FOR A GOOD REASON GRUNDIG

en

Owner's Manual

IP Cameras

GCI-F4616T	3 MP Mini Bullet Outdoor Camera with IR LEDs
GCI-F4616W	3 MP Flat Mini Dome with IR LEDs
GCI-F4626T	3 MP Bullet Outdoor Camera with IR LEDs
GCI-F4626V	3 MP Vandal Proof Dome Camera with IR LED

GCI-F4616T.175.1.01.03.2016

Content:

1. Introduction

This Manual applies to the Grundig IP Cameras GCI-F4616W, GCI-F4616T, GCI-F4626V and GCI-F4626T.

The Manual includes instructions for using and managing the products. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version on the company website.
Please use this user manual under the guidance of professionals.

EU Conformity Statement:
This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive):
Products marked with the “(Crossed out bin)” symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive):
This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with a “(Crossed out bin)” symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance:
This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

FCC Information:

FCC Compliance:
This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions:
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

2. Important Safety Instructions

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.
The precaution measure is divided into ‘Warnings’ and ‘Cautions’:

Warnings:
Serious injury or death may be caused if any of these warnings are neglected. Follow these safeguards to prevent serious injury or death.

Cautions:
Injury or equipment damage may be caused if any of these cautions are neglected. Follow these precautions to prevent potential injury or material damage.

Warnings:
- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard and source it with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackout equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorised repair or maintenance.)

Cautions:
- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a cleaning cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at strong light such as the sun or an incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor is not exposed to the laser beam.
- Do not install the camera in extremely hot or cold temperatures (the operating temperature should be between -30°C ~ 60°C, or -40°C ~ 60°C if the camera model has an "H" in ist suffix), or in a dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required to ensure a proper operating environment.
- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed into its original packing.
- Improper use or replacement of the battery may result in the hazard of explosion. Please use the battery type recommended by the manufacturer.

NOTE: For the camera which supports IR, you are required to pay attention to the following precautions to prevent IR reflection:

- Dust or grease on the dome cover will cause IR reflection. Please do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with a clean soft cloth and isopropyl alcohol.
- Make sure that the installation location does not have any reflective surfaces of objects that are too close to the camera. The IR light from the camera may reflect back into the lens causing a reflection in the video image.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDS. Fasten the dome cover to the camera body so that the foam ring and the dome cover are attached seamlessly.

3. System Requirements

Operating System: Microsoft Windows XP SP1 and above version / Vista / Win7 / Server 2003 / Server 2008 32bits
CPU: Intel Pentium IV 3.0 GHz or higher
RAM: 1GB or higher
Display: 1024×768 resolution or higher
Web Browser: Internet Explorer 6.0 and above version, Apple Safari 5.02 and above version, Mozilla Firefox 3.5 and above version and Google Chrome 8 and above version.

4. Network Setup

Regarding the Network Connection:

- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.
- To ensure the network security of the network camera, we recommend that you assess and maintain the network camera termly.

Before you start:
- If you want to set the network camera via a LAN (Local Area Network), please refer to Section 4.1 "Setting the Network Camera over LAN".
- If you want to set the network camera via a WAN (Wide Area Network), please refer to Section 4.2 "Setting the Network Camera over WAN".

4.1. Network Camera Setup over LAN

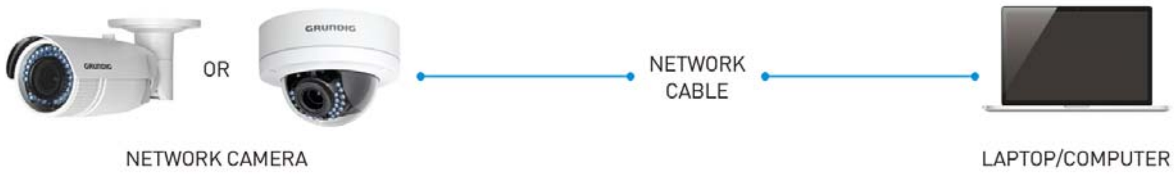
To view and configure the camera via a LAN, you need to connect the network camera in the same subnet with your computer, and install the SCMS software to search and change the IP of the network camera.

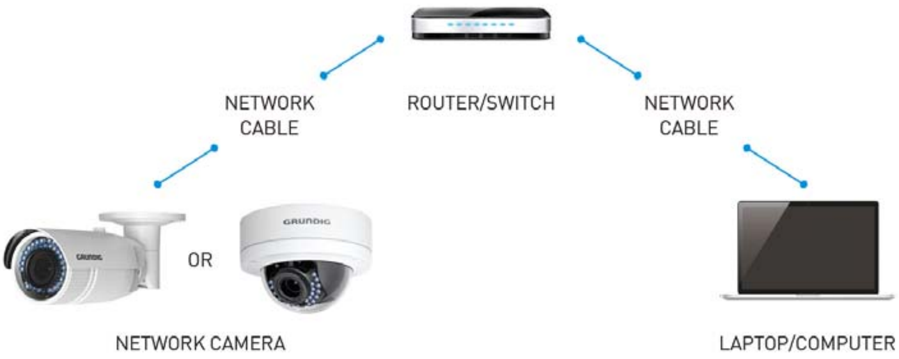
NOTE: For a detailed introduction of the SCMS, please refer to the last chapter.

4.1.1. Wiring over the LAN

The following figures show the two ways of cable connection of a network camera and a computer:

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown below.
- Refer to the picture below to set the network camera over the LAN via a switch or a router.





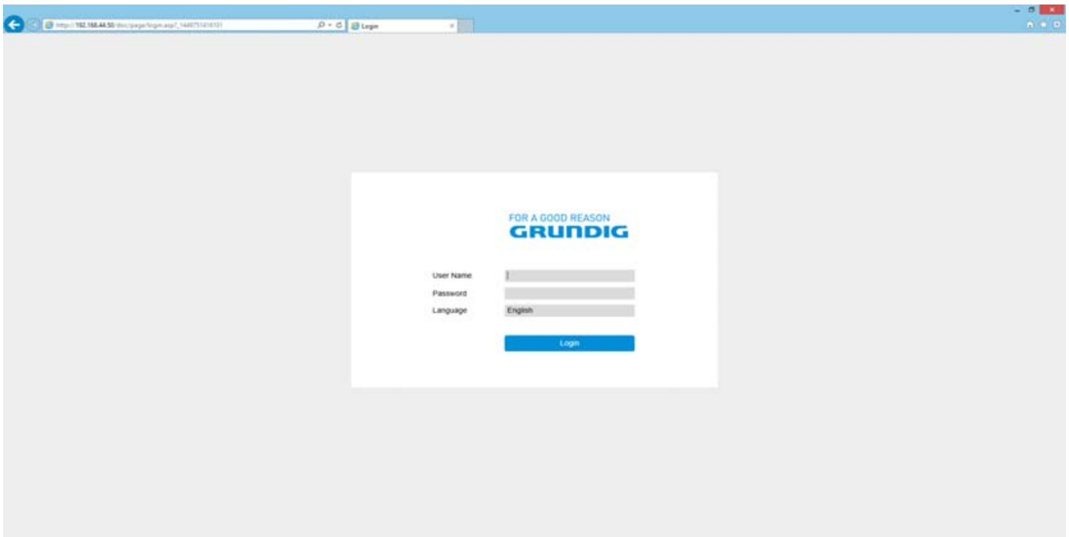
4.1.2. Creating a Password

An Admin user is set as a default user in the camera.
The default user is: admin
The default password is: 1234
After inputting this information, you will be asked to set a stronger password. But this is not necessarily needed. You can carry on by using the default user account information mentioned above.
Creating a Password via a Web Browser is supported.

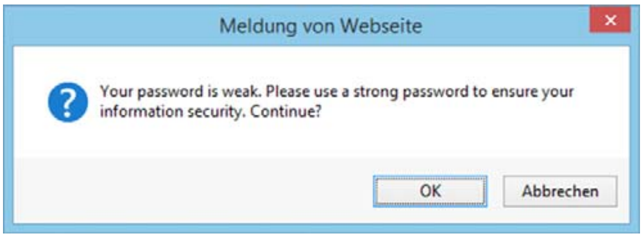
- Creating a Password via Web Browser:

Steps:
1. Power on the camera, and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click "Enter" to enter the activation interface.

NOTE:
- The default IP address of the camera is 192.168.1.100.

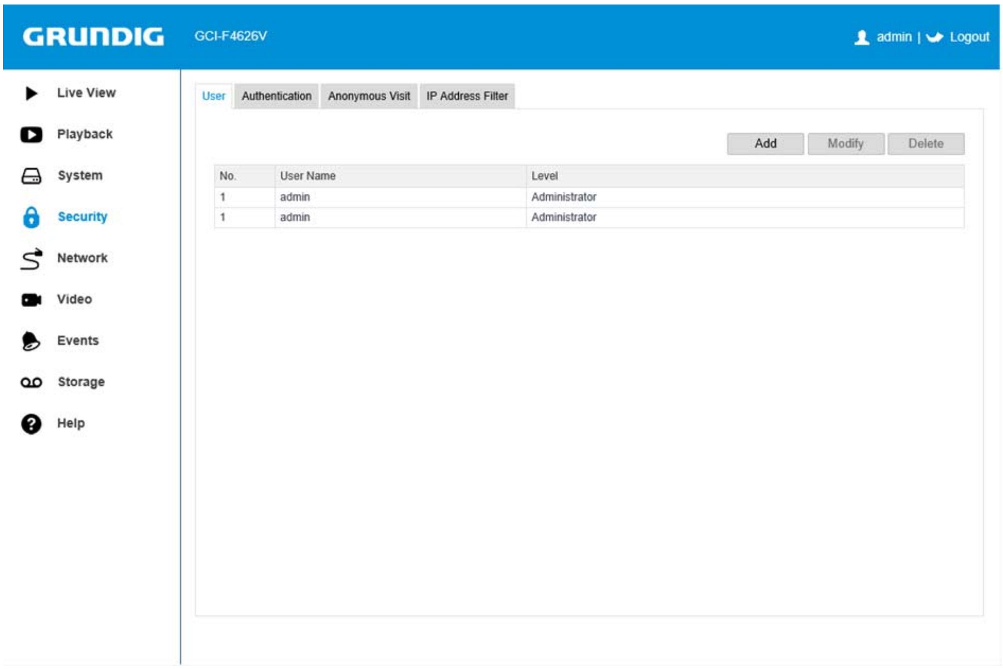


- For the camera that enables the DHCP by default, the IP address is allocated automatically.
- To log in, use the Default User ID and Password: admin/1234
- You will be asked to create a stronger password.



Your password is weak. Please use a strong password to ensure your information security. Continue?

- If you push the button "Cancel" (Abbrechen), you will be led directly to the Live image page.
- If you push "OK", you will be led directly to the “Security” page where you can create a new user ID and password.



No.	User Name	Level
1	admin	Administrator
1	admin	Administrator

3. Create a password and input the password into the password field.

STRONG PASSWORD RECOMMENDED: We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in a high security system, resetting the password monthly or weekly can protect your product better.

4. Confirm the password.
5. Click "OK" to save the password and to enter the live view interface.

4.2. Network Camera Setup over WAN

This section explains how to connect the network camera to the WAN with a static IP or a dynamic IP.

4.2.1. Static IP Connection

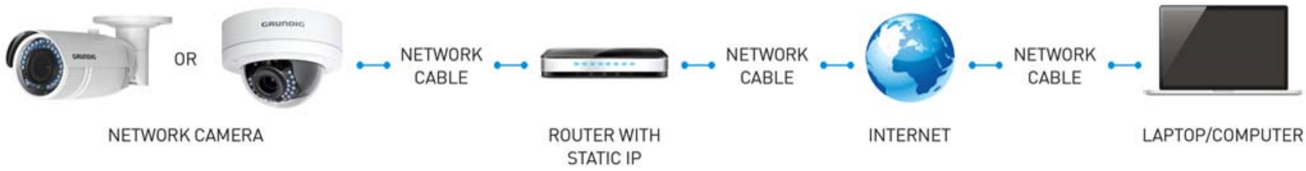
Before you start:
Please apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the network camera via a router or connect it to the WAN directly.

- Connecting the network camera via a router:

Steps:
1. Connect the network camera to the router.
2. Assign a LAN IP address, the subnet mask and the gateway. Please refer to Section 4.1.2 for detailed IP address configuration of the network camera.
3. Save the static IP in the router.
4. Set the port mapping, e.g., 80, 8000, and 554 as the ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

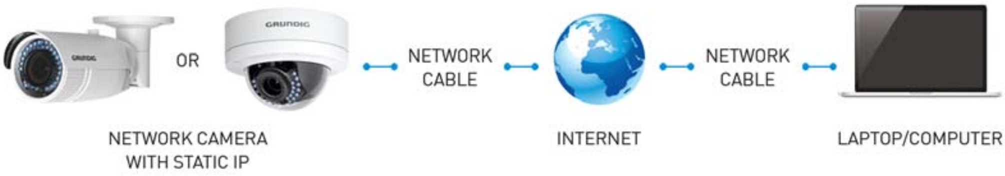
NOTE: Refer to chapter 11 for detailed information about port mapping.

5. Visit the network camera through a web browser or the SCMS over the internet.



- Connecting the network camera directly through a static IP:

You can also save the static IP on the camera and directly connect it to the internet without using a router. Refer to Section 4.1.2 for detailed IP address configuration of the network camera.



4.2.2. Dynamic IP Connection

Before you start:
Please apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the network camera to a modem or a router.

- Connecting the network camera via a router:

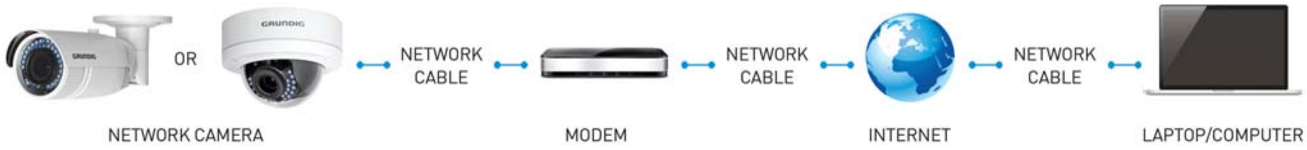
Steps:
1. Connect the network camera to the router.
2. On the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to Section 4.1.2 for detailed IP address configuration of the network camera.
3. In the router, set the PPPoE user name, password and confirm the password.
4. Set the port mapping, e.g. 80, 8000, and 554 as the ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with the port mapping.

NOTE: Refer to Chapter 11 for detailed information about the port mapping.

5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

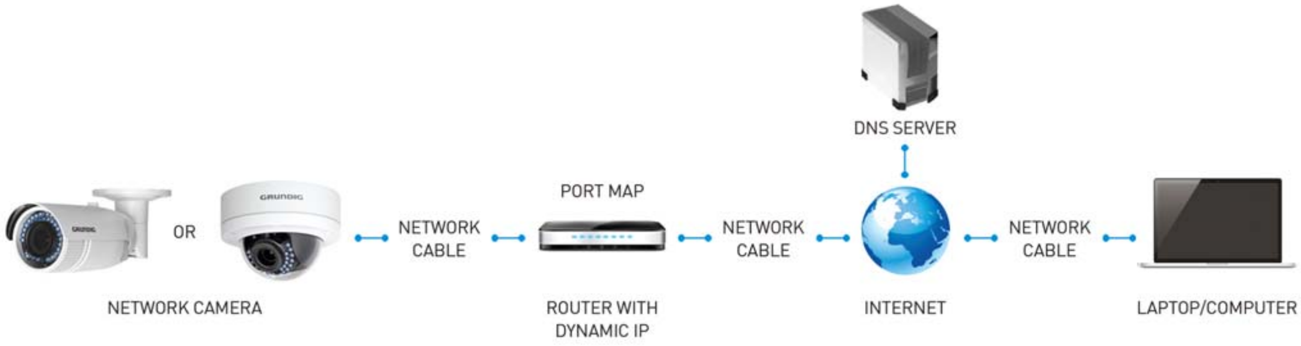
- Connecting the network camera via a modem:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to Section 8.3.3 "Configuring the PPPoE Settings" for the detailed configuration.



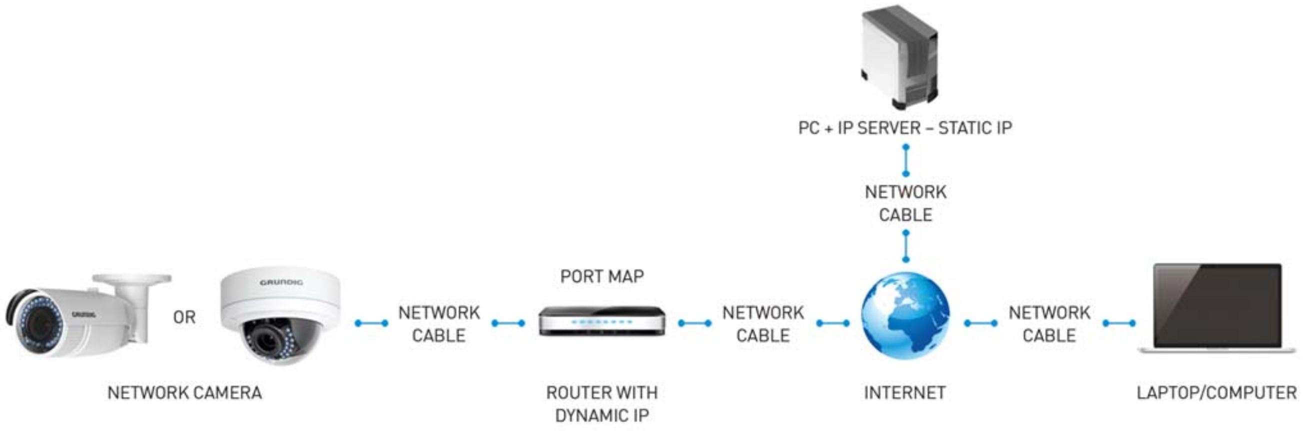
NOTE: The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Please follow the steps below for setting a normal domain name resolution and a private domain name resolution to solve the problem.

- Normal Domain Name Resolution:



Steps:
1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the "DDNS Settings" interface of the network camera. Refer to Section 8.3.2 "DDNS" for the detailed configuration.
3. Visit the camera via the applied domain name.

- Private Domain Name Resolution:



Steps:
1. Install and run the IP Server software on a computer with a static IP.
2. Access the network camera through the LAN through a web browser or the SCMS.
3. Enable "DDNS" and select "IP Server" as the protocol type. Refer to Section 8.3.2 "DDNS" for information about the detailed configuration.

5. Accessing the Camera

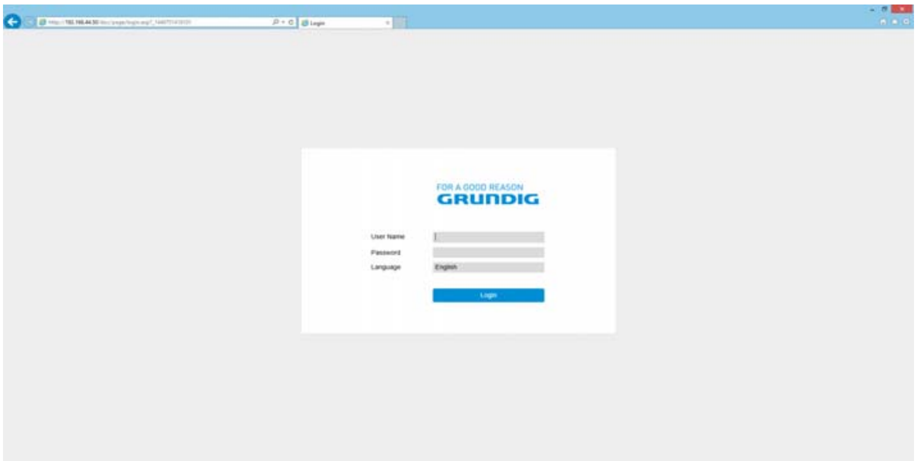
5.1. Accessing through Web Browsers

Steps:
1. Open the web browser in Administrator mode.
2. In the browser address bar, input the IP address of the network camera, and press the “Enter” key to enter the login interface.

NOTE:
- The default IP address is 192.168.1.100.

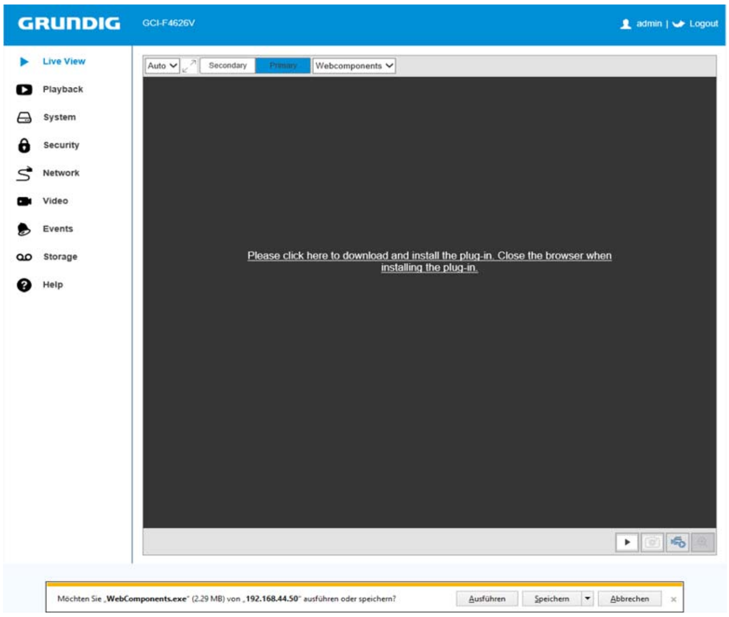
4. Select “English” or another language as the interface language - above the "Login" button.
5. Input the user name and password and click on "Login".
The admin user should configure the device accounts and user/operator permissions properly. Delete any unnecessary accounts and user/operator permissions.

NOTE:
The IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).



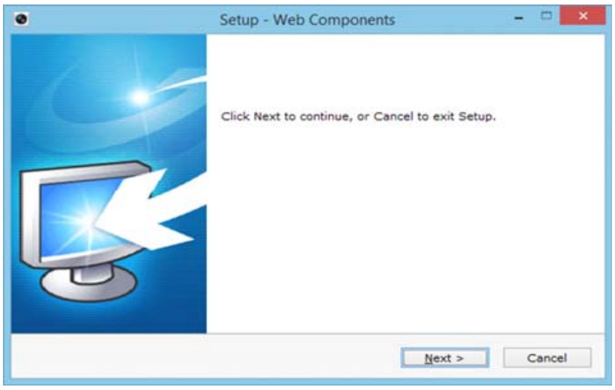
Language: English

6. Install the plug-in before viewing the live video and operating the camera. Please follow the installation prompts to install the plug-in.



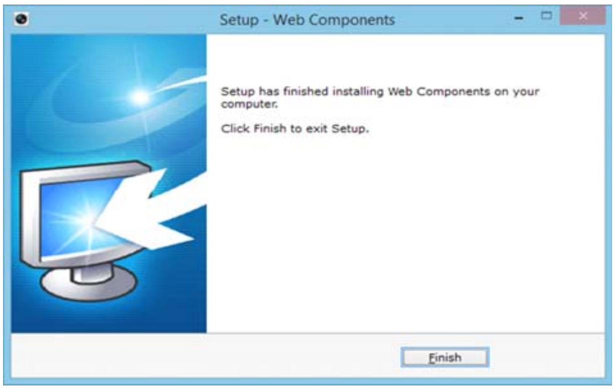
Please click here to download and install the plug-in. Close the browser when installing the plug-in.

Möchten Sie „WebComponents.exe“ (2.29 MB) von „192.168.44.50“ ausführen oder speichern?



Setup - Web Components

Click Next to continue, or Cancel to exit Setup.



Setup - Web Components

Setup has finished installing Web Components on your computer.

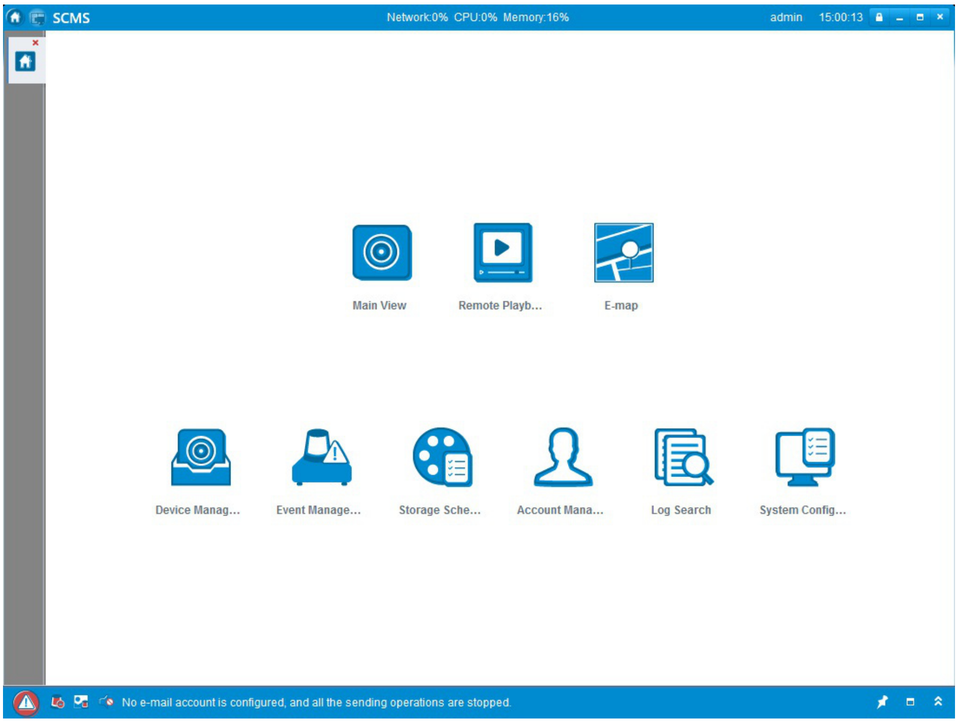
Click Finish to exit Setup.

NOTE: You may have to close the web browser to install the plug-in. Please re-open the web browser and log in again after installing the plug-in.

5.2. Accessing through Client Software

The product CD contains the SCMS software. You can view the live video and manage the camera with the software.
Follow the installation prompts to install the software. The control panel of the SCMS software is shown below.

NOTE: For detailed information about the software, please refer to the user manual of the SCMS.



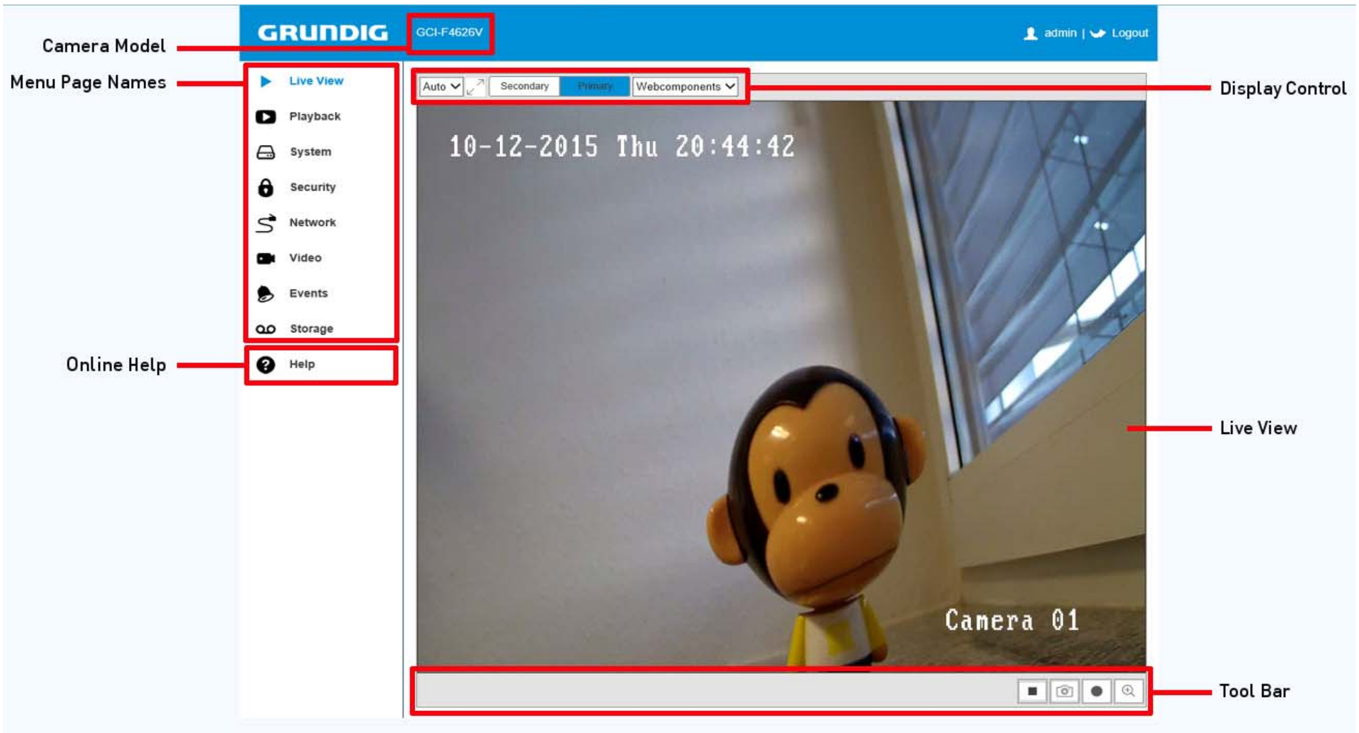
No e-mail account is configured, and all the sending operations are stopped.

