



FCS-1131
2-Megapixel PoE Network Camera



User Manual

Ver 1.0

HW Ver: 2.0

Table of Contents

1.	Overview	4
1.1	Features.....	5
1.2	Package Contents	5
1.3	Dimensions.....	6
1.4	Connectors	6
2.	Camera Cabling	7
2.1	Connect Power	7
2.2	Connect Ethernet Cable	7
2.3	Connect Alarm I/O	7
3.	System Requirements	8
4.	Accessing Camera.....	9
4.1	Recording Software	14
4.2	Installing DC Viewer Software Online	15
5.	Operation & Configuration.....	17
5.1	Browser-based Viewer Introduction.....	17
5.2	Home Page	19
5.2.1	Function Items on Home Page.....	19
5.3	System.....	21
5.3.1	System.....	21
5.3.2	Security	23
5.3.2.1	User	23
5.3.2.2	HTTPS	25
5.3.2.3	IP Filter	28
5.3.2.4	IEEE 802.1X.....	29
5.3.3	Network	31
5.3.3.1	Basic	31
5.3.3.2	QoS.....	34
5.3.3.3	SNMP.....	35
5.3.3.4	UPnP.....	37
5.3.3.5	DDNS	39
5.3.3.6	Mail	41
5.3.3.7	FTP.....	42
5.3.3.8	HTTP	43
5.3.3.9	Application	44
5.3.3.10	Motion Detection.....	49

5.3.3.11	Network Failure Detection	55
5.3.3.12	Tampering	57
5.3.3.13	Storage Management (Local Recording).....	61
5.3.3.14	Recording (Local Recording)	63
5.3.3.15	File Location (Snapshots and Web Recording)	64
5.3.3.16	Iris Adjustment (Fixed Focal Lens Excluded)	65
5.3.3.17	View Information	66
5.3.3.17.1	Log File	66
5.3.3.17.2	User Information	67
5.3.3.17.3	Parameters	68
5.3.3.18	Factory Default.....	69
5.3.3.19	Software Version	70
5.3.3.20	Software Upgrade	71
5.3.3.21	Maintenance	73
5.4	Streaming	74
5.4.1	Video Format (Video Resolution and Rotate Type)	74
5.4.2	Video Compression	76
5.4.3	Video ROI	78
5.4.4	Video OCX Protocol.....	80
5.4.5	Video Frame Rate	81
5.4.6	Video Mask	82
5.4.7	Audio (Audio Mode and Bit Rate Settings)	84
5.5	Camera	86
5.5.1	Exposure Setting	87
5.5.2	White Balance Setting.....	89
5.5.3	Picture Adjustment	90
5.3.4	Backlight.....	91
5.3.5	Digital Zoom	91
5.3.6	IR Function	91
5.3.7	WDR Function	91
5.3.8	Noise Reduction	92
5.3.9	TV System Setting.....	92
5.4	Logout	92
Appendix A: Specifications.....		94
Appendix B: Internet Security Settings		96
Appendix C: DC Viewer Download Procedure		99
Appendix D: Install UPnP Components.....		101

Default ID / Password

Login ID	Password
root	

1. Overview

Level1's FCS-1131 is a 2 Megapixel PoE Network Camera, ideal for video surveillance systems where clear images and greater image detail are required. It is the perfect solution for securing areas where high quality identification is needed, such as airports, passport control and casinos.

The FCS-1131 Network Camera delivers HDTV performance in compliance with the SMPTE standard for installations that demand the highest resolution, perfect focus and good color representation. It delivers HDTV 1080p or 720p resolution, 16:9 aspect ratio and supports both H.264 and Motion JPEG. The camera has a built-in slot for an Mirco SD/SDHC card, enabling local storage of several days of recording, without any external equipment.

The integrated BNC connector allows the FCS-1131 to be connected directly to an analog monitor provides enhanced flexibility and usability and ease of installation. Together with PoE, activity adaptive streaming, and the included 64-CH LevelOne IP CamSecure surveillance management software, the FCS-1131 is indisputably the top choice for reliable and high performance surveillance.

1.1 Features

Progressive Scan CMOS Sensor

2M Resolution*

C / CS Mount Lens

Quad Streams support

Dual Streams, Full HD 1080P 13/15fps + D1 real-time

Dual Streams Compression: H.264 Baseline / Main / High Profile + MJPEG

Multi-language support

Tampering Alarm

Wide Dynamic Range

Motion Detection

Privacy Masks

Smart Picture Quality / 3D Noise Reduction

Vertical View Mode (Image rotation by 90 degrees)

Smart IR Mode

Network Failure Detection

Day / Night (ICR)

Auto Iris Lens support

Micro SD support

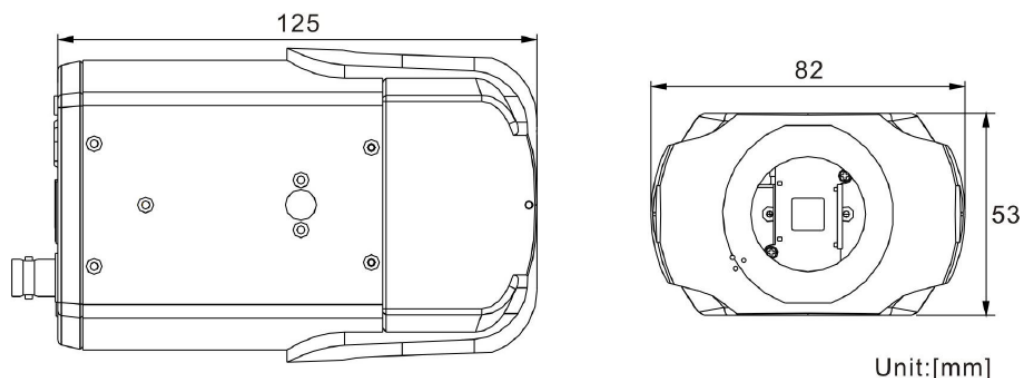
BNC Analog Output

ONVIF Support

1.2 Package Contents

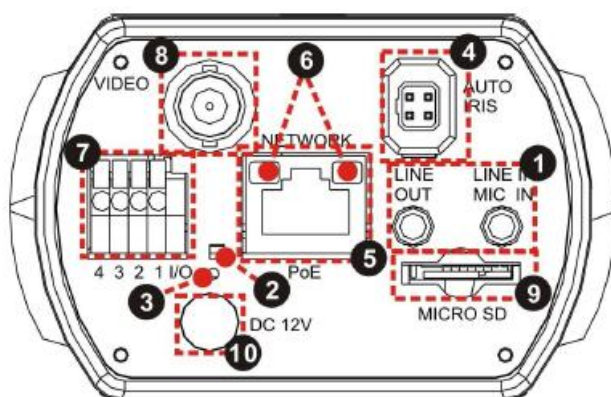
- ✧ FCS-1131
- ✧ Power Adapter
- ✧ Camera Stand
- ✧ Quick Installation Guide
- ✧ CD Manual / Utility

1.3 Dimensions



1.4 Connectors

The diagram below shows the IP Camera's reset button and various connectors. Definition for each connector will be given as follows.



No.	Definition	Remarks
1	LINE OUT & LINE IN	Two-way audio transmission
2	Power LED	Power connection indication (green light)
3	Reset Button	Reset to factory default
4	AUTO IRIS connector	Auto iris lens connector
5	NETWORK (with PoE)	RJ-45 connector
6	NETWORK LEDs	Network connection and activity indication
7	Alarm I/O	Alarm connection
8	VIDEO (BNC)	For video output
9	Micro SD Card slot	For video recording storage
10	DC 12V connector	DC 12V power connection

2. Camera Cabling

Please follow the instructions below to complete IP Camera installation.

2.1 Connect Power

Please refer to Section: Connectors. Alternatively, connect the Ethernet cable to the camera's PoE port and plug the other end of the cable into a PoE switch.



NOTE: If using PoE, make sure Power Sourcing Equipment (PSE) is in use in the network.

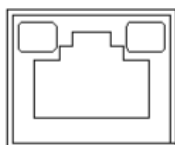
2.2 Connect Ethernet Cable

Use of Category 5 Ethernet cable is recommended for network connection; to have best transmission quality, cable length shall not exceed 100 meters. Connect one end of the Ethernet cable to the RJ-45 connector of the IP Camera, and the other end of the cable to the network switch or PC.



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

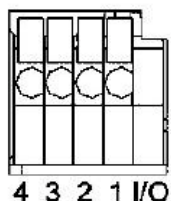
Check the status of the link indicator and activity indicator LEDs; if the LEDs are unlit, please check LAN connection.



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

2.3 Connect Alarm I/O

The camera equips one alarm input and one relay output for alarm application. Refer to alarm pin definition below to connect alarm devices to the IP Camera if needed.



PIN 1: Output+
PIN 2: Output-
PIN 3: Input+
PIN 4: Input-

3. System Requirements

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

Items	System Requirement
Personal Computer	1. Intel® Pentium® M, 2.16 GHz or Intel® Core™2 Duo, 2.0 GHz 2. 2 GB RAM or more
Operating System	Windows VISTA/ Windows XP/ Windows 7
Web Browser	Microsoft Internet Explorer 6.0 or later Firefox Chrome Safari
Network Card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

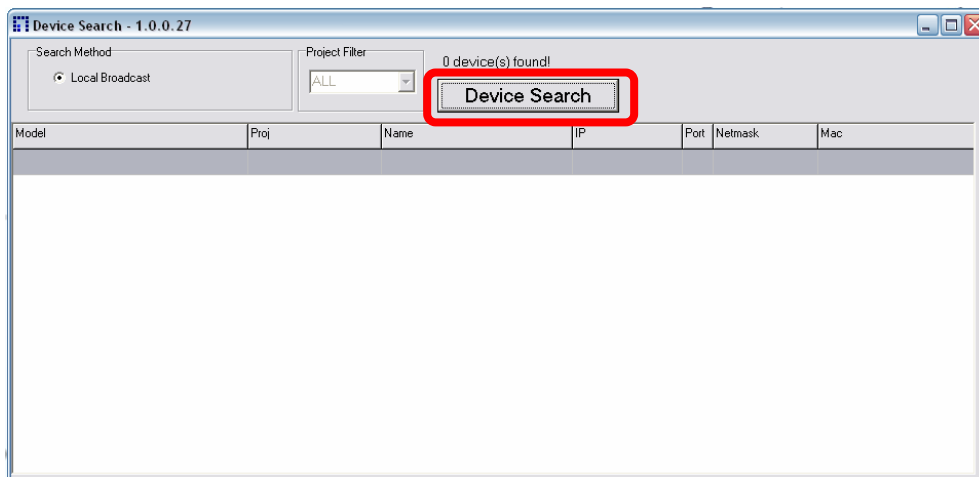
4. Accessing Camera

For initial access to the IP Camera, users can search the camera through the installer program: DeviceSearch.exe, which can be found in “DeviceSearch” folder in the supplied CD.

Device Search Software

Step 1:

Double click on the program Device Search.exe (see the icon below); its window will appear as shown below. Then click the “Device Search” button.



