher security level, which allows users to set the Authentication password and the Encryption password.

- Enable SNMP v3: Check the corresponding box to activate SNMP v3.

- Initial User Password (=Security Name): The community name set on NMS(Network-management station). The maximum length of the string is 32 alphanumeric characters.

- Authentication type: Select MD5 or SHA as the authentication method.

- Authentication password: Enter the password for authentication (at least 8 characters).

- Encryption type: Select DES or AES as the encryption method.

- Encryption password: Enter a password for encryption (at least 8 characters).

Traps for SNMP v1/v2/v3 :

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 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.

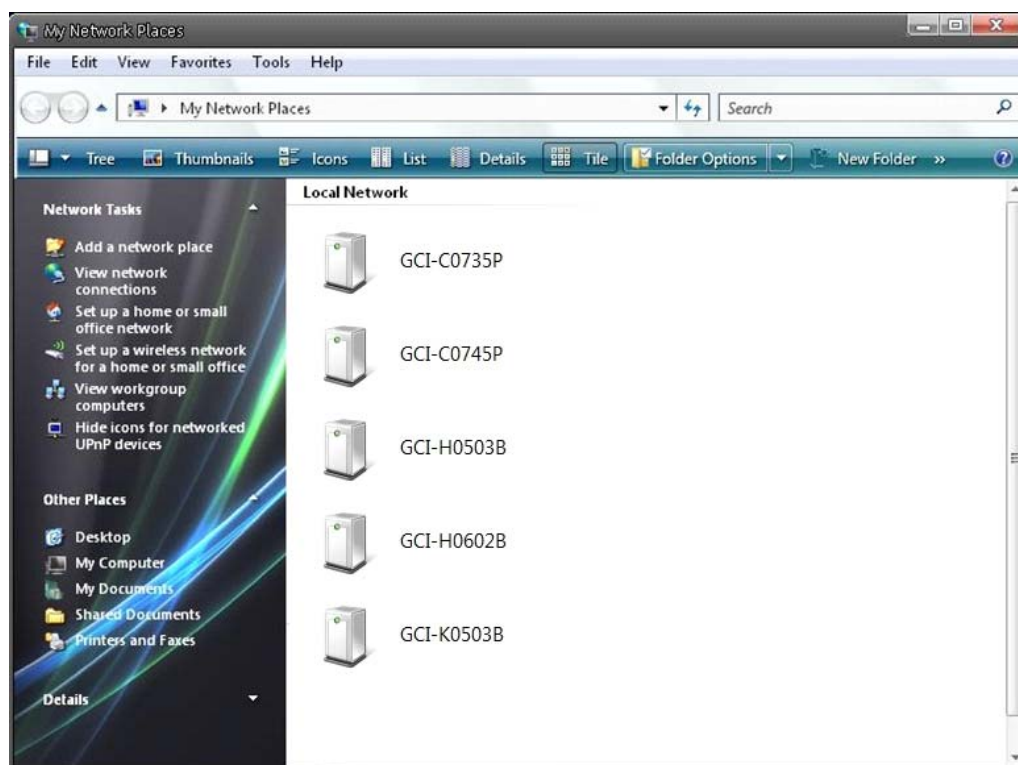
9.3.4. UPnP

The screenshot displays the Grundig web interface for configuring UPnP settings. On the left is a vertical navigation menu with the following items: >System, System, Security, Network (with expand/collapse arrows), Basic, QoS, SNMP, UPnP, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, 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 field labeled 'Friendly name' containing the text 'GCI-XXXXXX'. A 'Save' button is located at the bottom right of the settings area.

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 17. 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.

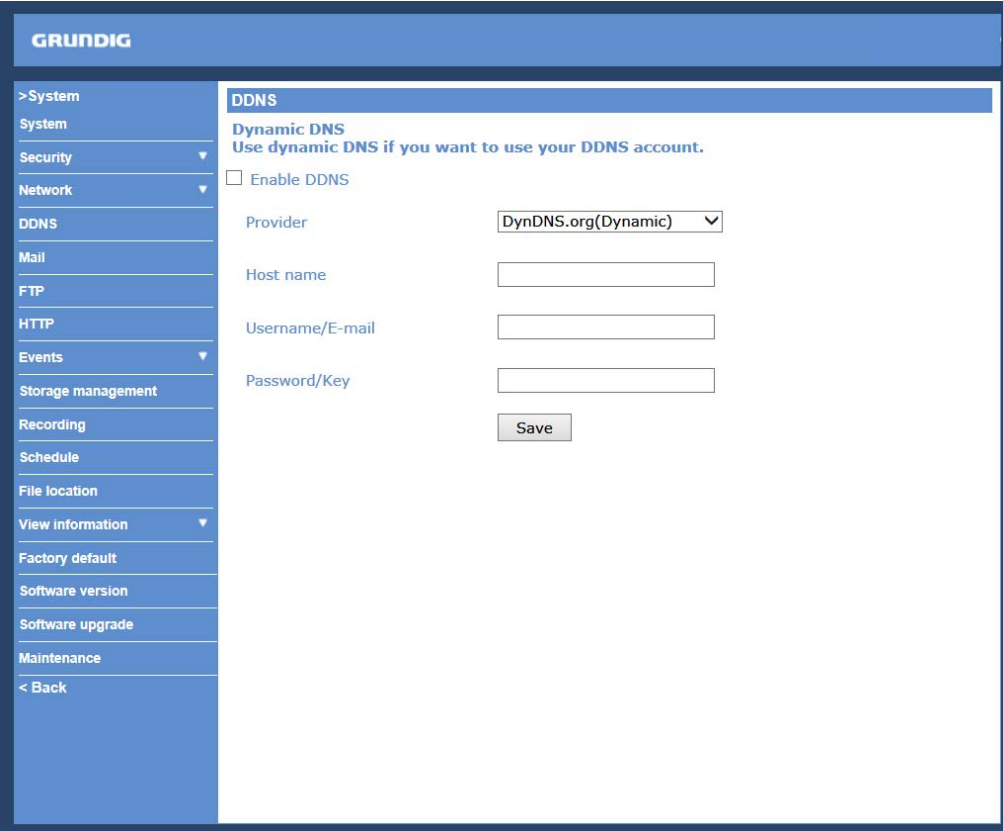
9.3.9. SNMP

- Trap community:

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

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.



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 an event is triggered. SMTP is a protocol for sending e-mail messages from server to server. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and to whom the message text is transferred.

The configuration page is shown below:

GRUNDIG

>System

System

Security

Network

DDNS

Mail

FTP

HTTP

Events

Storage management

Recording

Schedule

File location

View information

Factory default

Software version

Software upgrade

Maintenance

< Back

Mail

SMTP

1st SMTP (mail) server

1st SMTP (mail) server port

1st SMTP account name

1st SMTP password

1st recipient email address

☐ 1st SMTP SSL

2nd SMTP (mail) server

2nd SMTP (mail) server port

2nd SMTP account name

2nd SMTP password

2nd recipient email address

☐ 2nd SMTP SSL

Sender email address

25

25

Save

Note:

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

Two sets of SMTP can be configured. Each set includes the SMTP Server, Server Port, Account Name, Password and E-mail Address settings. Check the box "SMTP SSL" to send emails via encrypted transmission. 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 an event 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. Check the box "passive mode" to be connected to the FTP server by passively receiving the FTP server's IP address through a dynamic port. Alternatively, uncheck the box to directly connect with the FTP server via active mode. You can also test whether the designated FTP is connected properly by pressing "Test".

Click "Save" when the setting is finished.

GRUNDIG

>System

System

Security

Network

DDNS

Mail

FTP

HTTP

Events

Storage management

Recording

Schedule

File location

View information

Factory default

Software version

Software upgrade

Maintenance

< Back

FTP

FTP

1st FTP server

1st FTP server port

1st FTP user name

1st FTP password

1st FTP remote folder

☐ 1st FTP passive mode

Test the connection to the specified FTP server

2nd FTP server

2nd FTP server port

2nd FTP user name

2nd FTP password

2nd FTP remote folder

☐ 2nd FTP passive mode

Test the connection to the specified FTP server

Save

Note:

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

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 HTTP configuration interface. The left sidebar contains a menu with the following items: >System, System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, Software version, Software upgrade, Maintenance, and < Back. The main panel 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 positioned below the 2nd HTTP password field.

Please also refer to: 9.8.1. Application (Alarm Settings): Send HTTP notification / 9.8.2. Motion Detection for HTTP Notification settings.

9.8. Events

9.8.1. 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 Grundig web interface for alarm settings. The left sidebar lists various system functions. The main panel is titled 'Application' and contains several configuration sections. The 'Alarm Switch' section has three radio buttons: 'Off' (selected), 'On', and 'By schedule'. The 'Alarm Type' section has two radio buttons: 'Normal close' and 'Normal open' (selected). The 'Alarm Output' section has two radio buttons: 'Output high' (selected) and 'Output low'. The 'Triggered Action' section has two columns of checkboxes. The first column includes 'Enable alarm output' (checked), 'Send message by FTP', 'Upload image by FTP', and 'Send HTTP notification'. The second column includes 'IR cut filter' (checked with a dropdown set to 'on'), 'Send message by E-Mail', 'Upload image by E-Mail', and 'Record stream to sd card'. The 'File Name' section has a text input for 'File name' (image.jpg) and four radio buttons: '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'. A 'Save' button is located at the bottom of the configuration area.

For details on how to connect the alarm input/output, please refer to the Chapter 4.1. Camera Overview.

Alarm Switch :

The default setting for the Alarm Switch function is <Off>. Enable this function by selecting <On>. Users can also activate the function according to the schedule previously set in the <Schedule> setting page. Select <By schedule> and click <Please select...> to choose the desired schedule from the drop-down menu.

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 the alarm is triggered. 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 Message by FTP:

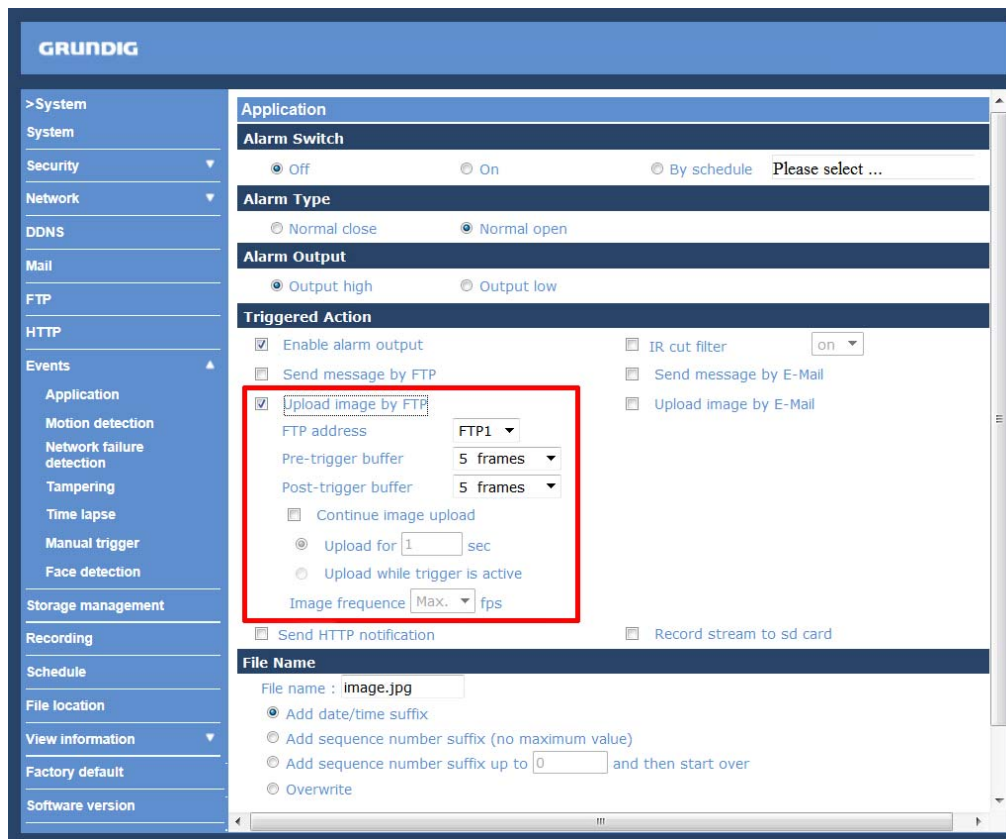
The Administrator can choose to send an alarm message by FTP when an alarm is detected.

- Send 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 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: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.10. 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 screenshot shows the Grundig web interface for configuring the 'Upload image by E-Mail' feature. The interface is divided into a sidebar menu on the left and a main content area. The sidebar menu includes categories like System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, and Software version. The main content area is titled 'Application' and contains sections for 'Alarm Switch', 'Alarm Type', 'Alarm Output', and 'Triggered Action'. The 'Triggered Action' section is highlighted with a red box and contains the following settings: 'Enable alarm output' (checked), 'Send message by FTP' (unchecked), 'Upload image by FTP' (unchecked), 'IR cut filter' (on), 'Send message by E-Mail' (checked), 'Upload image by E-Mail' (checked), 'E-Mail address' (E-Mail 1), 'Pre-trigger buffer' (5 frames), 'Post-trigger buffer' (5 frames), 'Continue image upload' (unchecked), 'Upload for 1 sec' (selected), 'Upload while trigger is active' (unchecked), and 'Image frequency' (Max. fps). Below the 'Triggered Action' section is the 'File Name' section with options for 'File name', 'Add date/time suffix', 'Add sequence number suffix (no maximum value)', 'Add sequence number suffix up to 0 and then start over', and 'Overwrite'.

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 by E-Mail 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 via E-Mail 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: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

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

The screenshot displays the Grundig web interface for configuring alarm settings. On the left is a navigation menu with categories like System, Security, Network, and Events. The 'Events' section is expanded, showing options like Motion detection, Network failure detection, and Tampering. The main content area is titled 'Application' and 'Alarm Switch'. It includes sections for 'Alarm Type' (Normal close, Normal open), 'Alarm Output' (Output high, Output low), and 'Triggered Action'. In the 'Triggered Action' section, the 'Send HTTP notification' checkbox is checked and highlighted with a red rectangle. Below it, the 'HTTP address' is set to 'HTTP1' and 'Custom parameters' is empty. The 'File Name' section shows 'File name : image.jpg' and options for adding date/time suffix, sequence number suffix, or overwriting. A 'Save' button is at the bottom.

GRUNDIG

>System

System

Security

Network

DDNS

Mail

FTP

HTTP

Events

Application

Motion detection

Network failure detection

Tampering

Time lapse

Manual trigger

Face detection

Storage management

Recording

Schedule

File location

View information

Factory default

Software version

Application

Alarm Switch

☒ Off ☐ On ☐ By schedule Please select ...

Alarm Type

☐ Normal close ☒ Normal open

Alarm Output

☒ Output high ☐ Output low

Triggered Action

☒ Enable alarm output ☐ IR cut filter on

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

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

☒ Send HTTP notification

HTTP address HTTP1

Custom parameters

File Name

File name : image.jpg

☒ Add date/time suffix

☐ Add sequence number suffix (no maximum value)

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

☐ Overwrite

Save

- Record Stream to SD Card:

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

The screenshot shows the Grundig web interface for alarm settings. On the left is a navigation menu with categories: >System, System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, and Software version. The 'Events' category is expanded, showing sub-items: Application, Motion detection, Network failure detection, Tampering, Time lapse, Manual trigger, and Face detection. The 'Application' sub-item is selected. The main content area is titled 'Application' and contains sections for 'Alarm Switch' (Off, On, By schedule), 'Alarm Type' (Normal close, Normal open), 'Alarm Output' (Output high, Output low), and 'Triggered Action'. In the 'Triggered Action' section, several checkboxes are present: 'Enable alarm output' (checked), 'Send message by FTP', 'Upload image by FTP', 'Send HTTP notification', 'IR cut filter' (set to 'on'), 'Send message by E-Mail', and 'Upload image by E-Mail'. The 'Record stream to sd card' checkbox is checked and highlighted with a red rectangle. Below it, the 'Pre-trigger buffer' is set to '1' sec. Two radio buttons are available: 'Upload for 1 sec' (selected) and 'Upload while trigger is active'. The 'File Name' section at the bottom shows a text box with 'image.jpg' and four radio button options: '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'. A 'Save' button is at the bottom.