6. Live View

6.1. Live View Page

The live view page allows you to view the real-time video, capture images, set/call presets and configure video parameters.
Log in the network camera to enter the live view page, or you can click "Live View" in the menu bar of the main page to enter the live view page.

Descriptions of the live view page:



Camera Model:
This shows the camera model you are connecting to.

Online Help:
Click "?" to get the online help, which will guide you through the basic operations for each function.

Menu Page Names:
Click on each tab to enter the menu pages.

Display Control:
Click on each tab to adjust the layout and the streaming type of the live view. And you can click on the drop-down list to select the plug-in. For IE (internet explorer) users, "webcomponents" and "quick time" are selectable. And for Non-IE users, "webcomponents", "quick time", "VLC" or "MJPEG" are selectable, if they are supported by the web browser.

Live View Window:
Displays the live video.

Tool Bar:
Operations on the live view page, e.g., live view, capture, record, etc.

6.2. Starting the Live View

In the live view window as shown in picture below, click on ">" (Play) in the toolbar to start the live view of the camera.

6.3. Manual Recording & Snapshots

In the live view interface, click on the "(photo camera)" icon in the toolbar to capture the live pictures or click on the "record (dot)" icon to record the live view. The saving paths of the captured pictures and clips can be set on the "System> Local Configuration" page. To configure the remote scheduled recording, please refer to Section 8.6.1 "Record Schedule".

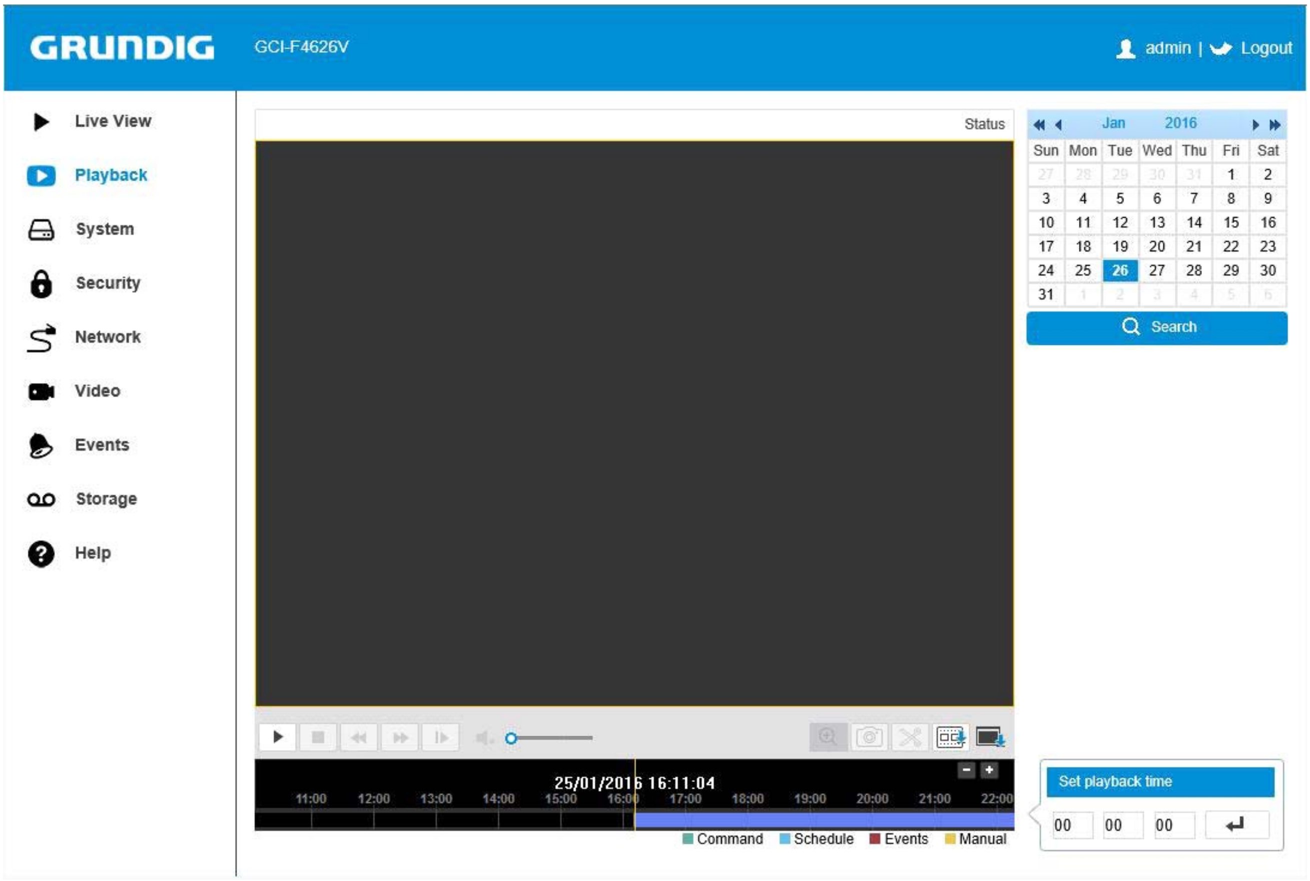
NOTE: The captured images will be saved as JPEG files or BMP files on your computer.

7. Playback

This section explains how to view the remotely recorded video files stored on the network disks or on the SD cards.

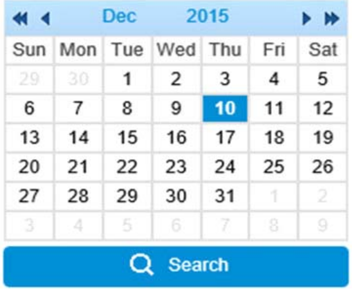
Steps:

1. Click "Playback" on the menu bar to enter the playback interface.



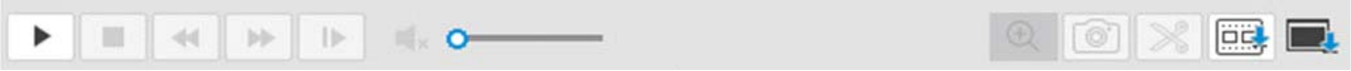
Jan			2016			
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

2. Select the date and click on "Search".



Dec			2015			
Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

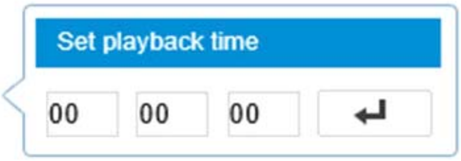
3. Click on ">" (Play) to play the video files found on this date. The toolbar on the bottom of the Playback interface can be used to control the playing process.



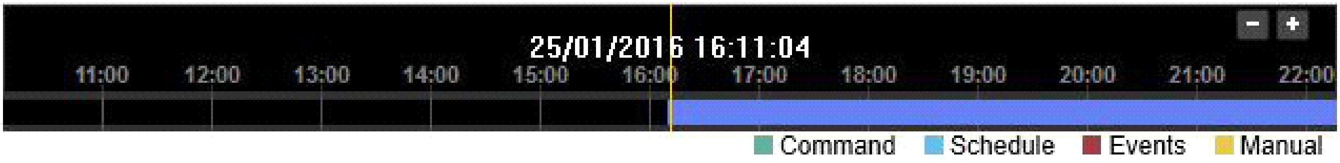
Button	Operation	Button	Operation
▶	Play	📷	Capture a picture
⏸	Pause	✂	Start/Stop clipping the video files
■	Stop	⬇	Download the video files
⏪	Speed down	⬇	Download the captured pictures
⏩	Speed up	🔍	Enable/Disable the digital zoom
⏯	Playback by frame		

NOTE: You can choose the file paths locally for the downloaded playback video files and pictures in the System> Local Configuration interface. Please refer to Section 8.1.7 "Local Configuration" for the details.

Drag the progress bar with the mouse to locate the exact playback point. You can also input the time and click on the "Enter (arrow)" button to locate the playback point in the "Set playback time" field. You can also click on the "-"/"+" to zoom out/in the progress bar.



The different colours of the video on the progress bar stand for the different video types.



8. Camera Settings

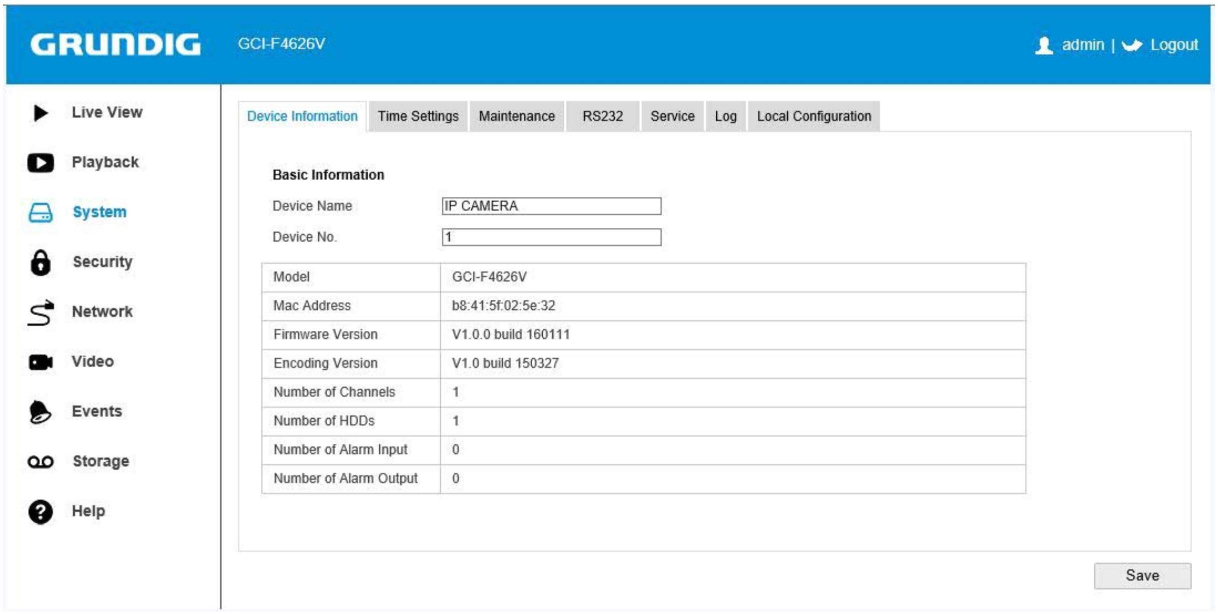
8.1. System Settings

8.1.1. Device Information

Enter the Device Information interface: System> Device Information.

In the "Device Information" interface, you can edit the Device Name.

Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.



Basic Information

Device Name: IP CAMERA

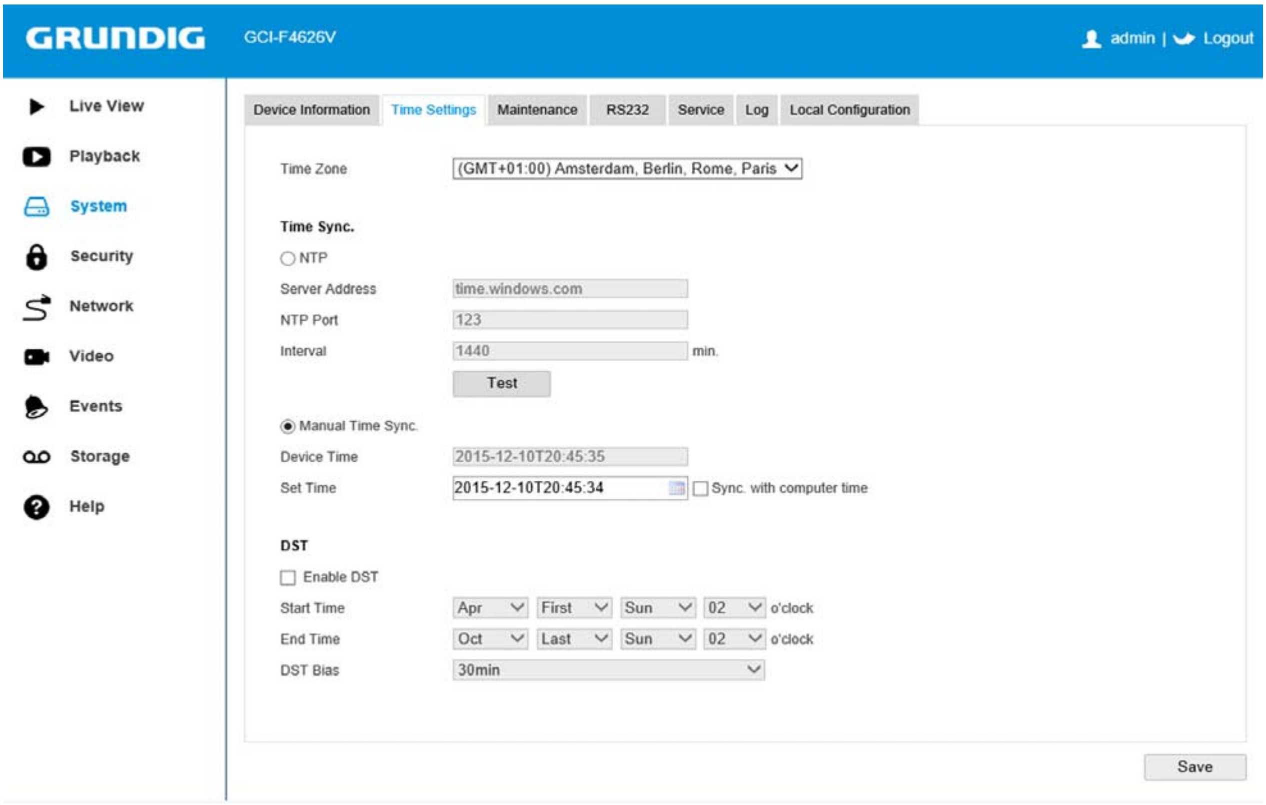
Device No.: 1

Model	GCI-F4626V
Mac Address	b8:41:5f:02:5e:32
Firmware Version	V1.0.0 build 160111
Encoding Version	V1.0 build 150327
Number of Channels	1
Number of HDDs	1
Number of Alarm Input	0
Number of Alarm Output	0

8.1.2. Time Settings

You can follow the instructions in this section to configure the time synchronisation and DST settings.

Steps:
1. Enter the Time Settings interface: System> Time Settings



GCI-F4626V

admin | Logout

Live View
Playback
System
Security
Network
Video
Events
Storage
Help

Device Information | Time Settings | Maintenance | RS232 | Service | Log | Local Configuration

Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Paris

Time Sync.

○ NTP

Server Address: time.windows.com

NTP Port: 123

Interval: 1440 min.

Test

● Manual Time Sync.

Device Time: 2015-12-10T20:45:35

Set Time: 2015-12-10T20:45:34 □ Sync. with computer time

DST

□ Enable DST

Start Time: Apr | First | Sun | 02 o'clock

End Time: Oct | Last | Sun | 02 o'clock

DST Bias: 30min

Save

- Select the Time Zone. Select the Time Zone of your location from the drop-down menu.

> Synchronising the time by NTP Server:

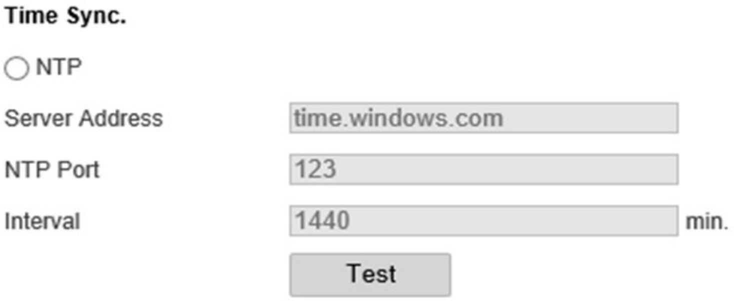
(1) Check the checkbox to enable the “NTP” function.

(2) Configure the following settings:

>> Server Address: IP address of the NTP server.

>> NTP Port: Port of the NTP server.

>> Interval: The time interval between the two synchronising actions with the NTP server.



Time Sync.

○ NTP

Server Address: time.windows.com

NTP Port: 123

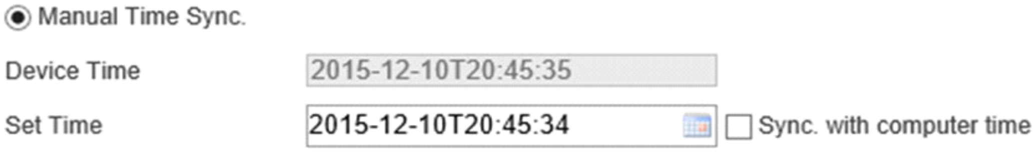
Interval: 1440 min.

Test

NOTE: If the camera is connected to a public network, you should use an NTP server that has a time synchronisation function, such as the server at the National Time Center (IP Address: ptbtime1.ptb.de). If the camera is set up in a customised network, the NTP software can be used to establish an NTP server for time synchronisation.

> Synchronising the time synchronisation manually
Enable the "Manual Time Sync" function and then click on the "(calendar)" icon to set the system time from the pop-up calendar.

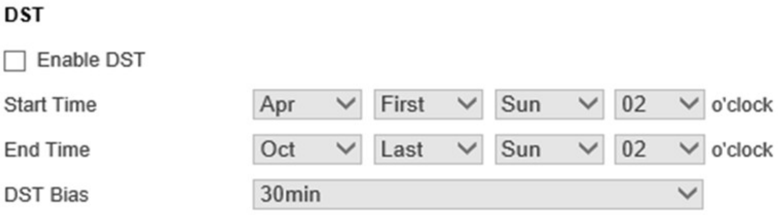
NOTE: You can also check the "Sync with computer time" checkbox to synchronise the time of the camera with that of your computer.



● Manual Time Sync.

Device Time	2015-12-10T20:45:35
Set Time	2015-12-10T20:45:34 □ Sync. with computer time

- Click on the "DST" tab page to enable the DST function and to set the date of the DST period.



DST

□ Enable DST

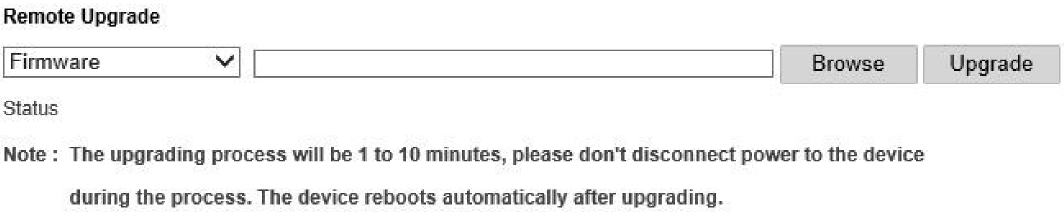
Start Time	Apr	First	Sun	02	o'clock
End Time	Oct	Last	Sun	02	o'clock
DST Bias	30min				

2. Click on "Save" to save the settings.

8.1.3. Maintenance

TO UPGRADE THE SYSTEM:

Steps:
1. Enter the Maintenance interface: System> Maintenance
2. Select the firmware or the firmware directory to locate the upgrade file.
- Firmware: Locate the exact path of the upgrade file.
- Firmware Directory: Only the directory the upgrade file belongs to is required.
3. Click on "Browse" to select the local upgrade file and then click on "Upgrade" to start the remote upgrade.



Remote Upgrade

Note : The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

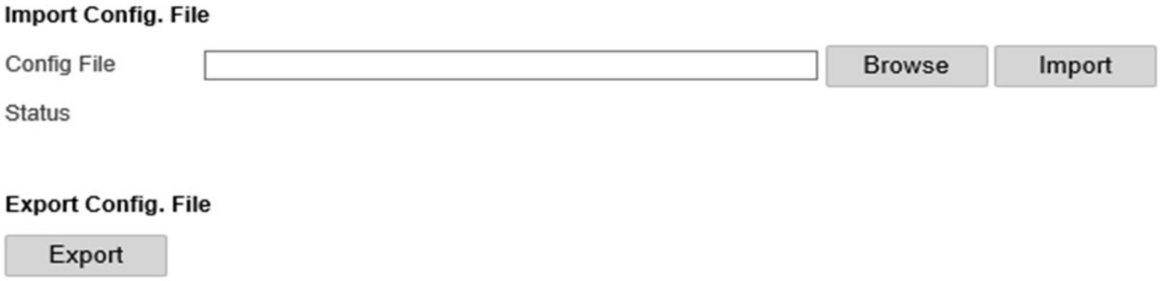
TO IMPORT / EXPORT THE CONFIGURATION:

The Configuration File is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

Steps:
1. Enter the Maintenance interface: System> Maintenance
2. Click on “Export” to export the current configuration file, and save it to a certain place.
3. Click on “Browse” to select the saved configuration file and then click on “Import” to start importing the configuration file.

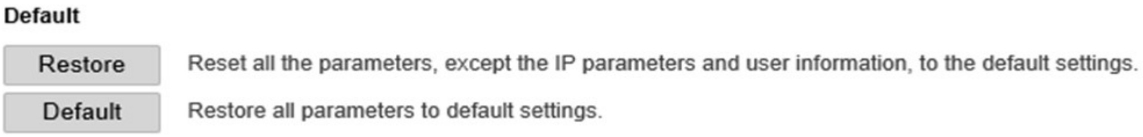
NOTE: You need to reboot the camera after importing the configuration file.

4. Click on “Export” and set the saving path to save the configuration file in the local storage.



TO RESTORE THE DEFAULT SETTINGS:

Steps:
1. Enter the Maintenance interface: System> Maintenance
2. Click on “Restore” or “Default” to restore the default settings.

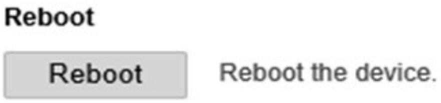


Reset all the parameters, except the IP parameters and user information, to the default settings.

Restore all parameters to default settings.

TO REBOOT THE CAMERA:

Steps:
1. Enter the Maintenance interface: System> Maintenance:
2. Click on “Reboot” to reboot the network camera.



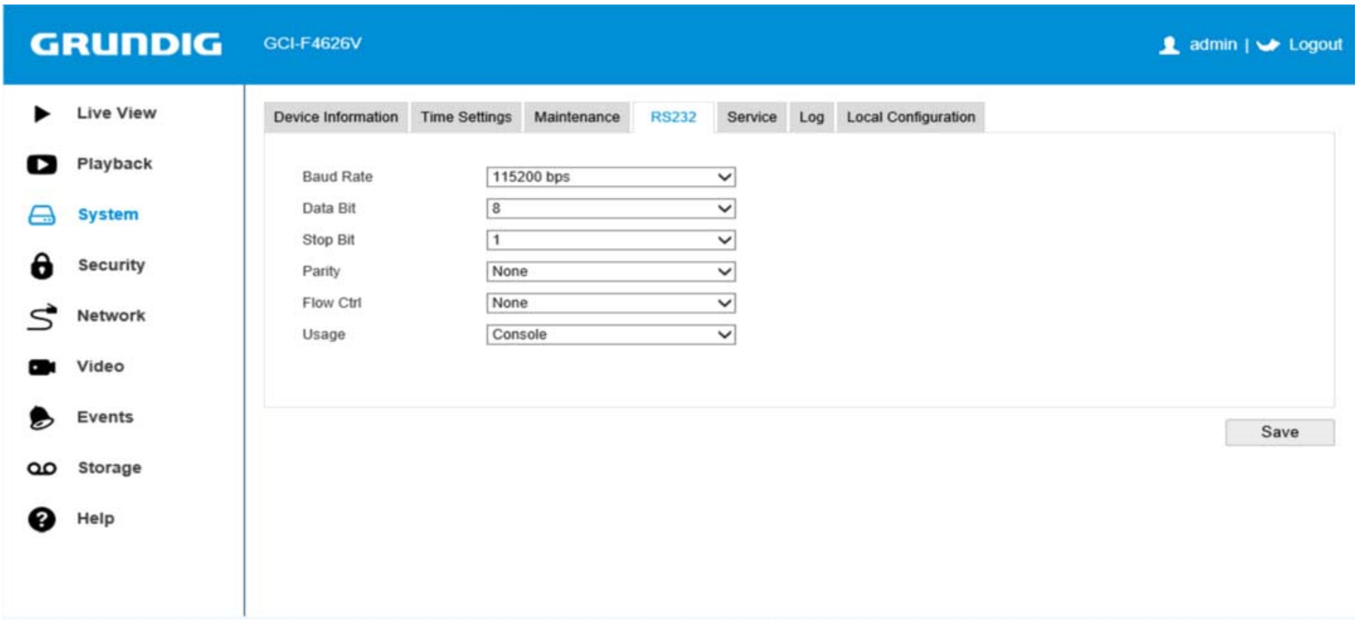
Reboot the device.

NOTE: After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.

NOTE: The upgrading process will take 1~10 minutes. Please do not disconnect the power of the camera during the process. The camera will reboot automatically after the upgrade.

8.1.4. RS232

Here you can configure the RS-232 Settings of your camera.

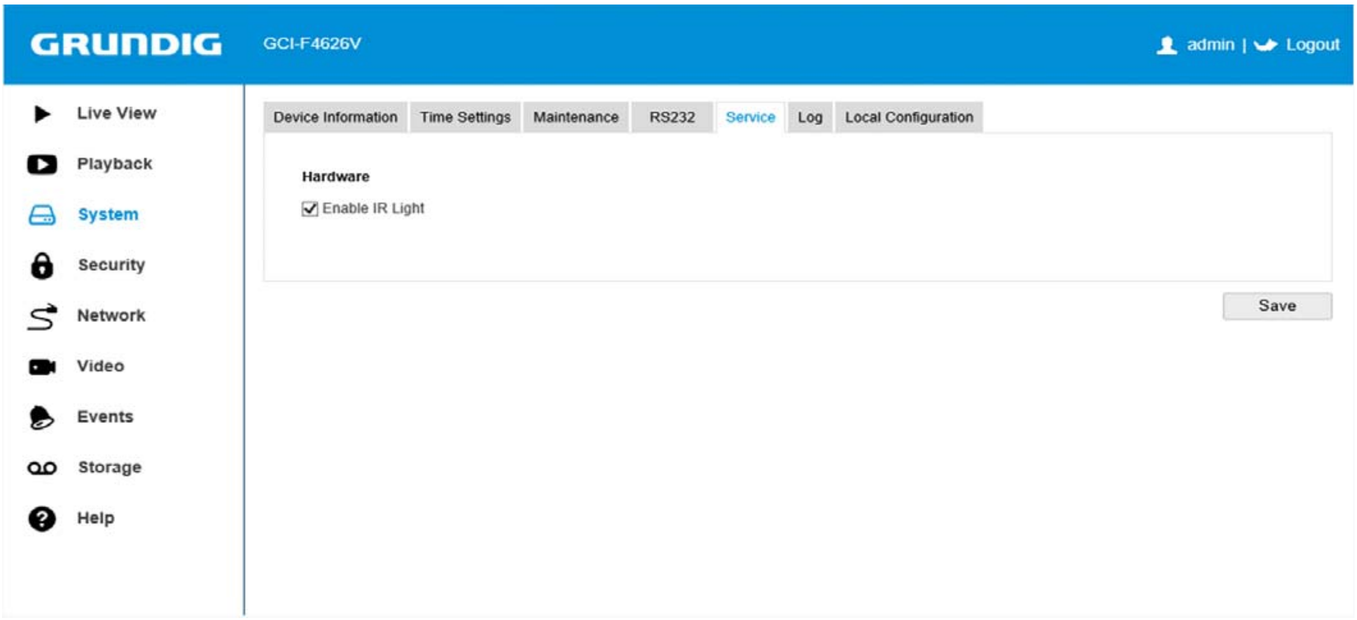


Baud Rate 115200 bps
Data Bit 8
Stop Bit 1
Parity None
Flow Ctrl None
Usage Console

8.1.5. Service

NOTE: This menu item is only for use by the servicing department.

Go to System> Service to enter the service settings interface.
The Service Settings refer to the hardware service the camera supports, and it varies according to the different cameras.
For the cameras supporting IR LED, you can go to the hardware service, and select to enable or disable the corresponding service according to the actual demands.