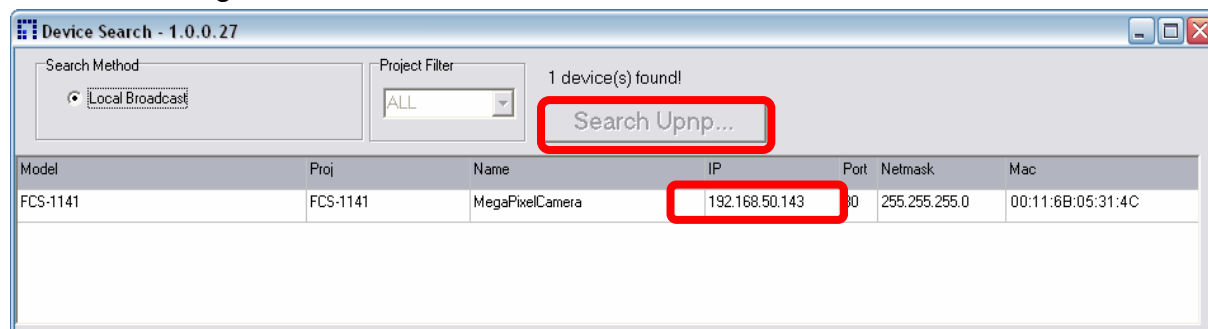
Step 2:

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



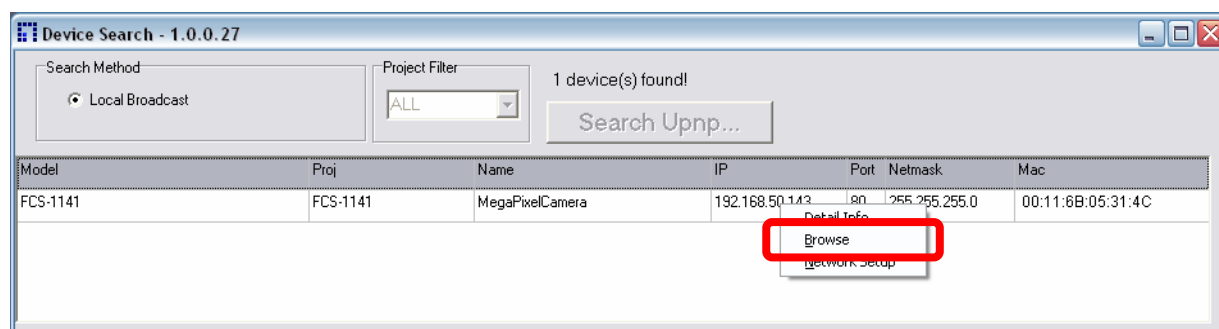
Step 3:

Click “Device Search” again, and all the finding IP devices will be listed in the page, as shown in the figure below. The IP Camera’s default IP address is: 192.168.0.250.



Step 4:

Double click or right click and select “Browse” to access the camera directly via web browser.



Step 5:

Then the prompt window of request for entering default username and password (as shown below) will appear for login to the IP Camera.



The default login ID and password for the Administrator are:

Login ID	Password
root	



NOTE: ID and password are case sensitive.



NOTE: It is strongly advised that administrator's password be altered for the security concerns.

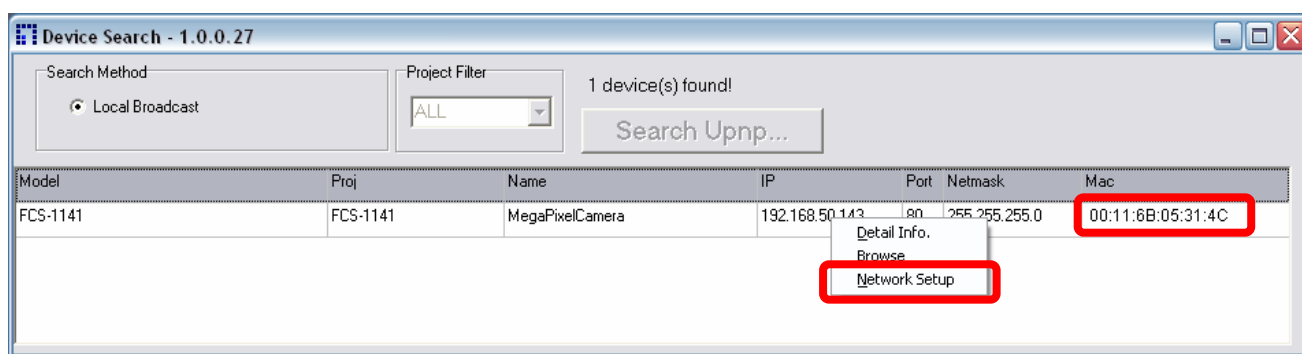
Additionally, users can change the IP Camera's network property, either DHCP or Static IP directly in the device finding list. Refer to the following section for changing the IP Camera's network property.

Example of Changing IP Camera's Network Property

Users can directly change an IP Camera's network property, ex. from static IP to DHCP, in the finding device list. The way to change the IP Camera's network property is specified below:

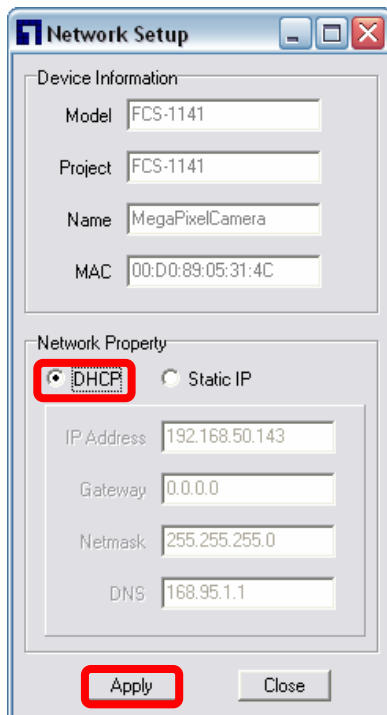
Step 1:

In the finding device list, click on the IP Camera that you would like to change its network property. On the selected item, right click and select "Network Setup." Meanwhile, record the IP Camera's MAC address, for future identification.



Step 2:

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



Network Setup

Device Information

Model: FCS-1141

Project: FCS-1141

Name: MegaPixelCamera

MAC: 00:D0:89:05:31:4C

Network Property

☒ DHCP ☐ Static IP

IP Address: 192.168.50.143

Gateway: 0.0.0.0

Netmask: 255.255.255.0

DNS: 168.95.1.1

Apply Close

Step 3:

Click “OK” on the Note of setting change. Wait for one minute to re-search the IP Camera.



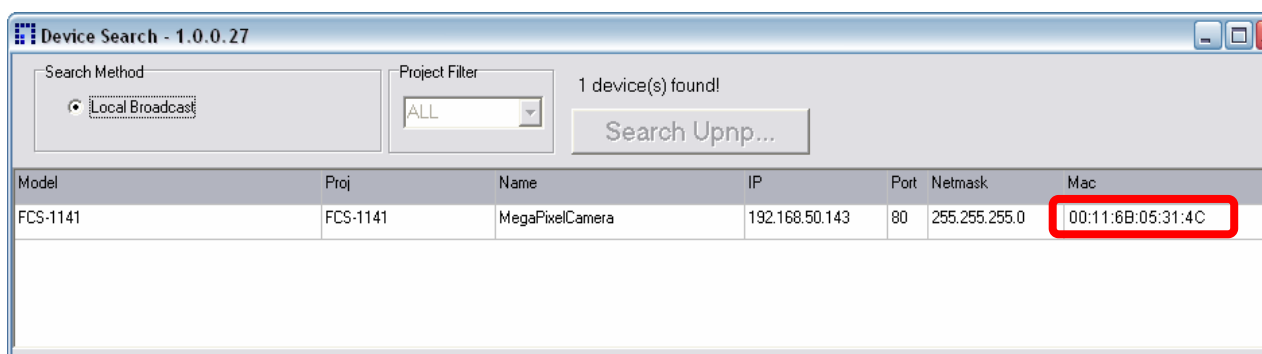
Note

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

確定

Step 4:

Click the “Device Search” button to re-search all the devices. Then select the IP Camera with the correct MAC address. Double click on the IP Camera, and the login window will appear.



Device Search - 1.0.0.27

Search Method: ☒ Local Broadcast

Project Filter: ALL

1 device(s) found!

Search Upnp...

Model	Proj	Name	IP	Port	Netmask	Mac
FCS-1141	FCS-1141	MegaPixelCamera	192.168.50.143	80	255.255.255.0	00:11:6B:05:31:4C

Step 5:

Enter User name and Password to access the IP Camera.



The image shows a login dialog box for a device named "MegapixelIPCamera". The dialog has a blue header bar with a yellow key icon on the left. Below the header, the title "MegapixelIPCamera" is displayed. There are two input fields: "User name:" and "Password:". The "User name:" field contains a small user icon and a dropdown arrow. The "Password:" field is empty. Below the password field is a checkbox labeled "Remember my password", which is currently unchecked. At the bottom of the dialog are two buttons: "OK" and "Cancel".

MegapixelIPCamera

User name:

Password:

☐ Remember my password

OK Cancel

4.1 Recording Software

The product software CD also contains recording software- IP CamSecure, allowing simultaneous monitoring and video recording for multiple network cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use IP CamSecure, please refer to the user's manual of the software or download it at <http://global.level1.com>.



4.2 Installing DC Viewer Software Online

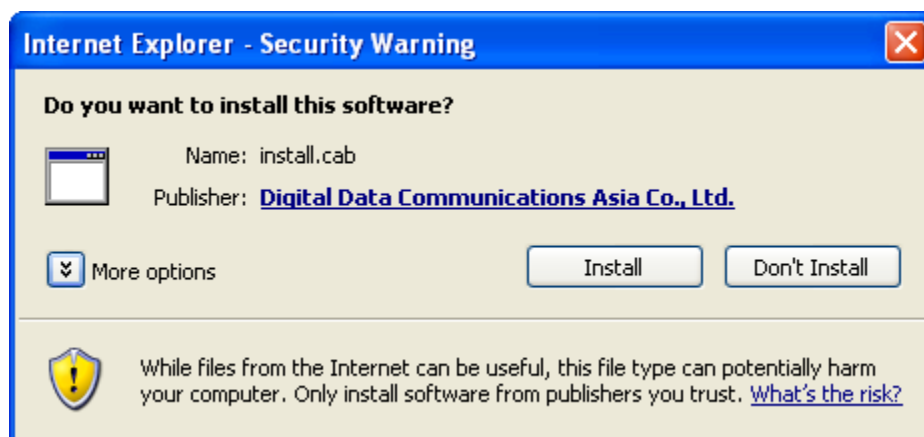
For the initial access to the IP Camera, a client program, DC Viewer, will be automatically installed to your PC when connecting to the IP Camera.

If the Web browser doesn't allow DC Viewer installation, please check the Internet security settings or ActiveX controls and plug-ins settings (see [Appendix B: Internet Security Settings](#)) to continue the process.

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

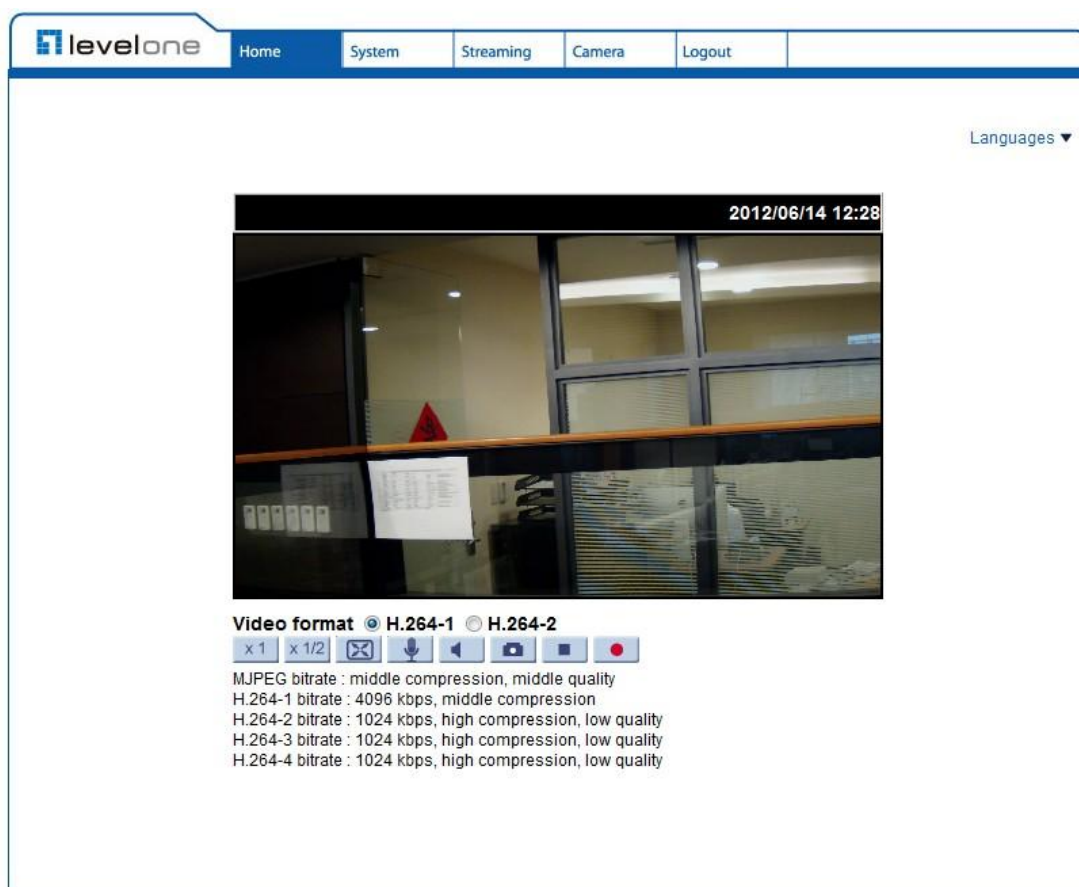


Then the security warning window will pop up. Click "Install" to carry on software installation.