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.

9.8.2. 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.

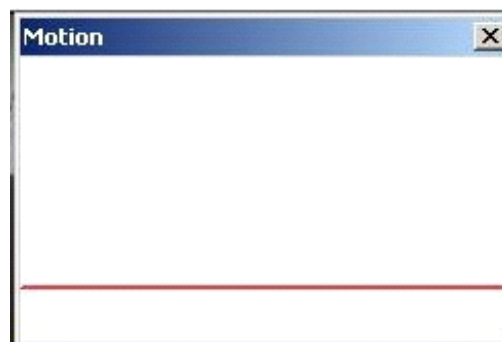
The screenshot shows the Grundig web interface for Motion Detection settings. On the left is a navigation menu with categories: >System, System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, and Software version. The 'Events' category is expanded, showing sub-items: Application, Motion detection, Network failure detection, Tampering, Time lapse, Manual trigger, and Face detection. The 'Motion detection' sub-item is selected. The main content area is titled 'Motion Detection' and contains several sections: 1. 'Motion Detection' with a dropdown menu set to '1' and radio buttons for 'Off' (selected) and 'On'. 2. 'By schedule' with a 'Please select ...' dropdown. 3. 'Motion Detection Setting' with input fields for 'Sampling pixel interval [1-10]' (value: 1), 'Detection level [1-100]' (value: 10), 'Sensitivity level [1-100]' (value: 80), and 'Time interval(sec) [0-7200]' (value: 10). 4. 'Triggered Action' with checkboxes for 'Enable alarm output' (selected, with a 'high' dropdown), 'Record stream to sd card', 'Send alarm message by FTP', 'Send alarm message by E-mail', 'Upload image by FTP', 'Upload image by E-Mail', and 'Send HTTP notification'. 5. 'File Name : image.jpg' with 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'. A 'save' button is at the bottom. On the right, there is a live video pane showing a conference room with a red square indicating a motion detection window. Below the video pane are 'add' and 'delete' buttons for 'Motion Detection Windows'.

This function supports up to 4 sets of Motion Detection Settings. The settings can be chosen from the drop-down menu beside <Motion Detection>. In each set of the setting, there is a frame (Motion Detection Window) displayed on the Live Video Pane (shown in the picture below).

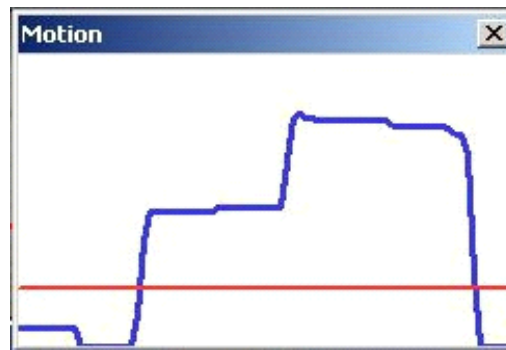
The Motion Detection Window is for defining the motion detection area. To change the size of the Motion Detection Window, move the mouse cursor to the edge of the frame and draw it outward/inward. Moving the mouse to the center of the frame can shift the frame to the intended location.

Up to 10 Motion Detection Windows can be set. 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 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 :

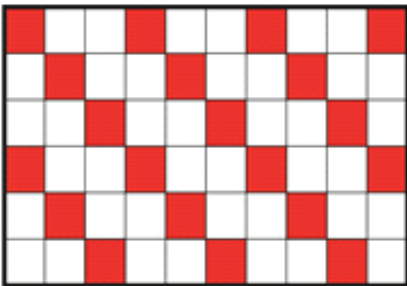
In each set of the Motion Detection Setting, the default setting for the Motion Detection function is <Off>. Enable this function by selecting <On>. Users can also activate the function according to the schedule previously set in the <Schedule> setting page. Select <By schedule> and click <Please select...> to choose the desired schedule from the drop-down menu.

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) :

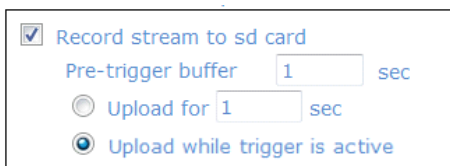
The Administrator can specify alarm actions that will take place when motion is detected. All options are listed as follows:

- Enable Alarm Output:

Check this item and select the predefined type of alarm output to enable alarm relay output when 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 9.10. 'Recording (on Camera)' for further details.

- Send Message by FTP:

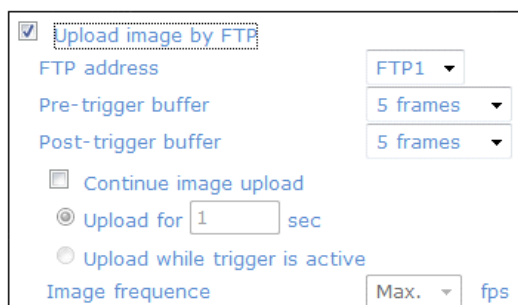
The Administrator can choose to send an alarm message by FTP when a motion is detected.

- Send 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.

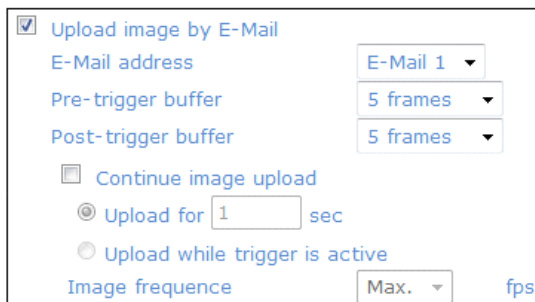
- Select <Upload while trigger is active> to keep the images being uploaded to the FTP while the trigger is active, i.e. until the alarm is stopped.

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

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

- 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.



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 via E-Mail 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 via E-Mail 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: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

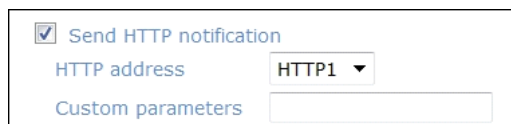
NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

NOTE: Make sure SMTP and/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.



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 9.8.1. 'Application (Alarm Settings)').

Save :

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

9.8.3. Network failure detection

The Network Failure Detection function allows the IP Camera to ping another IP device (e.g. NVR, VSS, Video Server, etc.) within the network periodically and generates some actions in case of network failure occurrence, for instance, when a Video Server is somehow disconnected.

Being capable of implementing local recording (through Micro SD card) or the remote recording (via NAS) when a network failure happens, the IP Camera can be a backup recording device for the surveillance system.

The screenshot shows the Grundig web interface for configuring Network Failure Detection. The left sidebar lists various system settings, with 'Network failure detection' selected under the 'Events' section. The main panel is titled 'Network Failure Detection' and includes the following configuration options:

- Detection Switch:** Three radio buttons are present: 'Off' (selected), 'On', and 'By schedule' (with a 'Please select ...' dropdown).
- Detection Type:** A text field for 'Ping the IP address' contains '192.168.128.254', and a dropdown for frequency is set to 'every 5 seconds'.
- Triggered Action:** Four checkboxes are shown: 'Enable alarm output' (checked, with a 'high' dropdown), 'Record stream to sd card', 'Send message by FTP', and 'Send message by E-Mail'.
- A 'Save' button is located at the bottom of the configuration area.

Detection Switch :

The default setting for the Detection Switch function is <Off>. Enable this function by selecting <On>. Users can also activate the function according to the schedule time that is was previously set in the <Schedule> setting page. Select <By schedule> and click <Please select...> to choose the desired schedule from the drop-down menu.

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.

The ping time setting range is from 1 to 99 minutes.

Triggered Action (Multi-option) :

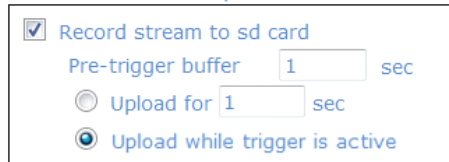
The Administrator can specify alarm actions that will take place when Network Failure is detected. All options are listed as follows:

- 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.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.10. 'Recording (on Camera)' for further details.

- Send Message by FTP:

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

- Send Message by E-Mail:

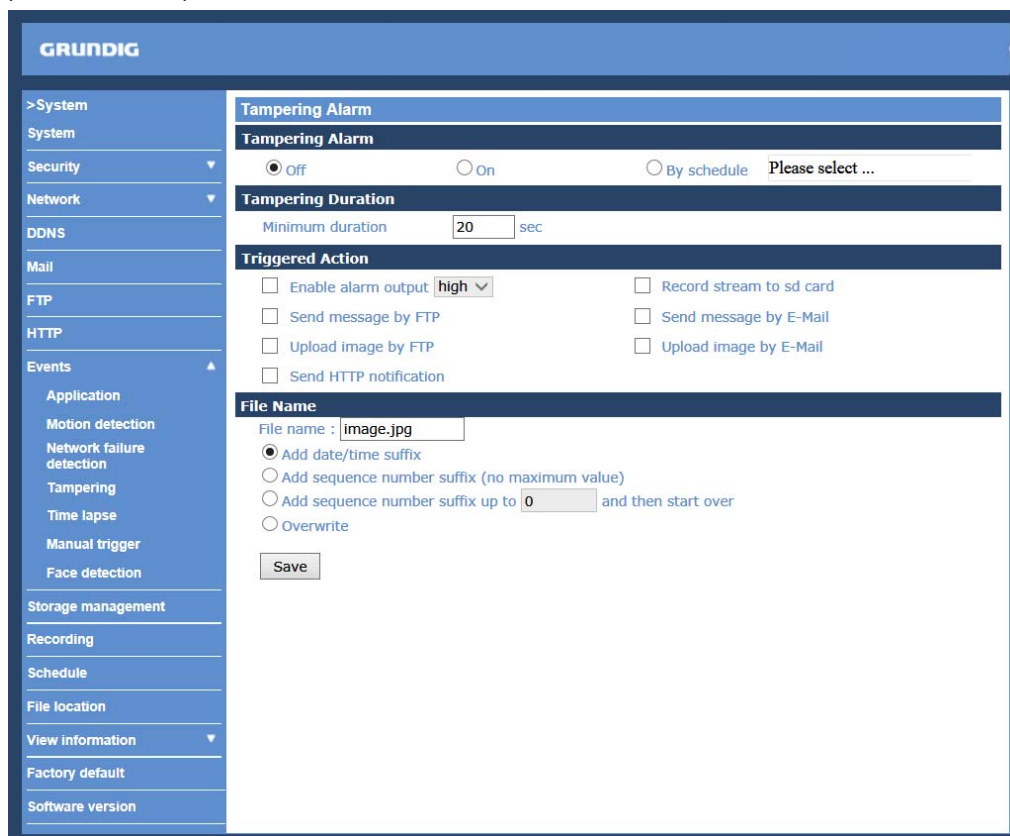
The Administrator can choose to send an alarm message by E-Mail when Network Failure is detected.

Save :

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

9.8.4. 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).



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.

☒ Record stream to sd card

Pre-trigger buffer

1

sec

☐

Upload for 1 sec

☒

Upload while trigger is active

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 9.10. 'Recording (on Camera)' for further details.

- Send Message by FTP:

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

- Send Message by E-Mail:

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

- Upload Image by FTP:

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

☒ Upload image by 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

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: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

- 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 via E-Mail 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 via E-Mail 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: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

NOTE: Make sure SMTP and/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 9.8.1. 'Application (Alarm Settings)').

Save :

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

9.8.5. Time lapse

In the Time Lapse setting, users can set the camera to upload images periodically to an FTP site or an E-Mail address. For example, if the time interval is set to 60 seconds, the camera will upload images to the assigned FTP site or E-Mail address every 60 seconds. The images to be uploaded are the images before and after the triggered moment. Users can define how many images will be uploaded in the <Triggered Action> section of this setting page.

GRUNDIG

>System

System

Security ▼

Network ▼

DDNS

Mail

FTP

HTTP

Events ▲

Application

Motion detection

Network failure detection

Tampering

Time lapse

Manual trigger

Face detection

Storage management

Recording

Schedule

File location

View information ▼

Factory default

Software version

Time Lapse

Time Lapse

☒ Off ☐ On

Time interval

Minimum interval sec

Triggered Action

☐ Upload image by FTP

FTP address FTP1 ▼

Pre-trigger buffer 5 frames ▼

Post-trigger buffer 5 frames ▼

☐ Upload image by E-Mail

E-Mail address E-Mail 1 ▼

Pre-trigger buffer 5 frames ▼

Post-trigger buffer 5 frames ▼

☐ Upload image to sd card

Pre-trigger buffer 5 frames ▼

Post-trigger buffer 5 frames ▼

File Name

File name :

☒ Add date/time suffix

☐ Add sequence number suffix (no maximum value)

☐ Add sequence number suffix up to and then start over

☐ Overwrite

Save

Time Lapse :

The default setting for the Time Lapse function is <Off>. Enable the function by selecting <On>.

Time Interval :

The default value of the time interval is 60 seconds. The setting range of the time interval is from 60 to 3600 seconds.

Triggered Action (Multi-option) :

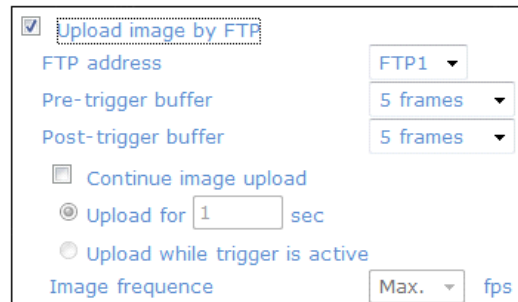
The administrator can specify alarm actions that will take place at alarm occurrence. All options are listed as follows.

Triggered Action (Multi-option) :

The administrator can specify alarm actions that will take place at alarm occurrence. All options are listed as follows.

- 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 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.

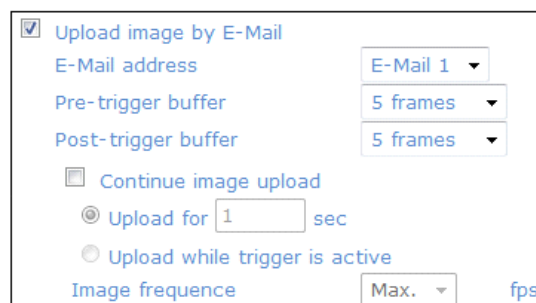
Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.10. 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 picture below. When a motion is detected, 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 via E-Mail 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 via E-Mail 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: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

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

- Upload image to SD card:

Enable the SD card recording by ticking the box next to "Upload image to SD card".

Pre-trigger buffer: The device will send designated frame numbers before the event (1~20 frames).

Post-trigger buffer: The device will send designated frame numbers after the event (1~20 frames).

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 :

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

9.8.6. Manual trigger

In the Manual Trigger setting, the current image(s) or video(s) can be upload to the appointed destination, such as an FTP site or an E-mail address. The administrator can specify the triggered actions that will take place when the users switched the Manual Trigger button to <On>. All options are listed as follows.