Hardware

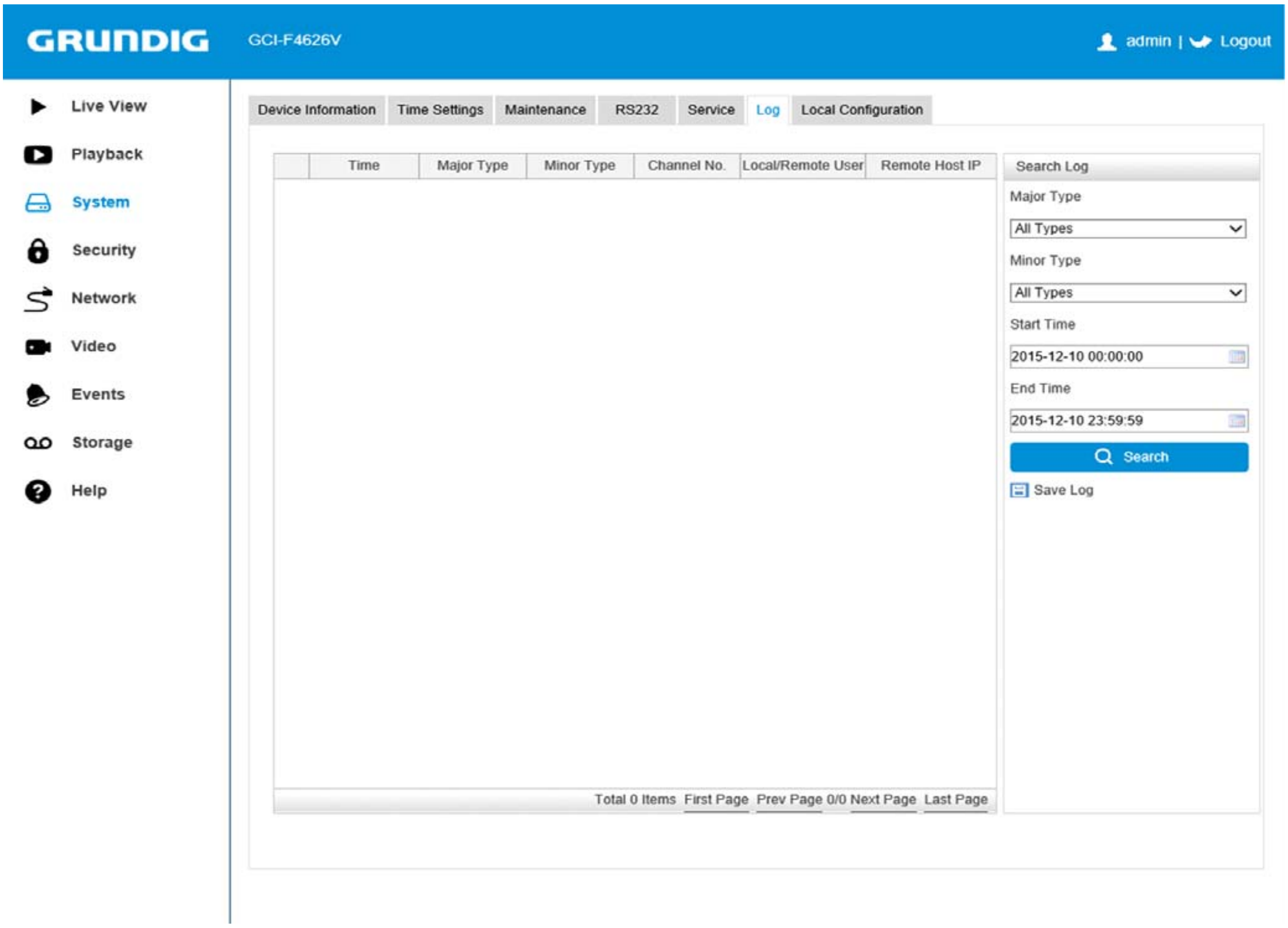
☑ Enable IR Light

8.1.6. Log

The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:
Please configure the network storage for the camera or insert an SD card into the camera.

Steps:
1. Click on “System> Log” in the menu to enter the log searching interface.



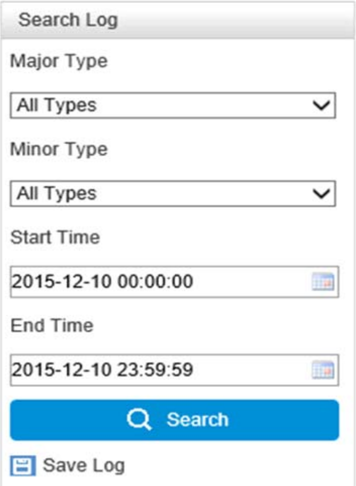
	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP

Total 0 Items First Page Prev Page 0/0 Next Page Last Page

Search Log

Major Type: All Types
Minor Type: All Types
Start Time: 2015-12-10 00:00:00
End Time: 2015-12-10 23:59:59

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
3. Click on “Search” to search the log files. The matched log files will be displayed in the “Log” interface.



Search Log

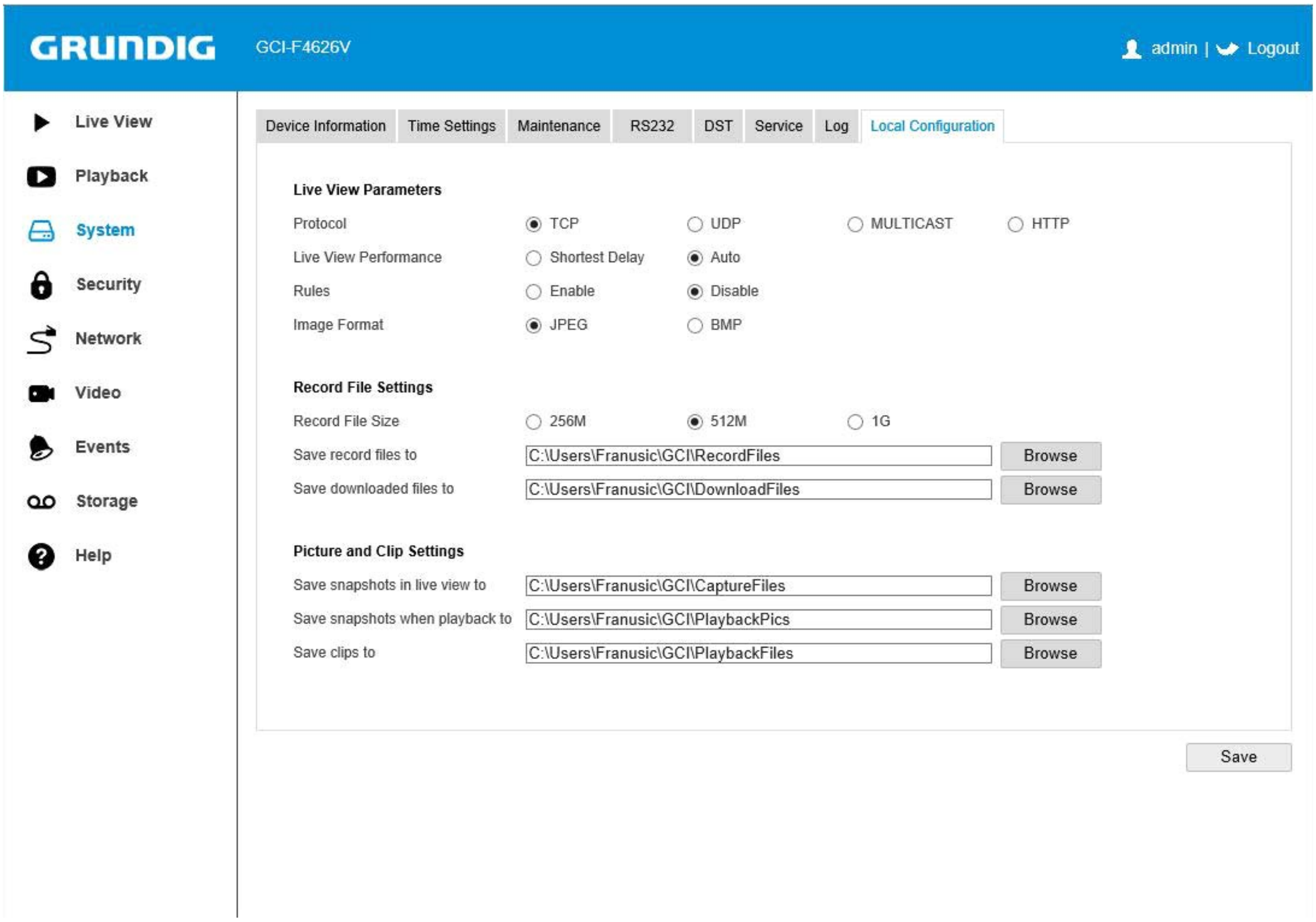
Major Type: All Types
Minor Type: All Types
Start Time: 2015-12-10 00:00:00
End Time: 2015-12-10 23:59:59

4. To export the log files, click on “Save log” to save the log files on your computer.

8.1.7. Local Configuration

The local configuration refers to the parameters of the live view, recording files and captured pictures. The recording files and captured pictures are the ones you recorded and captured using the web browser and thus the saving paths of them are on the PC running the browser.

Steps:
1. Enter the Local Configuration interface: System> Local Configuration



Live View Parameters

Protocol ● TCP ○ UDP ○ MULTICAST ○ HTTP

Live View Performance ○ Shortest Delay ● Auto

Rules ○ Enable ● Disable

Image Format ● JPEG ○ BMP

Record File Settings

Record File Size ○ 256M ● 512M ○ 1G

Save record files to C:\Users\Franusic\GCI\RecordFiles

Save downloaded files to C:\Users\Franusic\GCI\DownloadFiles

Picture and Clip Settings

Save snapshots in live view to C:\Users\Franusic\GCI\CaptureFiles

Save snapshots when playback to C:\Users\Franusic\GCI\PlaybackPics

Save clips to C:\Users\Franusic\GCI\PlaybackFiles

2. Configure the following settings:

- Live View Parameters: Set the protocol type and live view performance.
> Protocol Type: TCP, UDP, MULTICAST and HTTP are selectable.

>> TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.
>> UDP: Provides real-time audio and video streams.
>> HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.
>> MULTICAST: It's recommended to select the MCAST type when using the Multicast function. For detailed information about Multicast, refer to Section 8.3.1 "TCP/IP".

> Live View Performance: Set the live view performance to "Shortest Delay" or "Auto".
> Rules: It refers to the rules on your local browser, select enable or disable to display or not to display the coloured marks when the motion detection e.g. is triggered. E.g.: enabled as the rules are, and the motion detection is enabled as well: when a motion is detected, it will be marked in the live view.
> Image Format: Choose the image format for the picture capture.

- Record File Settings: Set the saving path of the recorded video files. Valid for the recording files you recorded with the web browser.
> Record File Size: Set the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the setting, the maximum recording file size is the value you selected.
> Save record files to: Set the saving path for the manually recorded video files.
> Save downloaded files to: Set the saving path for the downloaded video files in playback mode.

- Picture and Clip Settings: Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you captured with the web browser.
> Save snapshots in live view to: Set the saving path of the manually captured pictures in live view mode.
> Save snapshots when playback to: Set the saving path of the captured pictures in playback mode.
> Save clips to: Set the saving path of the clipped video files in playback mode.

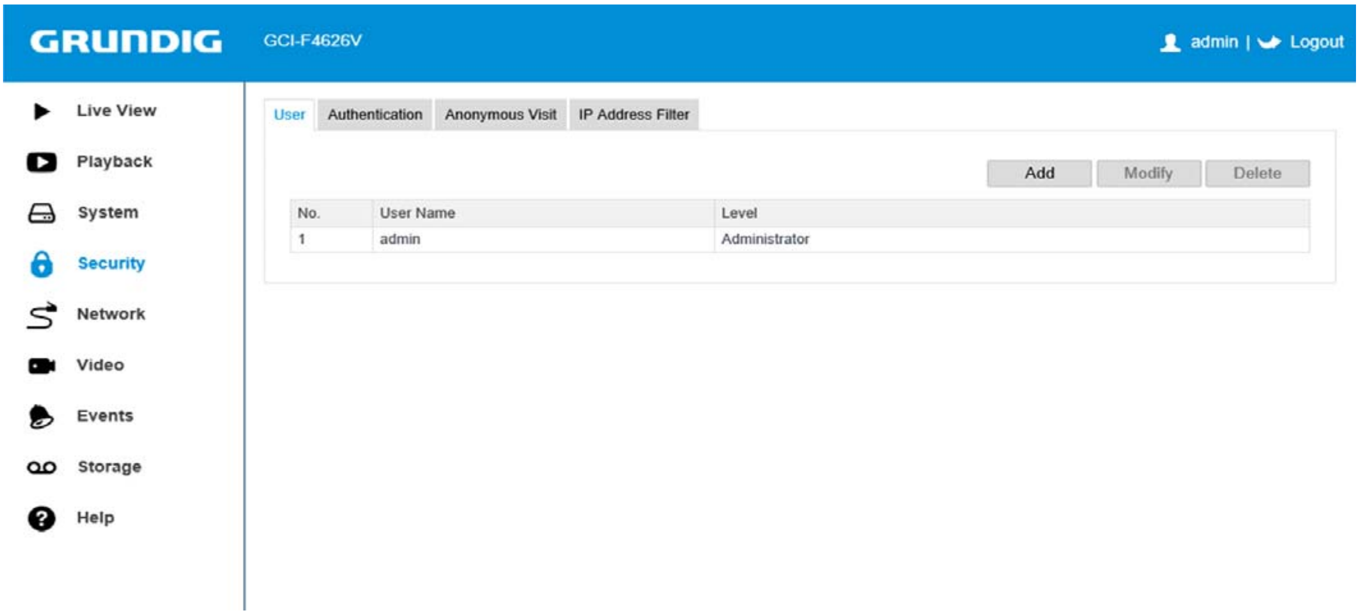
NOTE: You can click on “Browse” to change the directory for saving the clips and pictures.

3. Click on “Save” to save the settings.

8.2. Security Settings

8.2.1. User

Enter the User Management interface: Security> User



No.	User Name	Level
1	admin	Administrator

- Adding a User:
The “admin” user has all permissions by default and can create / modify / delete other accounts. The “admin” user cannot be deleted and you can only change the “admin” password.

Steps:
1. Click on “Add” to add a user.
2. Input the “User Name”, select the “Level” and input the “Password”.

NOTE:
- Only 1 administrator account exists.
- Up to 31 user/operator accounts can be created.
- Users of different levels own different permissions. The options “Operator” and “User” are selectable.

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. In the "Basic Permission" field and "Camera Configuration" field, you can check or uncheck the permissions for the new user.
4. Click on "OK" to finish the user addition.

- Modifying a User:

Steps:
1. Left-click to select the user from the list and click on "Modify".
2. Modify the "User Name", "Level" or "Password".
3. In the "Basic Permission" field and "Camera Configuration" field, you can check or uncheck the permissions.
4. Click on "OK" to finish the user modification.

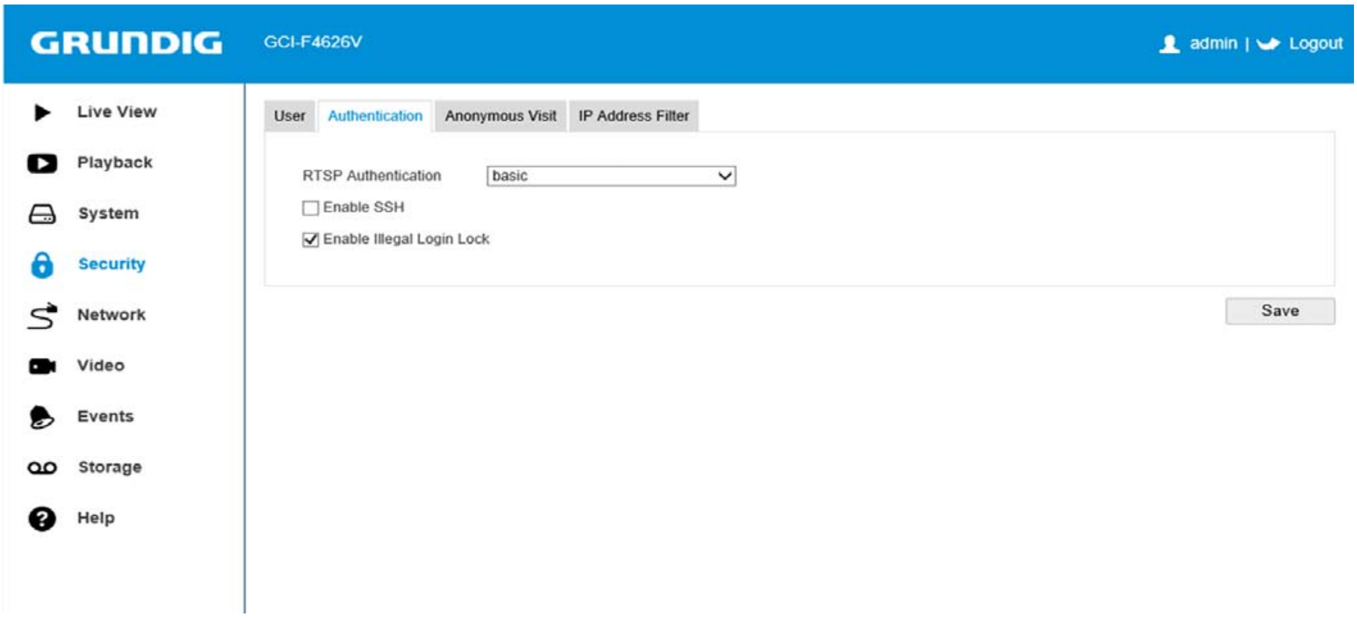
- Deleting a User:

Steps:
1. Click to select the user you want to delete and click on "Delete".
2. Click on "OK" on the pop-up dialogue box to delete the user.

8.2.2. Authentication

You can specifically secure the stream data of the live view.

Steps:
1. Enter the Authentication interface: Security> Authentication



RTSP Authentication basic

□ Enable SSH

☑ Enable Illegal Login Lock

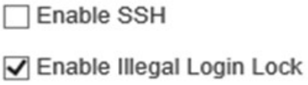
2. Select for the "RTSP Authentication" type the options "Basic" or "Disable" in the drop-down list to enable or disable the RTSP authentication.

NOTE: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol via the IP address.

3. Click on "Save" to save the settings.

To enable the remote login, and improve the data communication security, the camera provides the security service for a better user experience.

Steps:
1. Go to Security> Authentication to enter the security service configuration interface.



□ Enable SSH

☑ Enable Illegal Login Lock

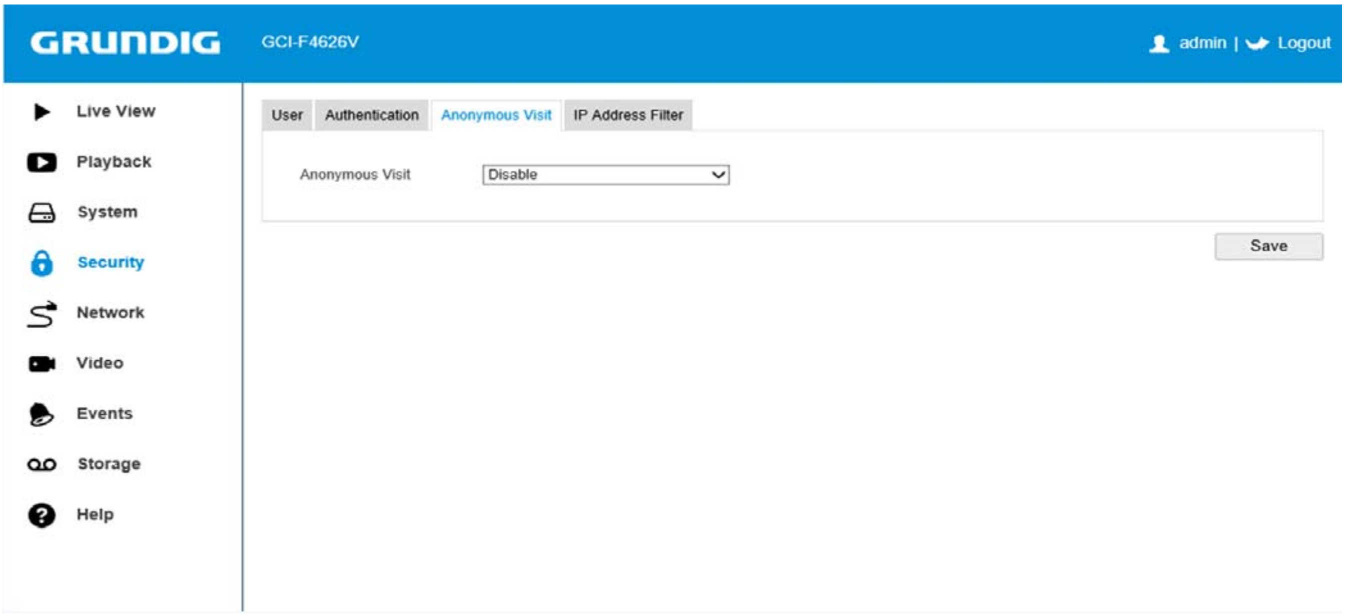
2. Check the checkbox of "Enable SSH" to enable the data communication security, and uncheck the checkbox to disable the SSH.
3. Check the checkbox of "Enable Illegal Login Lock", and then the IP address will be locked if the admin user performs 7 failed user name/password attempts (5 times for the operator/user).
NOTE: If the IP address is locked, you can try to login into the device after 30 minutes.

8.2.3. Anonymous Visit

Enabling this function allows that somebody visits the device who does not have the user name and password of the device.

NOTE: Only live view is available for the anonymous user.

Steps:
1. Enter the Anonymous Visit interface: Security> Anonymous Visit



Anonymous Visit: Disable

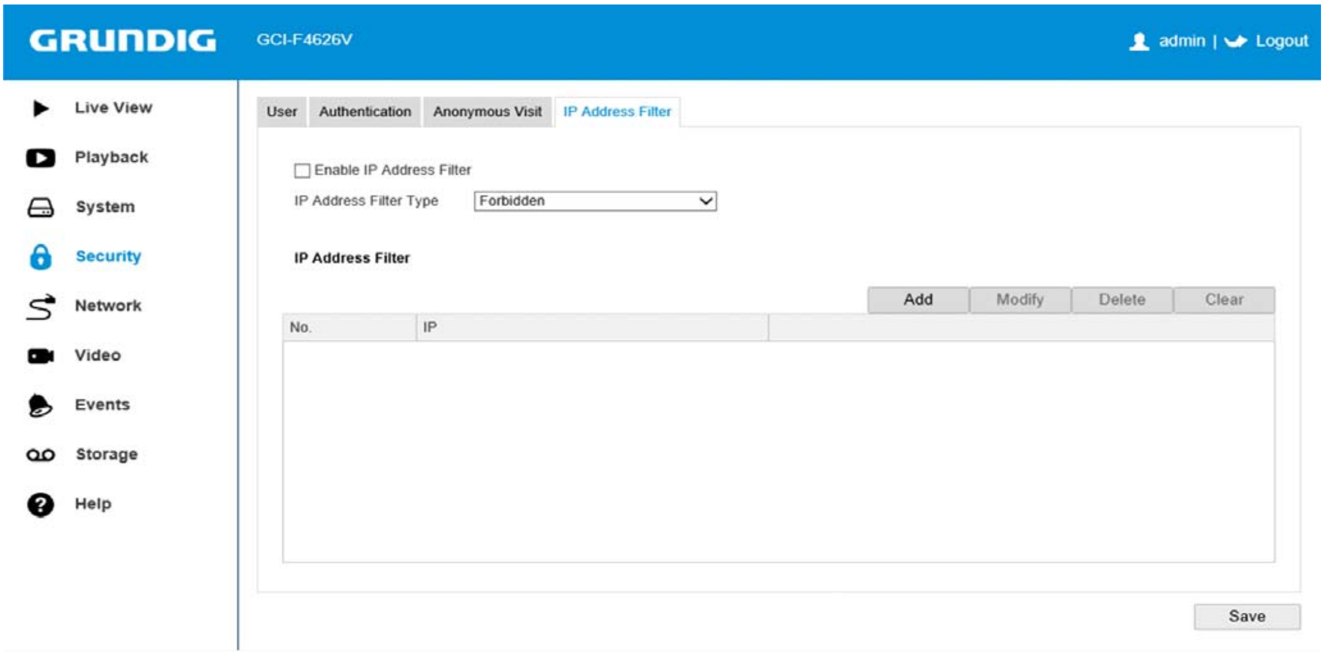
2. Set the "Anonymous Visit" permission to "Enable" or "Disable" in the drop-down list to enable or disable the anonymous visit.
3. Click on "Save" to save the settings.
There will be a checkbox next to "Anonymous" the next time you are logging in.

4. Check the checkbox of "Anonymous" and click on "Login". By permitting the Anonymous "Live View" function, you may enable others to access your camera and view live images without providing the login credentials. It is therefore critical when permitting the Anonymous "Live View" function to ensure that your camera's field of view does not impact the privacy of individuals whose images might be captured without authorisation. Given ist inherent intrusiveness, video surveillance is inappropriate in areas where people have a higher expectation of privacy.

8.2.4. IP Address Filter

This function makes access control possible.

Steps:
1. Enter the IP Address Filter interface: Security> IP Address Filter



□ Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter

2. Check the checkbox of “Enable IP Address Filter”.
3. Select the type of the IP Address Filter in the drop-down list, the options “Forbidden” and “Allowed” are selectable.
4. Set the IP Address Filter list.

- Add an IP Address:

Steps:
(1) Click on “Add” to add an IP.
(2) Input the IP Adreess.

(3) Click on “OK” to finish the adding.
- Modify an IP Address:

Steps:
(1) Left-click on an IP address from the filter list and click on “Modify”.
(2) Modify the IP address in the text filed.

(3) Click on “OK” to finish the modifying.
- Delete an IP Address:
Left-click on an IP address from the filter list and click on “Delete”.
- Delete all IP Addresses:
Click on “Clear” to delete all the IP addresses.

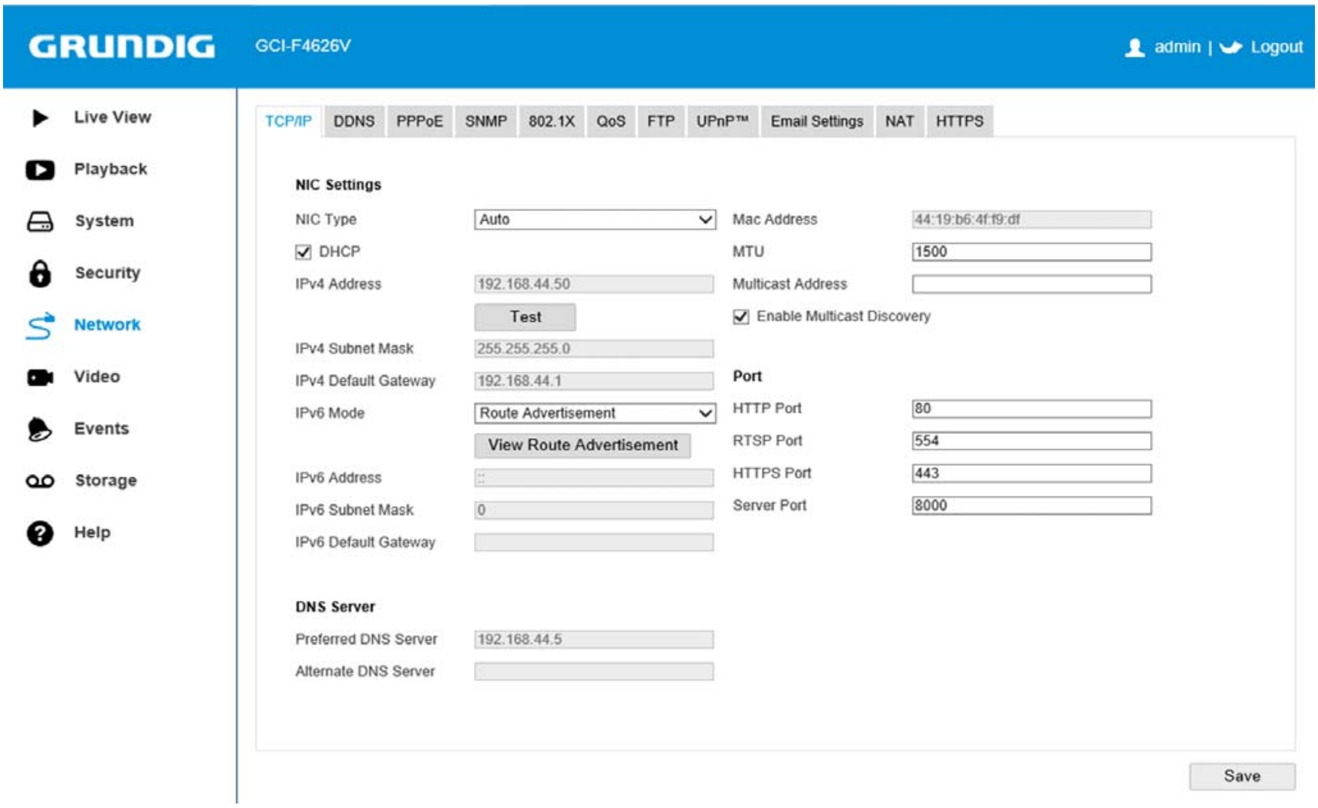
5.Click on “Save” to save the settings.