Click "Finish" to close the DC Viewer window when download is finished. For the detailed software download procedure, please refer to [Appendix C: DC Viewer Download Procedure](#).

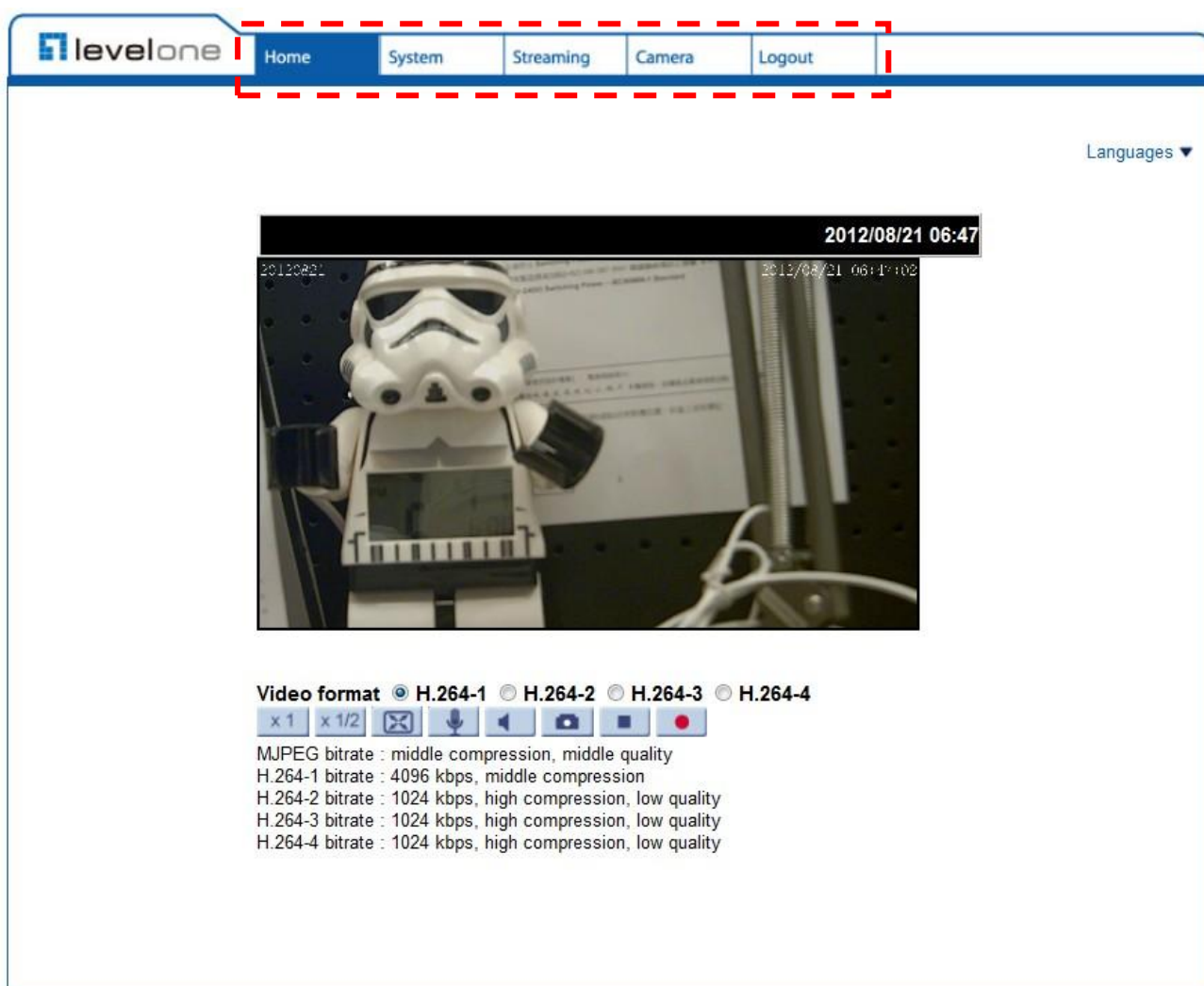
Once login to the IP Camera, users will see the Home page as shown below:



5. Operation & Configuration

The IP Camera is provided with a user-friendly browser-based configuration interface for video playback and recording. In this chapter, information about main page introduction, system related settings and camera settings will be described in detail.

5.1 Browser-based Viewer Introduction



There are five main tabs including <Home>, <System>, <Streaming>, <Camera> and <Logout> on the Home Page.

Home

Users can monitor live video of the targeted area.

System setting

The administrator can set host name, system time, root password, network related settings, etc. Further details will be interpreted in chapter System.

Streaming setting

The administrator can modify video resolution and rotate type and select audio compression mode in this page.

Camera setting

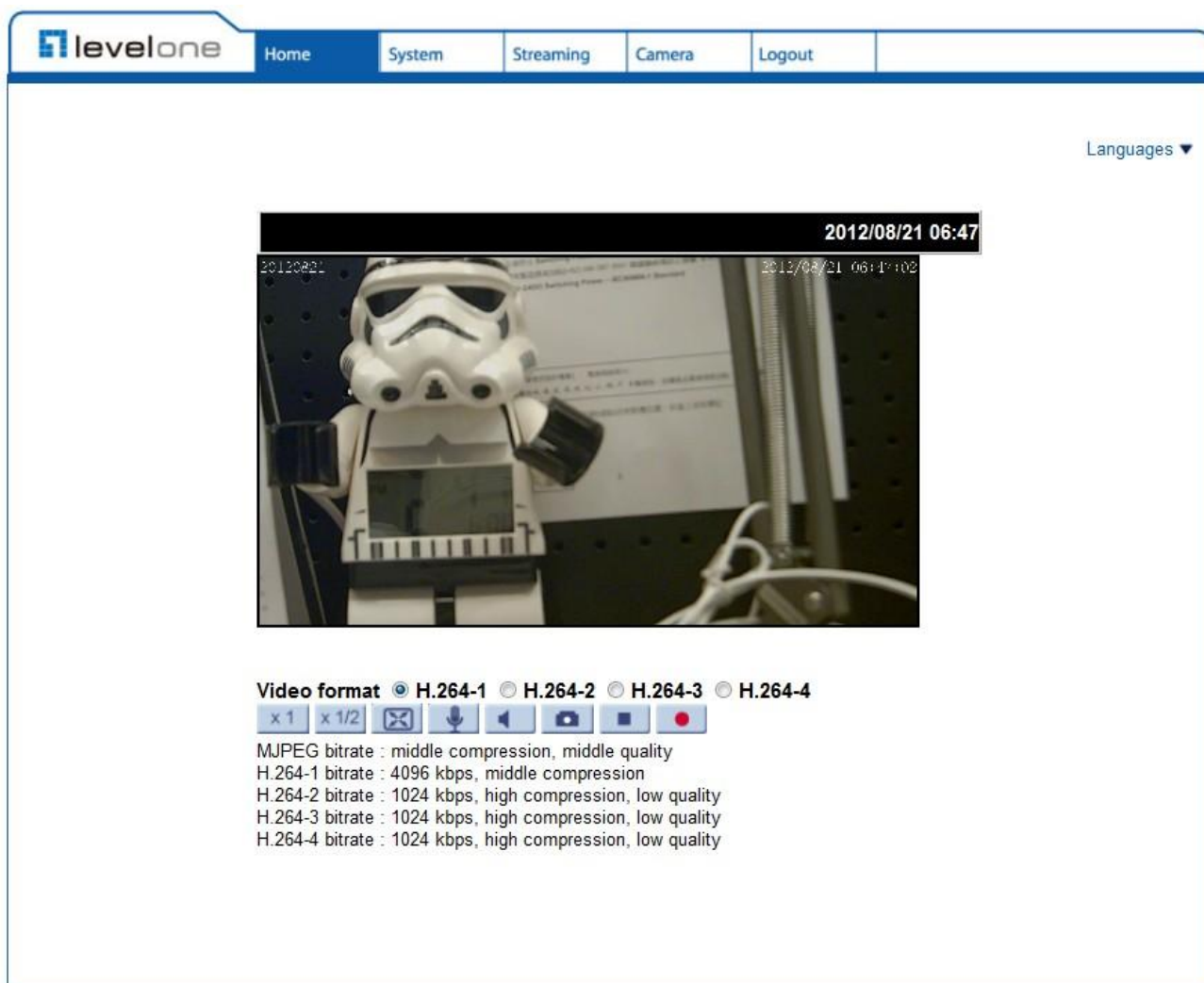
Users can adjust various camera parameters, including <Exposure>, <White Balance>, <Picture Adjustment>, <Backlight>, <Digital Zoom>, <IR Function>, <WDR Function>, <Noise Reduction> and <TV System>.

Logout

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

5.2 Home Page

Click on the tab <Home> to access the Home Page. There are several function buttons on the Home page. Detailed information of each item is as described in the following chapter.



5.2.1 Function Items on Home Page

Multiple Languages Support

Multiple languages are supported, including German, English, French, Italian, Simplified Chinese, Traditional Chinese, Russian for the viewer window interface.

Digital Zoom Control

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

Screen Size Adjustment

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

Talk button (on/off)

Talk function allows the local site to talk to the remote site. Click on the button to switch it to on/off. Please refer to [Security: Add user > Talk/Listen](#) for further details. This function is only open to “User” who has been granted this privilege by the Administrator.

Speaker button (on/off)

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



NOTE: This function is only available for User who has granted this privilege by the Administrator.

Snapshot button

Click on the button and the JPEG snapshots will automatically be saved in the appointed place. The default place of saving snapshots is: C:\. To change the storage location, please refer to [File Location](#) for further details.



NOTE: For users with Windows 7 operating system, it is required to log on as an Administrator to implement the Snapshot function.

Video Streaming Pause /Restart button (pause/restart)

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

Web Recording button (on/off)

Click on the <Recording> button and the Live View through the web browsing will be directly recorded to the specific location on the local hard drive, which could be configured in the <File Location> page. The default storage location for the web recording is: C:\. Please refer to [File Location](#) for further details.



NOTE: For users with Windows 7 operating system, it is required to log on as an Administrator to implement the Web Recording function.

5.3 System

Under the tab <System>, there are submenus including: <System>, <Security>, <Network>, <DDNS>, <Mail>, <FTP>, <HTTP>, <Application>, <Motion Detection>, <Network Failure Detection>, <Tampering>, <Storage Management>, <Recording>, <File Location>, <Iris Adjustment>, <View Information>, <Factory Default>, <Software Version>, <Software Upgrade>, and <Maintenance>.