The screenshot shows the Grundig web interface for the Manual Trigger configuration. The left sidebar contains a navigation menu with categories like System, Security, Network, and Events. The main panel is titled 'Manual Trigger' and includes a toggle switch to enable or disable the function. Below this, there is a 'Triggered Action' section with several checkboxes and dropdown menus for configuring actions like enabling alarm output, sending messages via FTP or email, and recording to an SD card. A 'File Name' section allows setting a default filename and choosing how to handle subsequent files (e.g., add date/time suffix, sequence number, or overwrite).

Manual Trigger :

The default setting for the Manual Trigger function is <Off>. Enable the function by selecting <On>. After the Manual Trigger function is enabled, click on the Manual Trigger button on the Home page to start uploading data. Click again to stop uploading.

Triggered Action (Multi-option) :

The administrator can specify alarm actions that will take place at alarm occurrence. All options are listed as follows.

Triggered Action (Multi-option) :

The administrator can specify alarm actions that will take place at alarm occurrence. All options are listed as follows.

- Enable Alarm Output:

Select this item to enable the alarm relay outputs.

- IR Cut Filter:

Select the item and the IR cut filter (ICR) of the camera will be removed (on) or blocked (off) when an alarm is triggered.

Note: The IR Function (Please refer to the section "IR Function") cannot be set as <Auto> mode if this trigger action is enabled.

- Send Message by FTP:

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

- Send 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 screenshot shows a configuration window titled 'Upload image by FTP'. It contains the following settings: 'FTP address' is set to 'FTP1'; 'Pre-trigger buffer' is set to '5 frames'; 'Post-trigger buffer' is set to '5 frames'; the 'Continue image upload' checkbox is unchecked; 'Upload for' is set to '1 sec' with a radio button selected; 'Upload while trigger is active' is an unselected radio button option; and 'Image frequency' is set to 'Max.' with 'fps' as the unit.

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

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

- 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 screenshot shows a configuration window titled 'Upload image by E-Mail'. It contains the following settings: 'E-Mail address' is set to 'E-Mail 1'; 'Pre-trigger buffer' is set to '5 frames'; 'Post-trigger buffer' is set to '5 frames'; the 'Continue image upload' checkbox is unchecked; 'Upload for' is set to '1 sec' with a radio button selected; 'Upload while trigger is active' is an unselected radio button option; and 'Image frequency' is set to 'Max.' with 'fps' as the unit.

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 by E-Mail 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 via E-Mail 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 and/or FTP configuration has been completed. See section 9.5. Mail and 9.6. FTP for further details.

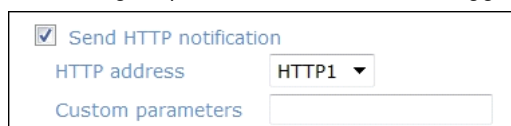
NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

- Send HTTP notification:

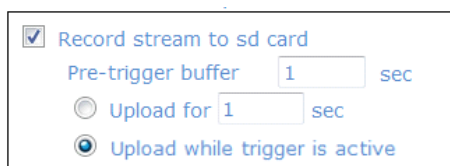
Check this item, select the destination HTTP address, and specify the parameters for event notifications when an <Alarm> is triggered. As soon as an alarm is triggered, the notification will be sent to the specified HTTP server.

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 manually triggered recording will be saved on your Micro SD card.



The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 seconds.

Select <Upload for __ sec> to set the recording duration after an 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 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 9.10. Recording (on Camera) for further details.

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.

9.8.7. Face detection

Here you can adjust the settings for the Face detection. The camera will display a green box when a face is detected.

The screenshot shows the Grundig web interface for Face Detection settings. The left sidebar lists various system settings, with 'Face detection' selected. The main panel is titled 'Face Detection' and contains the following sections:

- Face Detection:** Radio buttons for 'Off' and 'On' (selected).
- Face Detection Setting:** Radio buttons for 'By schedule' (selected) and 'Please select ...'. Below are input fields for 'Sensitivity level [0-64]' (29), 'Minimum size [120-960]' (120), and 'Maximum size [120-960]' (960).
- Triggered Action:** Checkboxes for 'Enable alarm output' (selected), 'Send message by FTP', 'Upload image by FTP', 'Send HTTP notification', 'Record stream to sd card', 'Send message by E-Mail', and 'Upload image by E-Mail'. The 'Enable alarm output' dropdown is set to 'high'.
- File Name:** 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'.

A 'Save' button is located at the bottom of the settings panel. A small video feed in the top right corner shows a room with a green box indicating a detected face.

Face Detection :

The default setting for the Face Detection function is <Off>. Enable this function by selecting <On>. Users can also activate the function according to the schedule time that is was previously set in the <Schedule> setting page. Select <By schedule> and click <Please select...> to choose the desired schedule from the drop-down menu.

- Sensitivity level [0-64]:

Here you can set the sensitivity level of the face detection. The bigger the value, the more sensitive the detection is.

- Minimum size [120-960]:

Please choose the minimum size of the face to be detected here.

- Maximum size [120-960]:

Please choose the maximum size of the face to be detected here.

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 a face is detected.

- 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.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.10. 'Recording (on Camera)' for further details.

- Send Message by FTP:

The Administrator can choose to send an alarm message by FTP when an alarm 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.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

NOTE: Please make sure that the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 9.10. 'Recording (on Camera)' for further details.

- Send 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 screenshot shows a configuration window titled 'Upload image by FTP'. It contains the following settings: 'FTP address' is set to 'FTP1'; 'Pre-trigger buffer' is set to '5 frames'; 'Post-trigger buffer' is set to '5 frames'; 'Continue image upload' is unchecked; 'Upload for' is set to '1 sec' with a radio button selected; 'Upload while trigger is active' is unselected with a radio button; and 'Image frequency' is set to 'Max.' with a dropdown arrow and 'fps' unit.

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: Please make sure that the local recording (with Micro SD/SDHC card) or the remote recording (with NAS) is activated so that this function can be implemented. See section 9.10. Recording (on Camera) for further details.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

- 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 screenshot shows a configuration window titled 'Upload image by E-Mail'. It contains the following settings: 'E-Mail address' is set to 'E-Mail 1'; 'Pre-trigger buffer' is set to '5 frames'; 'Post-trigger buffer' is set to '5 frames'; 'Continue image upload' is unchecked; 'Upload for' is set to '1 sec' with a radio button selected; 'Upload while trigger is active' is unselected with a radio button; and 'Image frequency' is set to 'Max.' with a dropdown arrow and 'fps' unit.

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 by E-Mail 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 via E-Mail 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.

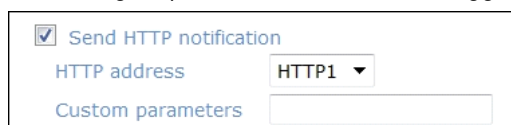
NOTE: Make sure SMTP and/or FTP configuration has been completed. See section 9.5. Mail and 9.6. FTP for further details.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range will change accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

- 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.



The screenshot shows a configuration box for 'Send HTTP notification'. It contains a checked checkbox labeled 'Send HTTP notification'. Below it, there are two rows: 'HTTP address' with a dropdown menu showing 'HTTP1', and 'Custom parameters' with an empty text input field.

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. 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 9.10. ‘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.

The screenshot shows the Grundig Storage Management web interface. On the left is a navigation menu with options: >System, System, Security, Network, DDNS, Mail, FTP, HTTP, Events, Storage management, Recording, Schedule, File location, View information, Factory default, Software version, Software upgrade, Maintenance, and < Back. The main content area is titled 'Storage Management' and contains several sections: 'Device information' showing 'Device type: SD card - n/a', 'Free space: 0KB', 'Total size: 0KB', 'Status: No', and 'Full: No'; 'Device setting' with a 'Format device' button; 'Disk cleanup setting' with checkboxes for 'Enable automatic disk cleanup', 'Remove recordings older than' (set to 1 day(s)), and 'Remove oldest recordings when disk is' (set to 85% full), with a 'Save' button; and 'Recording list' with search filters for 'From' and 'to' dates (both 2010-04-22), a 'Search' button, radio buttons for 'VIDEO' (selected) and 'JPEG', and a table with columns 'FileName' and 'Size'. Below the table are 'Remove', 'Sort', and 'download' buttons.

NOTE: It is not recommended to record with the microSD card for 24/7 continuously as it may not be able to support long term continuous data reading/writing. Please contact the manufacturer of the microSD card for information regarding the reliability and the life expectancy.

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.

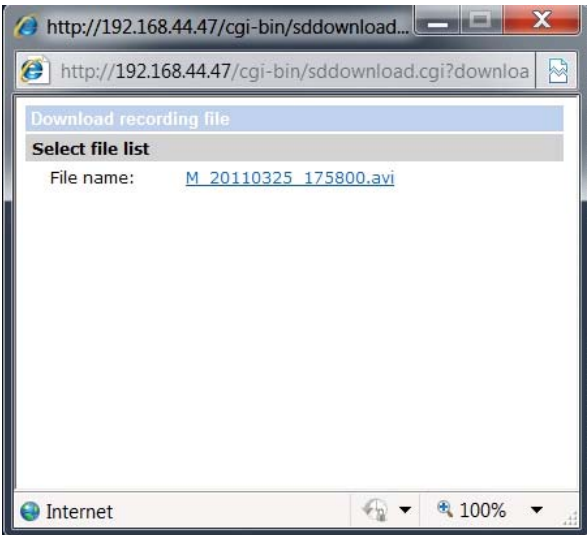
- Sort:

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 / N / R / T / V) appearing in the very beginning of a name denote the sort of the recording: A stands for Alarm, M stands for Motion, N stands for Network Failure, R stands for regular recording, T stands for Tampering and V stands for Manual Trigger.

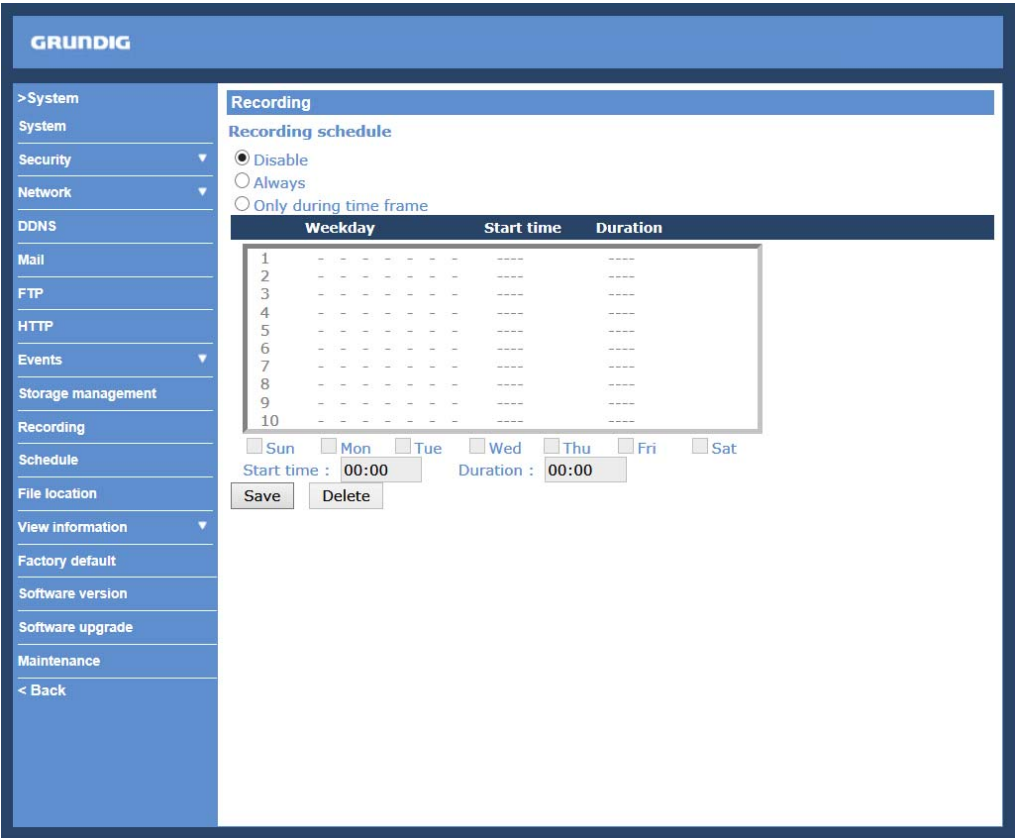
- Download:

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.



9.10. Recording (on Camera)

In the Recording setting page, the Micro SD Card recording schedule supports up to ten sets of time frames. Users can specify the recording schedule to fit their present surveillance requirements.



Activating the Recording Schedule :
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. Or select a set of schedules from the time frame blank, check specific weekdays and set up the start time (hour:minute) and time period (hour:minute) to activate the recording in certain time frames. The setting range for the time period hour is from 0 to 168.

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

Select a recording schedule from the schedule list, and click "Delete" to delete the recording schedule.

Terminating the Recording Schedule :
Select "Disable" to terminate the recording function.

9.11. Schedule

This function allows the users to setup schedules for features including: <Alarm Switch>, <Motion Detection> and <Network Failure Detection>. The function supports up to 10 sets of time frames in the time frame list.

	Weekday	Start time	Duration
1	- - - - -	----	----
2	- - - - -	----	----
3	- - - - -	----	----
4	- - - - -	----	----
5	- - - - -	----	----
6	- - - - -	----	----
7	- - - - -	----	----
8	- - - - -	----	----
9	- - - - -	----	----
10	- - - - -	----	----

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Day
☐ Night
☒ Time

Start time : 00:00 Duration : 24:00

Save Delete

Setting a schedule:

To set a schedule, please select a time frame from the time frame list first. Then check the boxes at the bottom of the time frame to choose the specific weekdays. At last, type in the start time (hour:minute) and the duration time (hour:minute) for activation of the schedule triggered features. The setting range for the duration time is from 00:00 to 168:59.

Click "Delete" to delete a chosen time frame.

Click on "Save" to confirm the setting.

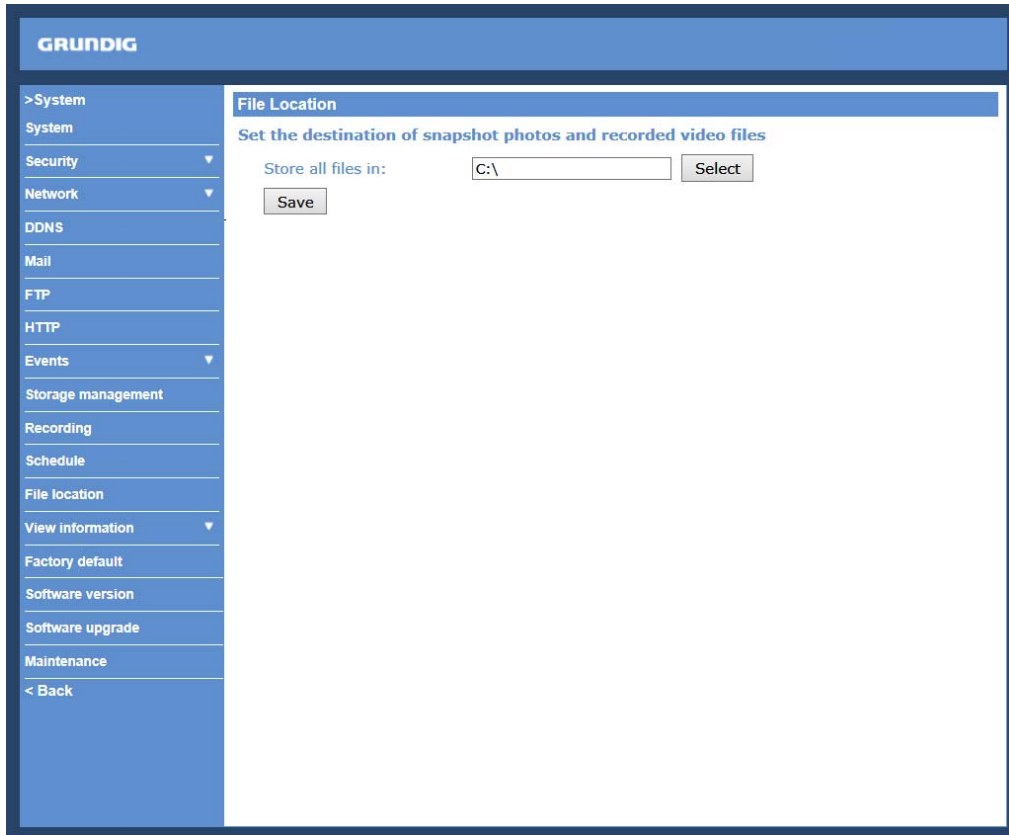
NOTE: Users MUST select <By schedule> for each feature (in the setting page of the feature) to enable the schedule function for this feature.