8.3. Network Settings

8.3.1. TCP/IP

The TCP/IP settings must be properly configured before you operate the camera over the network. The camera supports both the IPv4 and IPv6. Both versions may be configured simultaneously without conflicting each other, and at least one IP version should be configured.

Steps:
1. Enter the TCP/IP Settings interface: Network> TCP/IP



NIC Settings

NIC Type: Auto
☑ DHCP
IPv4 Address: 192.168.44.50
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 192.168.44.1
IPv6 Mode: Route Advertisement
IPv6 Address: ::
IPv6 Subnet Mask: 0
IPv6 Default Gateway:
Mac Address: 44:19:b6:4f:f9:df
MTU: 1500
Multicast Address:
☑ Enable Multicast Discovery

Port

HTTP Port: 80
RTSP Port: 554
HTTPS Port: 443
Server Port: 8000

DNS Server

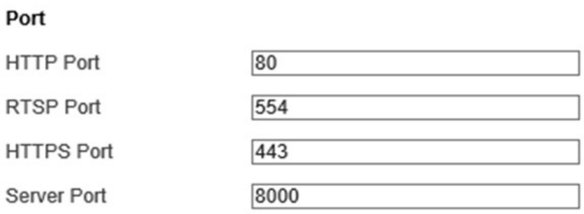
Preferred DNS Server: 192.168.44.5
Alternate DNS Server:

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
3. (Optional) If you check the checkbox next to “Enable Multicast Discovery”, then the online network camera can be automatically detected by the SCMS software via the private multicast protocol in the LAN.
4. Click on “Save” to save the above settings.

NOTE:
- The valid value range of MTU is 1280 ~ 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilising this function, you have to enable the Multicast function of your router.
- A reboot is required for the settings to take effect.

You can set the port No. of the camera, e.g. HTTP port, RTSP port and HTTPS port.

Steps:
1. Enter the Port Settings interface under: Network> TCP/IP



Port

HTTP Port: 80
RTSP Port: 554
HTTPS Port: 443
Server Port: 8000

2. Set the HTTP port, RTSP port, HTTPS port and server port of the camera.
- HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.
- RTSP Port: The default port number is 554, and it can be changed to any port No. ranges from 1024 to 65535.
- HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.
- Server Port: The default server port number is 8000, and it can be changed to any port No. That ranges from 2000 to 65535.

3. Click on “Save” to save the settings.

NOTE: A reboot is required for the settings to take effect.

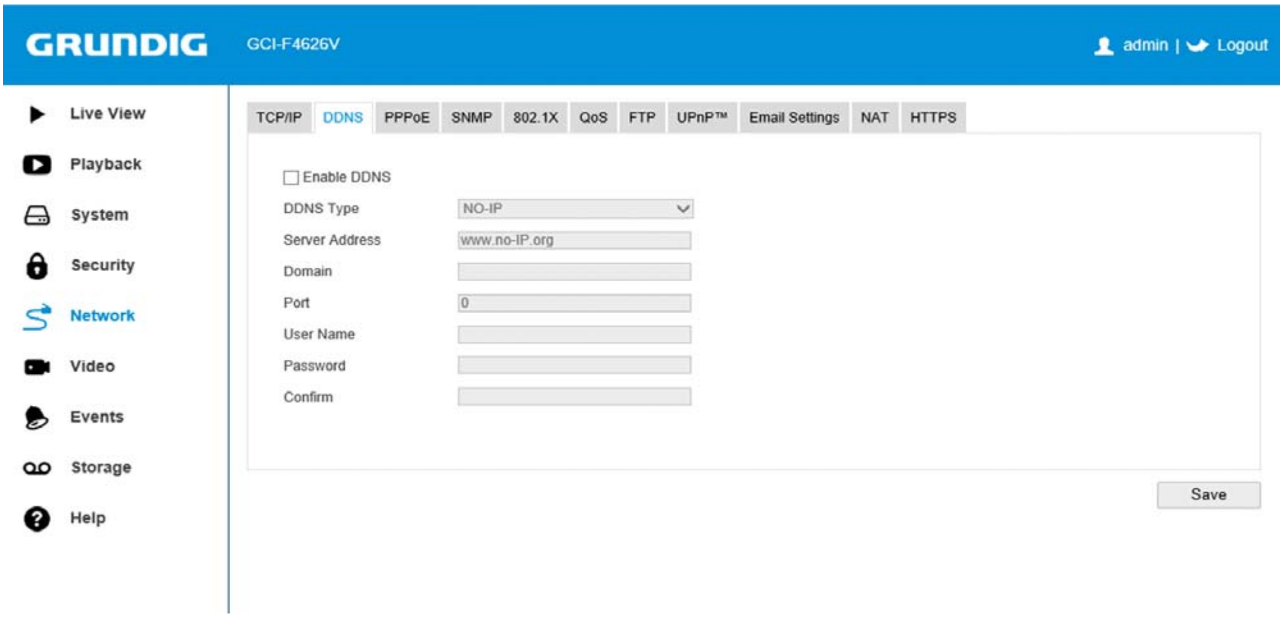
8.3.2. DDNS

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

Before you start:
Registration on the DDNS server is required before configuring the DDNS settings of the camera.

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Steps:
1. Enter the “DDNS” Settings interface: Network> DDNS



□ Enable DDNS
DDNS Type: NO-IP
Server Address: www.no-IP.org
Domain:
Port: 0
User Name:
Password:
Confirm:

2. Check the “Enable DDNS” checkbox to enable this feature.
3. Select the “DDNS Type”. Four DDNS types are selectable: HiDDNS, IPServer, NO-IP, and DynDNS.

- DynDNS:

Steps:
(1) Enter Server the Address of DynDNS (e.g. members.dyndns.org).
(2) In the Domain text field, enter the domain name obtained from the DynDNS website.
(3) Enter the “Port” of the DynDNS server.
(4) Enter the “User Name” and “Password” registered on the DynDNS website.
(5) Click on “Save” to save the settings.

- IP Server:

Steps:
(1) Enter the "Server Address" of the IP Server.
(2) Click on “Save” to save the settings.

NOTE: For the IP Server, you have to apply a static IP, subnet mask, gateway and preferred DNS from the ISP. Under “Server Address” should be entered the static IP address of the computer that runs the IP Server software.

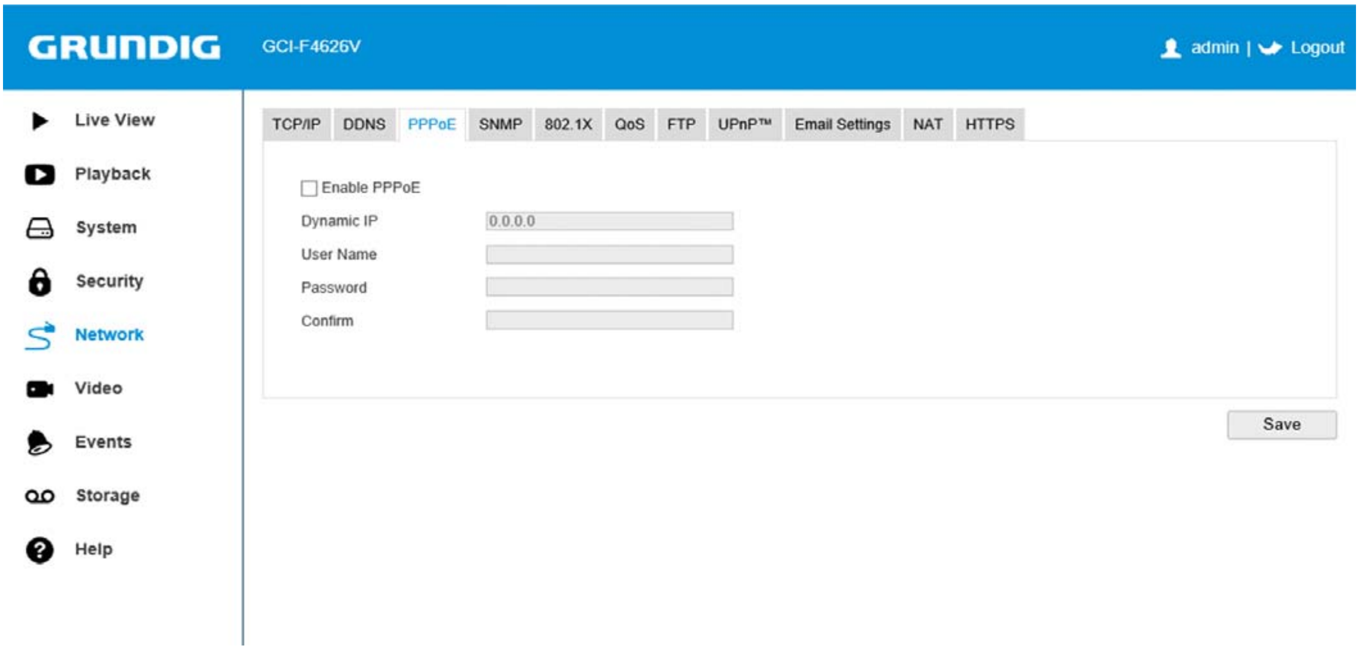
- NO-IP:

Steps:
(1) Choose for the “DDNS Type” the option “NO-IP”.

(2) Enter the “Server Address” as www.noip.com
(3) Enter the “Domain” name you registered.
(4) Enter the “Port” number, if needed.
(5) Enter the “User Name” and “Password”.
(6) If you click on “Save”, then you can view the camera with the domain name.

8.3.3. PPPoE

Steps:
1. Enter the PPPoE Settings interface: Network> PPPoE



□ Enable PPPoE
Dynamic IP 0.0.0.0
User Name
Password
Confirm

2. Check the “Enable PPPoE” checkbox to enable this feature.
3. Enter the “User Name”, “Password”, and “Confirm” the password for the PPPoE access.

NOTE: The User Name and Password should be assigned by your ISP (Internet Service Provider).

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

NOTE: A reboot is required for the settings to take effect.

8.3.4. SNMP

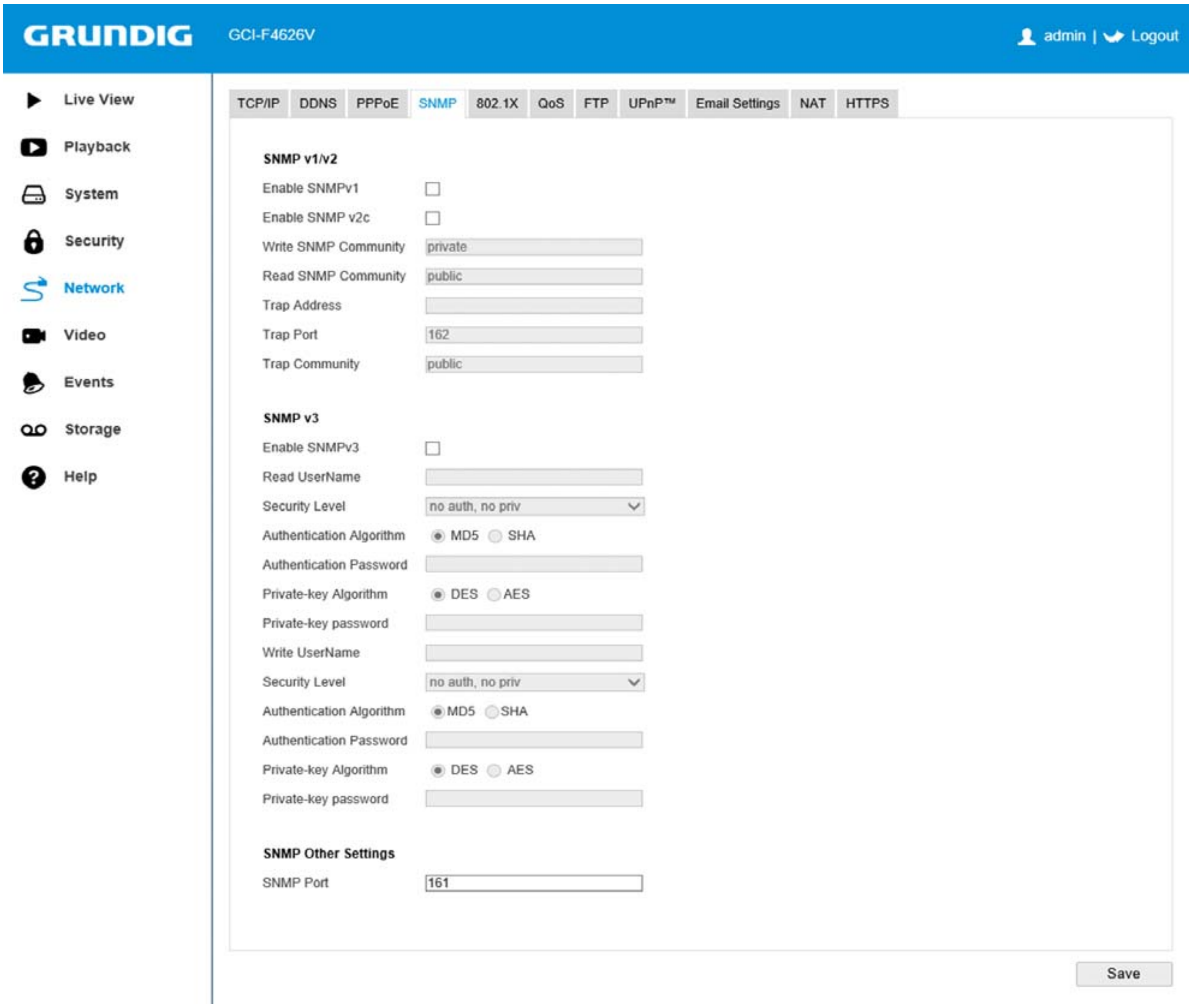
You can set the SNMP function to get camera status, parameters and alarm related information and manage the camera remotely when it is connected to the network.

Before you start:
Before setting the SNMP, please download the SNMP software and manage to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

NOTE: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires a password for access. SNMP v3 provides encryption and if you use the third version, a HTTPS protocol must be enabled.

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Steps:
1. Enter the "SNMP" Settings interface: Network> SNMP



SNMP v1/v2

Enable SNMPv1 □

Enable SNMP v2c □

Write SNMP Community: private

Read SNMP Community: public

Trap Address:

Trap Port: 162

Trap Community: public

SNMP v3

Enable SNMPv3 □

Read UserName:

Security Level: no auth, no priv

Authentication Algorithm: ● MD5 ○ SHA

Authentication Password:

Private-key Algorithm: ● DES ○ AES

Private-key password:

Write UserName:

Security Level: no auth, no priv

Authentication Algorithm: ● MD5 ○ SHA

Authentication Password:

Private-key Algorithm: ● DES ○ AES

Private-key password:

SNMP Other Settings

SNMP Port: 161

2. Check the corresponding version checkbox ("Enable SNMP" v1/v2 or: "Enable SNMP v3") to enable this feature.
3. Configure the SNMP settings.

NOTE: The settings of the SNMP software should be the same as the settings you configure here.

4. Click on “Save” to save and finish the settings.

NOTE: A reboot is required for the settings to take effect.

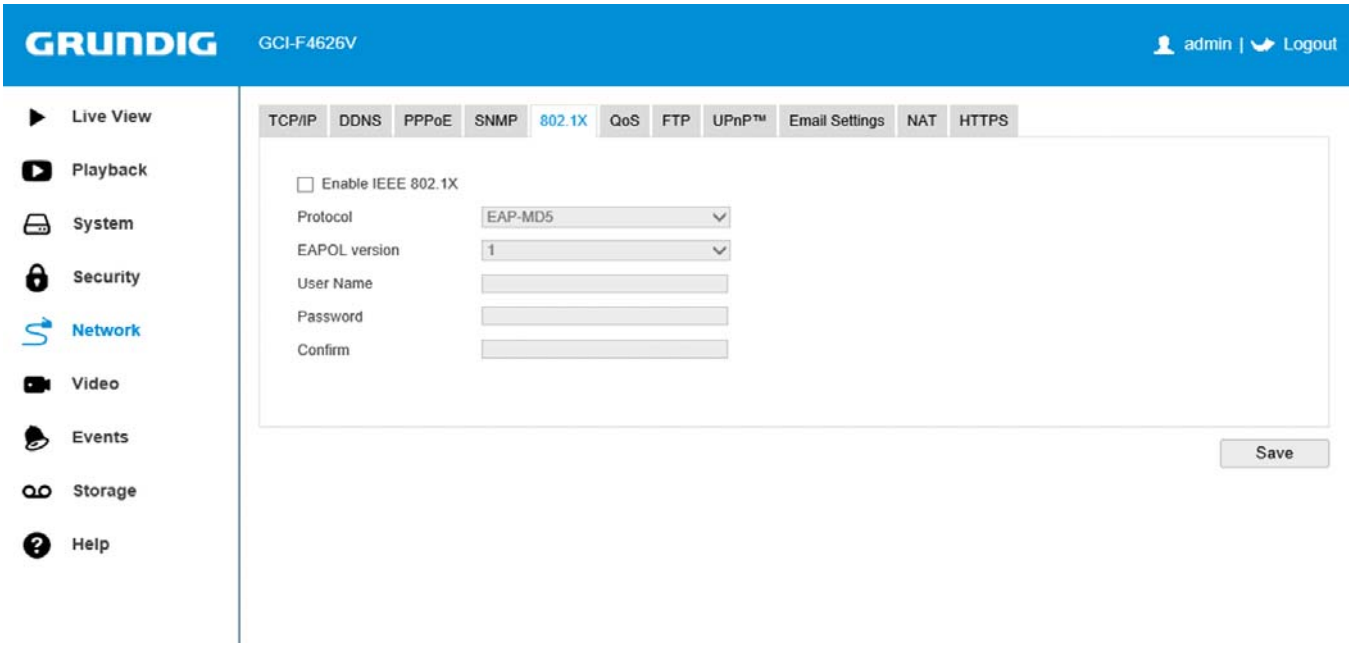
8.3.5. 802.1X

The IEEE 802.1X standard is supported by these network cameras, and when this feature is enabled, the camera data is secured and the user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

Before you start:
The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Steps:
1. Enter the 802.1X Settings interface: Network> 802.1X



□ Enable IEEE 802.1X
Protocol EAP-MD5
EAPOL version 1
User Name
Password
Confirm

2. Check the “Enable IEEE 802.1X” checkbox to enable this feature.
3. Configure the 802.1X settings, including the EAPOL version, user name and password.

NOTE: The EAPOL version must be identical with that of the router or the switch.

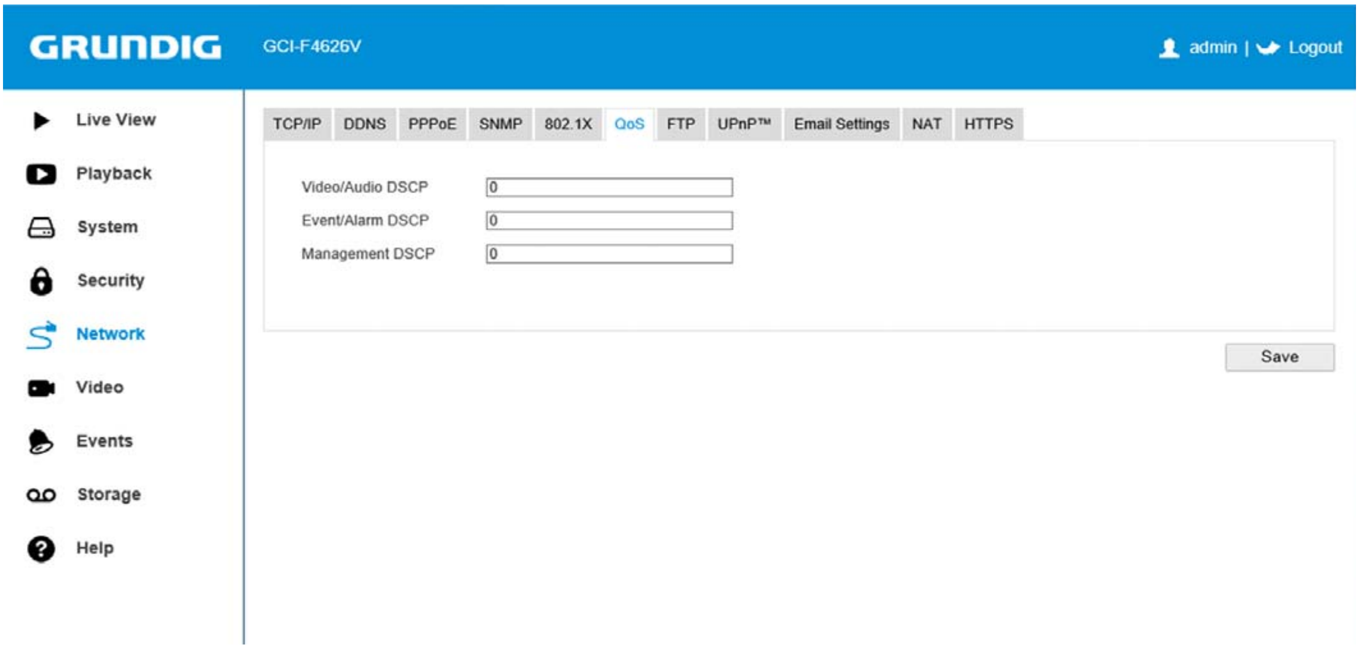
4. Enter the user name and password to access the server.
5. Click on “Save” to finish the settings.

NOTE: A reboot is required for the settings to take effect.

8.3.6. QoS

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending.

Steps:
1. Enter the QoS Settings interface: Network> QoS



Video/Audio DSCP 0
Event/Alarm DSCP 0
Management DSCP 0

2. Configure the QoS settings, including “Video/Audio DSCP”, “Event/Alarm DSCP” and “Management DSCP”. The valid value range of the DSCP is 0-63. The bigger the DSCP value is, the higher the priority is.

NOTE: DSCP refers to the Differentiated Service Code Point and the DSCP value is used in the IP header to indicate the priority of the data.

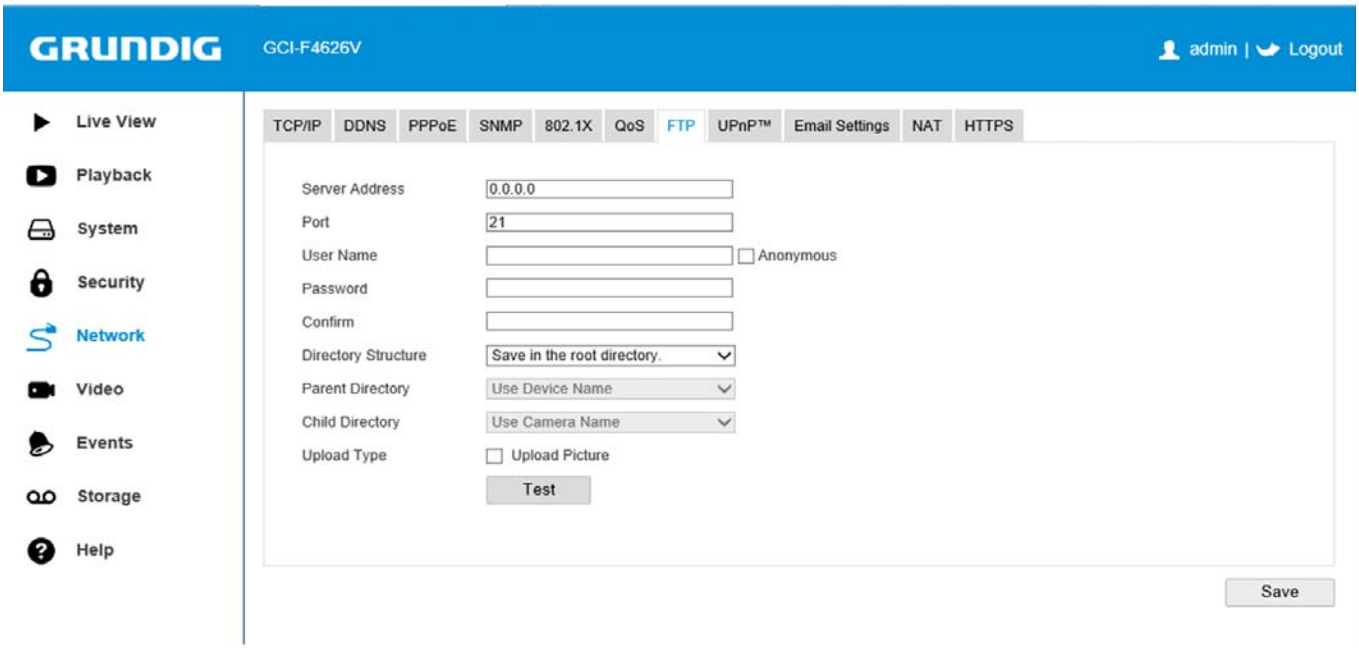
3. Click on “Save” to save the settings.

NOTE: A reboot is required for the settings to take effect.

8.3.7. FTP

You can configure the FTP server related information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

Steps:
1. Enter the FTP Settings interface: Network> FTP



Server Address: 0.0.0.0
Port: 21
User Name: □ Anonymous
Password:
Confirm:
Directory Structure: Save in the root directory.
Parent Directory: Use Device Name
Child Directory: Use Camera Name
Upload Type: □ Upload Picture

2. Configure the FTP settings. Put in the user name and password that are required for login to the FTP server.

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- Directory: In the “Directory Structure” field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. As the name of the directory.
- Upload type: To enable uploading the captured picture to the FTP server.
- Anonymous Access to the FTP Server (in which case the user name and password won’t be required.): Check the “Anonymous” checkbox to enable the anonymous access to the FTP server.

NOTE: The anonymous access function must be supported by the FTP server.

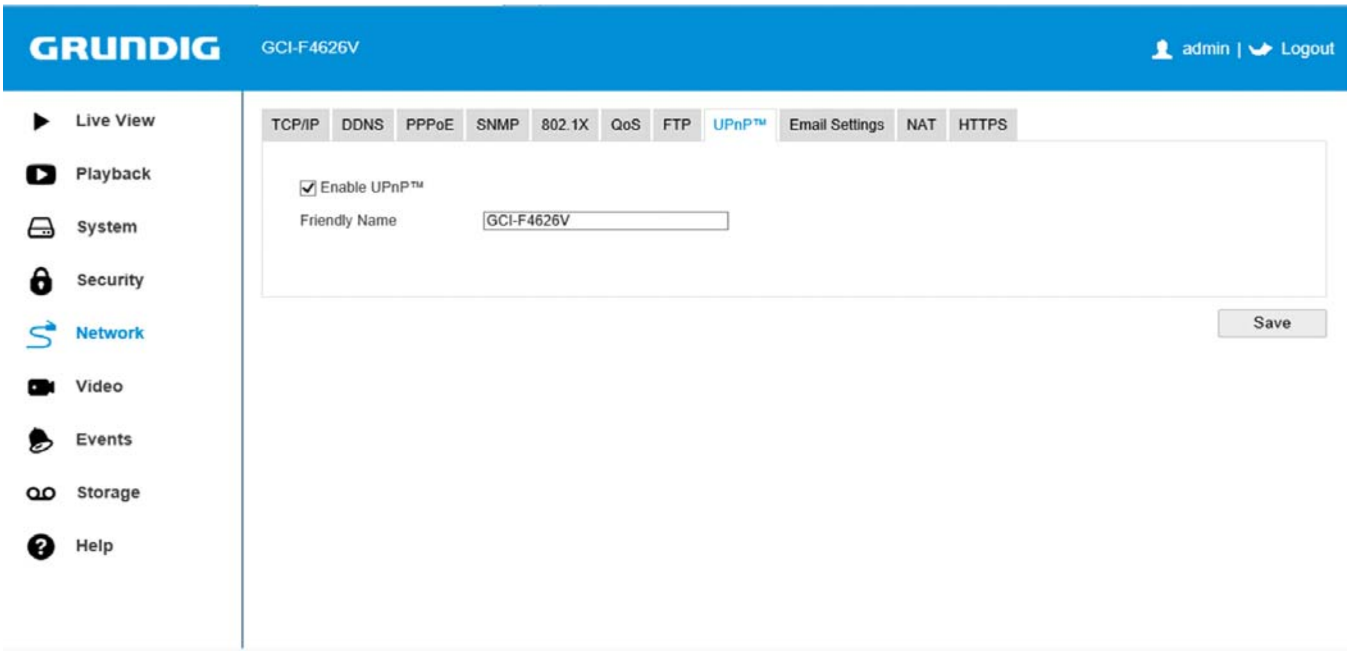
3. Click on “Save” to save the settings.

NOTE: If you want to upload the captured pictures to the FTP server, you have to enable the timing snapshot or event-triggered snapshot on the “Snapshot” page. For detailed information, please refer to Section 9.3.