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

5.3.1 System

The System Setting can be found under the path: System> System.

levelone Home System Streaming Camera Logout

System

Host Name : MegaPixelCamera

Time zone : GMT+00:00 Gambia, Liberia, Morocco, England

☐ Enable daylight saving time

time offset: 01:00:00

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

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

☐ Sync with computer time

PC date: 2012/08/21 [yyyy/mm/dd]

PC time: 14:54:07 [hh:mm:ss]

☒ Manual

Date: 2010/04/01 [yyyy/mm/dd]

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

☐ Sync with NTP server

NTP server: 0.0.0.0 [host name or IP address]

Update interval: Every hour

Save

Host Name

The name is for camera identification. If alarm function (refer to [Application](#)) is enabled and is set to send alarm message by Mail/FTP, the host name entered here will display in the alarm message. The maximum length of the Host Name is 30 characters.

Time Zone

Select the time zone you are in from the drop-down menu.

Enable Daylight Saving Time

To enable DST, please check the item and then specify time offset and DST duration. The format for time offset is [hh:mm:ss]; for instance, if the amount of time offset is one hour, please enter "01:00:00" into the field.

Sync With Computer Time

Select the item, and video date and time display will synchronize with the PC's.

Manual

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

Sync with NTP server

Network Time Protocol (NTP) is an alternate way to synchronize your camera's clock with a NTP server. Please specify the server you wish to synchronize in the enter field. Then select an update interval from the drop-down menu. For further information about NTP, please refer to the web site: www.ntp.org.

5.3.2 Security

The Security setting can be found under this path: System> Security.

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

5.3.2.1 User

The User setting can be found under this path: System> Security> User.

The screenshot displays the LevelOne web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various system settings, with 'Security' expanded to show 'User', 'HTTPS', 'IP filter', and 'IEEE 802.1X'. The main content area is titled 'Security' and contains three sections: 'Admin Password' with input fields for 'Admin password' and 'Confirm password' (both masked with dots) and a 'Save' button; 'Add User' with input fields for 'User name' and 'User password', checkboxes for 'I/O access', 'Camera control', 'Talk', and 'Listen', and an 'Add' button; and 'Manage User' with a dropdown menu showing '-- no user --' and 'Delete' and 'Edit' buttons.

Admin Password

Change the administrator's password by inputting the new password in "Admin password" and "Confirm password" text boxes. The input characters/numbers will be displayed as dots for security purposes. After clicking on <Save>, the web browser will ask the Administrator for the new password for accessing. The maximum length of the password is 14 characters.



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

Add user

Type the new user's name and password and click on <Add> to add the new user. User name can be up to 16 characters, and the maximum length of the password is 14 characters. The new user will be displayed in the user name list. There is a maximum of twenty user accounts. Each user can be assigned the privileges of “Camera control”, “Talk” and “Listen”.

◆ **I/O access**

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

◆ **Camera control**

This item allows the appointed User to change camera parameters on the Camera Setting page.

◆ **Talk/Listen**

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

Manage User

◆ **Delete user**

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

◆ **Edit user**

Pull down the user list and select a user name. Click on <Edit> to edit the user's password and privilege.



NOTE: It is required to enter the User password as well as check the function items which will be available for the user. When finished, click on <Save> to modify the account authority.

5.3.2.2 HTTPS

The HTTPS setting can be found under this path: System> Security> HTTPS.

The screenshot shows the LevelOne web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various system settings, with 'Security' expanded to show 'User', 'HTTPS', 'IP filter', and 'IEEE 802.1X'. The main content area is titled 'HTTPS' and contains sections for 'Create self-signed certificate', 'Install signed certificate', and 'Created Request'. The 'Create self-signed certificate' section has a 'Create' button. The 'Install signed certificate' section has a 'Create Certificate Request' button and an 'Upload signed certificate' section with a file input and an 'Upload' button. The 'Created Request' section shows a table with one row: 'Subject' with the value 'No certificate request created.' and buttons for 'Properties' and 'Remove'. The 'Installed Certificate' section shows a table with one row: 'Subject' with the value 'No certificate installed.' and buttons for 'Properties' and 'Remove'.

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

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

Create Self-signed Certificate

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

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



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

Install Signed Certificate

Click on the <Create Certificate Request> button to create and submit a certificate request in order to obtain a signed certificate from CA.

Provide the request information in the create dialog. Please refer to the following [Provide the Certificate Information](#) for more details.

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

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

Provide the Certificate Information

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

	Create Self Signed Certificate	Create Certificate Request
Country	√	√
State or Province	√	√
Locality	√	√
Organization	√	√
Organizational Unit	√	√
Common Name	√	√
Valid Day	√	-

◆ **Country**

Enter a 2-letter combination code to indicate the country the certificate will be used in. For instance, type in “US” to indicate United States.

◆ **State or province**

Enter the local administrative region.

◆ **Locality**

Enter other geographical information.

◆ **Organization**

Enter the name of the organization to which the entity identified in “Common Name” belongs.

◆ **Organization Unit**

Enter the name of the organizational unit to which the entity identified in “Common Name” belongs.

◆ **Common Name**

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

◆ **Valid days**

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

Click on <OK> to save the Certificate Information after complete.

5.3.2.3 IP Filter

The IP Filter setting can be found under this path: System> Security> IP Filter.

The screenshot shows the LevelOne web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various system settings: System, Security (expanded), User, HTTPS, IP filter, IEEE 802.1X, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, and View information. The main content area is titled 'IP Filter' and contains the following elements:

- An unchecked checkbox labeled 'Enable IP filter'.
- A dropdown menu set to 'Deny' followed by the text 'the following IP addresses' and an 'Apply' button.
- A section titled 'Filtered IP Addresses' containing an empty list box.
- A 'Delete' button positioned to the right of the list box.
- An input field containing '0.0.0.0' and an 'Add' button.

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

◆ Enable IP Filter

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

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

◆ Add/ Delete IP Address

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

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

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

5.3.2.4 IEEE 802.1X

The IEEE 802.1X setting can be found under this path: System> Security> IEEE 802.1X.

The screenshot shows the 'levelone' web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar menu is expanded to 'Security', which includes 'User', 'HTTPS', 'IP filter', and 'IEEE 802.1X'. The 'IEEE 802.1X' option is selected, displaying the 'IEEE 802.1X/EAP-TLS' configuration page. This page has three main sections: 'CA certificate' with a file upload field and an 'Upload' button; 'Client certificate' with a file upload field and an 'Upload' button; and 'Private key' with a file upload field and an 'Upload' button. Below these is a 'Settings' section containing an 'Identity' field with the value 'admin', a 'Private key password' field with masked characters, and a checkbox labeled 'Enable IEEE 802.1X'. A 'Save' button is located at the bottom right of the settings section.

The IP Camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN).

Users need to contact with the network administrator for gaining certificates, user IDs and passwords

CA Certificate

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

Client Certificate/ Private Key

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

Settings

◆ Identity

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

◆ Private Key Password

Enter the password (maximum 16 characters) for your user identity.

Enable IEEE 802.1X

Check the box to enable IEEE 802.1X.

Click on <Save> to save the IEEE 802.1X/ EAP- TLS setting.

5.3.3 Network

The Network setting can be found under this path: System> Network.

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

5.3.3.1 Basic

The Basic setting can be found under this path: System> Network> Basic.

The screenshot shows the LevelOne web interface for Network configuration. The left sidebar contains a menu with categories: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, and View information. The 'Network' category is expanded, showing sub-items: Basic, QoS, SNMP, and UPnP. The 'Basic' sub-item is selected. The main content area is titled 'Network' and contains three sections: 'General', 'Advanced', and 'IPv6 Address Configuration'. The 'General' section has two radio buttons: 'Get IP address automatically' (selected) and 'Use fixed IP address'. Below these are input fields for IP address (192.168.50.116), Subnet mask (255.255.255.0), Default gateway (192.168.50.1), Primary DNS (0.0.0.0), and Secondary DNS (0.0.0.0). The 'Use PPPoE' radio button is also present, with input fields for User name and Password, and a 'Save' button. The 'Advanced' section has input fields for Web Server port (80), RTSP port (554), MJPEG over HTTP port (8008), and HTTPS port (443), with a 'Save' button. The 'IPv6 Address Configuration' section has a checkbox for 'Enable IPv6' and an 'Address' input field with a 'Save' button.

Category	Sub-category	Setting	Value
Network	General	Get IP address automatically	<input checked="" type="radio"/>
		Use fixed IP address	<input type="radio"/>
		IP address	192.168.50.116
		Subnet mask	255.255.255.0
		Default gateway	192.168.50.1
	General	Primary DNS	0.0.0.0
		Secondary DNS	0.0.0.0
	General	Use PPPoE	<input type="radio"/>
		User name	
	Advanced	Web Server port	80
RTSP port		554	
MJPEG over HTTP port		8008	
HTTPS port		443	
IPv6 Address Configuration	Enable IPv6	<input type="checkbox"/>	
	Address		

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

General

◆ **Get IP address automatically (DHCP)**

The camera's default setting is <Use fixed IP address>.

If select <Get IP address automatically>, after the IP Camera restarts, users can search it through the installer program: DeviceSearch.exe, which can be found in "DeviceSearch" folder in the supplied CD.



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

◆ **Use fixed IP address**

To setup static IP address, select <Use fixed IP address> and move the cursor to the IP address blank and insert the new IP address, ex. 192.168.7.123; then go to the Default gateway (explained later) blank and change the setting, ex. 192.168.7.254. Click on <Save> to confirm the new setting.

When using static IP address to login to the IP Camera, users can access it either through "DeviceSearch" software or input the IP address in the URL bar and click on <Enter>.

IP address

This is necessary for network identification.

Subnet mask

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

Default gateway

This is the gateway used to forward frames to destinations in different subnet. Invalid gateway setting will fail the transmission to destinations in different subnet.

Primary DNS

Primary DNS is the primary domain name server that translates hostnames into IP addresses.

Secondary DNS

Secondary DNS is a secondary domain name server that backups the primary DNS.

Use PPPoE

For the PPPoE users, enter the PPPoE Username and Password into the fields, and click on the <Save> button to complete the setting.

Advanced

◆ Web Server port

The default web server port is 80. Once the port is changed, the user must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the IP Camera whose IP address is 192.168.0.100 from 80 to 8080, the user must type in the web browser “http://192.168.0.100:8080” instead of “http://192.168.0.100”.

◆ RTSP port

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

◆ MJPEG over HTTP port

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

◆ HTTPS port

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



NOTE: Be aware to choose the different port from the one set for the web server port.

IPv6 Address Configuration

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

5.3.3.2 QoS

The QoS (Quality of Service) setting can be found under this path: System> Network> QoS.

The screenshot shows the 'levelone' web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar menu is expanded to 'Network', which includes 'Basic', 'QoS', 'SNMP', and 'UPnP'. The 'QoS' page is displayed, featuring a 'DSCP Settings' section with three input fields: 'Video DSCP' (0), 'Audio DSCP' (0), and 'Management DSCP' (0). A 'Save' button is located below these fields.

QoS allows providing differentiated service levels for different types of traffic packets, which guarantees delivery of priority services especially when network congestion occurs. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Codepoint) values, and thus receive the corresponding forwarding treatment from DiffServ capable routers.

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled. The IP Camera uses the following QoS Classes: Video, Audio and Management.

◆ **Video DSCP**

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

◆ Audio DSCP

This setting is only available for the IP Cameras that support audio.

◆ Management DSCP

The class consists of HTTP traffic: Web browsing.



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

5.3.3.3 SNMP

The SNMP (Simple Network Management Protocol) setting can be found under this path: System> Network> SNMP.