The features are: <Alarm Switch> (in the "Application" page), <Motion Detection> and <Network Failure Detection>.

9.12. 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.



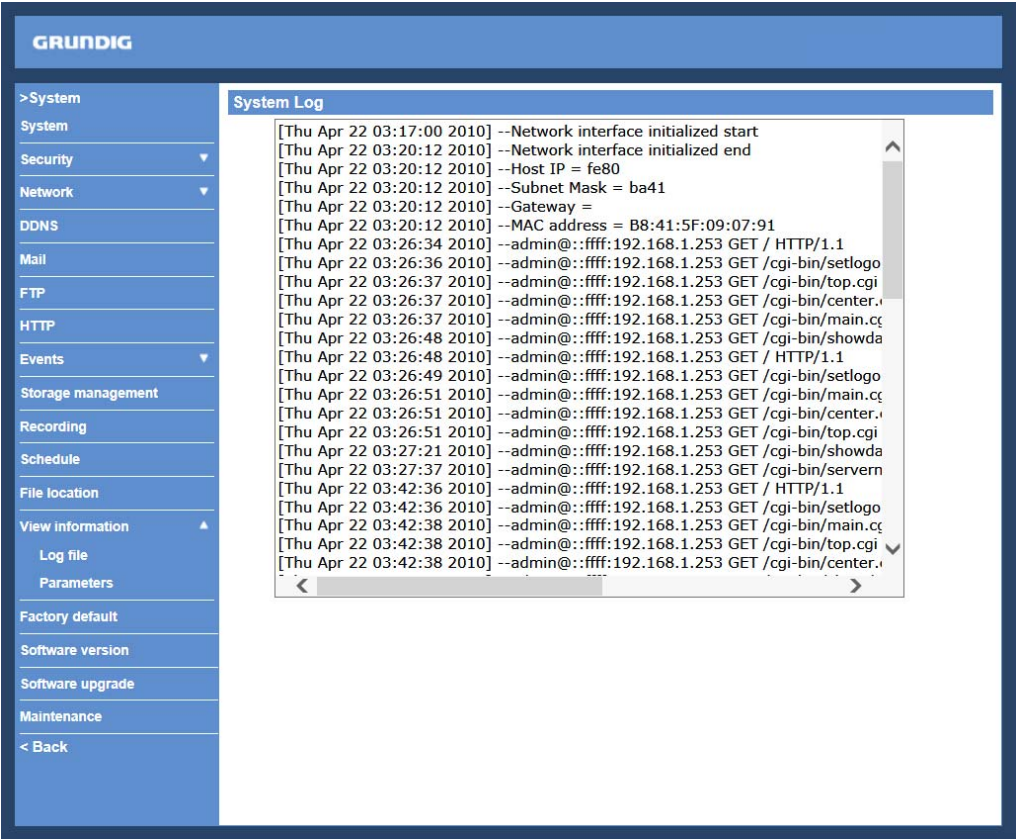
The screenshot displays the Grundig web interface. On the left is a blue sidebar menu with the following items: >System, System, Security (with a dropdown arrow), Network (with a dropdown arrow), DDNS, Mail, FTP, HTTP, Events (with a dropdown arrow), Storage management, Recording, Schedule, File location, View information (with a dropdown arrow), Factory default, Software version, Software upgrade, Maintenance, and < Back. The main content area has a blue header bar with the text "GRUNDIG" on the left and "File Location" on the right. Below the header, the text "Set the destination of snapshot photos and recorded video files" is displayed. Underneath, there is a label "Store all files in:" followed by a text input field containing "C:\", a "Select" button, and a "Save" button.

NOTE: Users with the Windows 7 or Windows 8 operating system on their PC need to follow the following procedure to be able to use the Snapshot and Web Recording 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).

9.13. View Information

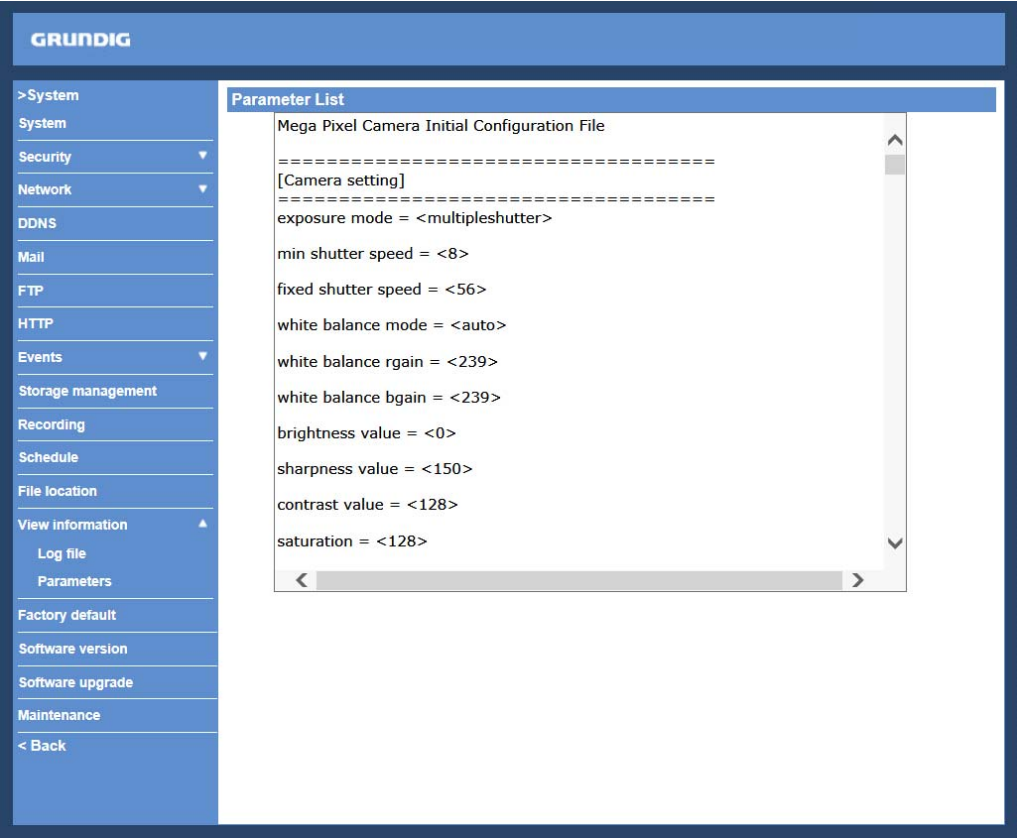
9.13.1. Log file

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.



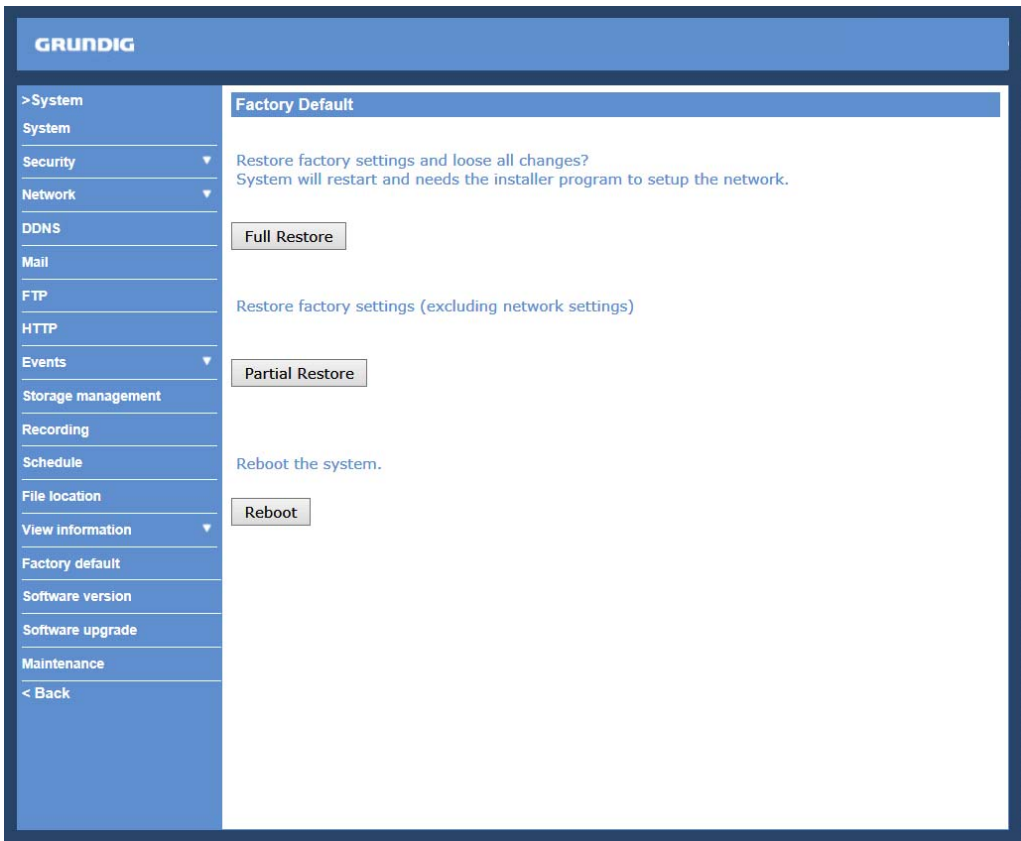
9.13.2. Parameters

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



9.14. Factory Default

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



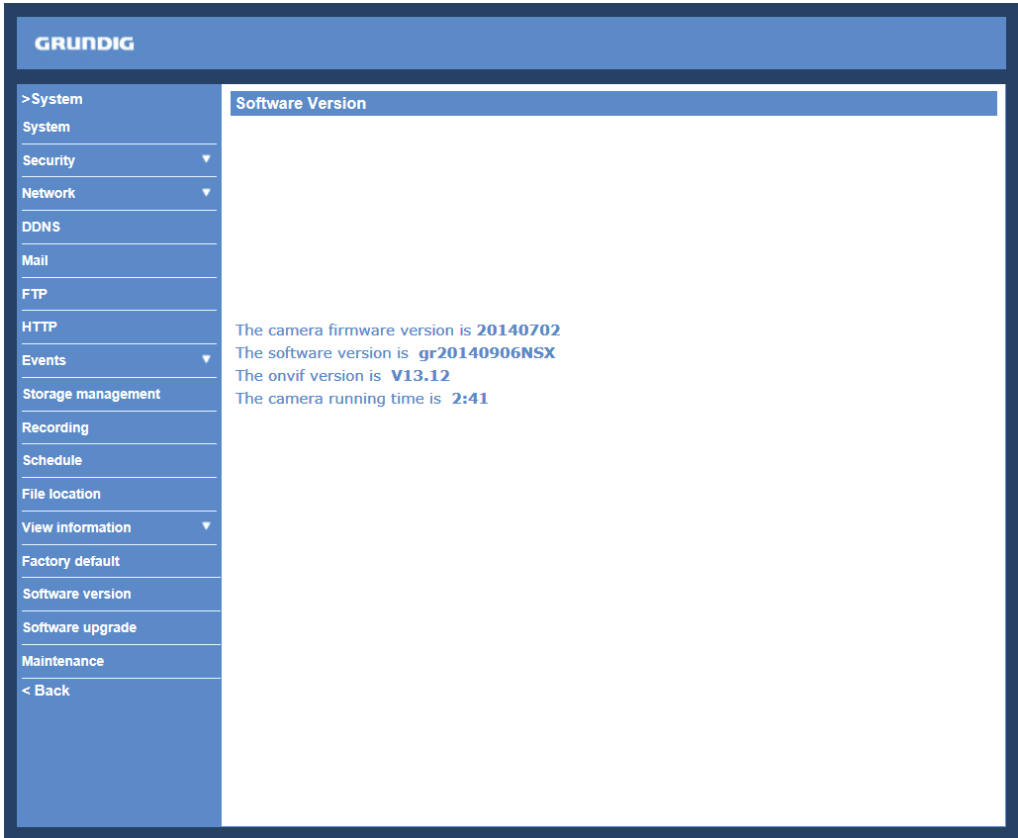
Full Restore :
Click on the “Full Restore” button to recall the factory default settings. After 30 seconds the system will restart.
NOTE: The IP address will also be restored to default (192.168.1.1).

Partial Restore :
Click on the “Partial Restore” button to recall the factory default settings, except for the network settings.

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

9.15. Software Version

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



9.16. 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: GCI-Firmware.

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 “GCI-Firmware”.

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.

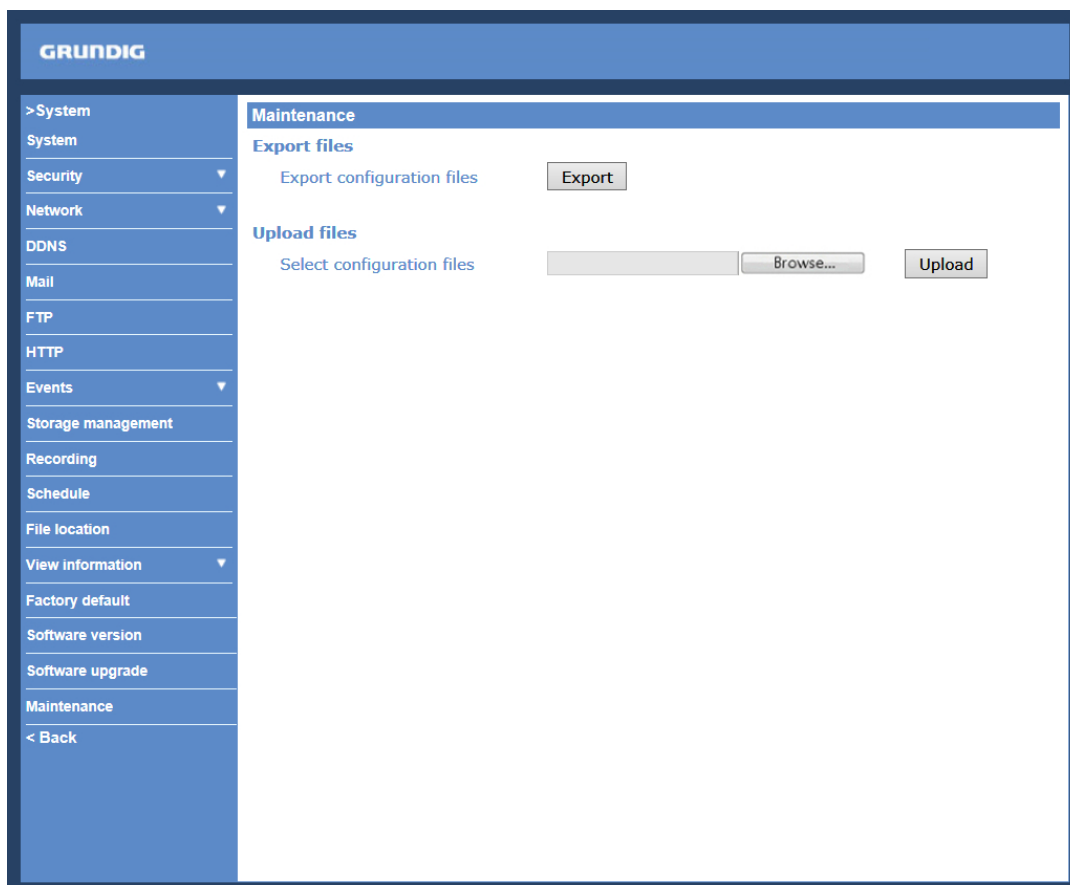
Step 4: Close the video browser.