8.3.8. UPnP

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of the networks in the home and corporate environments.
With this function enabled, you do not need to configure the port mapping for each port, and the camera will be connected to the Wide Area Network via the router.

Steps:
1. Enter the UPnP™ settings interface: Network> UPnP
2. Check the checkbox "Enable UPnP" to enable the UPnP™ function. The name of the device when detected online can be edited.



☑ Enable UPnP™

Friendly Name: GCI-F4626V

8.3.9. Email Settings

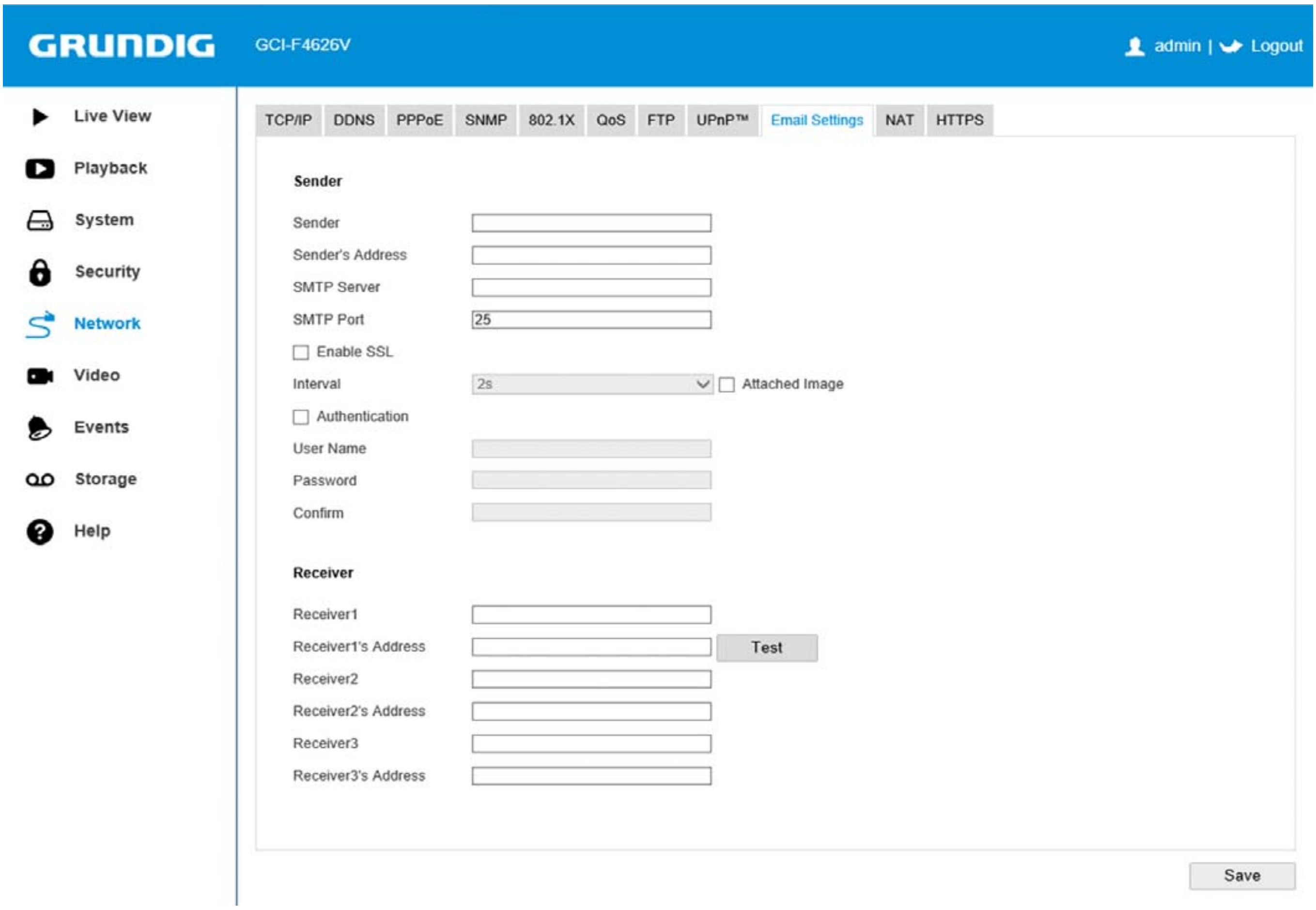
The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before you start:
Please configure the DNS Server settings under Network> TCP/IP before using the Email function.

Steps:
1. Enter the TCP/IP Settings (Network> TCP/IP) to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

NOTE: Please refer to Section 8.3.1 "TCP/IP" for detailed information.

2. Enter the Email Settings interface:
Network> Email Settings



Sender

Sender
Sender's Address
SMTP Server
SMTP Port 25
□ Enable SSL
Interval 2s □ Attached Image
□ Authentication
User Name
Password
Confirm

Receiver

Receiver1
Receiver1's Address
Receiver2
Receiver2's Address
Receiver3
Receiver3's Address

3. Configure the following settings:
- Sender: The name of the email sender.
- Sender's Address: The email address of the sender.
- SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
- SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.
- Enable SSL: Check the checkbox of “Enable SSL” to enable SSL if it is required by the SMTP server.
- Attached Image: Check the checkbox of “Attached Image” if you want to send emails with attached alarm images.
- Interval: The interval refers to the time between two actions of sending attached pictures.
- Authentication (optional): If your email server requires authentication, check this checkbox to use the authentication to log in to this server and enter the login user name and password.

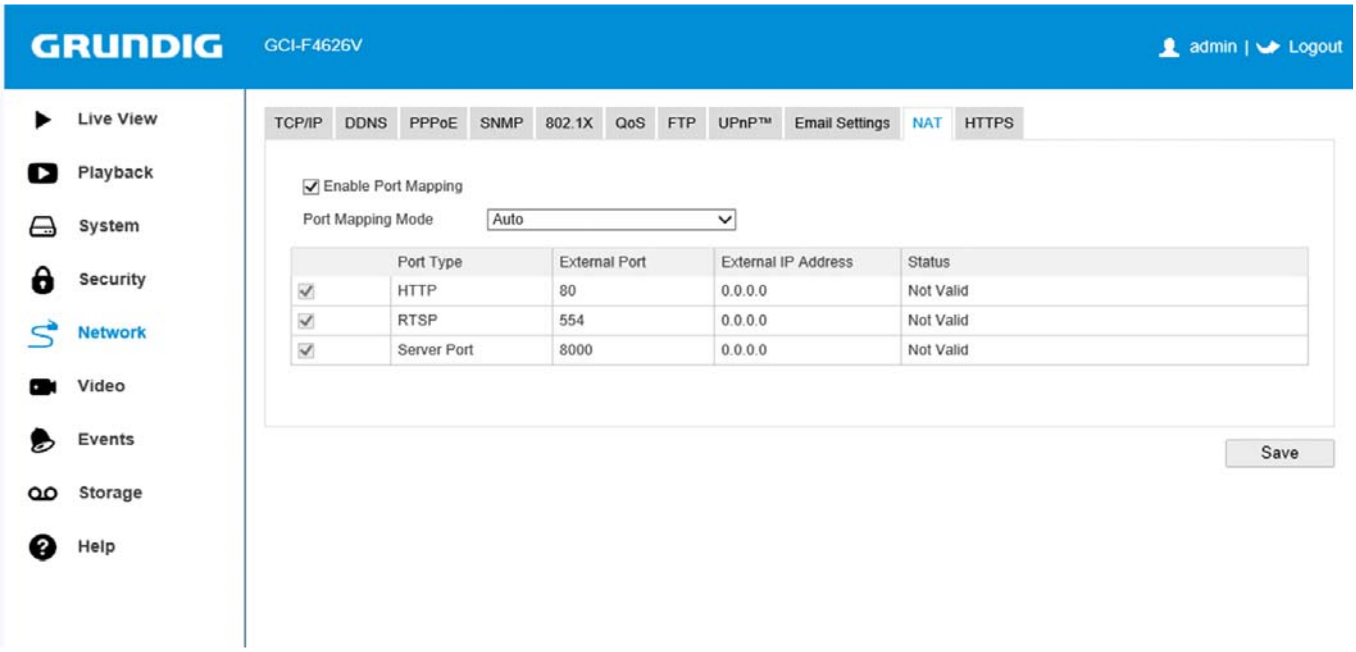
ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- Choose Receiver: Select the receiver to which the email will be sent. Up to 2 receivers can be configured.
- Receiver: The name of the user to be notified.
- Receiver's Address: The email address of the user to be notified.

4.Click on "Save" to save the settings.

8.3.10. NAT (Network Address Translation)

1. Enter the NAT settings interface. Network> NAT
2. Choose the port mapping mode.
To do port mapping with the default port numbers:
Choose for the "Port Mapping Mode" the option"Auto". To do port mapping with the customised port numbers: Choose for the "Port Mapping Mode" the option "Manual". And for manual port mapping, you can customise the value of the port number by yourself.
3. Click on "Save" to save the settings.



☑ Enable Port Mapping

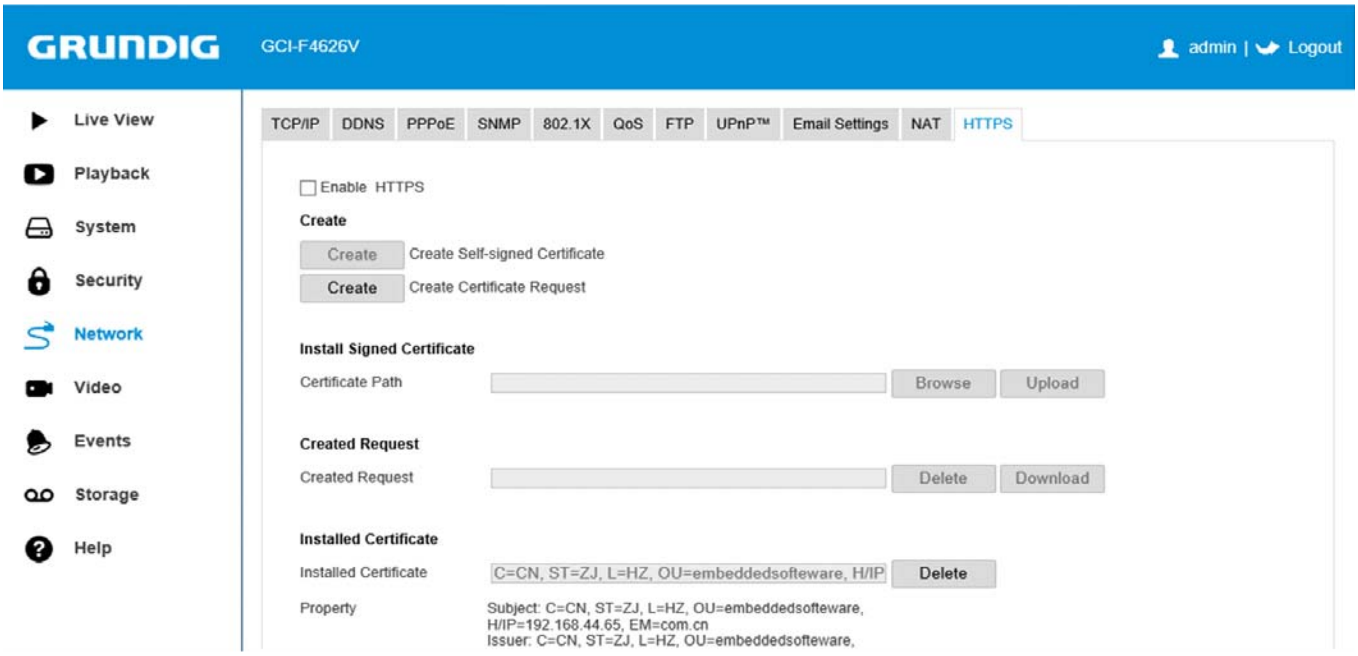
Port Mapping Mode: Auto

	Port Type	External Port	External IP Address	Status
☑	HTTP	80	0.0.0.0	Not Valid
☑	RTSP	554	0.0.0.0	Not Valid
☑	Server Port	8000	0.0.0.0	Not Valid

8.3.11. HTTPS

HTTPS provides authentication of the web site and associated web server that you are communicating with, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.
E.g.: If you set the port number as 443 and the IP address is 192.168.1.100, you may access the device by inputting "https://192.168.1.100:443" into the web browser.

Steps:
1. Enter the HTTPS settings interface: Network> HTTPS
2. Check the checkbox of "Enable HTTPS "to enable the function.
3. Create the self-signed certificate or authorised certificate.



☐ Enable HTTPS

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

Installed Certificate

Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP

Property: Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=192.168.44.65, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware,

- Create the self-signed certificate:

1) Click on the "Create" button to enter the creation interface.

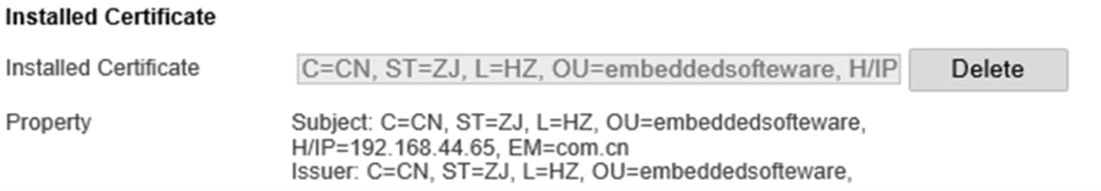
2) Enter the country, host name/IP, validity and other information.
3) Click on "OK" to save the settings.

NOTE: If you already have a certificate installed, the "Create Self-signed Certificate" will be grayed out.

- Create the authorised certificate:

1) Click on the "Create" button to create the certificate request.
2) Download the certificate request and submit it to the trusted certificate authority for signature.
3) After receiving the signed valid certificate, import the certificate to the device.

4. There will be the following certificate information after you successfully created and installed the certificate.



Installed Certificate

Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP

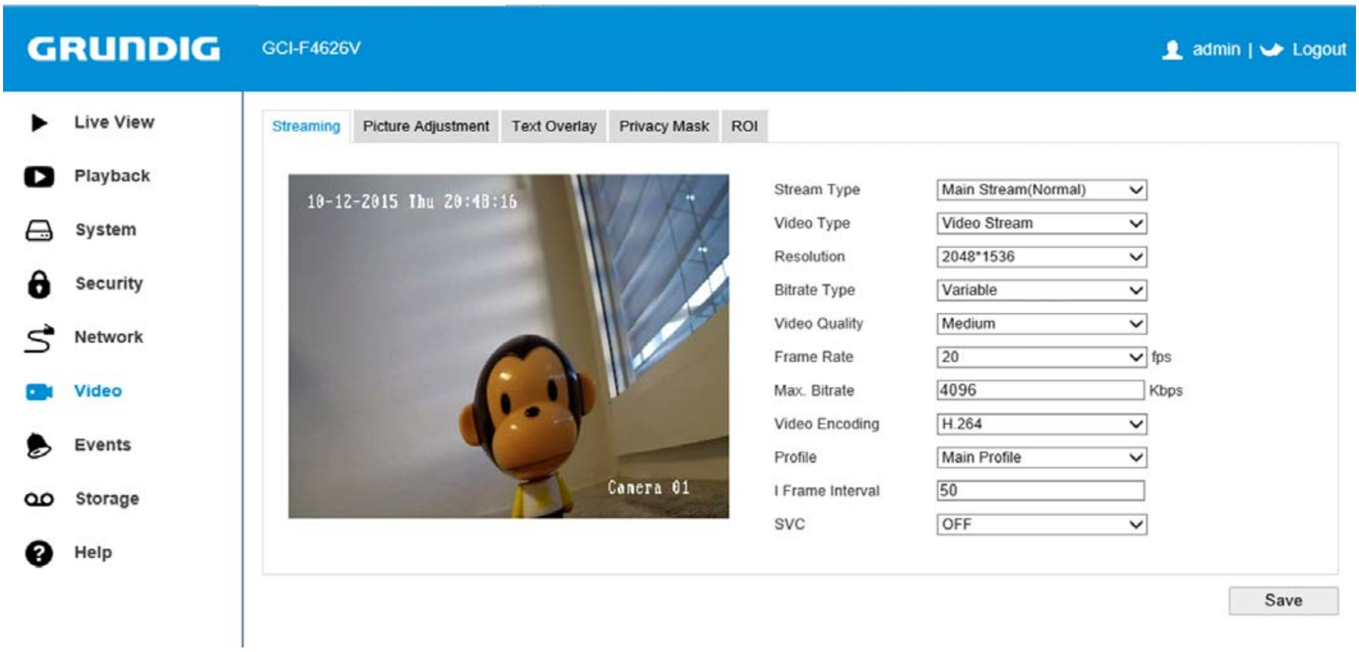
Property: Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=192.168.44.65, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware,

5. Click on the "Save" button to save the settings.

8.4. Video Settings

8.4.1. Streaming

Steps:
1. Enter the Video Settings interface: Video> Streaming



Stream Type: Main Stream(Normal)
Video Type: Video Stream
Resolution: 2048*1536
Bitrate Type: Variable
Video Quality: Medium
Frame Rate: 20 fps
Max. Bitrate: 4096 Kbps
Video Encoding: H.264
Profile: Main Profile
I Frame Interval: 50
SVC: OFF

2. Set the "Stream Type" of the camera to "Main Stream(Normal)" or "Sub-Stream"
The main stream is usually for recording and live viewing with good bandwidth, whereas the sub-stream can be used for live viewing when the bandwidth is limited.
3. You can customise the following parameters for the selected main stream or sub-stream:

- Video Type:
Set the stream type to "Video Stream", or "Video & Audio Composite Stream". The audio signal will be recorded only when the "Video Type" is set to "Video & Audio".

- Resolution:
Select the resolution of the video output.

- Bitrate Type:
Set the "Bitrate Type" to "Constant" or "Variable".

- Video Quality:
When the "Bitrate Type" is set as "Variable", 6 levels of video quality are selectable.

- Frame Rate:
Set the frame rate to 1/16~25 fps. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains the image quality throughout.

- Max. Bitrate:
Set the "Max. Bitrate" to 32~12288 Kbps. A higher value means a higher video quality, but a higher bandwidth is required.

- Video Encoding:
If the "Stream Type" is set to "Main Stream": H.264 is selectable. If the "Stream Type" is set to "Sub Stream" or "Third Stream", H.264 and MJPEG are selectable.

- Profile:
Only Main Profile is selectable for the encoding.

- I Frame Interval:
Set the I-Frame interval to 1~250.

- SVC:
Scalable Video Coding is an extension of the H.264/AVC standard. Select "OFF" / "ON" to disable / enable the SVC function. If you select "Auto", the device will automatically extract frames from the original video when the network bandwidth is insufficient.

4. Click on "Save" to save the settings.

8.4.2. Picture Adjustment

You can set the image quality of the camera, including brightness, contrast, saturation, hue, sharpness, etc.

Steps:
1. Enter the Picture Adjustment interface:
Video> Picture Adjustment

2. Set the image parameters of the camera.

NOTE: In order to guarantee the image quality in different illuminations, the camera provides two sets of parameters for the user to configure.

- Switch Day and Night (Day/Night Auto-switch):

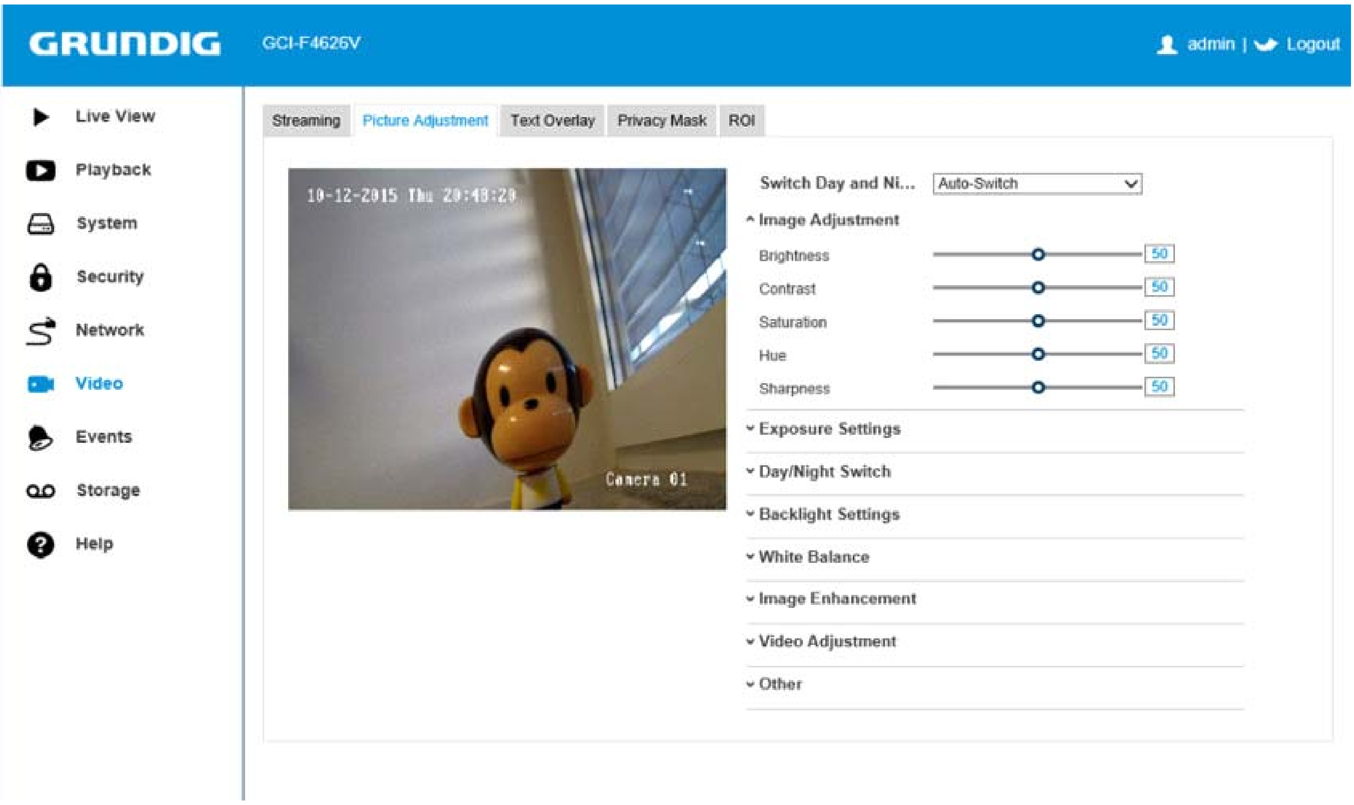
The Day/Night scheduled-switch configuration interface enables you to set separate camera parameters for day and night to guarantee the image quality in different illuminations.

Steps:
1. Click on the time line to select the start time and the end time of the switch.
2. Click on the “Common” tab to configure the common parameters applicable to day mode and night mode.

NOTE: The detailed information of each parameter refers to the day/night auto switch session.

3. Click on the “Day” tab to configure the parameters applicable for day mode.
4. Click on the “Night” tab to configure the parameters applicable for night mode.

NOTE: The settings saved automatically if any parameter is changed.



Switch Day and Ni... Auto-Switch

Brightness	50
Contrast	50
Saturation	50
Hue	50
Sharpness	50

> Image Adjustment:
>> Brightness: Describes the brightness of the image, which ranges from 1~100, and the default value is 50.
>> Contrast: Describes the contrast of the image, which ranges from 1~100, and the default value is 50.
>> Saturation: Describes the colourfulness of the image colour, which ranges from 1~100, and the default value is 50.
>> Sharpness: Describes the edge contrast of the image, which ranges from 1~100, and the default value is 50.

> Exposure Settings
If the camera is equipped with a fixed lens, only “Manual” is selectable.
The exposure time refers to the electronic shutter time, which ranges from 1/3 ~ 1/100,000s. Adjust it according to the actual luminance condition.

> Day/Night Switch:
Select the “Day/Night Switch” mode, and configure the smart IR settings from this option.

Day, night, auto, schedule are selectable for the day/night switch.
>> Day: The camera stays at day mode.
>> Night: The camera stays at night mode.
>> Auto: The camera switches between day mode and night mode automatically according to the illumination. The sensitivity ranges from 0~7. The higher the value is, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.
>> Schedule: Set the start time and the end time to define the duration for day/night mode.
>> Smart IR: The Smart IR function gives users an option to adjust the power of the IR LED, thus providing a clear image that is not overexposed or too dark. Select "ON" to enable the smart IR.

> Backlight Settings:
>> BLC: If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates the light to the object in the front to make it clear. "OFF", "Up", "Down", "Left", "Right" and "Center" and customise are selectable.
>> WDR: The Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

> White Balance:
The White Balance is the white rendition function of the camera used to adjust the colour temperature according to the environment.

> Image Enhancement:
>> Digital Noise Reduction:
The DNR reduces the noise in the video stream. "OFF" and "ON" are selectable. Set the DNR level from 0~100, the default value is 50 in Normal Mode. Set the DNR level for thespace DNR level [0~100].

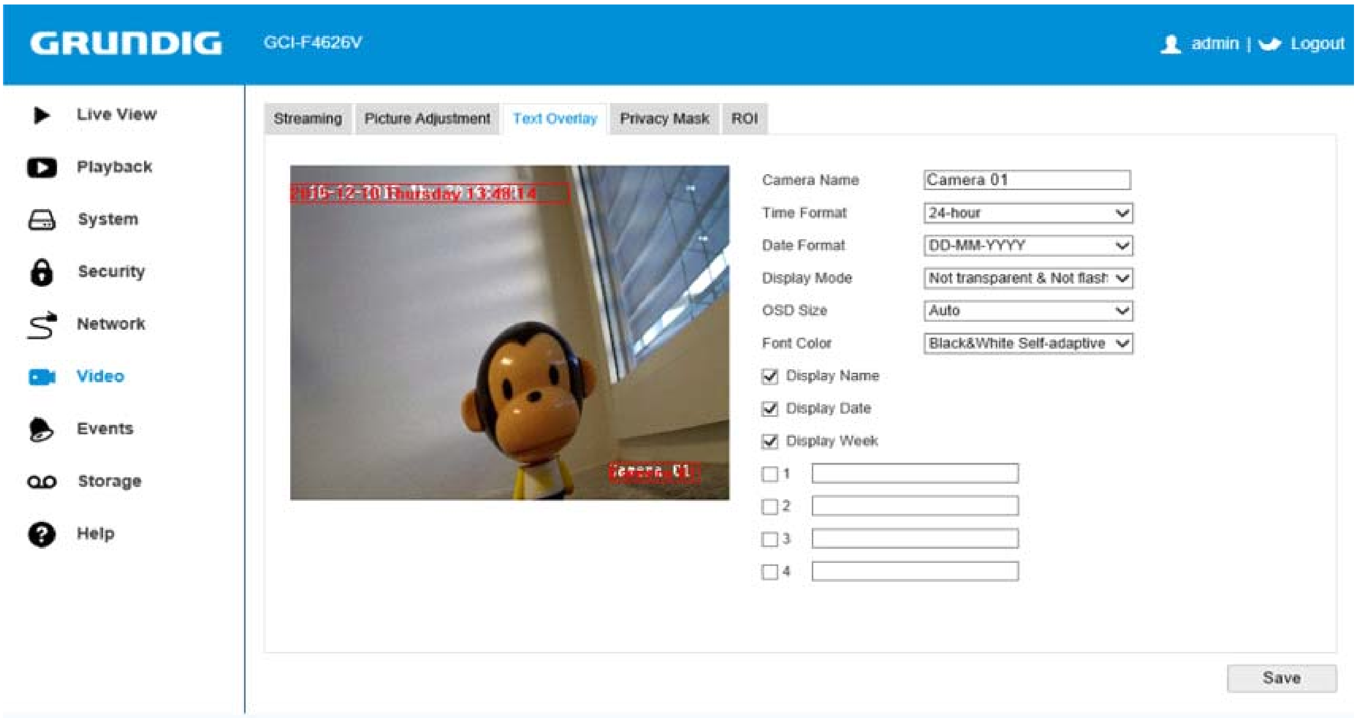
> Video Adjustment:
>> Camera Rotation: It rotates the image so you can see it inversed. Normal, Mirror, flip and 180° are selectable.
>> Rotate (Vertical Mode): To make a complete use of the 16:9 aspect ratio, you can enable the "Rotate" function when you use the camera in a narrow view scene.
When installing the camera, turn it to 90 degrees or rotate the 3-axis lens to 90 degrees, and set the "Rotate Mode" as on. You will get a normal view of the scene with a 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.
>> Scene Mode: Select for the "Scene Mode" the option "Indoor" or "Outdoor" according to the real environment.
>> Video Standard: "50 Hz" and "60 Hz" are selectable. Choose an option according to the different video standards: normally 50 Hz is selected for the PAL standard and 60 Hz for the NTSC standard.
>> Capture Mode: It is the selectable video input mode to meet the different demands of the field of view and the resolution.