The screenshot shows the LevelOne web interface. The top navigation bar includes links for Home, System, Streaming, Camera, and Logout. The left sidebar menu is expanded to the 'Network' section, which includes sub-items: Basic, QoS, SNMP, and UPnP. The main content area is titled 'SNMP Settings'. Under the 'SNMP v1/v2' section, there are checkboxes for 'Enable SNMP v1' and 'Enable SNMP v2'. Below these are text input fields for 'Read Community' (containing 'public') and 'Write Community' (containing 'private'). The 'Traps for SNMP v1/v2' section has a checkbox for 'Enable traps', a text field for 'Trap address', and a text field for 'Trap community' (containing 'public'). The 'Trap Option' section has a checkbox for 'Warm start'. A 'Save' button is located at the bottom left of the settings area.

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

SNMP v1/ v2

◆ **Enable SNMP v1/ v2**

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

◆ **Read Community**

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

◆ **Write Community**

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

Traps for SNMP v1/ v2

Traps are used by the IP Camera to send messages to a management system for important events or status changes.

◆ **Enable Traps**

Check the box to activate trap reporting.

◆ **Trap address**

Enter the IP address of the management server.

◆ **Trap community**

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

Trap Option

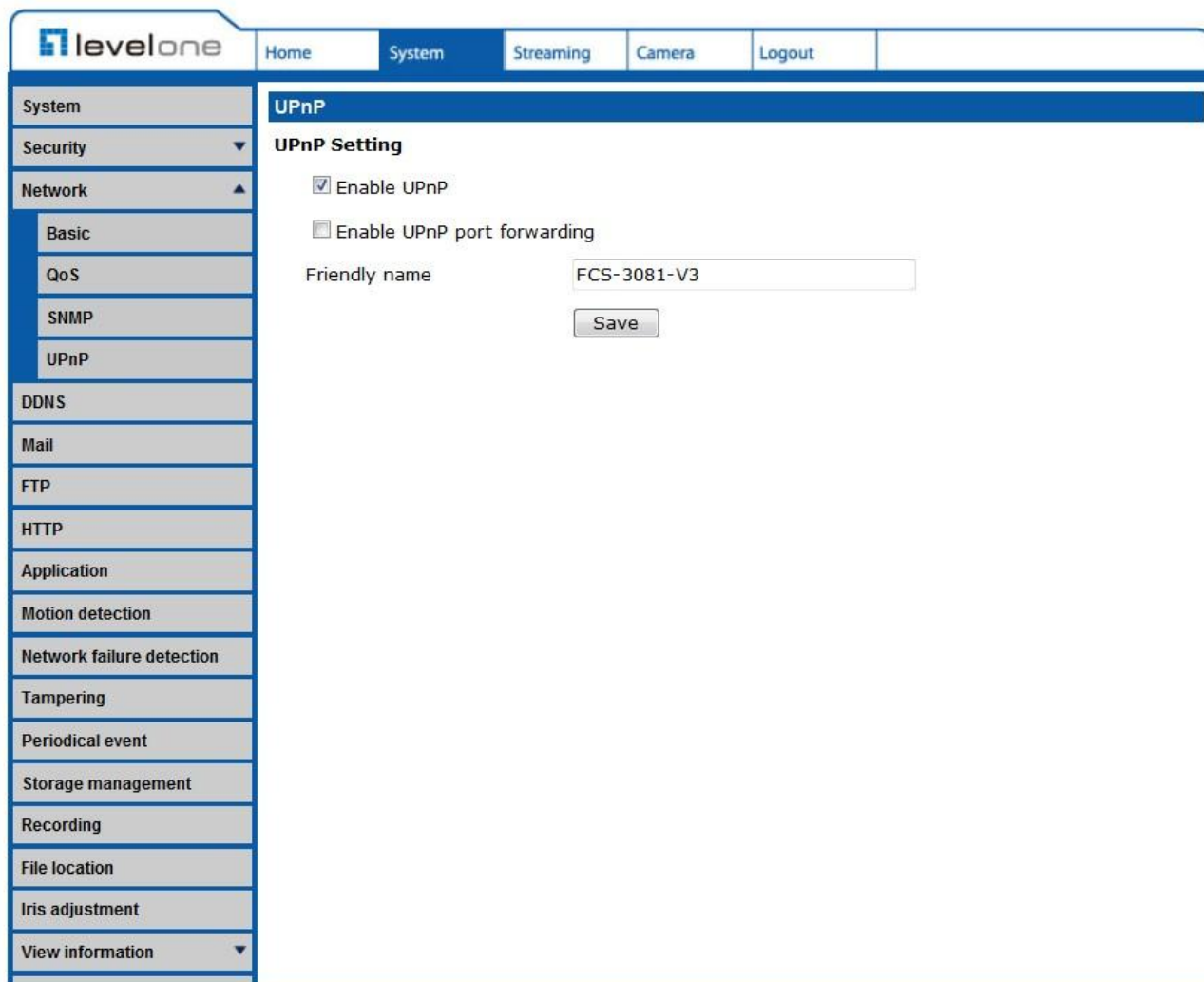
◆ **Warm Start**

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

Click on <Save> button when complete.

5.3.3.4 UPnP

The UPnP setting can be found under this path: System> Network> UPnP.



The screenshot shows the levelone web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various system settings: System, Security, Network (expanded), Basic, QoS, SNMP, UPnP, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, and View information. The main content area is titled 'UPnP' and contains the 'UPnP Setting' section. It features two checkboxes: 'Enable UPnP' (checked) and 'Enable UPnP port forwarding' (unchecked). Below these is a text field for 'Friendly name' containing 'FCS-3081-V3' and a 'Save' button.

UPnP Setting

◆ Enable UPnP

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



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

◆ **Enable UPnP port forwarding**

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



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

◆ **Friendly name**

Set the name for the IP Camera for identity.

5.3.3.5 DDNS

The DDNS setting can be found under this path: System> DDNS.

The screenshot shows the levelone web interface. The top navigation bar includes links for Home, System, Streaming, Camera, and Logout. On the left, a sidebar menu lists various system settings: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The main content area is titled 'DDNS' and contains the following text: 'Dynamic DNS Use Dynamic DNS If You Want To Use Your DDNS Account.' Below this text is a checkbox labeled 'Enable DDNS'. To the right of the checkbox are four input fields: 'Provider' (a dropdown menu currently showing 'DynDNS.org(Dynamic)'), 'Host name', 'Username/E-mail', and 'Password/Key'. A 'Save' button is located at the bottom right of the form.

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated to a static domain name so others can connect to it by name.

Enable DDNS

Check the item to enable DDNS.

Provider

Select one DDNS host from the provider list.

Host name

Enter the registered domain name in the field.

Username/E-mail

Enter the username or e-mail required by the DDNS provider for authentication.

Password/Key

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

5.3.3.6 Mail

The Mail setting can be found under this path: System> Mail.

The screenshot shows the LevelOne web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar menu is expanded to show 'Mail'. The main content area is titled 'Mail' and contains the 'SMTP' configuration section. It includes two sets of SMTP settings, each with fields for server, port, account name, password, recipient email address, and an SSL checkbox. The '1st SMTP (mail) server port' and '2nd SMTP (mail) server port' are pre-filled with '25'. A 'Save' button is located at the bottom right of the configuration area.

The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when event is triggered. SMTP is a protocol for sending e-mail messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

Two sets of SMTP can be configured. Each set includes SMTP Server, Server Port, Account Name, Password and E-mail Address settings. Check the box "SMTP SSL" to send emails via encrypted transmission. For SMTP server, contact your network service provider for more specific information.

5.3.3.7 FTP

The FTP setting can be found under this path: System> FTP.

The screenshot displays the LevelOne web interface. The top navigation bar includes 'Home', 'System' (selected), 'Streaming', 'Camera', and 'Logout'. A left sidebar lists various system settings: System, Security, Network, DDNS, Mail, FTP (highlighted), HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The main content area is titled 'FTP' and contains configuration fields for two FTP servers. For the 1st server, fields include '1st FTP server', '1st FTP server port' (set to 21), '1st FTP user name', '1st FTP password', and '1st FTP remote folder'. A checkbox for '1st FTP passive mode' is present. The 2nd server has identical fields. A 'Save' button is located at the bottom right of the form.

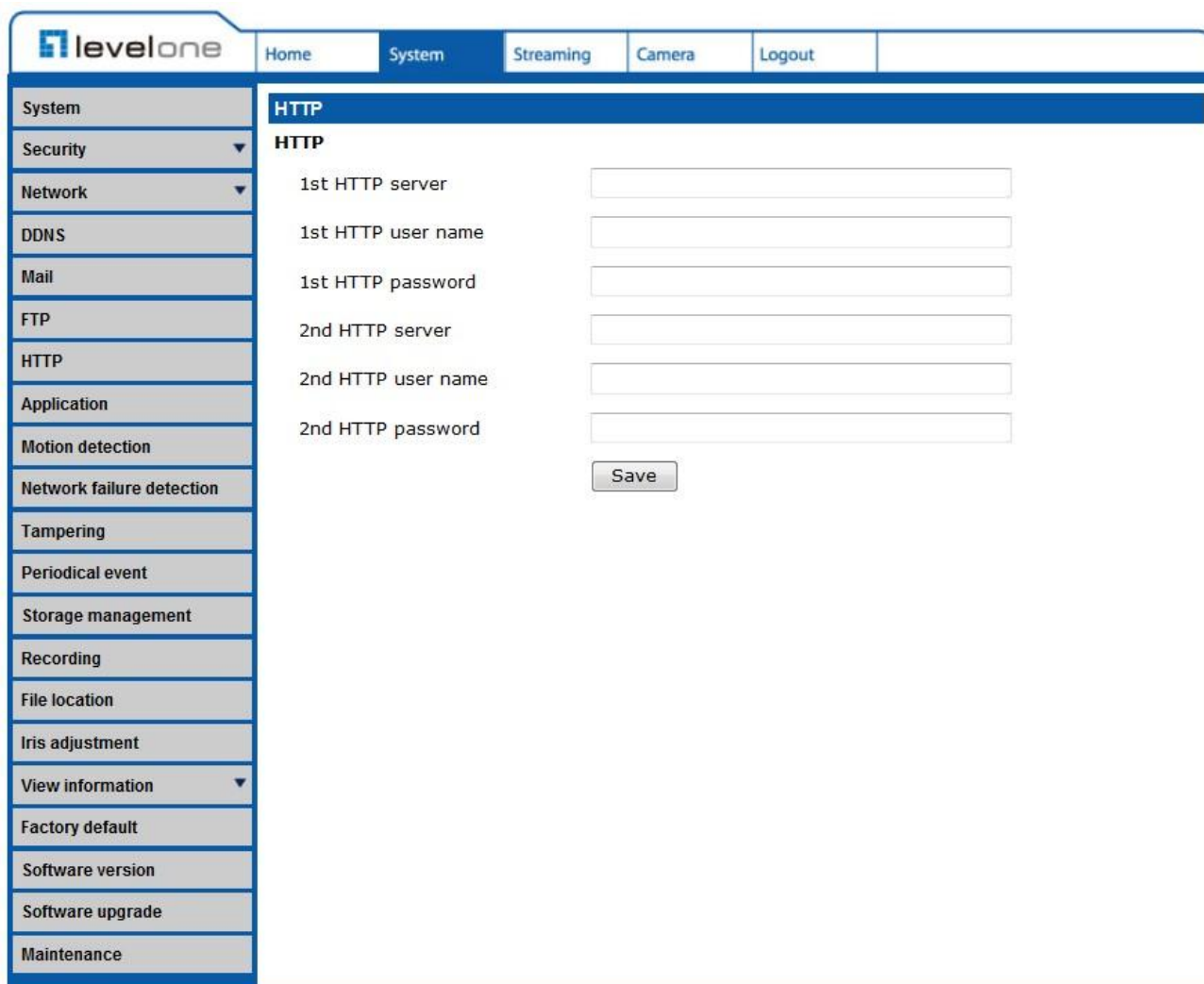
FTP	
1st FTP server	<input type="text"/>
1st FTP server port	<input type="text" value="21"/>
1st FTP user name	<input type="text"/>
1st FTP password	<input type="password"/>
1st FTP remote folder	<input type="text"/>
<input type="checkbox"/> 1st FTP passive mode	
2nd FTP server	<input type="text"/>
2nd FTP server port	<input type="text" value="21"/>
2nd FTP user name	<input type="text"/>
2nd FTP password	<input type="password"/>
2nd FTP remote folder	<input type="text"/>
<input type="checkbox"/> 2nd FTP passive mode	
<input type="button" value="Save"/>	

The Administrator can set as sending alarm message to a specific File Transfer Protocol (FTP) site when event is triggered. Users can assign alarm message to up to two FTP sites. Enter the FTP details, which include server, server port, user name, password and remote folder, in the fields. Check the box “passive mode” to be connected with the FTP server by passively receiving the FTP server’s IP address through a dynamic port. Alternatively, uncheck the box to directly connect the FTP server via active mode.