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.

9.17. 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.

GRUNDIG

> Streaming

Video Format

Video Compression

Video ROI

Video OCX Protocol

Video Frame Rate

Video Mask

Audio

< Back

Video Format

Video Resolution :

H.264 + H.264

Format 1 : 1920 x 1080 (25 fps)

H.264-1

Format 2 : 720 x 576 (25 fps)

H.264-2

BNC support : Yes

Portrait support : Yes

Save

Note :

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

Text Overlay Settings :

☐ Include date

☐ Include time

☐ Include text string:

Text color : black

Text background color : transparent

Save

Video Portrait Allow :

No

Save

Video Rotation Type :

Normal video

Save

GOV Settings :

H.264-1 GOV Length : 25

H.264-2 GOV Length : 25

H.264-3 GOV Length : 25

H.264-4 GOV Length : 25

Save

Click on “Save” to confirm the setting.

Text Overlay Settings :

Users can select these items to display data (date/time/text/subtitle) on the live video pane. The maximum length of the string for the text is 15 alphanumeric characters, and each subtitle can only be 16 characters. Users can choose the locations in which the items are to be displayed on the live pane. Please note that the items cannot be set to the same location.

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 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 1 to 255. The default setting of GOV is 60 which means there is one I-frame every 60 seconds. The default value for H.264-1/ H.264-2/ H.264-3/ H.264-4 is 60/ 60/ 30/ 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. Users can set each H.264 Profile to <Baseline Profile>, <Main Profile> or <High Profile> according to the compression needs. With the same bit rate, the higher the compression ratio, the better the image quality is. The default setting is <Main Profile>.

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 2048 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.

GRUNDIG

> Streaming
Video Format
Video Compression
Video ROI
Video OCX Protocol
Video Frame Rate
Video Mask
Audio
< Back

Video Compression

MJPEG Compression setting :
MJPEG Q factor : 35
Save

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

H.264-2 Compression setting :
H264-2 bit rate : 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.

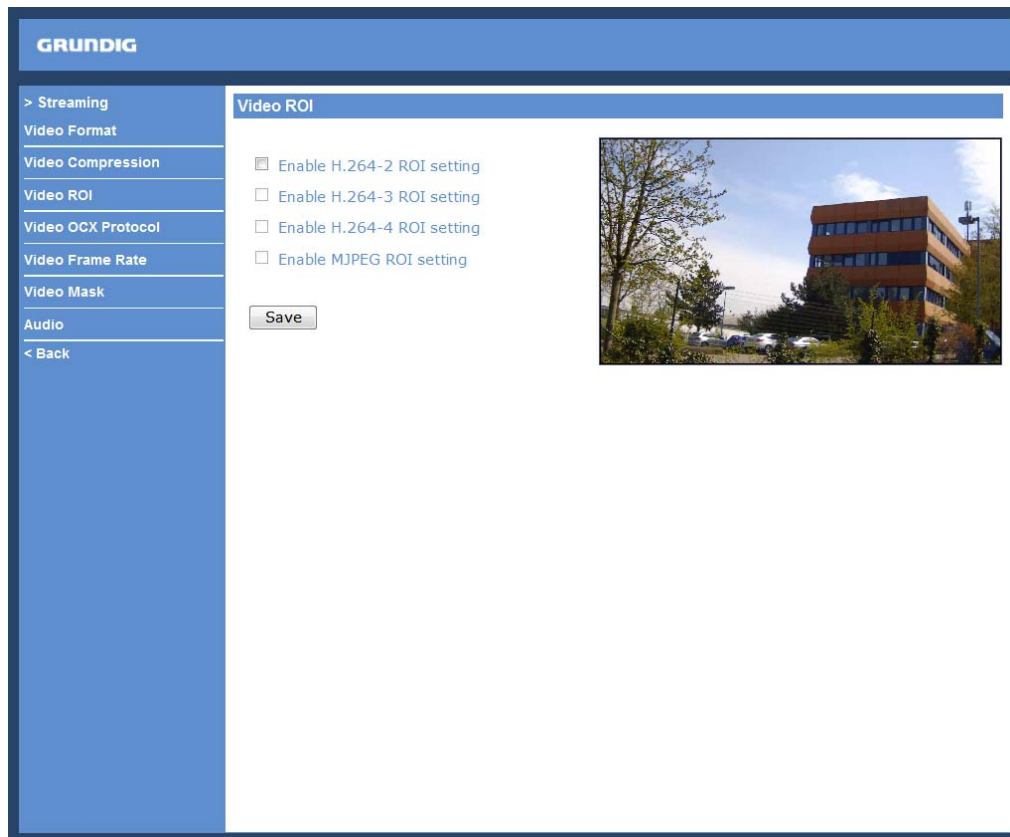
Click on "Save" to confirm the setting.

10.3. Video ROI

The "Video ROI" setting can be found under this path: "Streaming" > "Video ROI".

ROI stands for Region of Interest. This function allows the users to select a specific monitoring region for H.264-2, H.264-3, H.264-4 and MJPEG streams, instead of showing the full image.

NOTE: This function is only available when triple streams or above is selected under <Video Resolution> in the "Video Format" Setting.



Video ROI Setting:

- Enable the H.264-2 ROI Setting:

When you check the box, H.264-2 ROI Window will be displayed. To change the size of the H.264-2 ROI Window, move the mouse cursor to the edge of the frame and draw it outward / inward. Moving the mouse to the center of the frame can shift the frame to the intended location.

NOTE: The H.264-2 ROI setting is only available when at least H.264 + H.264 + H.264 (triple stream) is selected under <Video Resolution> in the Video Format Setting.

- Enable the H.264-3 ROI Setting:

When you check the box, the H.264-3 ROI Window will be displayed. To change the size of the H.264-3 ROI Window, move the mouse cursor to the edge of the frame and draw it outward / inward. Moving the mouse to the center of the frame can shift the frame to the intended location.

NOTE: The H.264-3 ROI setting is only available when at least H.264 + H.264 + H.264 (triple stream) is selected under <Video Resolution> in the Video Format Setting.

- Enable the H.264-4 ROI Setting:

When you check the box, the H.264-4 ROI Window will be displayed. To change the size of the H.264-4 ROI Window, move the mouse cursor to the edge of the frame and draw it outward / inward. Moving the mouse to the center of the frame can shift the frame to the intended location.

NOTE: The H.264-4 ROI setting is only available when H.264 + H.264 + H.264 + H.264 is selected under <Video Resolution> in the Video Format Setting.

- Enable the MJPEG ROI Setting:

When you check the box, the MJPEG ROI Window will be displayed. To change the size of the MJPEG ROI Window, move the mouse cursor to the edge of the frame and draw it outward / inward. Moving the mouse to the center of the frame can shift the frame to the intended location.

NOTE: The MJPEG ROI setting is only available when H.264 + H.264 + H.264 + MJPEG or H.264 + H.264 + MJPEG is selected under <Video Resolution> in Video Format Setting.

10.4. 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 H.264/MJPEG video address, H.264 video port, MJPEG video port, audio address, audio port and TTL into each blank.

Click on "Save" to confirm the setting.

10.5. Video Frame Rate

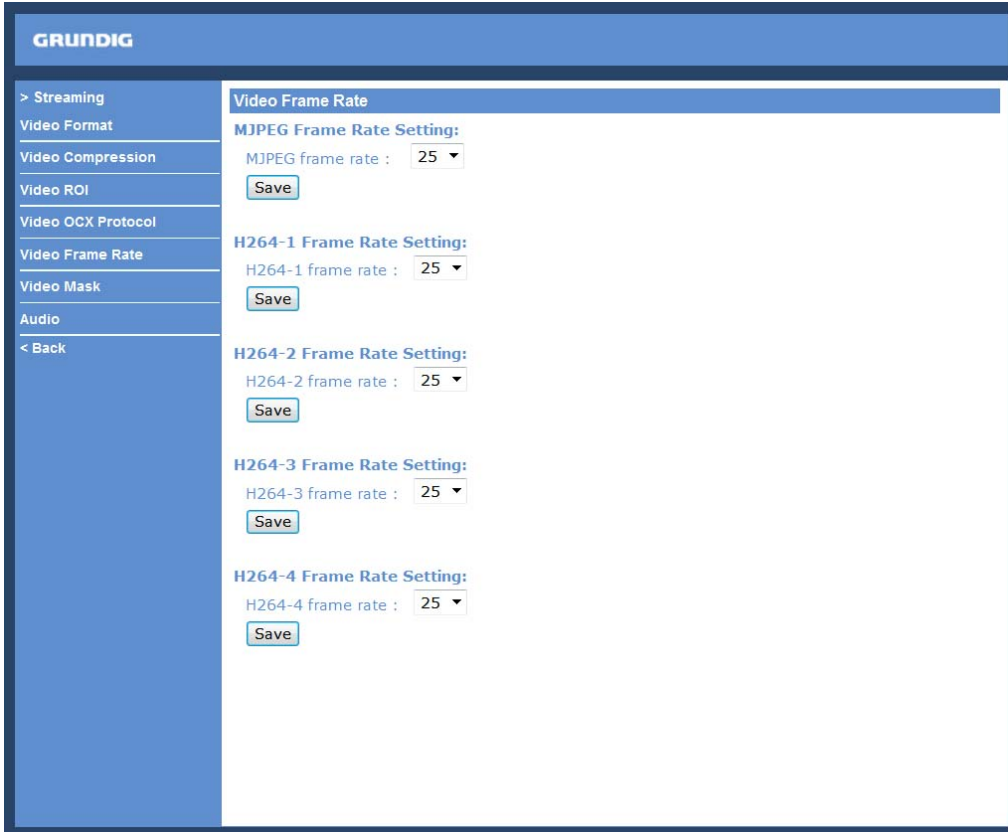
The video frame rate is for setting the frames per second (fps) if needed.

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

The default setting of the MJPEG Frame Rate is 25 fps; the setting range is from 1 to 25 (PAL).

Click on <Save> to confirm the setting.

NOTE: A lower frame rate will decrease the video smoothness.

The screenshot shows the Grundig web interface for video settings. On the left is a blue sidebar with a menu: > Streaming, Video Format, Video Compression, Video ROI, Video OCX Protocol, Video Frame Rate (highlighted), Video Mask, Audio, and < Back. The main content area has a blue header 'GRUNDIG' and a sub-header 'Video Frame Rate'. Below this, there are four settings sections: 'MJPEG Frame Rate Setting:' with 'MJPEG frame rate : 25' and a 'Save' button; 'H264-1 Frame Rate Setting:' with 'H264-1 frame rate : 25' and a 'Save' button; 'H264-2 Frame Rate Setting:' with 'H264-2 frame rate : 25' and a 'Save' button; and 'H264-3 Frame Rate Setting:' with 'H264-3 frame rate : 25' and a 'Save' button. There is also a partially visible 'H264-4 Frame Rate Setting:' section at the bottom.

H.264-1 Frame Rate:

The default setting and setting range for H.264-1 will change according to the video format selected for the <TV system> under the <Camera> menu.

For PAL, the default setting can be 25 fps or 50 fps. 50 fps is only available when a video format with "50 fps" is selected under <TV System>. The setting range is 1 to 25 or 1 to 50.

For NTSC, the default setting can be 30 fps or 60 fps. 60 fps is only available when a video format with "60 fps" is selected under <TV system>. The setting range is 1 to 30 or 1 to 60.

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

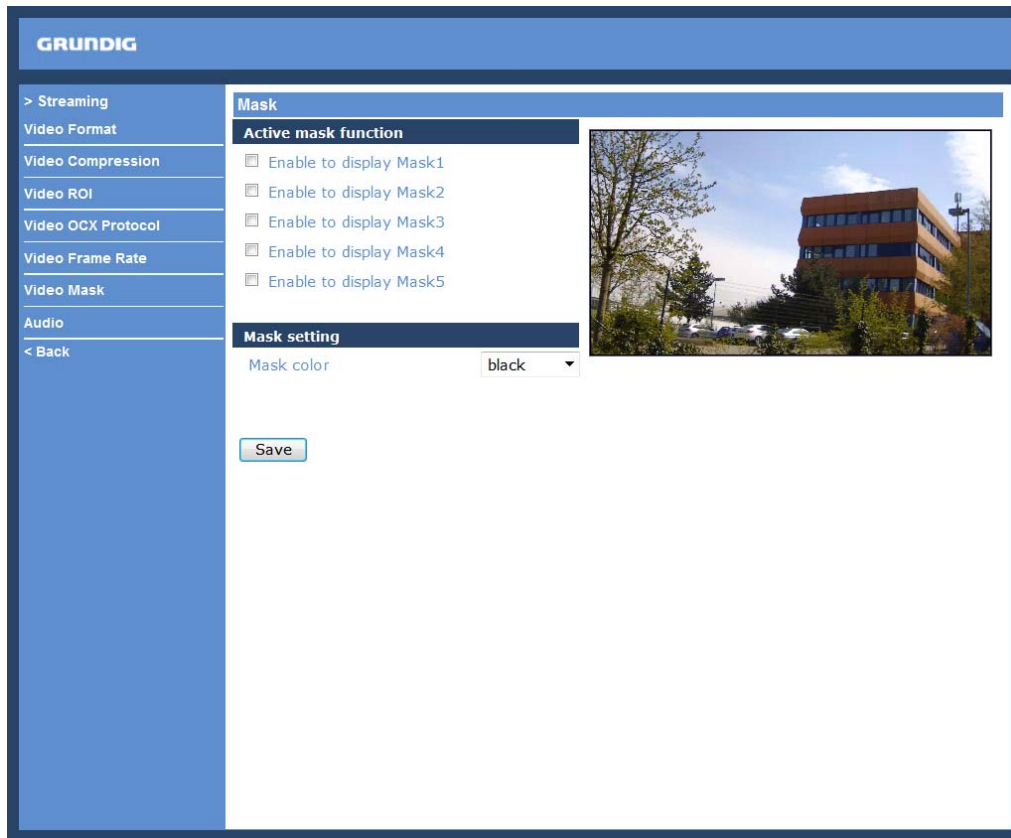
The default setting of the MJPEG / H.264-2 / H.264-3 / H.264-4 Frame Rate is 25 fps (PAL) or 30 fps (NTSC). The setting range is from 1 to 50 (PAL) or from 1 to 60 (NTSC). The maximum range of MJPEG / H.264-1 / H.264-2 / H.264-3 / H.264-4 Frame Rate will change according to the selected video resolution on the <Video Format> page.

Click on <Save> to confirm the setting.

NOTE: A lower frame rate will decrease video smoothness.

10.6. Video Mask

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



Active Mask Function :

- How to add a mask:

When you check a Video Mask checkbox ("Enable to display Mask..."), 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.

- How to 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.

10.7. 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.

The screenshot shows the Grundig Audio settings interface. The left sidebar lists various settings, with 'Audio' currently selected. The main panel displays the 'Audio' configuration options. Under 'Transmission mode', the 'Disable' option is selected. The 'Server gain setting' section shows both input and output gains set to 3. The 'Bit rate' is set to uLAW, and 'Recording to Storage' is set to Disable. Save buttons are provided for the bit rate and recording settings.