> Other:
Some of the camera support the CVBS output. Please refer to the actual camera model for details.

8.4.3. Text Overlay

You can customise the camera name and time on the screen.

Steps:
1. Enter the OSD Settings interface: Video> Text Overlay



Camera Name: Camera 01
Time Format: 24-hour
Date Format: DD-MM-YYYY
Display Mode: Not transparent & Not flash
OSD Size: Auto
Font Color: Black&White Self-adaptive

☑ Display Name
☑ Display Date
☑ Display Week
□ 1
□ 2
□ 3
□ 4

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of “Camera Name”.
4. Select from the drop-down list to set the time format, date format, display mode and the OSD font size.
5. Define the font colour of the OSD by clicking on the drop-down list: black & white self-adaptive and custom are selectable.

6. You can use the mouse to click and drag the text frame, eg. “Camera 01 (in a box)” in the live view window to adjust the OSD position.

7. Check the checkbox in front of one textbox with a number after the box (1 or 2 or 3...) to enable the on-screen display.
8. Input the characters in the textbox.
9. (Optional) Use the mouse to click and drag the red text frame in the live view window to adjust ist text overlay position.
10. Click on “Save” to save the settings.

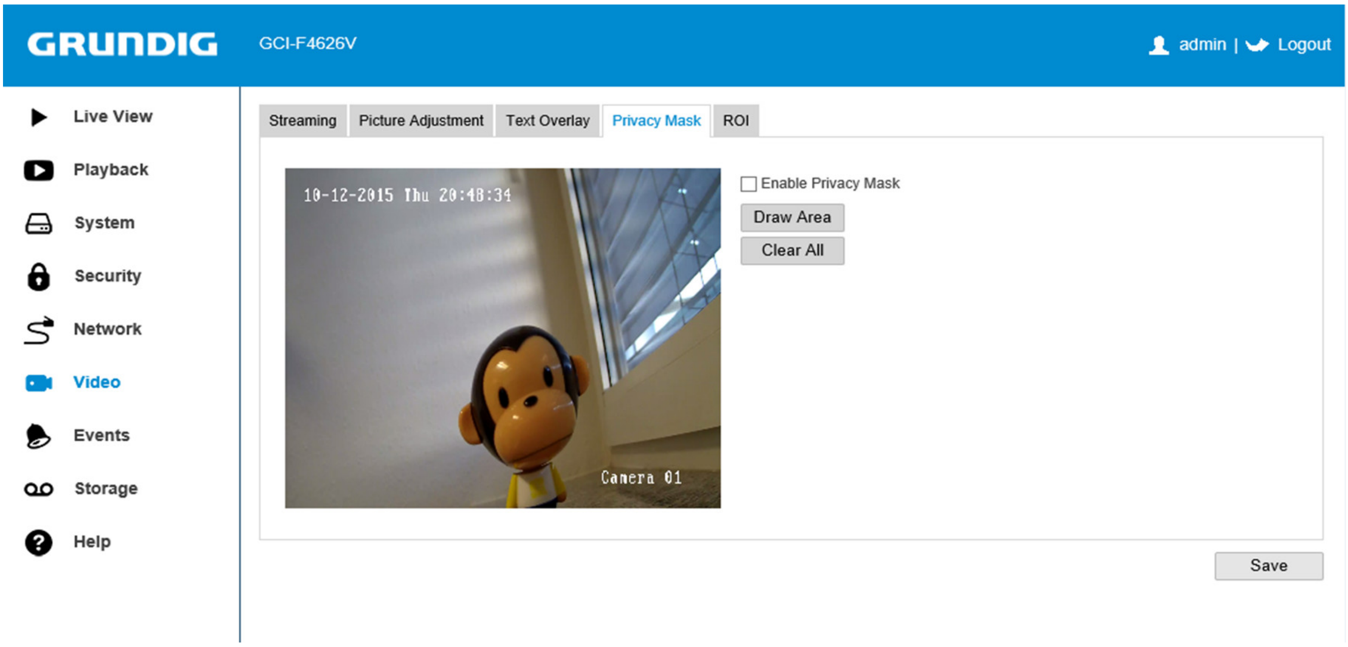
NOTE: Up to 4 text overlays are configurable.

11. Click on “Save” to activate the above settings.

8.4.4. Privacy Mask

The function "Privacy Mask" enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps:
1. Enter the Privacy Mask Settings interface: Video> Privacy Mask
2. Check the checkbox of "Enable Privacy Mask" to enable this function.
3. Click on "Draw Area".



4. Click and drag the mouse in the live video window to draw the mask area.

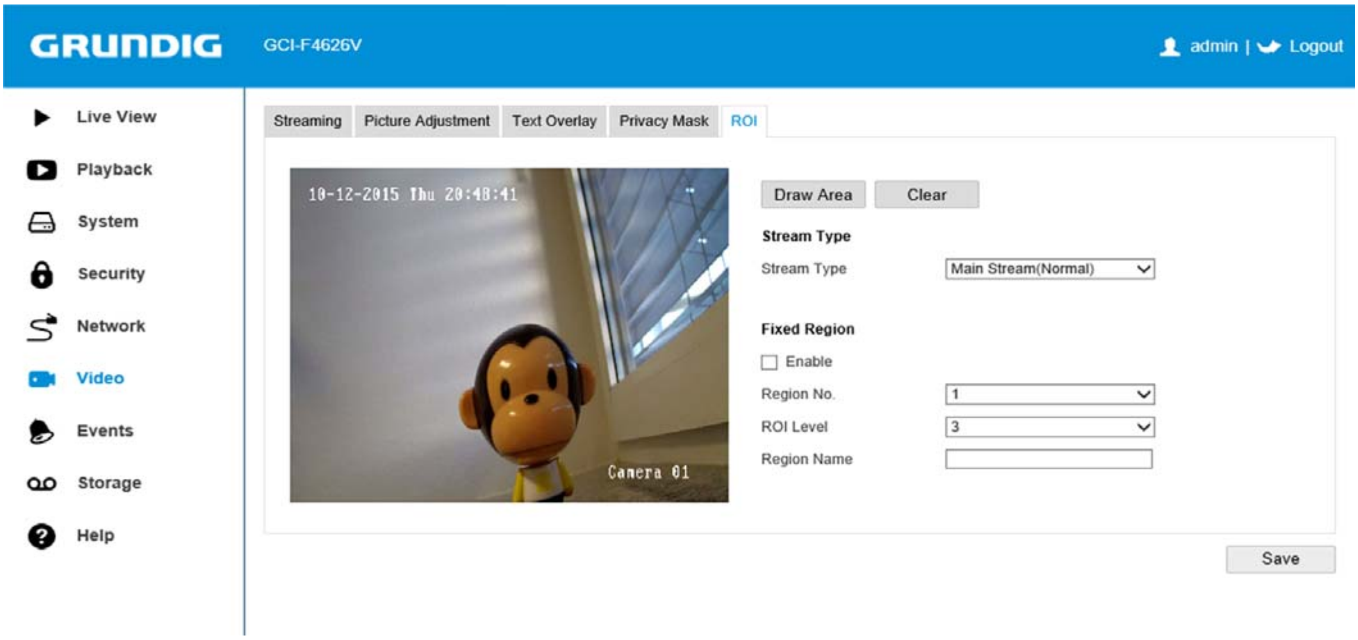
NOTE: You are allowed to draw up to 4 areas on the same image.

5. Click on "Stop Drawing" to finish drawing or click on "Clear All" to clear all of the areas you set without saving them.
6. Click on "Save" to save the settings.

8.4.5. ROI

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression, which means, the technology assigns more encoding resources to the region of interest, this happens to increase the quality of the ROI whereas the background information is less focused.

NOTE: The ROI function varies according to different camera models.



Stream Type

Stream Type: Main Stream(Normal)

Fixed Region

□ Enable

Region No.: 1

ROI Level: 3

Region Name:

Configuring the Fixed Region for the ROI:

Steps:
1. Enter the ROI settings interface: Video> ROI
2. Check the checkbox of "Enable" under "Fixed Region".
3. Select the "Stream Type" for the ROI encoding.
4. For these camera models, only one "Region No." is selectable.
5. Click on the "Draw Area" button, and then click-and-drag the mouse to draw the region of interest in the live video.
6. Select the "ROI Level" to set the image quality enhancing level. The larger the value is, the better the image quality will be.
7. Input the "Region Name" for the ROI as desired.
8. Click on "Save" to save the settings.

8.5. Events Settings

This section explains how to configure the network camera to respond to basic events, including motion detection, video tampering, exception, line crossing and intrusion detection. These events can trigger the linkage methods, such as the Notify IP Server, Send Email, etc.

NOTE:
Check the checkbox of Notify IP Server if you want the alarm information to be pushed to a PC or a mobile client software as soon as the alarm is triggered.

8.5.1. Motion Detection

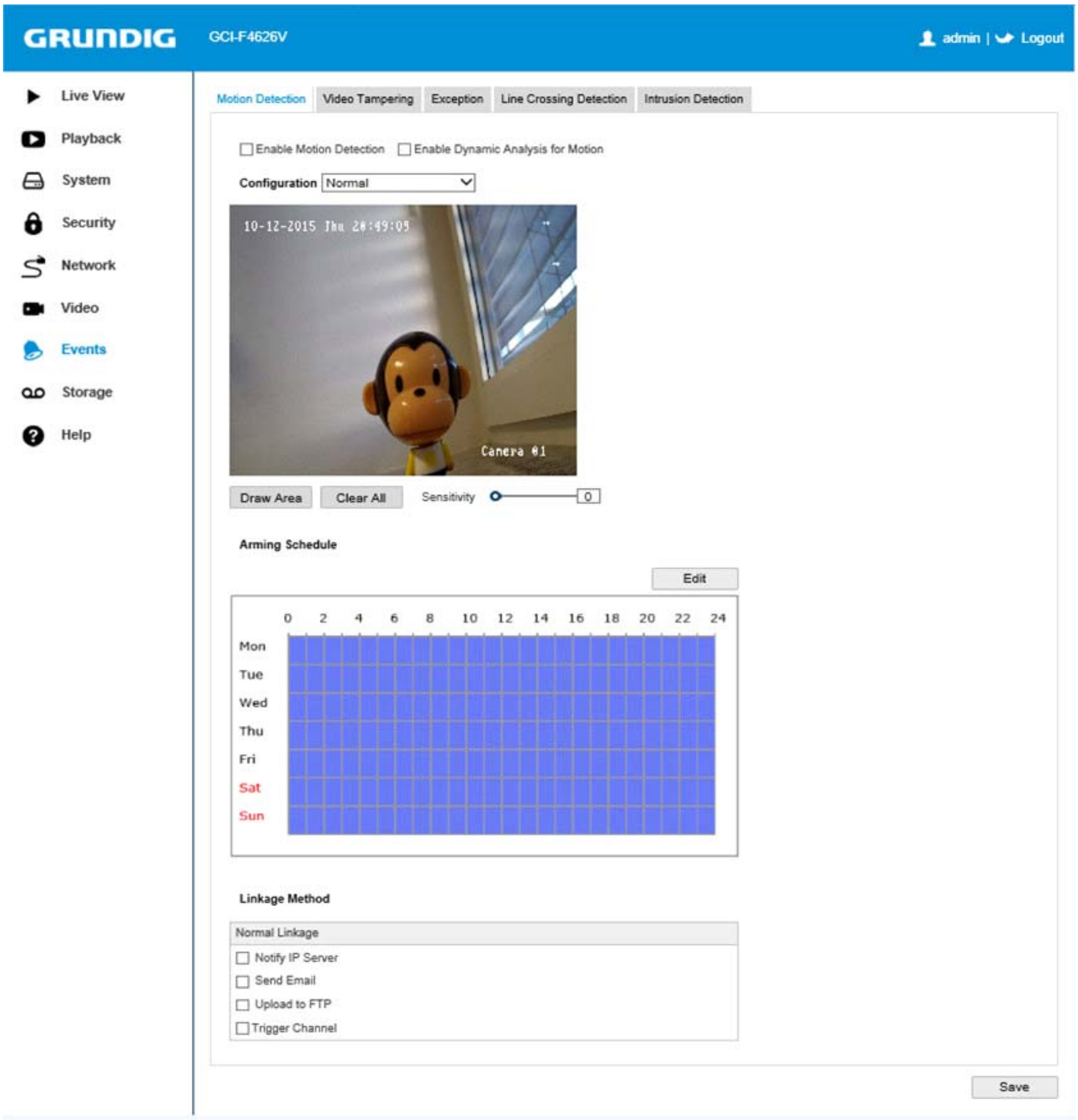
The Motion Detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.
In order to detect the moving objects accurately and reduce the false alarm rate, normal configuration and expert configuration are selectable for different motion detection environments.

- Normal Configuration:
The Normal Configuration adopts the same set of motion detection parameters in the daytime and at night.

Tasks:
1. Set the Motion Detection Area.

Steps:
(1) Enter the motion detection settings interface: Events> Motion Detection
(2) Check the checkbox of "Enable Motion Detection".
(3) Check the checkbox of "Enable Dynamic Analysis for Motion" if you want to mark the detected objects with green rectangles.

NOTE: Select "Disable" for rules if you do not want the detected objected displayed with the rectangles. Select "Disable" from System > Local Configuration > Rules.



□ Enable Motion Detection □ Enable Dynamic Analysis for Motion

Configuration: Normal

Sensitivity: 0

Arming Schedule

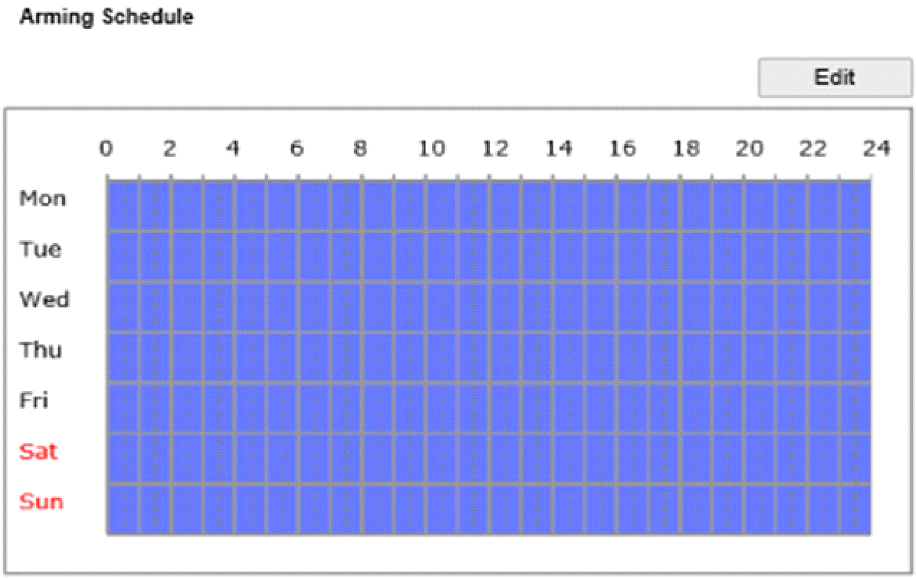
Linkage Method

Normal Linkage
□ Notify IP Server
□ Send Email
□ Upload to FTP
□ Trigger Channel

(4) Click on "Draw Area". Click and drag the mouse on the live video to draw a motion detection area.
(5) Click on "Stop Drawing" to finish the drawing of one area.
(6) (Optional) Click on "Clear All" to clear all of the areas.
(7) (Optional) Move the slider to set the sensitivity of the detection.

2. Set the Arming Schedule for Motion Detection.

Steps:



(1) Click on "Edit" to edit the arming schedule. The picture above shows the editing interface of the arming schedule.
(2) Choose the day you want to set the arming schedule for.
(3) Click on the "(square clock with red arm)" symbol to set the time period for the arming schedule.
(4) (Optional) After you set the arming schedule, you can copy the schedule to other days.
(5) Click on "OK" to save the settings.

NOTE: The time of each period cannot be overlapped. Up to 8 periods can be configured for each day.

3. Set the Alarm Actions for Motion Detection. Check the checkbox to select the linkage method. Notify IP Server, Send email, Upload to FTP and Trigger channel are selectable. You can specify the linkage method when an event occurs.

> Notify IP Server:
Send an exception or alarm signal to the remote management software (SCMS) when an event occurs.
> Send Email:
Send an email with alarm information to a user or users when an event occurs.

NOTE: To send the Email when an event occurs, you need to refer to Section 8.3.9 "Email Settings" to set the related parameters.

> Upload to FTP:
Capture the image when an alarm is triggered and upload the picture to an FTP server.

NOTE:
- Set the FTP address and the remote FTP server first. Refer to Section 8.3.7 "FTP" for detailed information.
- Go to the "Storage> Snapshot" page, enable the event-triggered snapshot, and set the capture interval and capture number.
- The captured image can also be uploaded to the available SD card or network disk.

> Trigger Channel:
The video will be recorded when the motion is detected. You have to set the recording schedule to realise this function. Please refer to Section 8.6.1 "Record Schedule" for detailed information.

- Expert Configuration:
Expert mode is mainly used to configure the sensitivity and proportion of the object in relation to the area of each area for each different day/night switch.

> Day/Night Switch: OFF
Steps:
(1) Draw the detection area as in normal configuration mode. Up to 8 areas are supported.
(2) Select "OFF" for the "Switch Day and Night Settings".
(3) Select the area by clicking on the Area No. In the drop-down list under "Area".
(4) Slide the cursor to adjust the sensitivity and proportion of the object in relation to the area for the selected area.
(5) Set the arming schedule and linkage method as in the normal configuration mode.
(6) Click on "Save" to save the settings.

> Day/Night Switch: Auto-Switch
Steps:
(1) Draw the detection area as in normal configuration mode. Up to 8 areas are supported.
(2) Select "Auto-Switch" for the "Switch Day and Night Settings".

(3) Select the area by clicking on the Area No. In the drop-down list under "Area".
(4) Slide the cursor to adjust the sensitivity and proportion of the object in relation to the area for the selected area in daytime under "Day".
(5) Slide the cursor to adjust the sensitivity and proportion of the object in relation to the area for the selected area at nighttime under "Night".
(6) Set the arming schedule and linkage method as in normal configuration mode.
(7) Click on "Save" to save the settings.

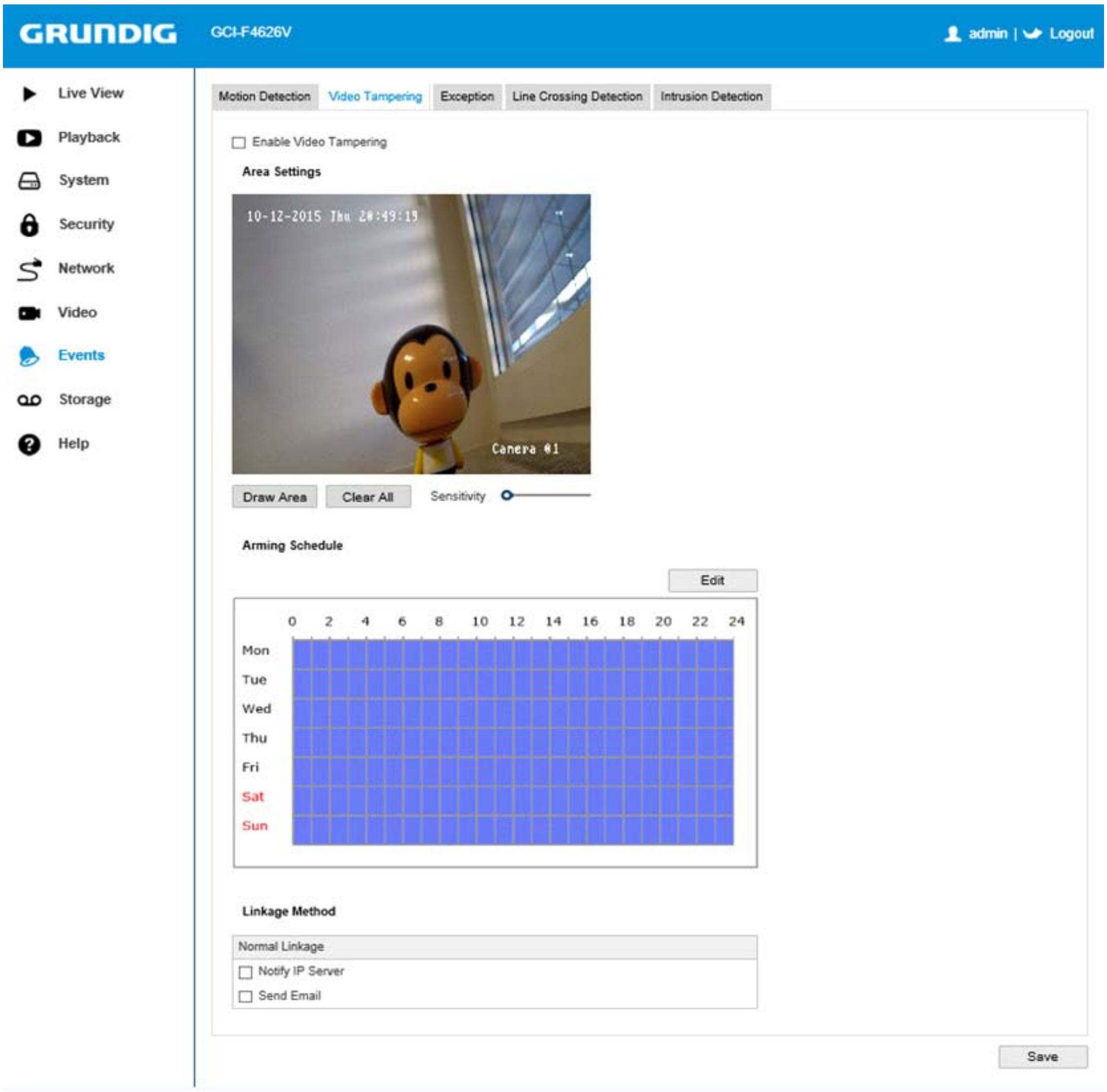
> Day/Night Switch: Scheduled-Switch
(1) Draw the detection area as in normal configuration mode. Up to 8 areas are supported.
(2) Select "Scheduled-Switch" for the "Switch Day and Night Settings".

(3) Select the start time and the end time for the switch timing.
(4) Select the area by clicking on the Area No. In the drop-down list under “Area”.
(5) Slide the cursor to adjust the sensitivity and proportion of the object in relation to the area for the selected area in daytime under “Day”.
(6) Slide the cursor to adjust the sensitivity and proportion of the object in relation to the area for the selected area at nighttime under “Night”.
(7) Set the arming schedule and linkage method as in normal configuration mode.
(8) Click on “Save” to save the settings.

8.5.2. Video Tampering

You can configure the camera to trigger the alarm when the lens is covered and take some certain alarm response actions.

Steps:
1. Enter the Video Tampering Settings interface: Events> Video Tampering



□ Enable Video Tampering

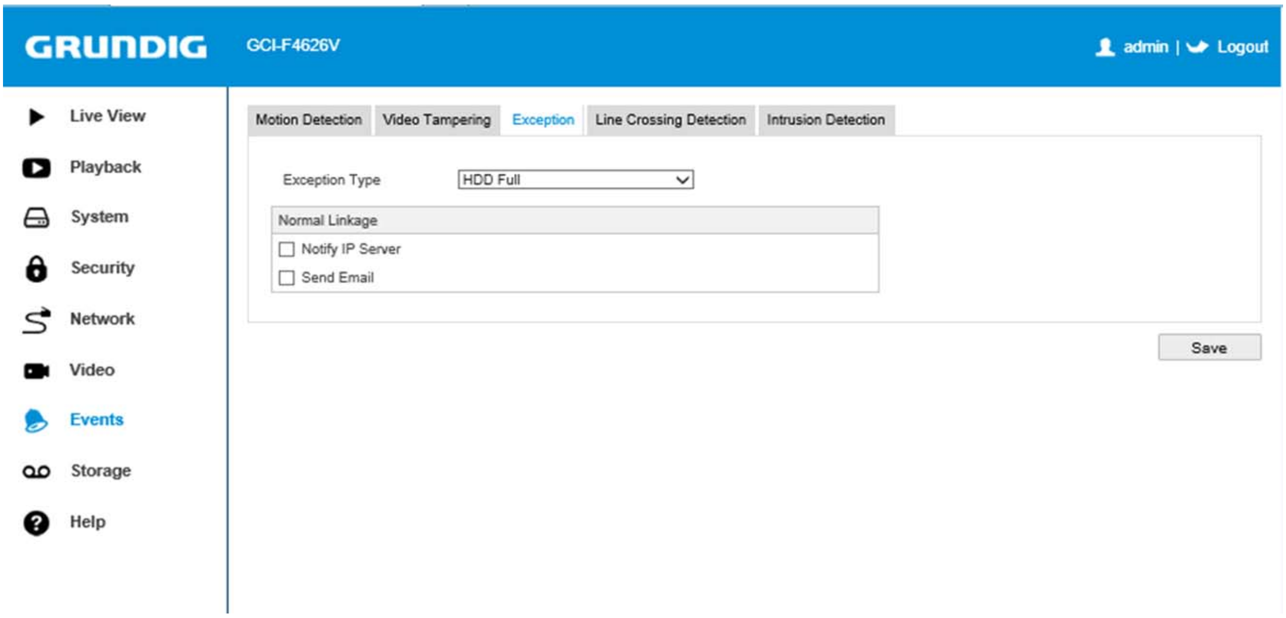
Normal Linkage
□ Notify IP Server
□ Send Email

2. Check the “Enable Video Tampering” checkbox to enable the video tampering detection.
3. Click on “Edit” to edit the arming schedule for the video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to Task 2 (“2. Set the Arming Schedule for Motion Detection.”) in Section 8.5.1 "Motion Detection".
4. Check the checkbox to select the linkage method to be taken for the video tampering. Notify IP Server and Send email are selectable.
5. Click on “Save” to save the settings.

8.5.3. Exception

The exception type can be HDD full, HDD error, Network disconnected, IP address conflicted and Illegal login to the cameras.

Steps:
1. Enter the Exception Settings interface: Events> Exception
2. Check the checkbox to set the actions to be taken for the Exception alarm. Refer to Task 3 ("3. Set the Alarm Actions for Motion Detection.") in Section 8.5.1 "Motion Detection".



Exception Type: HDD Full

Normal Linkage
□ Notify IP Server
□ Send Email

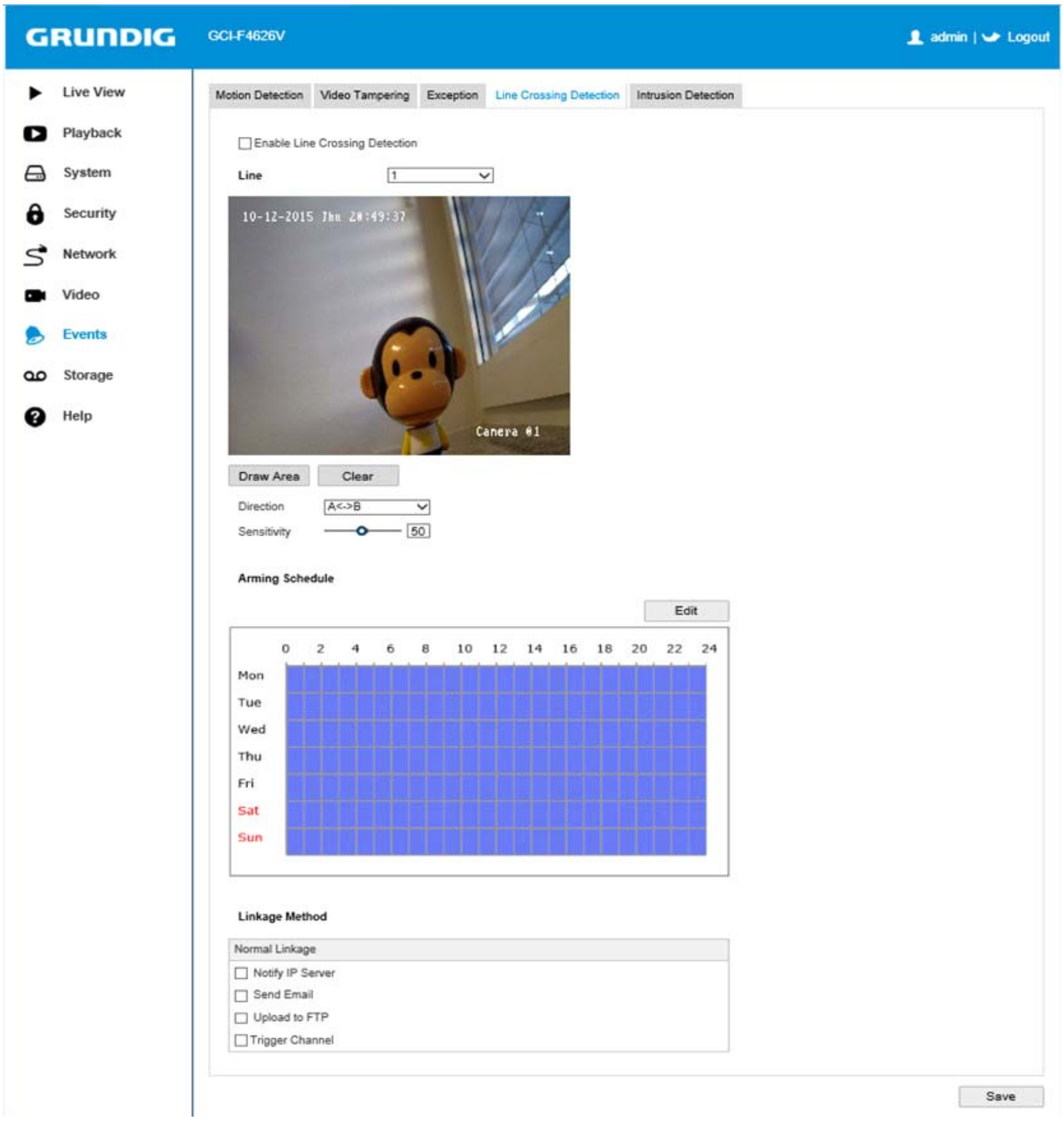
3. Click on "Save" to save the settings.