Click on <Save> when finished.

5.3.3.8 HTTP

The HTTP setting can be found under this path: System> HTTP.



The screenshot shows the LevelOne web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various system settings: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The 'HTTP' option is selected in the sidebar. The main content area is titled 'HTTP' and contains the following configuration fields:

Field	Input Type
1st HTTP server	Text box
1st HTTP user name	Text box
1st HTTP password	Text box
2nd HTTP server	Text box
2nd HTTP user name	Text box
2nd HTTP password	Text box
Save	Button

A HTTP Notification server can listen for notification messages from IP Cameras by triggered events. Enter the HTTP details, which include server name (for instance, `http://192.168.0.1/admin.php`), user name, and password in the fields. <Alarm> triggered and <Motion Detection> notifications can be sent to the specified HTTP server.

Click on <Save> when finished.



Please refer to: [Application> Send HTTP notification/ Motion Detection](#) for HTTP Notification settings.

5.3.3.9 Application

The Application setting can be found under this path: System> Application.

The screenshot shows the 'levelone' web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar menu is expanded to 'Application'. The main content area is titled 'Application' and contains the following sections:

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

The IP Camera equips one alarm input and one relay output for cooperating with alarm system to catch events' images. Refer to alarm pin definition below to connect alarm devices to the IP Camera if needed.

Alarm Pin Definition

Please refer to User's Manual for Alarm Pin Definition to connect the alarm devices.

Alarm Switch

The Administrator can enable or disable the alarm function.

Alarm Type

Select an alarm type, <Normal close> or <Normal open>, that corresponds with the alarm application.

Alarm Output

Define alarm output signal <high> or <low> as the normal alarm output status according to the current alarm application.

Triggered Action (Multi-option)

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

◆ **Enable Alarm Output**

Select the item to enable alarm relay output.

◆ **IR Cut Filter**

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



Note: The IR Function (Refer to IR Function) could not be set as <Auto> mode if this triggered action is enabled.

◆ **Send Message by FTP/E-Mail**

The Administrator can select whether to send an alarm message by FTP and/or E-Mail when an alarm is triggered.

◆ **Upload Image by FTP**

Select this item and the Administrator can assign a FTP site and configure various parameters. When the alarm is triggered, event images will be uploaded to the appointed FTP site.

<Pre-trigger buffer> function allows users to check what happened to cause the trigger. The <Pre-trigger buffer> frame rate could be pre-determined.

On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after the alarm input is triggered.

Check the box <Continue image upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to FTP when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to make the images keep being uploaded to FTP during the

trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.



NOTE: Make sure FTP configuration has been completed. Refer to FTP for further details.

◆ **Upload Image by E-Mail**

Select this item and the Administrator can assign an e-mail address and configure various parameters. When the alarm input is triggered, event images will be sent to the appointed e-mail address.

<Pre-trigger buffer> function allows users to check what happened to cause the trigger. The <Pre-trigger buffer> frame rate could be pre-determined.

On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after alarm input is triggered. Check the box <Continue image upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploading by E-mail when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to make the images keep being uploaded to E-mail during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.



NOTE: Make sure SMTP configuration has been completed. Refer to Mail for further details.

◆ **Send HTTP notification**

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

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

◆ **Record Stream to SD Card**

Select the item and the alarm-triggered recording will be saved into your Micro SD card.

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

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

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



NOTE: Please make sure the local recording (with Micro SD/SDHC card) is activated so that this function can be implemented. Refer to [Recording](#) for further details.

File Name

Enter a file name in the blank, ex. image.jpg. The uploaded image's file name format can be set in this section. Please select the one that meets your requirements.

◆ **Add date/time suffix**

File name: imageYYMMDD_HHNNSS_XX.jpg

Y: Year, M: Month, D: Day

H: Hour, N: Minute, S: Second

X: Sequence Number

◆ **Add sequence number suffix (no maximum value)**

File name: imageXXXXXXXXX.jpg

X: Sequence Number

◆ **Add sequence number suffix up to # and then start over**

File Name: imageXX.jpg

X: Sequence Number

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

◆ **Overwrite**

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

Save

After complete all the settings mentions above, please click on <Save> button to save all the settings in this page.

5.3.3.10 Motion Detection

The Motion Detection setting can be found under this path: System> Motion Detection.

The screenshot displays the LevelOne web interface for Motion Detection settings. The left sidebar lists various system functions, with 'Motion detection' highlighted. The main panel is titled 'Motion Detection' and contains several configuration sections. The 'Motion Detection' section has radio buttons for 'Off' (selected) and 'On'. The 'Motion Detection Setting' section includes input fields for 'Sampling pixel interval [1-10]' (1), 'Detection level [1-100]' (10), 'Sensitivity level [1-100]' (80), and 'Time interval(sec) [0-7200]' (10). The 'Triggered Action' section features checkboxes for 'Enable alarm output', 'Record stream to sd card', 'Send alarm message by FTP', 'Upload image by FTP', and 'Send HTTP notification', along with a 'high' dropdown menu. The 'Motion Detection Windows' section has 'add' and 'delete' buttons. A live video pane on the right shows a Star Wars Stormtrooper with a red rectangular motion detection window overlaid on its chest. Below the video pane is a 'Motion Detection Windows' section with 'add' and 'delete' buttons. At the bottom, there is a 'File Name' field set to 'image.jpg' and radio buttons for adding date/time suffix, sequence number suffix, or overwriting, followed by a 'save' button.

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

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

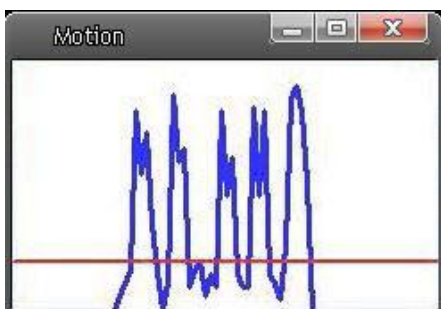


Up to 10 Motion Detection Windows can be set. Click on the <add> button under the Live Video Pane to add a Motion Detection Window. To cancel a Motion Detection Window, move the mouse cursor to the selected Window, and click on the <delete> button.

If Motion Detection function is activated, the pop-off window (Motion) with indication of motion will be shown.



When motion is detected, the signals will be displayed on the Motion window as shown below.



Motion Detection

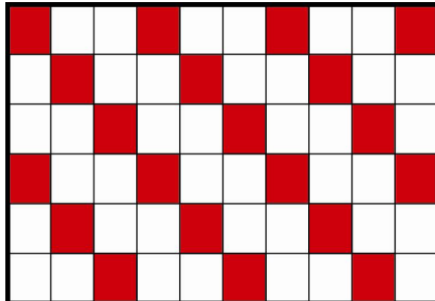
Users are able to turn on/off Motion Detection. Default setting is Off.

Motion Detection Setting

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

◆ **Sampling pixel interval [1-10]:**

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



◆ **Detection level [1-100]:**

The default level is 10. The item is to set detection level for each sampling pixel; the smaller the value, the more sensitive it is.

◆ **Sensitivity level [1-100]:**

The default level is 80, which means if 20% or more sampling pixels are detected differently, system will detect motion. The bigger the value, the more sensitive it is. Meanwhile, when the value is bigger, the red horizontal line in the motion indication window will be lower accordingly.

◆ **Time interval (sec) [0-7200]:**

The default interval is 10. The value is the interval between each detected motion.

Triggered Action (Multi-option)

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

◆ **Enable Alarm Output**

Check the item and select the predefined type of alarm output to enable alarm relay output when motion is detected.

◆ **Record stream to SD Card**

Select this item and the Motion Detection recording will be stored in Micro SD/ SDHC card when motion is detected.

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

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

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



NOTE: Please make sure the local recording (with Micro SD/SDHC card) is activated so that this function can be implemented. Refer to [Recording](#) for further details.

◆ **Send Alarm Message by FTP/E-Mail**

The Administrator can select whether to send warning messages by FTP and/or E-Mail when motion is detected.

◆ **Upload Image by FTP**

Select this item and the Administrator can assign a FTP site and configure various parameters. When motion is detected, event images will be uploaded to the appointed FTP site.

<Pre-trigger buffer> function allows users to check what happened to cause the trigger. The <Pre-trigger buffer> frame rate could be pre-determined.

On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after motion event occurs.

Check the box <Continue image upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to FTP when the motion event occurs. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to make the images keep being uploaded to FTP during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.



NOTE: Make sure FTP configuration has been completed. Refer to [FTP](#) for further details.

◆ **Upload Image by E-Mail**

Select this item and the Administrator can assign an e-mail address and configure

various parameters. When motion is detected, event images will be sent to the appointed e-mail address.

<Pre-trigger buffer> function allows users to check what happened to cause the trigger. The <Pre-trigger buffer> frame rate could be pre-determined.

On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after the motion event occurs.

Check the box <Continue image upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploading by E-mail when the motion event occurs. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to make the images keep being uploaded to E-mail during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.



NOTE: Make sure SMTP configuration has been completed. Refer to [Mail](#) for further details.

◆ **Send HTTP notification**

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

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

File Name

Enter a file name in the blank, ex. image.jpg. The uploaded image's file name format can be set in this section. Please select the one that meets your requirements.

◆ **Add date/time suffix**

File name: imageYYMMDD_HHNNSS_XX.jpg

Y: Year, M: Month, D: Day

H: Hour, N: Minute, S: Second

X: Sequence Number

◆ **Add sequence number suffix (no maximum value)**

File name: imageXXXXXXXX.jpg

X: Sequence Number

◆ **Add sequence number suffix up to # and then start over**

File Name: imageXX.jpg

X: Sequence Number

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

◆ **Overwrite**

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

Save

Click on the <Save> button to save all the Motion Detection settings mentioned above.

5.3.3.11 Network Failure Detection

The screenshot shows the 'levelone' web interface. The left sidebar contains a list of system settings: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection (highlighted), Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The main content area is titled 'Network failure detection' and contains three sections: 'Detection Switch' with 'Off' selected, 'Detection Type' with 'Ping the IP address 0.0.0.0 every 1 minutes', and 'Triggered Action' with 'Enable alarm output' selected and a 'high' priority dropdown. Other options include 'Send message by FTP', 'Record stream to sd card', and 'Send message by E-Mail'. A 'Save' button is located at the bottom of the configuration area.

Ne

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

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

Detection Switch

You will be able to turn on/off Network Failure Detection in System section. Default setting is Off.

Detection Type

Input the IP device address and the period of ping time to ping. The ping time setting range is from 1 to 99 minutes.

Triggered Action (Multi-option)

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

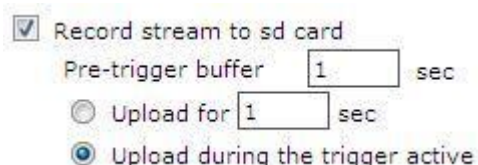
◆ **Enable Alarm Output**

Select the item to enable alarm relay output.

◆ **Record Stream to SD Card**

Select the item and the alarm-triggered recording will be saved into your Micro SD card.