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.

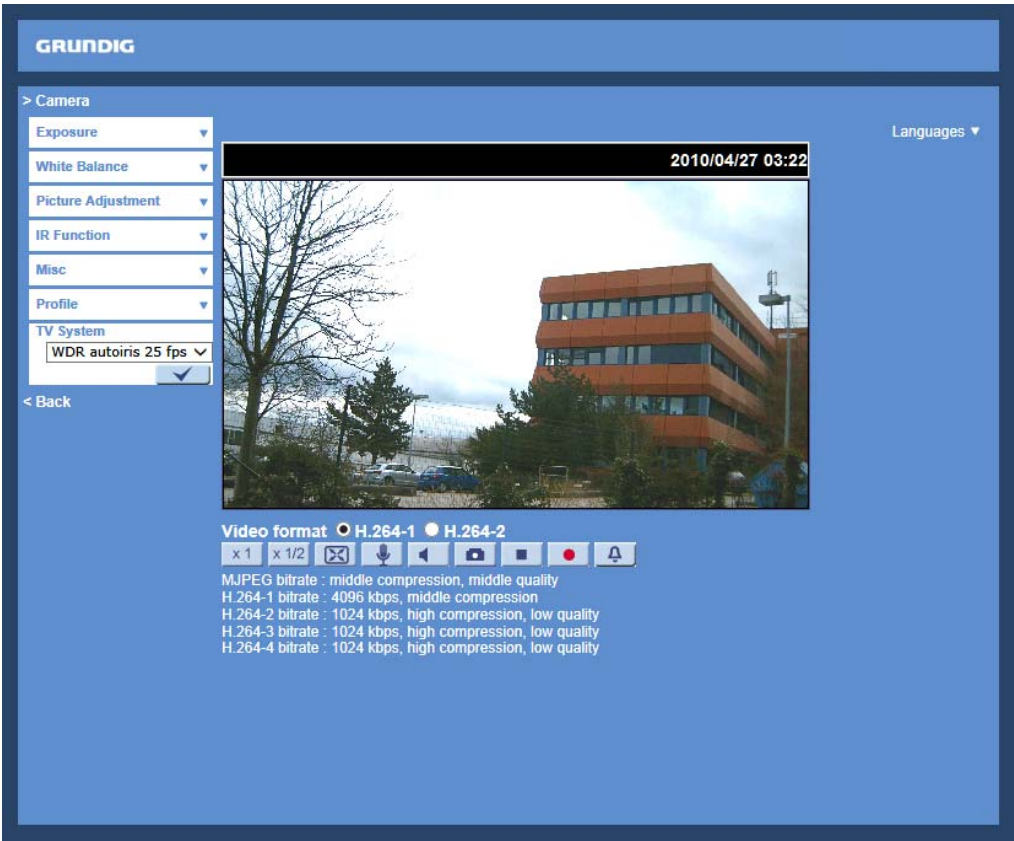
Recording to Storage :

Select <Enable> from the drop-down menu to enable the audio recording together with the videos onto an SD card.

NOTE: If the chosen bit rate is not compatible with the player, there will be no audio and noise will be heard during playback.

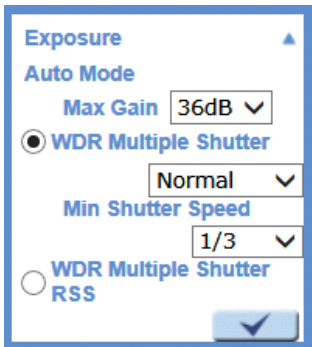
11. Camera Settings

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



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:

- Max Gain:
The maximum gain can be set to reduce the image noises.

- WDR Multiple Shutter Mode:

This mode provides the Wide Dynamic Range (WDR) function that solves high contrast or light changing issues. There are two different options available (Normal and WDR First). The default setting is <WDR First>. Please refer to the following descriptions to choose a suitable option from the drop down menu. The minimum shutter speed can be set from 1 to 1/500 sec. (NTSC) or from 1/1.5 to 1/425 sec. (PAL).

> Normal:

With this option, the WDR function is less effective with less image noise in the dark environments.

> WDR First:

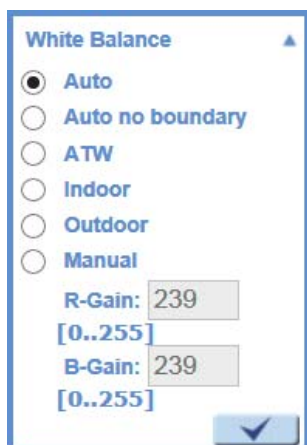
With this option, the WDR function is more effective in dark environments, but generates more image noise.

- WDR Multiple Shutter RSS Mode:

WDR Multiple Shutter RSS Mode is used to solve high contrast or light changing conditions and mainly to reduce the rolling shutter phenomenon. Please note that it is still recommended to choose the WDR Multiple Shutter Mode when the rolling shutter phenomenon is not occurring in the scene.

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.

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

Auto no boundary Mode :

With the Auto no boundary function, the white balance in a scene will automatically be adjusted when the colour temperature is changing. In this mode, the colour temperature boundary is not particularly specified. For example, if the street scene / image will turn extremely yellow due to some street lights, select the Auto No Boundary mode, and the hue of the current image will turn whiter. Please note that all objects in the image will also turn brighter and whiter which may cause the inaccurate colour of the displayed image.

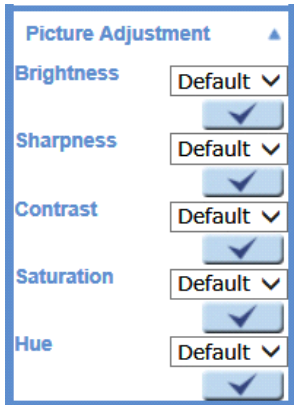
ATW Mode (Auto Tracking White Balance) :
With the Auto Tracking White Balance function, the white balance in a scene will be automatically adjusted while temperature colour is changing. The ATW Mode is suitable for environments with a light source having a colour temperature in the range roughly from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

Indoor/Outdoor Mode :
Select Indoor or Outdoor.

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.

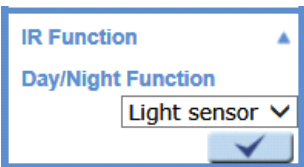
Contrast:
The camera image contrast level is adjustable. Please choose from a range of -6 to +19.
Click on < ✓ > to confirm the new setting.

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. IR Function

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



Day/Night Function :

This item is to define the action of the IR cut filter. Refer to the descriptions of each option below to select a suitable mode. Click on <√> to confirm the new setting.

- Auto Mode:

With this mode, the camera will decide according to the environment whether to remove the IR cut filter.

- Off (Night Mode):

Use this mode when the environment light level is low. The IR cut filter will be removed to allow the camera to deliver clear images in black and white.

- On (Day Mode):

Select this mode to turn on the IR cut filter. The IR cut filter can filter out the IR light and allows the camera to deliver high quality images in colour.

- 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.

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

- Light Sensor Mode :

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

- Light On Mode :

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

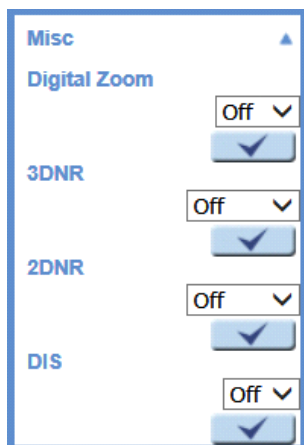
- Light Off Mode :

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

Click on < √ > to confirm the new setting.

11.5. Misc

Here you can set different camera settings (please see the following sub-chapters).



11.5.1. Digital Zoom

The camera's Digital Zoom is adjustable from x2 to x10.

Click on < √ > to confirm the new setting.

11.5.2. 3DNR

The IP Camera provides a 3DNR function for delivering an optimised image quality especially in extra low-light conditions.

Different levels of options (Low / Mid / High) for 3DNR are supported. A higher level of 3DNR generates relatively enhanced noise reduction.

Click on <√> to confirm the new setting.

11.5.3. 2DNR

The IP Camera provides a 2DNR function for delivering clear images without motion blurs in extra low-light conditions.

Different levels of options (Low / Mid / High) for 2DNR are supported. A higher level of 2DNR generates relatively enhanced noise reduction.

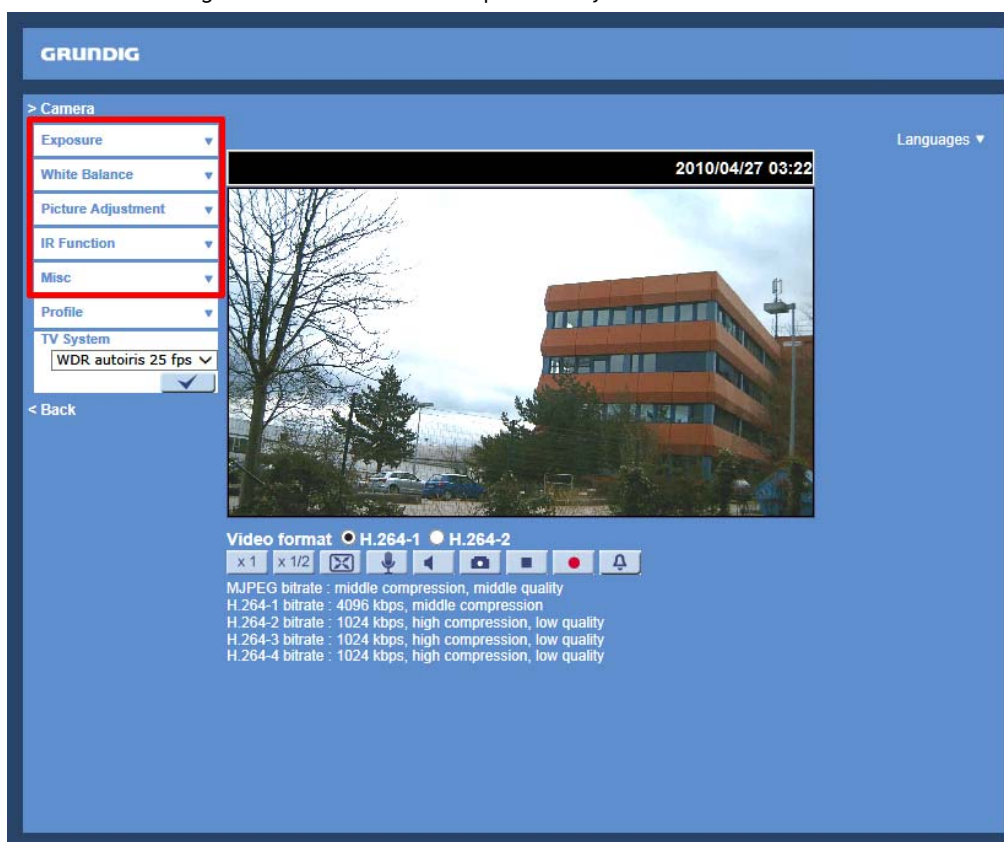
Click on <√> to confirm the new setting.

11.5.4. DIS

The DIS function can minimise blurry images caused by minor camera shake. The default setting is <On>. Click on <√> to confirm the new setting.

11.6. Profile

You can program up to 10 different Profiles which are specific desired camera parameters (they can be found under "Camera", see the picture below) for different environments and assign to them up to 10 schedule setups which need to be set under "System" > "Schedule". You need to set up the schedule(s) in advance. Then you can set up the camera parameters (like Exposure, White Balance, Brightness, Sharpness etc.) under "Camera" and save them as Profiles and assign to these Profiles the previously set schedule(s).



Schedule Setup :

First, you need to set up a schedule and select a time frame from the time frame list. Then please check the weekday boxes below to choose the specific weekdays. At last, select a time mode, Day mode, Night Mode or Time mode. Under Time mode, users can specify the start time and the duration time for activation of the schedule triggered features. The setting range for the duration time is from 00:00 to 168:59. Click on <Save> to save the setup.

	Weekday	Start time	Duration
1	- - - - -	----	----
2	- - - - -	----	----
3	- - - - -	----	----
4	- - - - -	----	----
5	- - - - -	----	----
6	- - - - -	----	----
7	- - - - -	----	----
8	- - - - -	----	----
9	- - - - -	----	----
10	- - - - -	----	----

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Day
☐ Night
☒ Time

Start time : 00:00 Duration : 24:00

Save Delete

Time Mode :

- Day: this profile will be loaded when IR cut is off.
- Night: this profile will be loaded when IR cut is on.
- Time: indicates the start time and time duration for the schedule.

Camera Profile Setup :

Step 1: In the "Camera" tab, set up the camera parameters, such as White Balance, Picture Adjustment, etc.

Step 2: Click on Profile under "Camera" and its setting menu will be displayed (see the picture below). Select a number from the Number drop-down list.

Step 3: Input a name for the profile in the Name field.

Step 4: Click on < ✓ > below the Name field. The camera parameter configuration is saved and applied to the profile.

Now a camera profile is created and saved.

Profile

Num: 1

Name:

☐ By schedule

1

Step 5: Select a profile from the Number drop-down list.

Step 6: Check the box beside <By schedule>. Select and check the schedule(s) from the schedule drop-down list (From Schedule 1 to Schedule 10). You can choose several schedules and assign them to one profile.

Step 7: Click on <√> below <By schedule>.

Now the schedule(s) are assigned to the camera profile.

Follow the steps above to set the rest of the desired profiles.

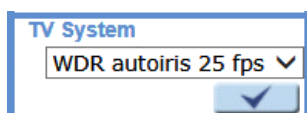
Alternatively, manually select a number from the Number drop-down list. Afterwards, click on the <Arrow/Dot> button under "Profile". Then the camera will load and apply the setting of the profile.

NOTE: If you wish to set the camera parameters to factory default setting, select <Normal> from the Number drop-down list. The Camera will start to load the default values.

NOTE: Users must set the camera parameter of the last profile as the default setting. Thus, if there are gaps between schedules, the camera will apply the setting of the last profile.

11.7. TV System Setup

Select a video format according to the user's TV system (PAL / NTSC). The default setting is <WDR autoiris 25 fps>. Click on <√> to confirm the new setting.



The following table shows the available video formats for these 2 Megapixel camera models. The supported video formats for these models are marked with "√".

Video Format		Model	1.3M	2M
PAL	autoiris 50 fps		√	√
	50 fps		√	√
	WDR autoiris 50 fps		√	-
	WDR autoiris 25 fps		√	√
	WDR 50 fps		√	-
	WDR 25 fps		√	√
NTSC	autoiris 60 fps		√	√
	autoiris 30 fps		-	-
	60 fps		√	√
	30 fps		-	-
	WDR autoiris 60 fps		√	-
	WDR autoiris 30 fps		√	√
	WDR 60 fps		√	-
	WDR 30 fps		√	√

NOTE: The <Exposure> setting will be fixed at the WDR Multiple Shutter mode when a video format with "WDR" is selected.

NOTE: For cameras that feature an Auto Iris Lens, the video format with "autoiris" MUST be selected to activate the Auto Iris function. Otherwise the live video will be displayed as black.

Autoiris:

Select a video format with "autoiris" to activate the Auto Iris function. Power will be supplied to trigger the Auto Iris Lens and hence enable the Auto Iris function.