8.5.4. Line Crossing Detection

The Line crossing detection function detects people, vehicles or other objects which cross a pre-defined virtual line, and certain actions can be taken when the alarm is triggered.

Steps:
1. Enter the Line Crossing Detection settings interface:
Events> Line Crossing Detection
2. Check the checkbox of "Enable Line Crossing Detection" to enable this function.
3. For these camera models, only one line is available.
4. If you click on the "Draw Area" button, a virtual line will be displayed on the live video.
5. If you click-and-drag the line, you can locate it on the live video as desired. If you click on the line, two red squares will be displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
6. Select the direction for the Line crossing detection. You can select the directions as A<->B, A ->B, and B->A.

- A<->B: An object going across the plane with both direction can be detected and the alarms are triggered.
- A->B: Only the object crossing the configured line from the A side to the B side can be detected.
- B->A: Only the object crossing the configured line from the B side to the A side can be detected.



☐ Enable Line Crossing Detection

Line: 1

Direction: A<->B

Sensitivity: 50

Arming Schedule

Linkage Method

Normal Linkage

☐ Notify IP Server

☐ Send Email

☐ Upload to FTP

☐ Trigger Channel

7. Click-and-drag the slider to set the detection sensitivity.
Sensitivity: Range [1-100]. The higher the value is, the more easily the line crossing action can be detected.
8. You can click on the "Clear" button to clear the pre-defined line.
9. Click on the "Edit" button to set the arming schedule.
10. Select the linkage methods for the Line crossing detection, including Notify IP Server, Send Email, Upload to FTP and Trigger Channel
11. Click on "Save" to save the settings.

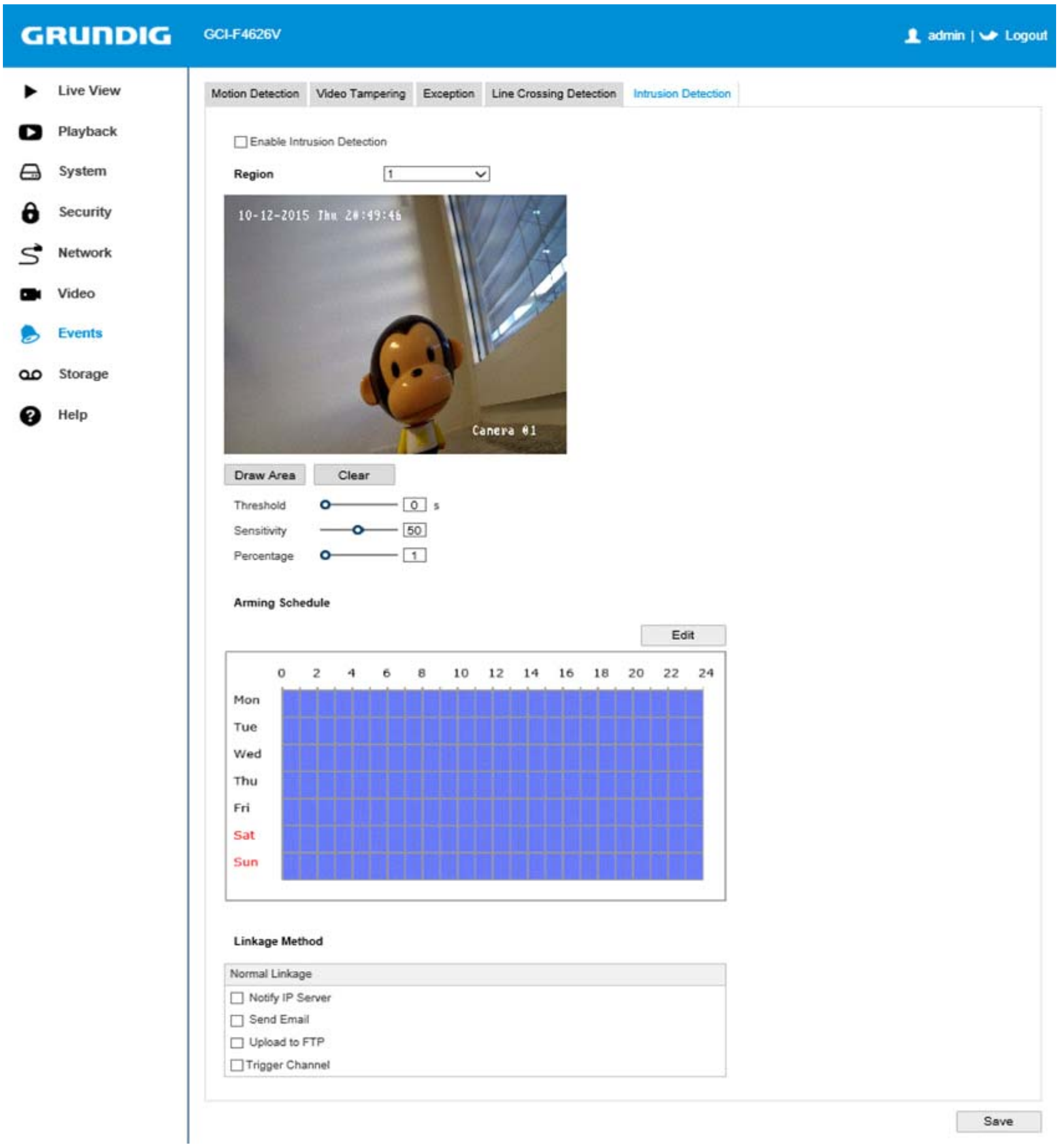
8.5.5. Intrusion Detection

The Intrusion detection function detects people, vehicles or other objects which enter and loiter in a pre-defined virtual region, and certain actions can be taken when the alarm is triggered.

NOTE: The Intrusion detection function varies according to the different camera models.

Steps:
1. Enter the Intrusion Detection settings interface: Events> Intrusion Detection
2. Check the checkbox of "Enable Intrusion Detection" to enable this function.
3. For these camera models, only one region is available.
4. Click on the "Draw Area" button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right-click to complete the drawing.
6. Set the Time threshold, Detection sensitivity and Object percentage for the Intrusion Detection.

- Threshold: Range [0s-10s]. This is the threshold for the time of the object loitering in the region. If you set the value as 0, the alarm will be triggered immediately after the object has entered the region.
- Sensitivity: Range [1-100]. This value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object can trigger the alarm.
- Percentage: Range [1-100]. This Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.



□ Enable Intrusion Detection

Region: 1

Threshold: 0 s

Sensitivity: 50

Percentage: 1

Normal Linkage

□ Notify IP Server

□ Send Email

□ Upload to FTP

□ Trigger Channel

7. You can click on the "Clear" button to clear tha pre-defined region.
8. Click on the "Edit" button to set the arming schedule.
9. Select the linkage methods for Intrusion detection, including Notify IP Server, Send Email, Upload to FTP and Trigger Channel.
10. Click on "Save" to save the settings.

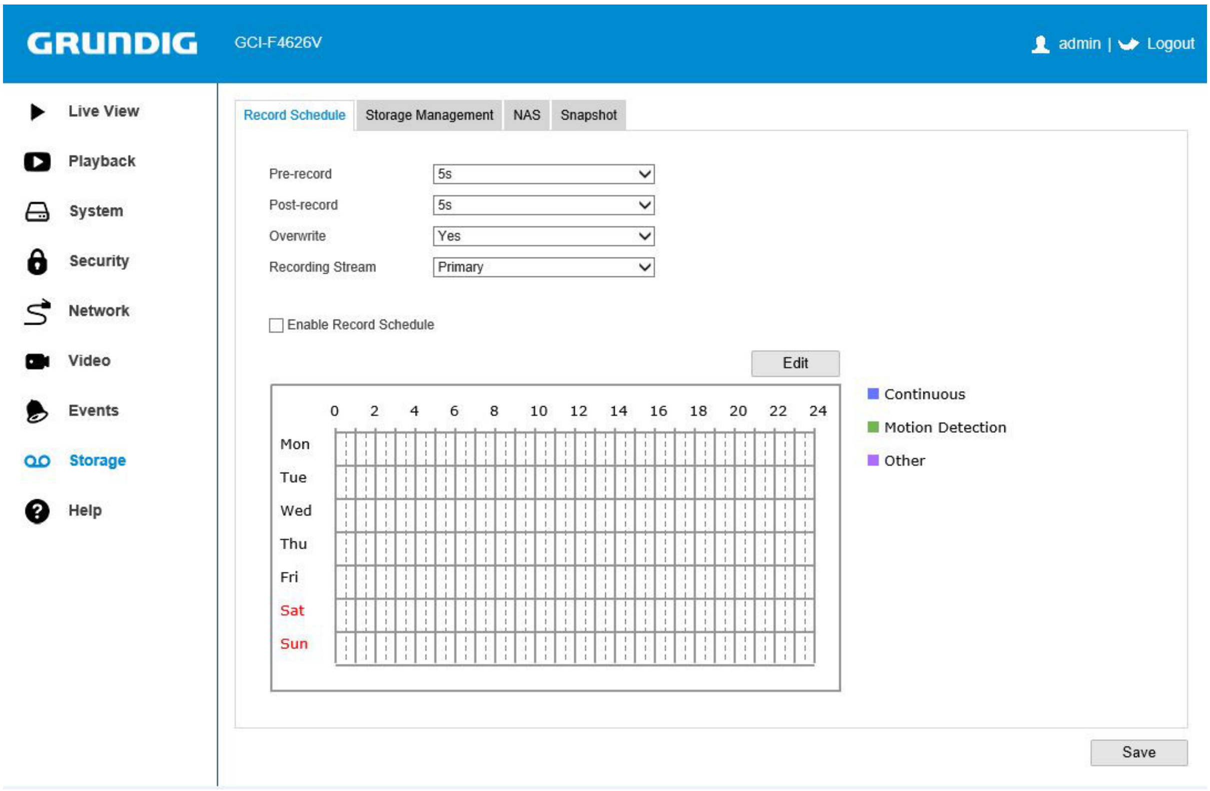
8.6. Storage Settings

Before you start:
To configure the record settings, please make sure that you have the network storage device in the network or the SD card inserted into your camera.

8.6.1. Record Schedule

There are two kinds of recording for the cameras: Manual Recording and Scheduled Recording. For the manual recording, refer to Section 6.3 "Manual Recording & Snapshots". In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of the scheduled recording are stored in the SD card (if supported) or in the network disk.

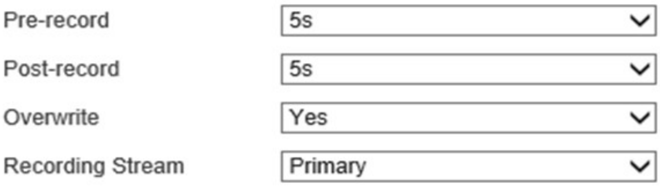
Steps:
1. Enter the Record Schedule Settings interface: Storage> Record Schedule



Pre-record	5s
Post-record	5s
Overwrite	Yes
Recording Stream	Primary

□ Enable Record Schedule

2. Check the checkbox of "Enable Record Schedule" to enable the scheduled recording.
3. Set the record parameters of the camera.

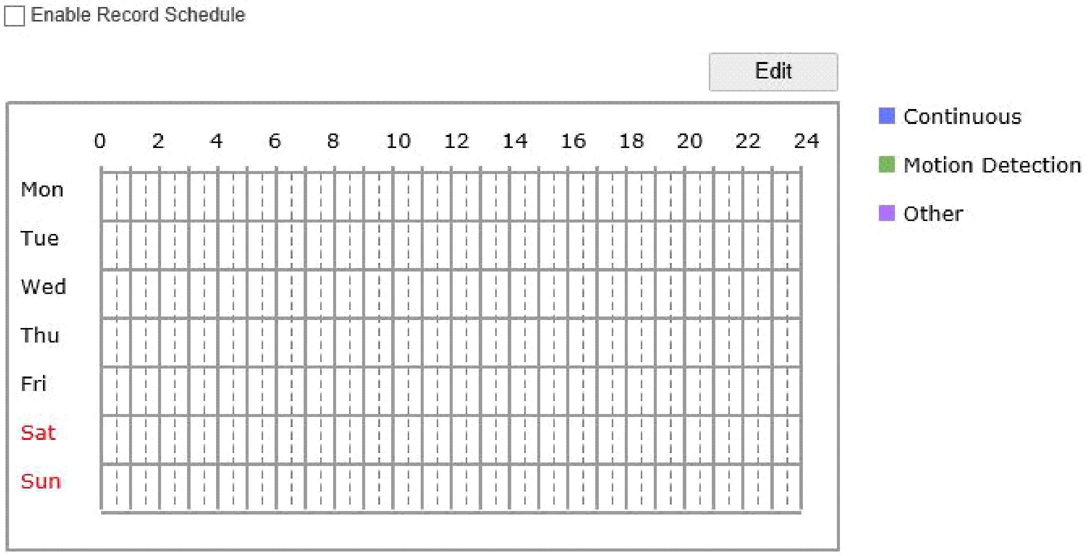


Pre-record	5s
Post-record	5s
Overwrite	Yes
Recording Stream	Primary

- Pre-record: The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers the recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55. The Pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.
- Post-record: The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05. The Post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.

NOTE: The record parameter configurations vary depending on the camera model.

4. Click on "Edit" to edit the record schedule.



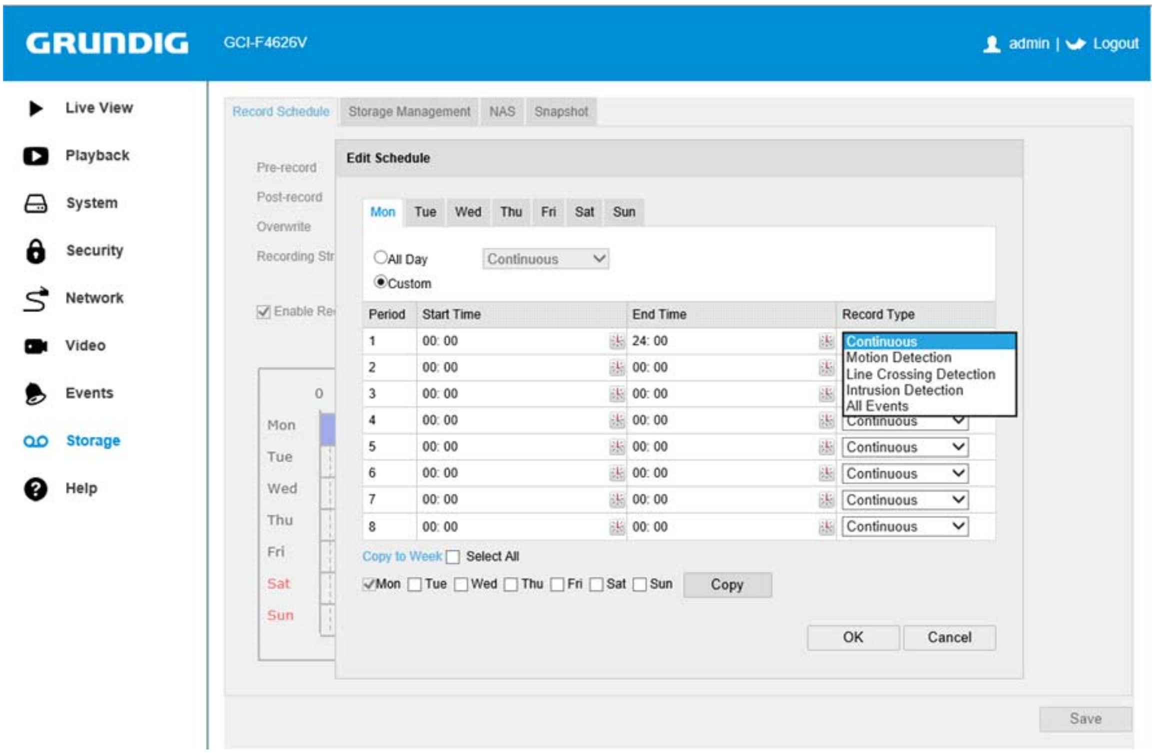
□ Enable Record Schedule

5. Choose the day to set the record schedule.

(1) Set all-day record or segment record:
> If you want to configure the all-day recording, please check the “All Day” checkbox.
> If you want to record in different time sections, check the “Customise” checkbox. Set the “Start Time” and “End Time”.

NOTE: The time of each segment can not be overlapped. Up to 4 segments can be configured.

(2) Select a “Record Type”. The record type can be Continuous, Motion Detection, and others.
> Continuous:
If you select “Continuous”, the video will be recorded automatically according to the time of the schedule.
> Record Triggered by Motion Detection:
If you select “Motion Detection”, the video will be recorded when the motion is detected. Besides configuring the recording schedule, you have to set the motion detection area and check the checkbox of “Trigger Channel” in the “Linkage Method” of the Motion Detection Settings interface. For detailed information, please refer to Task 1 (“1. Set the Motion Detection Area.”) in Section 8.5.1 "Motion Detection".



Edit Schedule

Mon Tue Wed Thu Fri Sat Sun

○All Day Continuous
●Custom

Period	Start Time	End Time	Record Type
1	00: 00	24: 00	Continuous
2	00: 00	00: 00	Motion Detection
3	00: 00	00: 00	Line Crossing Detection
4	00: 00	00: 00	Intrusion Detection All Events Continuous
5	00: 00	00: 00	Continuous
6	00: 00	00: 00	Continuous
7	00: 00	00: 00	Continuous
8	00: 00	00: 00	Continuous

Copy to Week □ Select All
☑Mon □Tue □Wed □Thu □Fri □Sat □Sun Copy

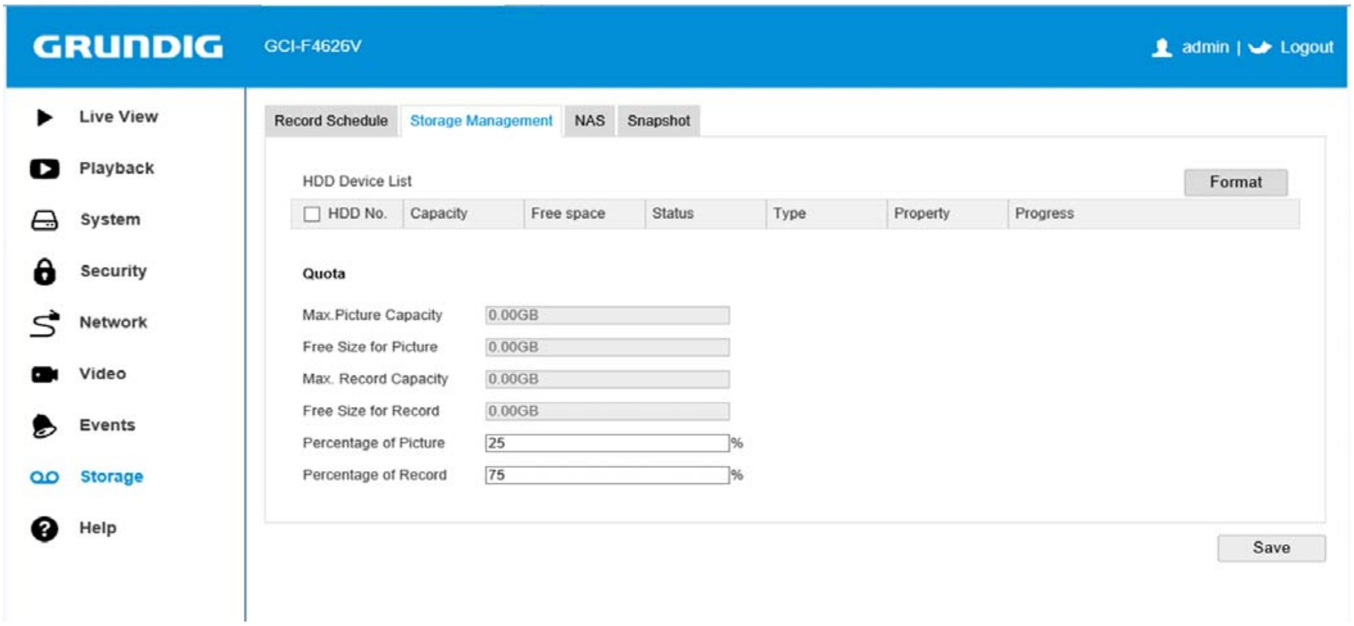
OK Cancel

(3) Check the checkbox of “Select All” and click “Copy” to copy settings of this day to the whole week. You can also check any of the checkboxes before the date and click on “Copy”.
(4) Click on “OK” to save the settings and exit the “Edit Record Schedule” interface.

6. Click on “Save” to save the settings.

8.6.2. Storage Management

Here you can view the Storage Management settings, like the HDD Device List (which includes the capacity, space, status, type and property of the connected HDD) and the Quota settings.



HDD Device List

□ HDD No.	Capacity	Free space	Status	Type	Property	Progress

Quota

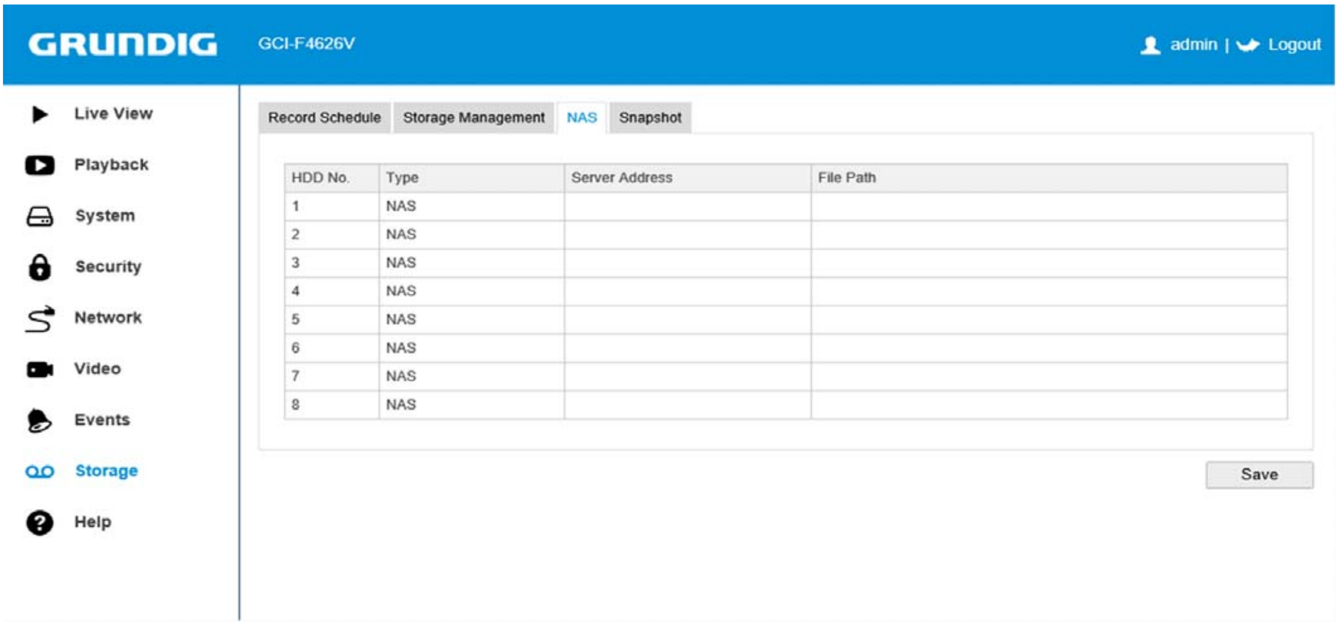
Max.Picture Capacity	0.00GB
Free Size for Picture	0.00GB
Max. Record Capacity	0.00GB
Free Size for Record	0.00GB
Percentage of Picture	25 %
Percentage of Record	75 %

8.6.3. NAS

Before you start:
The network disk should be available within the network and properly configured to store the recorded files, log files, etc.

Steps:
1. To add the network disk:

(1) Enter the NAS (Network-Attached Storage) Settings interface: Storage> NAS



HDD No.	Type	Server Address	File Path
1	NAS		
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

(2) Enter the IP address of the network disk, and enter the file path.
(3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

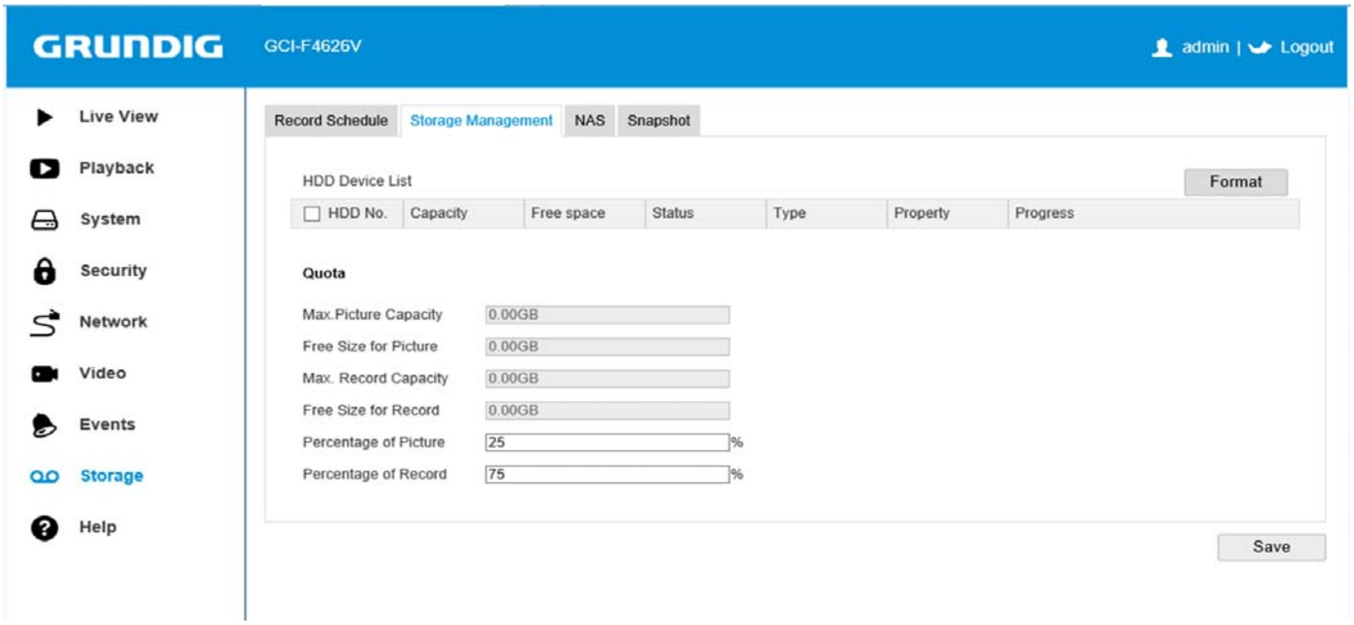
NOTE: Please refer to the User Manual of the NAS for creating the file path.

ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

(4) Click on "Save" to add the network disk.

2. Initialise (=format) the added network disk:

(1) Enter the HDD Settings interface (Storage> Storage Management), in which you can view the capacity, free space, status, type and property of the disk.



HDD Device List

□ HDD No.	Capacity	Free space	Status	Type	Property	Progress

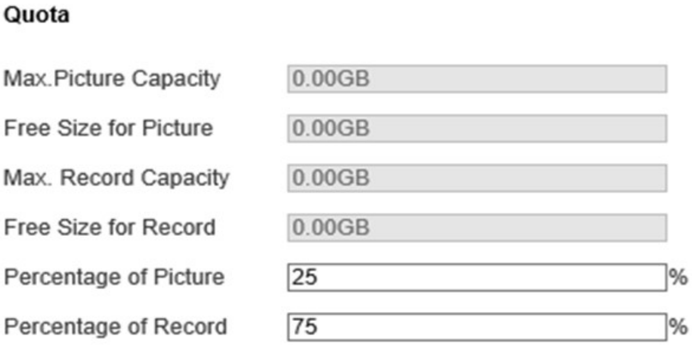
Quota

Max.Picture Capacity 0.00GB
Free Size for Picture 0.00GB
Max. Record Capacity 0.00GB
Free Size for Record 0.00GB
Percentage of Picture 25 %
Percentage of Record 75 %

(2) If the status of the disk is "Uninitialised", check the corresponding checkbox to select the disk and click on "Format" to start formatting the disk. When the formatting is completed, the status of disk will change to "Normal".