Pre-trigger buffer recording function allows users to check what happened to cause the trigger. The pre-trigger buffer time range is from 1 to 3 seconds. Select <Upload for ___ sec> to set the recording duration after alarm is triggered. The setting range is from 1 to 99999 seconds. Select <Upload during the trigger active> to record the triggered video until the trigger is off.



☒ Record stream to sd card
Pre-trigger buffer sec
☐ Upload for sec
☒ Upload during the trigger active



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

◆ **Send Alarm Message by FTP/E-Mail**

The Administrator can select whether to send an alarm message by FTP and/or E-Mail when an alarm is triggered.

Save

Click on the <Save> button to save all the settings mentioned above.

5.3.3.12 Tampering

The Tampering setting can be found under this path: System> Tampering.

The screenshot displays the LevelOne web interface for configuring the Tampering Alarm. The left sidebar lists various system settings, with 'Tampering' selected. The main configuration area includes:

- Tampering Alarm:** Radio buttons for 'Off' (selected) and 'On'.
- Tampering Duration:** A text input for 'Minimum duration' set to '20' with a 'sec' label.
- Triggered Action:** Checkboxes for 'Enable alarm output' (selected), 'Send message by FTP', 'Upload image by FTP', 'Send HTTP notification', 'Record stream to sd card', 'Send message by E-Mail', and 'Upload image by E-Mail'.
- File Name:** A text input for 'File name' set to 'image.jpg', and radio buttons for 'Add date/time suffix' (selected), 'Add sequence number suffix (no maximum value)', 'Add sequence number suffix up to 0 and then start over', and 'Overwrite'.
- A 'Save' button is located at the bottom of the configuration area.

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

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

Tampering Alarm

Users are able to turn on/off Tampering Alarm function in Tampering Alarm setting page. The default setting is Off.

Tampering Duration

Minimum Tampering Duration is the time for video analysis to determine whether camera tampering has occurred. Minimum Duration could also be interpreted as defining the Tampering threshold; longer duration represents higher threshold. Settable Tampering Duration time range is from 10 to 3600 seconds. The Default value is 20 seconds.

Triggered Action (Multi-option)

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

◆ Enable Alarm Output

Check the item and select the predefined type of alarm output to enable alarm output when tampering is detected.

◆ Record stream to SD Card

Select this item and the Tampering Alarm recording will be stored in Micro SD/ SDHC card when tampering is detected.

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

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

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



NOTE: Please make sure the local recording (with Micro SD/SDHC card) is activated so that this function can be implemented. Refer to [Recording](#) for further details.

◆ Send Message by FTP/E-Mail

The Administrator can select whether to send an alarm message by FTP and/or E-Mail when tampering is detected.

◆ Upload Image by FTP

Select this item and the Administrator can assign a FTP site and configure various parameters. When tampering is detected, event images will be uploaded to the

appointed FTP site.

<Pre-trigger buffer> function allows users to check what happened to cause the trigger. The <Pre-trigger buffer> frame rate could be pre-determined.

On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after tampering is triggered.

Check the box <Continue image upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to FTP when tampering is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to make the images keep being upload to FTP during the trigger active until the tampering stops. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.



NOTE: Make sure FTP configuration has been completed. Refer to [FTP](#) for further details.

◆ Upload Image by E-Mail

Select this item and the Administrator can assign an e-mail address and configure various parameters. When tampering is detected, event images will be sent to the appointed e-mail address.

<Pre-trigger buffer> function allows users to check what happened to cause the trigger. The <Pre-trigger buffer> frame rate could be pre-determined.

On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after tampering occurs.

Check the box <Continue image upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploading by E-mail when tampering is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to make the images keep being upload to E-mail during the trigger active until tampering stops. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 20 frames.



NOTE: Make sure SMTP configuration has been completed. Refer to [Mail](#) for further details.

◆ **Send HTTP notification**

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

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

File Name

Enter a file name in the blank, ex. image.jpg. The uploaded image's file name format can be set in this section. Please select the one that meets your requirements.

◆ **Add date/time suffix**

File name: imageYYMMDD_HHNNSS_XX.jpg

Y: Year, M: Month, D: Day

H: Hour, N: Minute, S: Second

X: Sequence Number

◆ **Add sequence number suffix (no maximum value)**

File name: imageXXXXXXXXX.jpg

X: Sequence Number

◆ **Add sequence number suffix up to # and then start over**

File Name: imageXX.jpg

X: Sequence Number

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

◆ **Overwrite**

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

Save

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

5.3.3.13 Storage Management (Local Recording)

The Storage Management setting can be found under this path: System> Storage Management.

The screenshot shows the LevelOne web interface for Storage Management. The left sidebar contains a menu with items: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The main content area is titled 'Storage Management' and includes sections for Device information, Device setting, Disk cleanup setting, and Recording list.

Storage Management			
Device information			
Device type:	SD card	Total size:	0 KB
Free space:	0 KB	Full:	No
Status:	No		
Device setting			
Format device :	<input type="button" value="Format"/>		
Disk cleanup setting			
<input type="checkbox"/> Enable automatic disk cleanup			
Remove recordings older than:	1	day(s)	
Remove oldest recordings when disk is:	85	% full	
<input type="button" value="Save"/>			
Recording list			
FileName		Size	
<div></div>			
<input type="button" value="Remove"/>		<input type="button" value="Sort"/>	<input type="button" value="download"/>

Users can implement local recording to the Micro SD/SDHC card up to 32GB. This page shows the capacity information of the Micro SD card and a recording list with all the recording files saved on the memory card. Users can also format the SD card and implement automatic recording cleanup through the setting page.

To implement Micro SD card recording, please go to the <Recording> page (refer to [Recording](#)) for activation.



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

Device information

When users insert the Micro SD/SDHC card, the card information such as the memory capacity and status will be shown at Device Information section.

For the memory card being successfully installed, its status shall be shown at <Device information> section in the Storage Management page.

Device setting

Click on the <Format> button to format the memory card.

Disk cleanup setting

Users can enable automatic recordings cleanup by specifying the time and storage limits

Recording List

Each video file on the Micro SD/SDHC card will be listed in the Recording list as shown below. The maximum file size is 60 MB (60 MB per file).

When the recording mode is set as “Always” (consecutive recording) and the Micro SD/SDHC card recording is also allowed to be enabled by events triggered, once events occur, the system will immediately implement events recording to the memory card. Then the IP Camera will return to the regular recording mode after events recording.

◆ Remove

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

◆ Sort

Click on the <Sort> button, and the files in the Recording list will be listed in name and date order.



NOTE: The capital letter A/M/R/T appears in the very beginning of name denotes the sort of the recording: A stands for Alarm; M stands for Motion; R stands for regular recording, and T stands for Tampering.

◆ Download

To open/download a video clip, select the file first, and then click on the <download> button below the Recording list field. The selected file window will pop up. Click on the AVI file to directly play the video in the player or download it to a specified location.

5.3.3.14 Recording (Local Recording)

The Recording setting can be found under this path: System> Recording.

The screenshot shows the LevelOne web interface. The top navigation bar includes 'Home', 'System' (selected), 'Streaming', 'Camera', and 'Logout'. A left sidebar lists various system settings: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording (selected), File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The main content area is titled 'Recording' and contains a 'Recording Schedule' section. It has three radio buttons: 'Disable' (selected), 'Always', and 'Only during time frame'. Below these is a table with 10 rows and 3 columns: 'Weekday', 'Start time', and 'Duration'. Each row is numbered 1 to 10. Under the table, there are checkboxes for each day of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat. At the bottom, there are input fields for 'Start time' (set to 00:00) and 'Duration' (set to 00:00), along with 'Save' and 'Delete' buttons.

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

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

Start time : 00:00 Duration : 00:00

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

Activating Micro SD/SDHC Card Recording

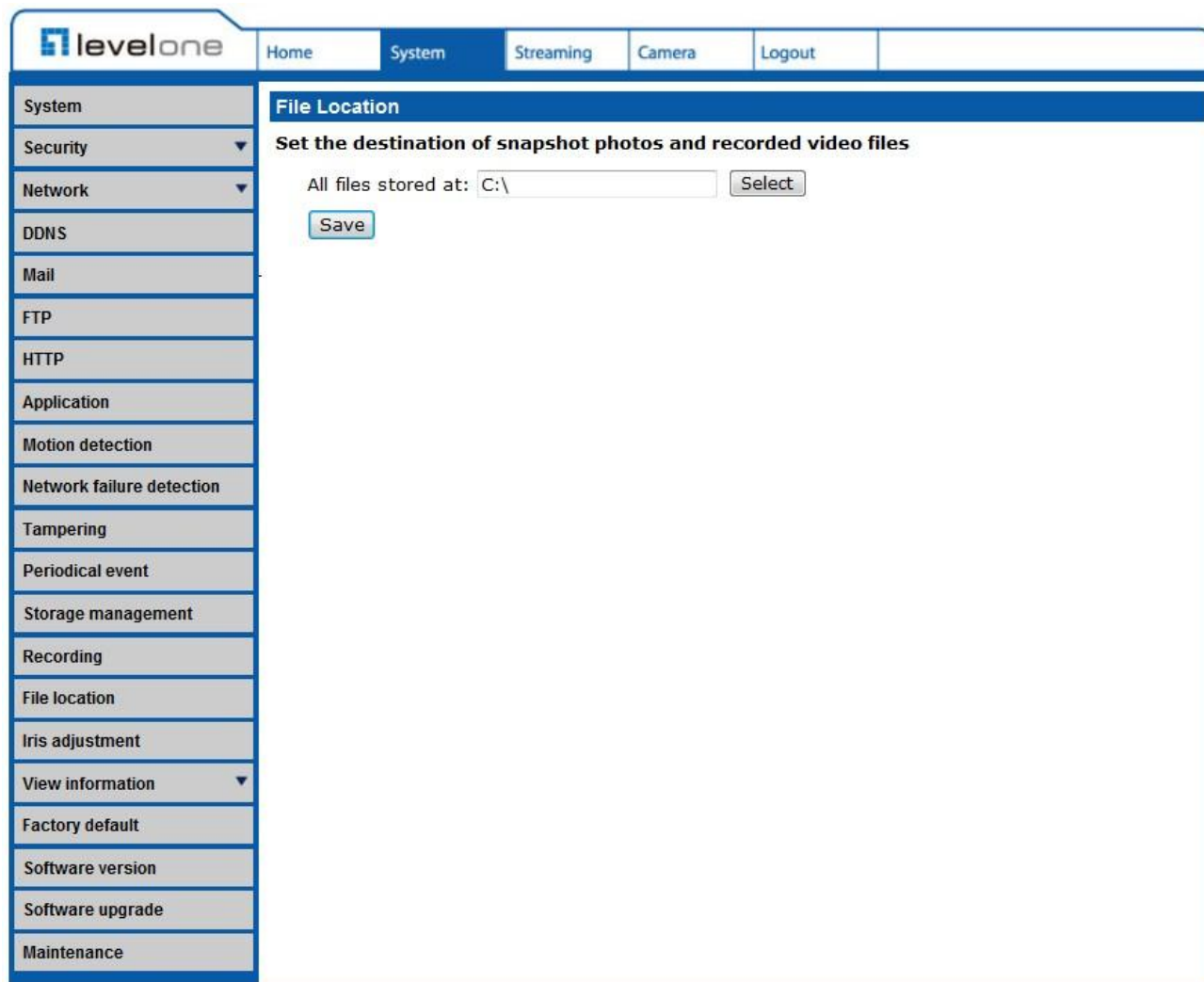
Two types of schedule mode are offered: <Always> and <Only during Time Frame>. Users can select <Always> to activate Micro SD/SDHC Card Recording all the time. Or select a set of schedule from the time frame blank, check specific weekdays and setup the start time (hour:minute) and time period (hour:minute) to activate Micro SD/SDHC Card Recording at certain time frames. The setting range for time period hour is from 0 to 168. Please click on <Save> to save the setup.