WDR:

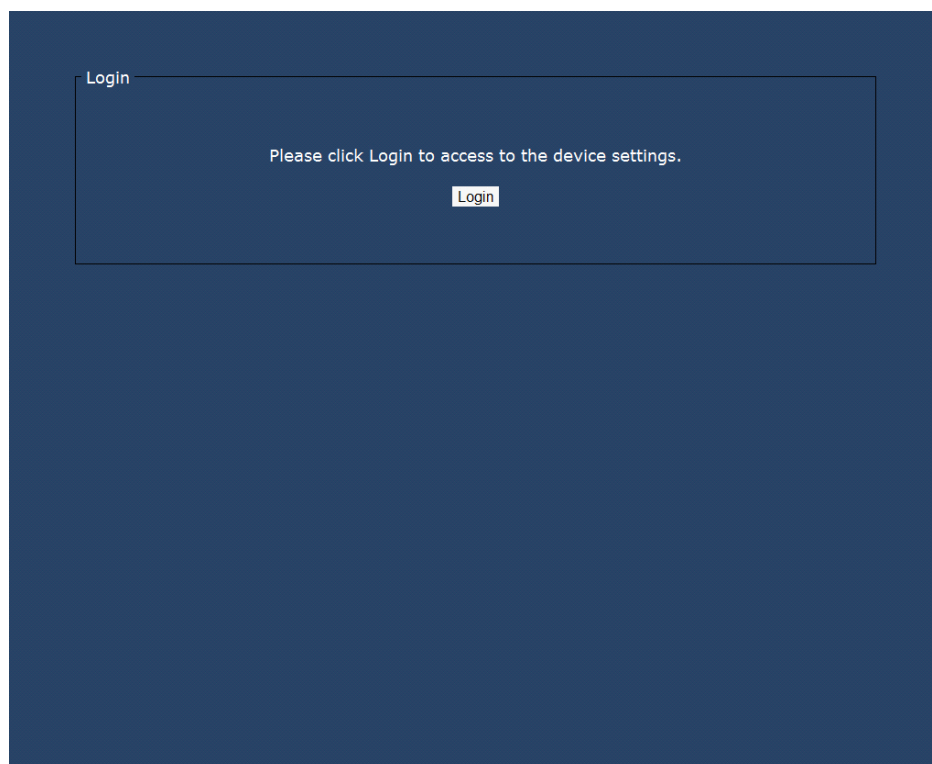
Select a video format with "WDR" to activate the WDR function. The Wide Dynamic Range (WDR) function is for solving high contrast or light changing issues to enhance the video qualities.

WDR autoiris:

Select a video format with “WDR autoiris” to activate both the WDR and the Auto Iris functions.

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.



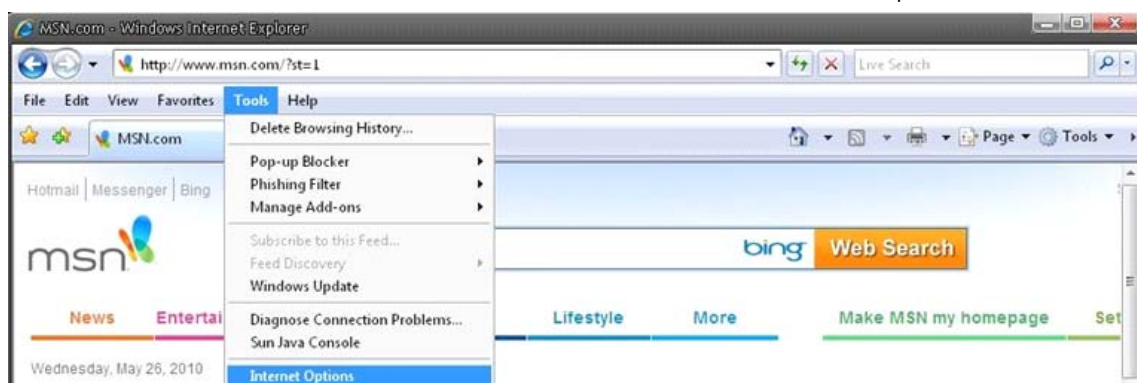
14. Internet Security Settings

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.



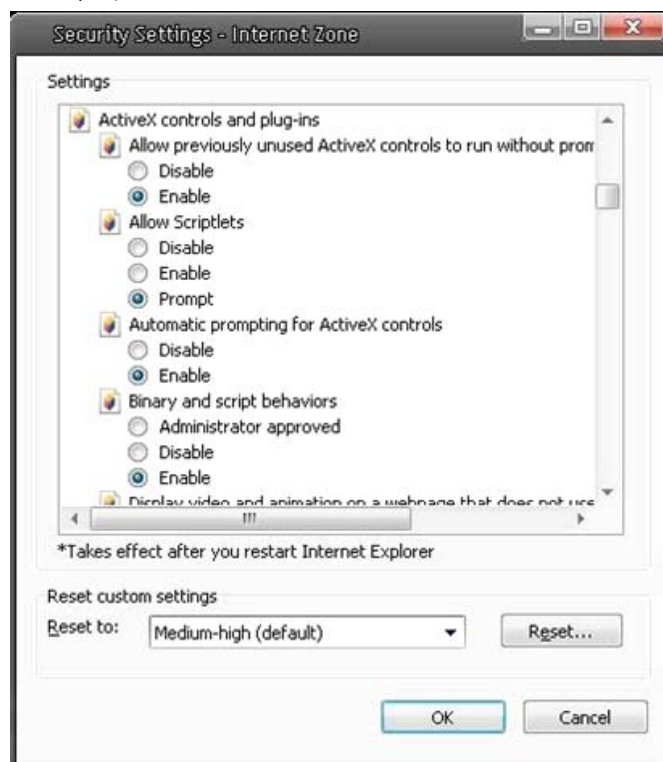
ActiveX Controls and Plug-in Settings :

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.

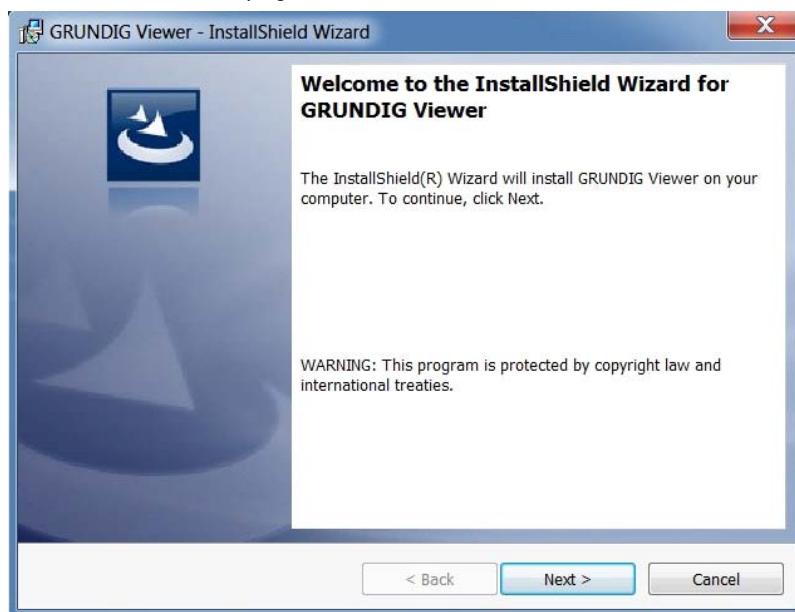
Step 7: Click on <OK> to close the Internet Options screen.

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

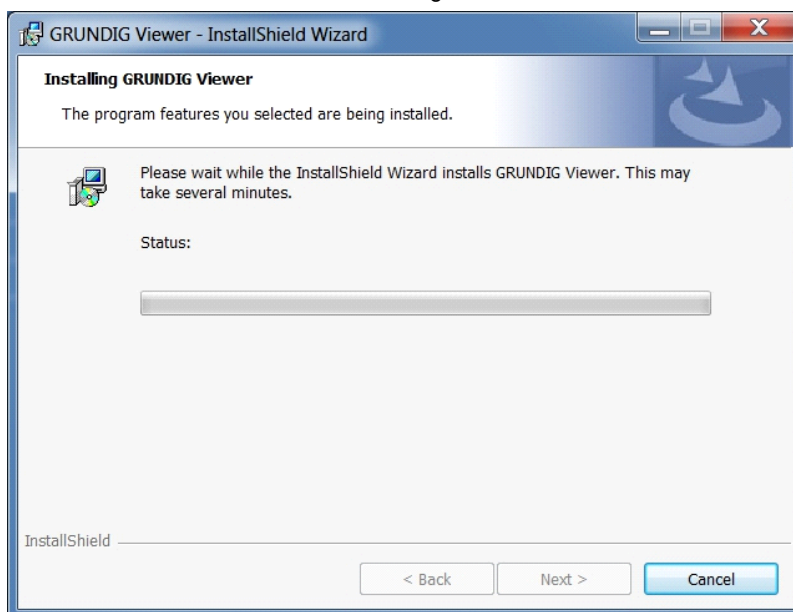
15. GRUNDIG Viewer Download Procedure

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

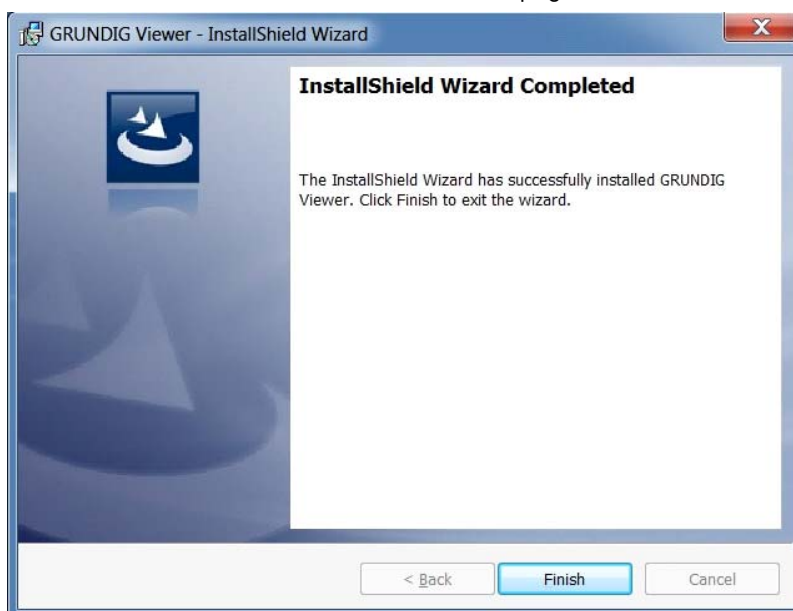
Step 1: In the GRUNDIG Viewer installation page, click “Next” to start the installation.



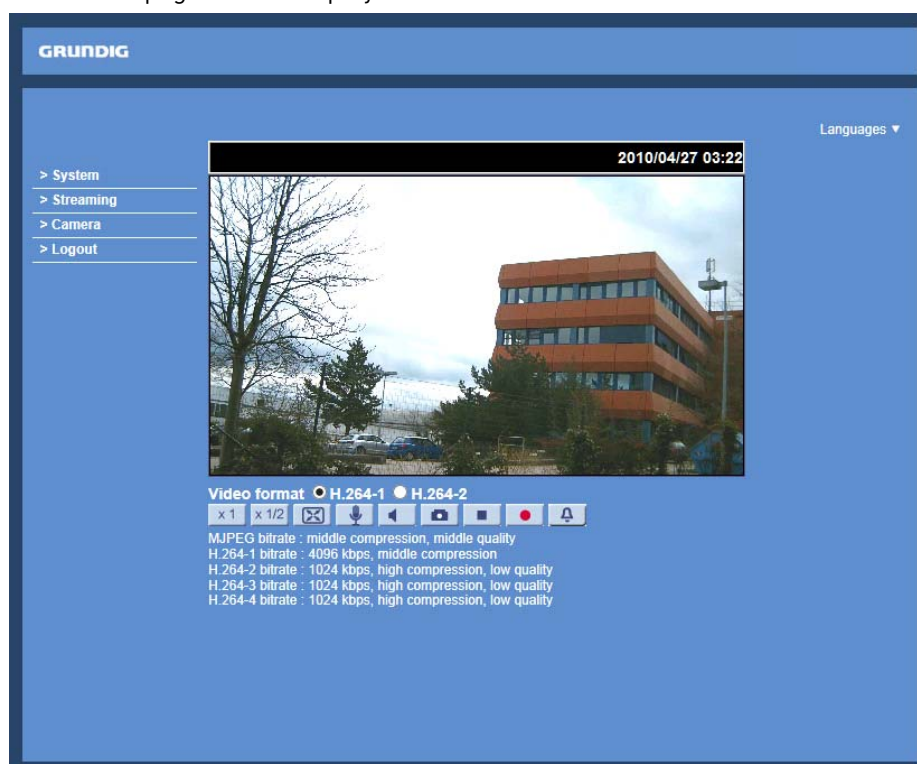
Step 2: Setup starts. Please wait for a while until the loading bar runs out.



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.

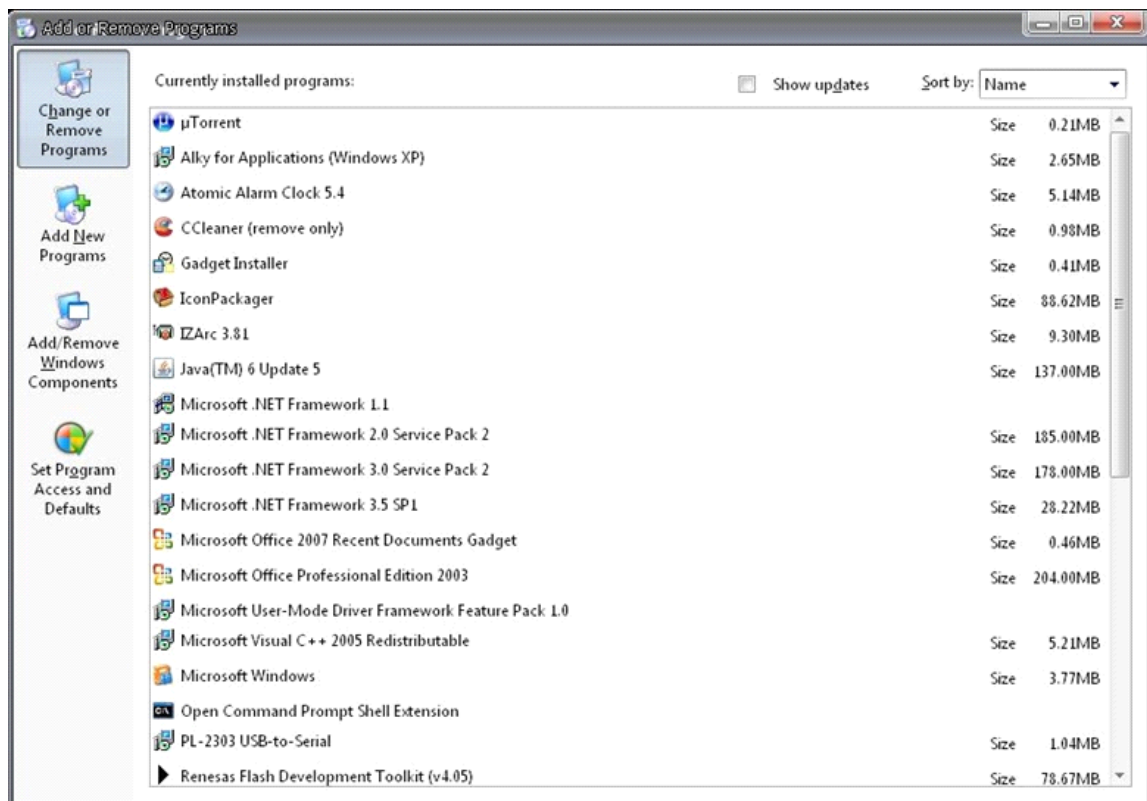
16. Install UPnP Components

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

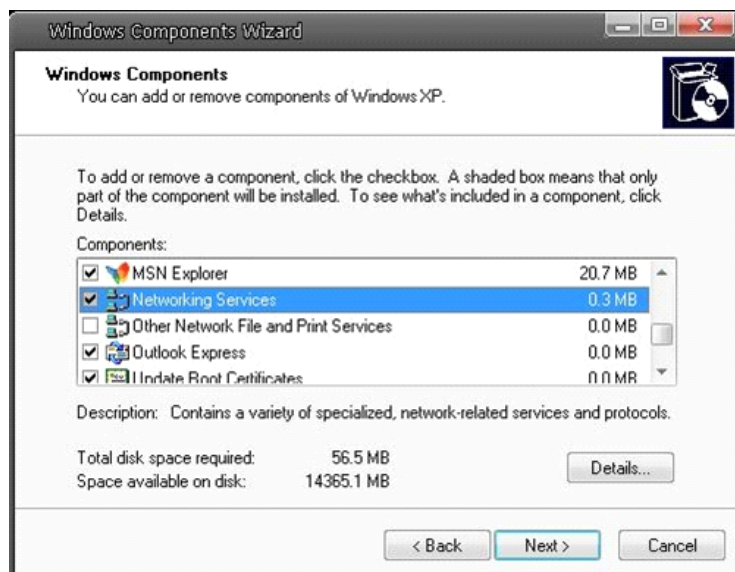
Step 1: Go to "Start", click on "Control Panel", and then double-click on "Add or Remove Programs".