3. Define the quota for the recording and the pictures:

(1) Input the quota percentage for the picture and for the recording.
(2) Click on "Save" and refresh the browser page to activate the settings.



Quota

Max.Picture Capacity 0.00GB
Free Size for Picture 0.00GB
Max. Record Capacity 0.00GB
Free Size for Record 0.00GB
Percentage of Picture 25 %
Percentage of Record 75 %

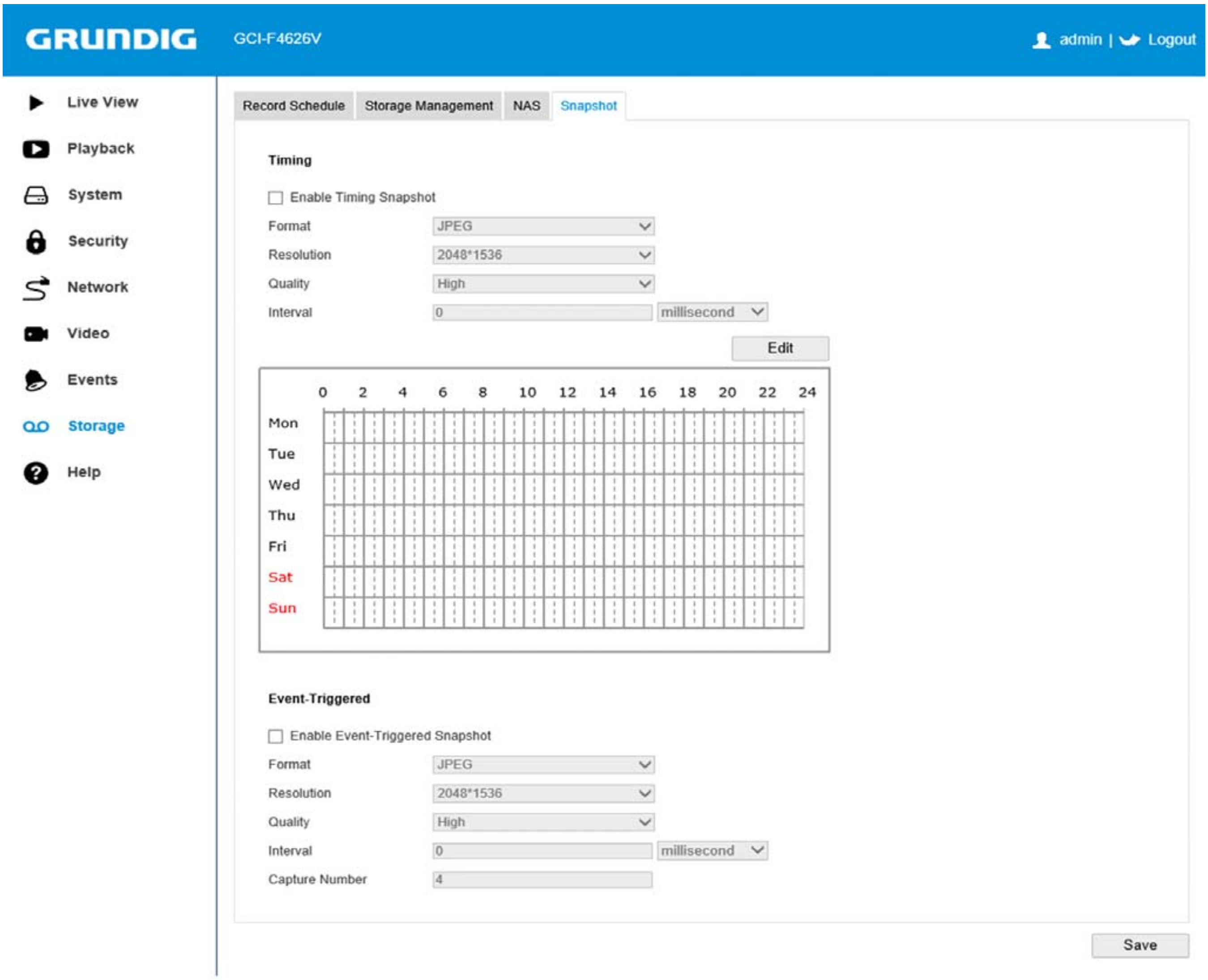
NOTE:
- Up to 8 NAS disks can be connected to the camera.
- To initialise and use the SD card after inserting it into the camera, please refer to the steps regarding the NAS disk formatting.

8.6.4. Snapshot

You can configure the scheduled snapshot and the event-triggered snapshot. The captured picture can be stored on the SD card (if supported) or the netHDD (for detailed information about the netHDD, please refer to Section 8.6.3 "NAS"). You can also upload the captured pictures to a FTP server.

Basic Settings:

Steps:
1. Enter the Snapshot Settings interface: Storage> Snapshot
2. Check the "Enable Timing Snapshot" checkbox to enable the continuous snapshot. Check the "Enable Event-triggered Snapshot" checkbox to check the event-triggered snapshot.
3. Select the quality of the snapshot.
4. Set the time interval between two snapshots.
5. Click on "Save" to save the settings.



Timing

☐ Enable Timing Snapshot

Format	JPEG
Resolution	2048*1536
Quality	High
Interval	0 millisecond

Event-Triggered

☐ Enable Event-Triggered Snapshot

Format	JPEG
Resolution	2048*1536
Quality	High
Interval	0 millisecond
Capture Number	4

Uploading to FTP:

You can follow below the configuration instructions to upload the snapshots to the FTP.

- Upload the continuous snapshots to the FTP:

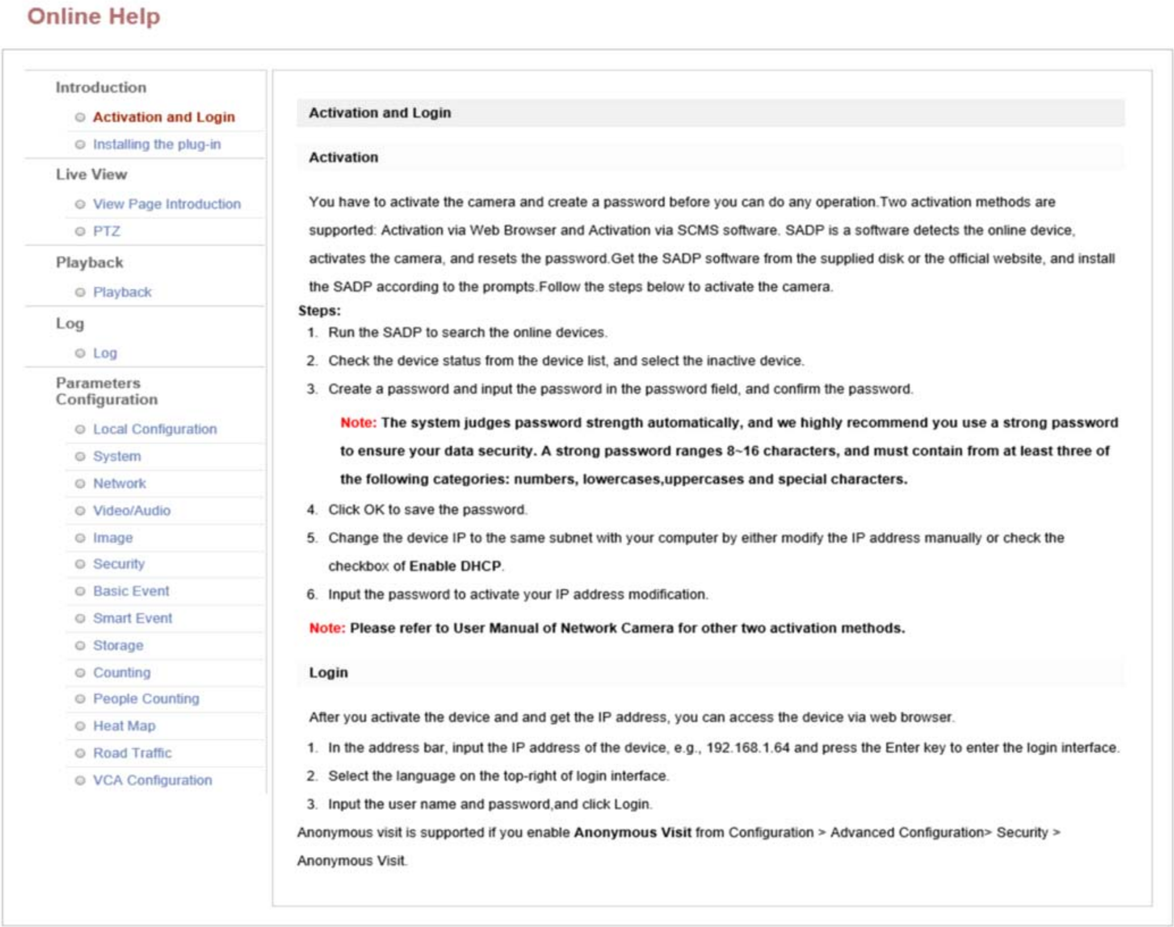
Steps:
1) Configure the FTP settings and check the “Upload Picture” checkbox in FTP Settings interface. Please refer to Section 8.3.7 “FTP” for more details to configure the FTP parameters.
2) Check the “Enable Timing Snapshot” checkbox.

- Upload the event-triggered snapshots to the FTP:

Steps:
1) Configure the FTP settings and check the “Upload Picture” checkbox in FTP Settings interface. Please refer to Section 8.3.7 “FTP” for more details to configure the FTP parameters.
2) Check the “Upload Picture” checkbox in the Motion Detection Settings or the Alarm Input interface. Please refer to Task 3 (“3. Set the Alarm Actions for Motion Detection.”) in Section 8.5.1 "Motion Detection".
3) Check the “Enable Event-triggered Snapshot” checkbox.

9. Help

Here you can view the Online Help. This is a tool that provides additional information and help about the camera and the possible settings.



Activation and Login

Activation

You have to activate the camera and create a password before you can do any operation.Two activation methods are supported: Activation via Web Browser and Activation via SCMS software. SADP is a software detects the online device, activates the camera, and resets the password.Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts.Follow the steps below to activate the camera.

Steps:

1. Run the SADP to search the online devices.
2. Check the device status from the device list, and select the inactive device.
3. Create a password and input the password in the password field, and confirm the password.

   Note: The system judges password strength automatically, and we highly recommend you use a strong password to ensure your data security. A strong password ranges 8~16 characters, and must contain from at least three of the following categories: numbers, lowercases,uppercases and special characters.
4. Click OK to save the password.
5. Change the device IP to the same subnet with your computer by either modify the IP address manually or check the checkbox of **Enable DHCP**.
6. Input the password to activate your IP address modification.

Note: Please refer to User Manual of Network Camera for other two activation methods.

Login

After you activate the device and and get the IP address, you can access the device via web browser.

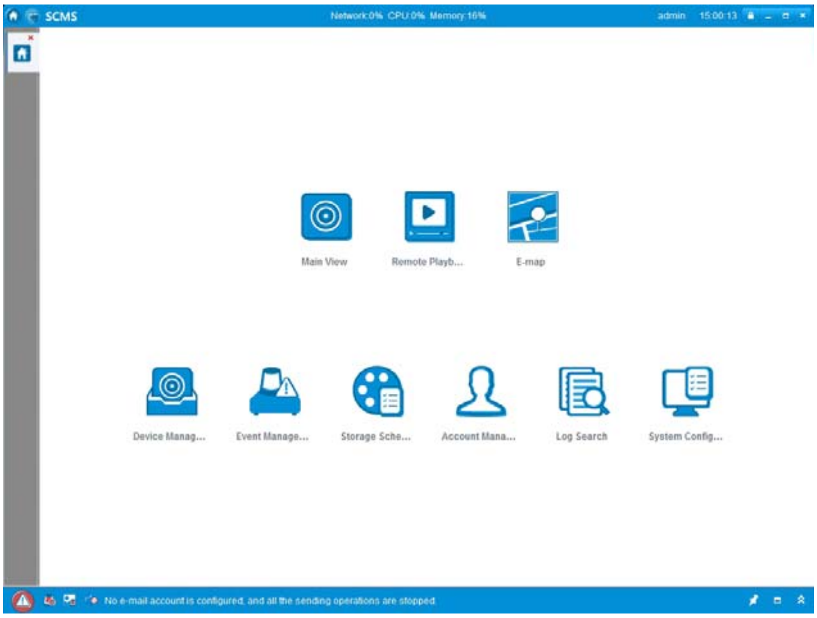
1. In the address bar, input the IP address of the device, e.g., 192.168.1.64 and press the Enter key to enter the login interface.
2. Select the language on the top-right of login interface.
3. Input the user name and password,and click Login.

Anonymous visit is supported if you enable **Anonymous Visit** from Configuration > Advanced Configuration> Security > Anonymous Visit.

10. SCMS Software Introduction

Description of the SCMS:
SCMS (Search Control Management Software) is a user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

You can see the start page / control panel of the SCMS below.



Network:0% CPU:0% Memory:16%

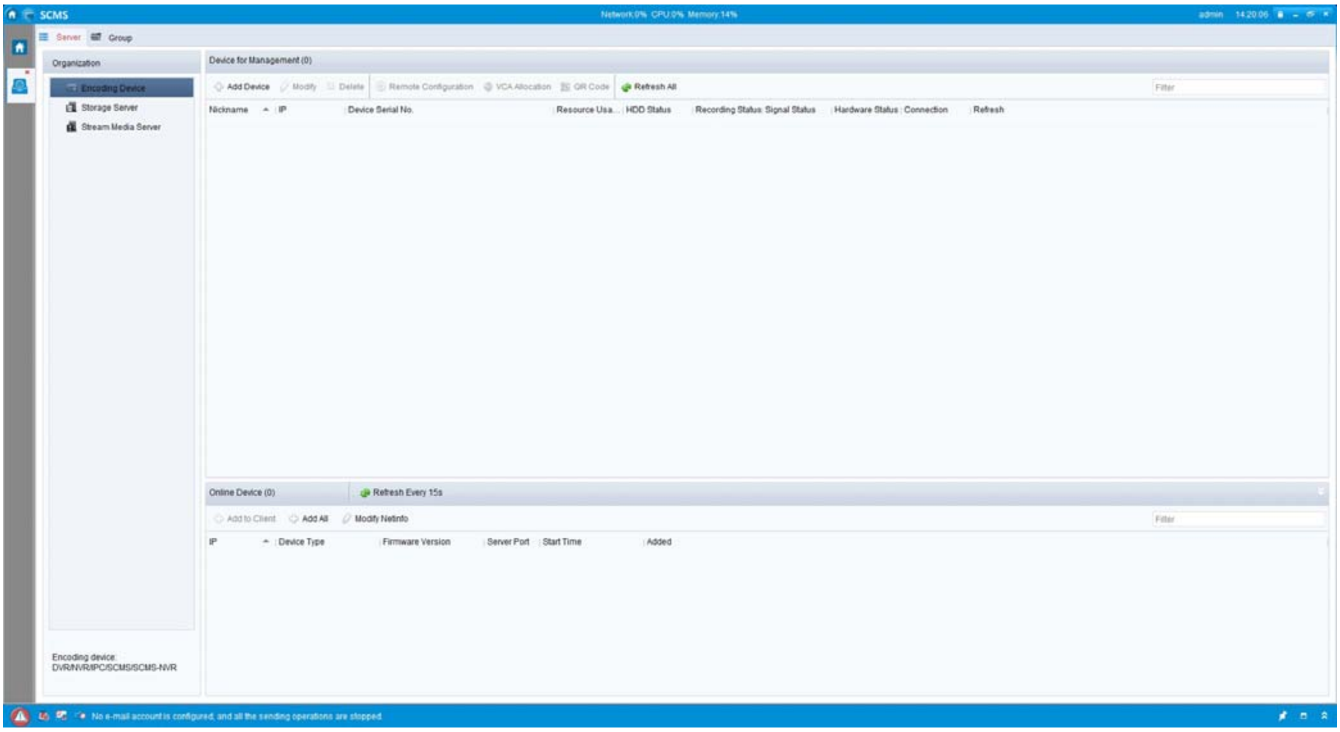
15:00:13

No e-mail account is configured, and all the sending operations are stopped

Search any active devices online:

- Search online devices automatically:

After launching the SCMS software, it automatically searches the online devices every 15 seconds from the subnet where your computer is located. It displays the total number and information of the searched devices in the Online Devices interface. The device information including the device type, IP address and port number, etc. will be displayed.



Nickname	IP	Device Serial No.	Resource Usa...	HDD Status	Recording Status	Signal Status	Hardware Status	Connection	Refresh

IP	Device Type	Firmware Version	Server Port	Start Time	Added

Encoding device:
DVR/NVR/IPC/SCMS/SCMS-NVR

No e-mail account is configured, and all the sending operations are stopped.

NOTE: The device can be searched and displayed in the list 15 seconds after it went online. It will be removed from the list 45 seconds after it went offline.

- Search online devices manually:

You can also click on the "Refresh" button to refresh the online device list manually. The newly searched devices will be added to the list.

NOTE: You can click on "/\" and \/" or in each column heading to order the information; you can click on ">" to expand the device table and hide the network parameter panel on the right side, or click on "<" to show the network parameter panel.

Modify the network parameters:

Steps:
1. Select the device to be modified in the device list and the network parameters of the device will be displayed in the "Modify Network Parameters" panel on the right side.
2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the password of the admin account of the device in the "Password" field and click on "Save" to save the changes.

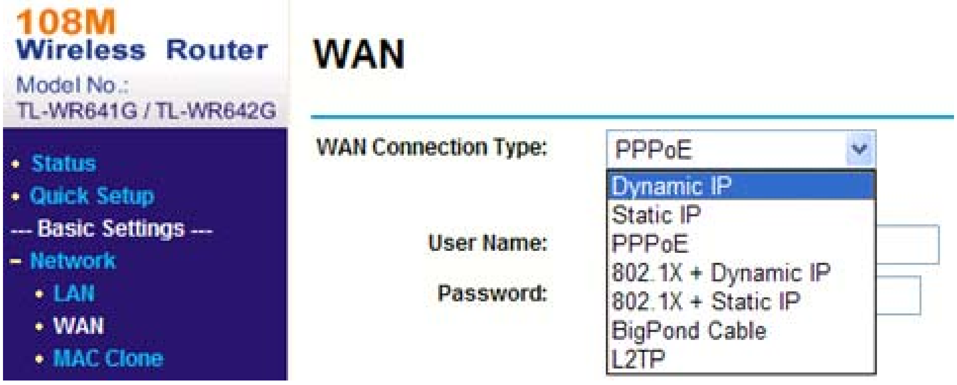
ATTENTION:
- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

11. Port Mapping

The following settings are for the TP-LINK router (TL-WR641G). The settings vary depending on the different models of the routers.

Steps:

1. Select the "WAN Connection Type", as shown below:



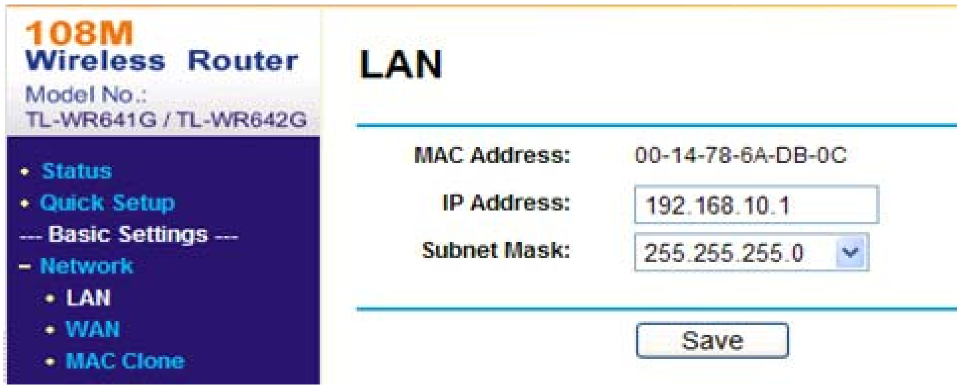
WAN

WAN Connection Type: PPPoE

User Name:

Password:

2. Set the "LAN" parameters of the router as in the following figure, including the IP address and the subnet mask settings.



LAN

MAC Address: 00-14-78-6A-DB-0C

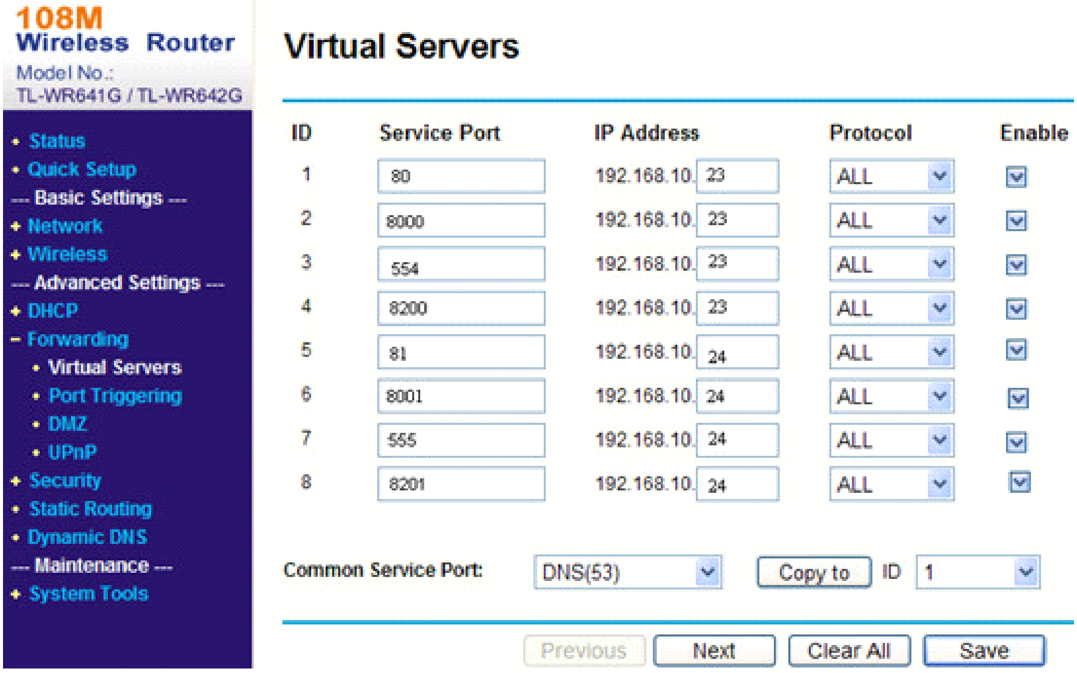
IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

3. Set the port mapping in the virtual severs under "Forwarding". By default, the camera uses port 80, 8000 and 554. You can change these ports value with the web browser or SCMS software.

Example:
When the cameras are connected to the same router, you can set the ports of a camera as 80, 8000, and 554 with the IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with the IP 192.168.1.24. Please refer to the steps below:

Steps:
1. As the settings mentioned above, please map the port 80, 8000, 554 and 8200 for the network camera at 192.168.1.23.
2. Map the port 81, 8001, 555 and 8201 for the network camera at 192.168.1.24.
3. Enable "ALL" or "TCP" protocols.
4. Check the "Enable" checkbox and click on "Save" to save the settings.



Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10. 23	ALL	☑
2	8000	192.168.10. 23	ALL	☑
3	554	192.168.10. 23	ALL	☑
4	8200	192.168.10. 23	ALL	☑
5	81	192.168.10. 24	ALL	☑
6	8001	192.168.10. 24	ALL	☑
7	555	192.168.10. 24	ALL	☑
8	8201	192.168.10. 24	ALL	☑

Common Service Port: DNS(53) Copy to ID 1

NOTE: The port of the network camera cannot conflict with other ports. For example, some web management ports of the router are set to 80. Change the camera port if it is the same as the management port.

Specifications GCI-F4616T

Image Sensor	1/3" Progressive Scan CMOS, 3 Megapixel
Pixels - Total	2048 (H) x 1536 (V)
Sensitivity Colour	0.1 lux @ F2.0 (AGC ON)
Sensitivity B&W	0.01 lux @ F2.0 (AGC ON)
Col/B&W	Auto/Timing/B&W/Color
Lens Focal Length	4.0 mm
Horizontal Viewing Angle	70°
Iris F-Number	F = 2.0
High Speed Shutter	1/3 ~ 1/100.000 sec
IR LED	30 pcs.
Max. IR Distance	15/25 m (according to scene reflexion)
Wavelength	850nm
BLC Back Light	On/ Off/ Area/ Level
WDR	D-WDR (Digital wide dynamic range)
Digital Noise Reduction (DNR)	3D-DNR, auto
Reverse	Mirror, 180°
Video Text Overlay	Text string (28 character), Subtitel (4 lines @ 44 character)
Privacy zones	4 zones, rectangle
Video Compression	H.264, MJPEG
Video Streaming	Dual stream: H.264 + H.264 or H.264 + MJPEG
Video Resolution	Main: 2048x1536 (20fps), 1920x1080 (25fps), 1280x720 (25fps) Sub: 704x576(25fps), 640x480(25fps), 352x288(25fps), 320x240(25fps)
Bit Rate	Mainstream: 32kbps~12288kbps Substream: 32kbps~8192Mbps
Alarm Trigger	Motion detection, Video Tampering, Network disconnect, IP address conflict, Storage exception, Line crossing Detection, Intrusion detection
Network Protocol	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SNMP, IGMP, 802.1x, QoS, IPv4/v6, Bonjour, ONVIF, PSIA, CGI
Interoperability	ONVIF, PSIA, CGI
Web Browser	Internet Explorer 7.0+, Firefox 3.5+, Chrome 8.0+, Safari 5.0+
Security	HTTPS, IP FILTER, IEEE802.1x, Admin/User account
SD memory	supports up to 128 GB capacity of SD/SDHC/SDXC memory
Network Interface	1x 10/100 Base T/TX (RJ-45)
Protection Rating	IP66
Operating Temperature	-30°C ~ +60°C
Humidity	less than 90%, non condensing
Supply Voltage	12 Vdc / PoE (IEEE 802.3af)
Power Consumption	7 W
Weight	0.5 kg
Dimensions (wxhxd)	61 x 77 x 140 mm

Specifications GCI-F4616W

Sensitivity Colour	0.28 lux @ F2.0 (AGC ON)
Sensitivity B&W	0.01 lux @ F2.0 (AGC ON)
Lens Focal Length	2.8 mm
Horizontal Viewing Angle	86°
IR LED	10 pcs.
Max. IR Distance	10 m
Power Consumption	7 W
Weight	0.25 kg
Dimensions (wxhxd)	Ø120 x 55 mm

Specifications GCI-F4626T

Sensitivity Colour	0.1 lux @ F1.4 (AGC ON)
Sensitivity B&W	0.01 lux @ F1.4 (AGC ON)
Lens Focal Length	2.8 ~ 12 mm
Horizontal Viewing Angle	91.2° (Wide) ~ 28.3° (Tele)
Iris F-Number	F= 1.4
IR LED	42 pcs.
Max. IR Distance	30 m
Power Consumption	7.5 W
Weight	1.2 kg
Dimensions (wxhxd)	95 x 105 x 259 mm

Specifications GCI-F4626V

Sensitivity Colour	0.07 lux @ F1.2
Sensitivity B&W	0 Lux LED IR on
Lens Focal Length	2.8 ~ 12 mm
Horizontal Viewing Angle	91.2° (Wide) ~ 28.3° (Tele)
Iris F-Number	F= 1.4
IR LED	24 pcs.
Max. IR Distance	20 m
Power Consumption	7 W
Weight	1 kg
Dimensions (wxhxd)	Ø140 x 100 mm

EC Declaration of Conformity

GCI-F4616T	3 MP Mini Bullet Outdoor Camera with IR LEDs
GCI-F4616W	3 MP Flat Mini Dome with IR LEDs
GCI-F4626T	3 MP Bullet Outdoor Camera with IR LEDs
GCI-F4626V	3 MP Vandal Proof Dome Camera with IR LED

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:

GCI-F4616T & GCI-F4626V:
EN 55022:2010, EN 50130-4:2011,
EN 61000-3-2:2006+A1:2009+A2:2009, EN 61000-3-3:2008

GCI-F4616W & GCI-F4626T:
EN 55022:2010, EN 50130-4:2011,
EN 61000-3-2:2006/A1:2009/A2:2009, EN 61000-3-3:2013

ASP AG
Lüttringhauser Str. 9
42897 Remscheid
Germany

GRUNDIG

Remscheid, 02.03.2016

Ludwig Bergschneider
CEO