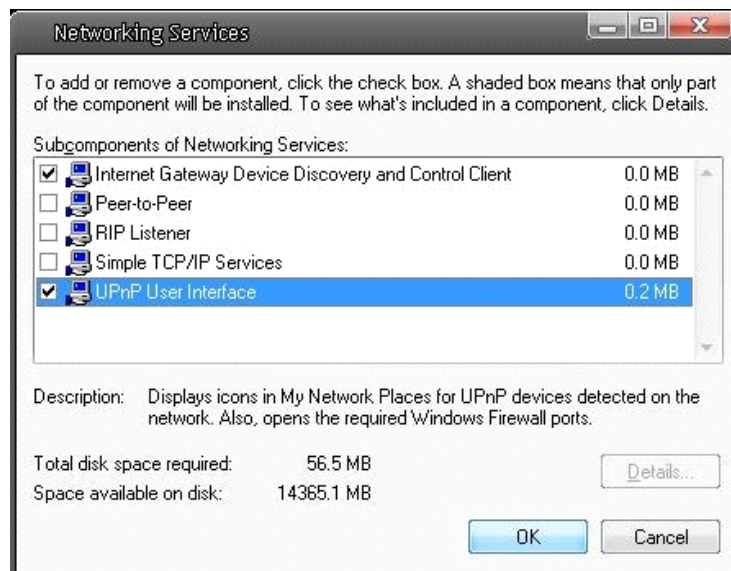
Step 2: Click on “Add/Remove Windows Components” in the Add or Remove Programs page.



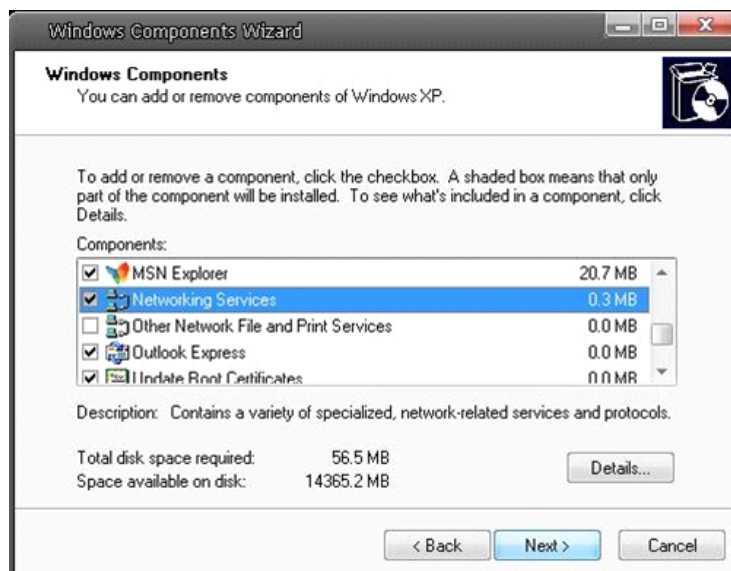
Step 3: Select “Networking Services” from the Components list in the Windows Components Wizard window, and then click on “Details”.



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.

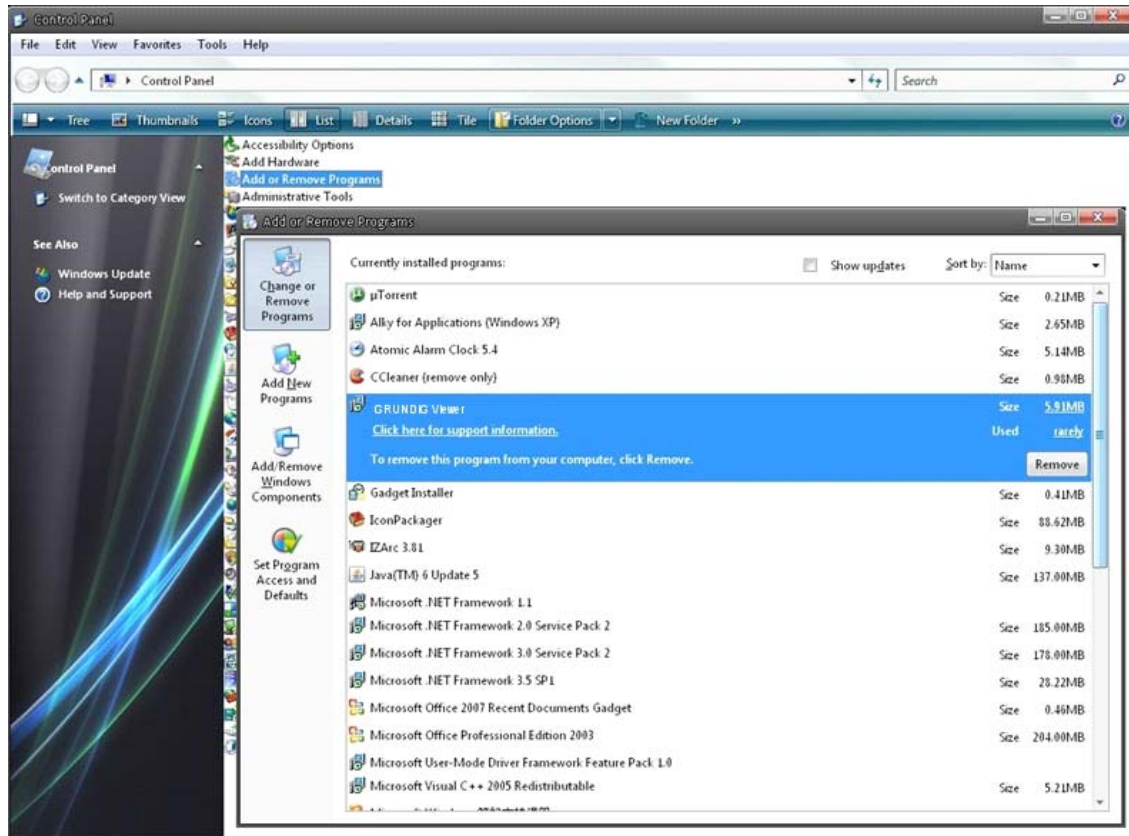


17. Deleting the Existing GRUNDIG Viewer

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 :

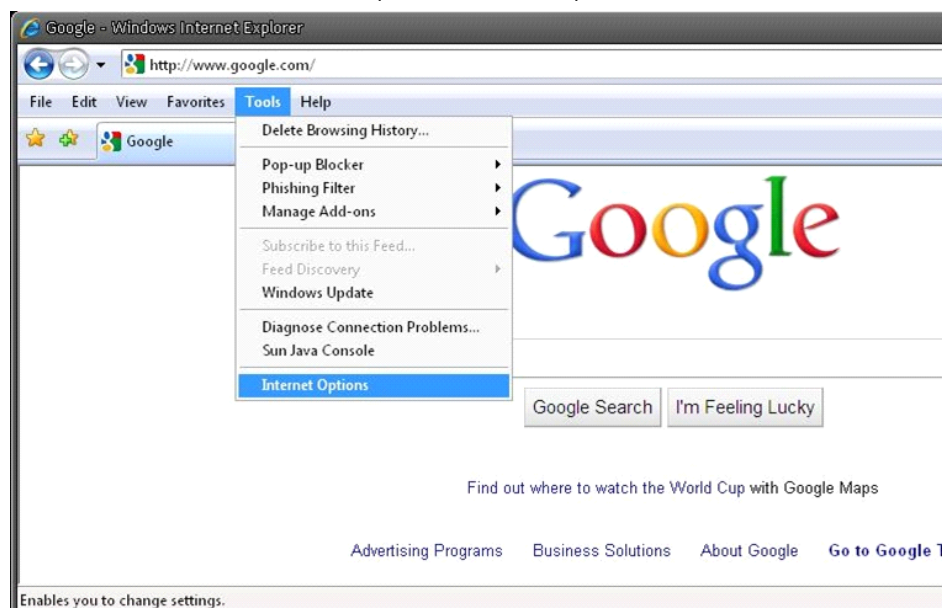
Click on “Control Panel”, and then click on “Add or Remove Programs”. In the “Currently installed programs” list, select “GRUNDIG Viewer” and click the button “Remove” to uninstall the existing GRUNDIG Viewer as shown in the figure below.



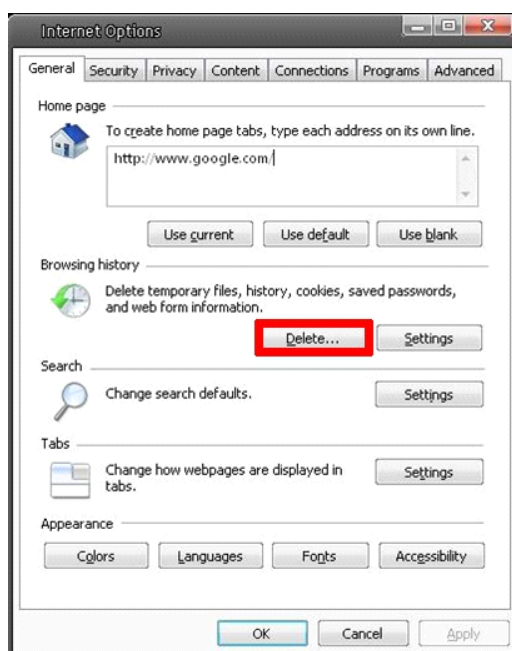
Deleting Temporary Internet Files :

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-K1627D

Image Sensor	1/2.8" Sony Exmor™ CMOS
Pixels - Total	1920(H) x 1080(V)
Digital Signal Processor (DSP)	Sony Xarina Solution
Sensitivity Colour	0.03 Lux @ F1.2
Sensitivity B&W	0 Lux LED IR on
Col/B&W	On/Off/Auto, IR-cut filter removable (ICR)
Lens Focal Length	3 ~ 10.5 mm
Viewing Angle	approx. 93°(w) ~ 32° (t)
Optical Zoom	3x
Digital Zoom	Off ~ 8x
Iris F-Number	F= 1.4 ~ 360
Lens Drive Type	Auto iris (DC)
Focus Adjustment	Manual
IR LED	21 pcs., 90° beaming angle
Max. IR Distance	15/25 m (according to scene reflexion)
Wavelength	850nm
Shutter Speed	1 ~ 1/10.000 sec
WDR	96dB (Shutter WDR)
BLC: Back Light	On/Off
White Balance	ATW, AWB, Manual, Push
Digital Noise Reduction (DNR)	On/off 2D/3D Noise Filter
Digital Image Stabilization (DIS)	Off/On
D&N Switching Mode:	Light Sensor (Auto with LED), Light ON, Light OFF, SMART, Auto, Night, Day
Alarm Input	On, Off, by Schedule
Motion Detection	On, Off, by Schedule
Tampering Alarm	On/Off
Time Lapse:	Off, On (60~3600s)
Manual Trigger:	On, Off
Schedule:	Daily, Weekly, Start Time and Duration
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
Camera ID	20 character
Reverse	Flip, Mirror, Vertical Mode, 180°
Privacy zones	5
Privacy Zone Typ:	rectangle, Color selection
Network	10/100Mbps
Video Compression	H.264 (MPEG-4Part 10/AVC), MJPEG
ONVIF compliant	Profile S
Video Streaming	Quad stream: 4xH.264 or 3xH.264+MJPEG Triple: 3xH.264 or 2xH.264+MJPEG Dual: 2xH.264 or H.264+MJPEG Single: H.264 or MJPEG
Video Resolution	Full HD 1080p/ SXGA/ HD 720p/ XGA/SVGA/ 4CIF/ VGA/ CIF
Frame Rate (Max@Resolution):	50fps@2MP, 25fps@2MP, 50fps@1,3MP, 25fps@1,3MP, etc.
Streaming Method:	Unicast, Multicast
Audio Compression	G.726, G.711
Audio Communication	Bi-directional
Audio Input/Output	Line In/Line Out (two way Audio)
Alarm Inputs	1 (5V, 10KΩ)
Alarm Outputs	1 (max.300VDC/AC, 39W)
Access protection	By log-in and Password, IP filter, IEEE802.1x

Number of Clients	Up to 20 simultaneously
Micro SDHC memory:	Supports up to 32GB
Recording Types:	on Micro SD/SDHC CARD Single Image Recording (JPEG) Video(AVI, LCK)
Web Browser	MS Internet Explorer 6.0 (or higher), Firefox, Google Chrome, Safari, Access over Mobile Devices
Network Protocol	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, DHCP, PPPoE, UPnP, SMTP, ICMP, IGMP, SNMP, IEEE802.1x, QoS, ONVIF, FTP, ARP
Firmware Upgrade	by Web Browser or Grundig finder from ver.1.17
Configuration	Over Remote PC
Multi Language Webpage:	English, German, French, Italian, Russian, Turkish
LED Indicator	Power, link, active
Video Outputs	1Vpp
Input/Output sockets	Power (Terminal 3-Pin), RJ-45, Micro SD Card Slot, 8-Pin Terminal (4- Pin Alarm IN/OUT),Audio IN/OUT (4-Pin), Video Output
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	10 (LED ON) W
Weight	0.31 kg
Dimensions (wxhxd)	Ø 123 x 90 mm

EC Declaration of Conformity



GCI-K1627D 2 MP Full HD Indoor Dome IP Camera
3~10.5mm ICR IR 24 LED WDR

It is hereby certified that the products meet the standards in
the following relevant provisions:
EC EMC Directive 2004/108/EC

Applied harmonised standards and technical specifications:
Measurement Procedure EMI:

AS/NZS CISPR 22: 2009, EN55022 CLASS A: 2010,
EN61000-3-2: 2006 + A1: 2009 + A2: 2009, EN61000-3-3: 2008

Measurement Procedure EMS:

AS/NZS CISPR 24: 2009, EN 50130-4: 1995 + A1: 1998 + A2:
2003, IEC/EN 61000-4-2: 2008, IEC/EN 61000-4-3: 2006 + A1:
2008 + A2: 2010, IEC/EN 61000-4-4: 2004 + A1: 2010, IEC/EN
61000-4-5: 2005, IEC/EN 61000-4-6: 2008, IEC/EN 61000-4-8:
2009, IEC/EN 61000-4-11: 2004

ASP AG

Lüttringhauser Str. 9
42897 Remscheid
Germany

GRUNDIG

Remscheid, 14.11.2014

Ludwig Bergschneider
CEO