Terminating Micro SD/SDHC Card Recording

Select <Disable> to terminate the recording function.

5.3.3.15 File Location (Snapshots and Web Recording)

The File Location setting can be found under this path: System> File Location.



The screenshot shows the levelone web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various system settings: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The 'File Location' page is active, displaying the title 'File Location' and the instruction 'Set the destination of snapshot photos and recorded video files'. Below this, there is a text input field labeled 'All files stored at:' with the value 'C:\' and a 'Select' button. A 'Save' button is also present.

Users can specify a storage location on the PC or in the hard drive for the snapshots and live video recording. The default setting is: C:\. Once confirm the setting, click on <Save>, and all the snapshots and web recording will be saved in the designate location.



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



NOTE: For users with Windows 7 operating system, it is required to log on as an Administrator to implement the Snapshot and Web Recording function.

5.3.3.16 Iris Adjustment (Fixed Focal Lens Excluded)

The Iris Adjustment function can be found under this path: System> Iris Adjustment.

levelone

HomeSystemStreamingCameraLogout

System

Security

Network

DDNS

Mail

FTP

HTTP

Application

Motion detection

Network failure detection

Tampering

Periodical event

Storage management

Recording

File location

Iris adjustment

View information


Factory default

Software version

Software upgrade

Maintenance

Iris adjustment



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

Step 1:

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

Step 2:

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

Step 3:

Start the iris adjustment.

For users who use Auto-iris lens, when it is required to implement iris adjustment, please refer to the Iris adjustment procedure in the setting page to adjust iris.

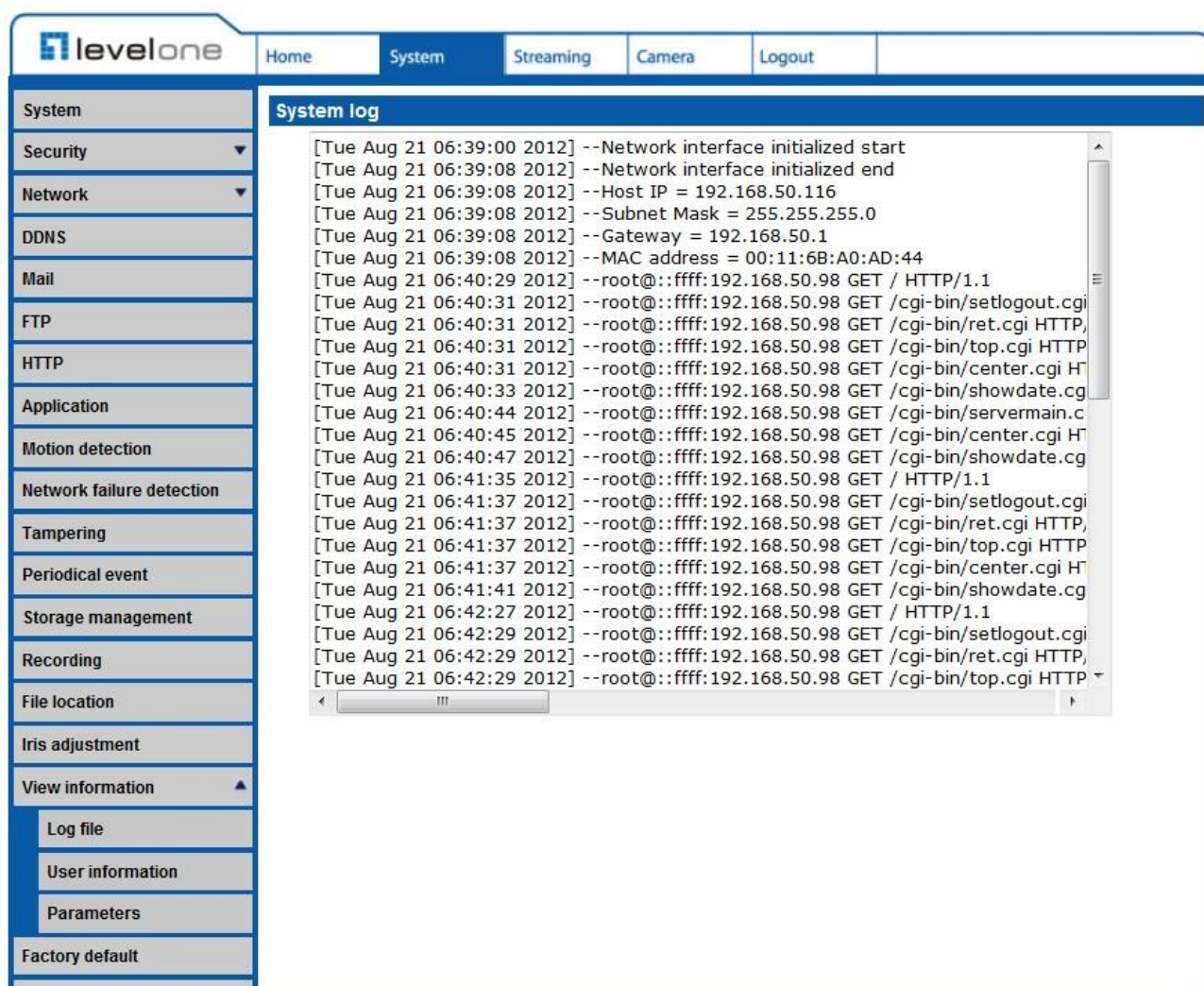
5.3.3.17 View Information

The View Information function can be found under this path: System> View Information.

Click on the category: <View Information>, there will be a drop-down menu with tabs including <Log File>, <User Information>, and <Parameters>.

5.3.3.17.1 Log File

The Log File function can be found under this path: System> Log File.



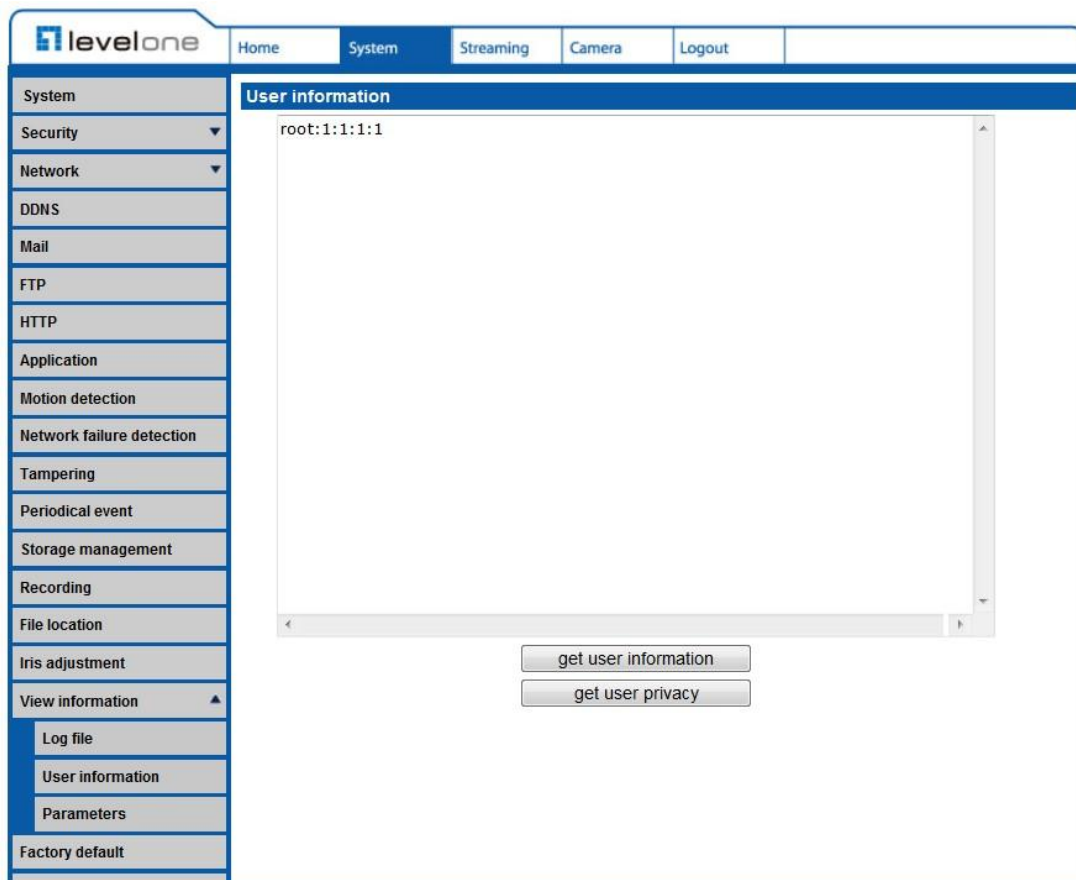
The screenshot displays the LevelOne web interface. The top navigation bar includes links for Home, System, Streaming, Camera, and Logout. On the left, a sidebar menu lists various system categories: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Log file, User information, Parameters, and Factory default. The 'View information' category is expanded, showing 'Log file', 'User information', and 'Parameters'. The main content area, titled 'System log', displays a list of system events with timestamps and descriptions. The log entries include network initialization, host IP, subnet mask, gateway, MAC address, and various HTTP requests from the root user to the system's CGI scripts.

Timestamp	Event Description
[Tue Aug 21 06:39:00 2012]	--Network interface initialized start
[Tue Aug 21 06:39:08 2012]	--Network interface initialized end
[Tue Aug 21 06:39:08 2012]	--Host IP = 192.168.50.116
[Tue Aug 21 06:39:08 2012]	--Subnet Mask = 255.255.255.0
[Tue Aug 21 06:39:08 2012]	--Gateway = 192.168.50.1
[Tue Aug 21 06:39:08 2012]	--MAC address = 00:11:6B:A0:AD:44
[Tue Aug 21 06:40:29 2012]	--root@::ffff:192.168.50.98 GET / HTTP/1.1
[Tue Aug 21 06:40:31 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/setlogout.cgi
[Tue Aug 21 06:40:31 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/ret.cgi HTTP/1.1
[Tue Aug 21 06:40:31 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/top.cgi HTTP/1.1
[Tue Aug 21 06:40:31 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/center.cgi HTTP/1.1
[Tue Aug 21 06:40:33 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/showdate.cgi
[Tue Aug 21 06:40:44 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/servermain.cgi
[Tue Aug 21 06:40:45 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/center.cgi HTTP/1.1
[Tue Aug 21 06:40:47 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/showdate.cgi
[Tue Aug 21 06:41:35 2012]	--root@::ffff:192.168.50.98 GET / HTTP/1.1
[Tue Aug 21 06:41:37 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/setlogout.cgi
[Tue Aug 21 06:41:37 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/ret.cgi HTTP/1.1
[Tue Aug 21 06:41:37 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/top.cgi HTTP/1.1
[Tue Aug 21 06:41:37 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/center.cgi HTTP/1.1
[Tue Aug 21 06:41:41 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/showdate.cgi
[Tue Aug 21 06:42:27 2012]	--root@::ffff:192.168.50.98 GET / HTTP/1.1
[Tue Aug 21 06:42:29 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/setlogout.cgi
[Tue Aug 21 06:42:29 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/ret.cgi HTTP/1.1
[Tue Aug 21 06:42:29 2012]	--root@::ffff:192.168.50.98 GET /cgi-bin/top.cgi HTTP/1.1

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

5.3.3.17.2 User Information

The User Information function can be found under this path: System> User Information.



The Administrator can view each added user's login information and privileges (refer to **Security**).

Get User Information

All the users in the network will be listed in the <User information> zone as shown below:

User: 4321

It indicates that one user's login username is "User", and the password is "4321".

Get User Privacy

Click on <get user privacy> at the bottom of the page, and the Administrator can view each user's privileges as shown below:

User: 1:1:0:1

1:1:0:1= I/O access : Camera control : Talk : Listen (refer to Security)

Therefore, it denotes the user is granted privileges of I/O access, Camera control and Listen.

5.3.3.17.3 Parameters

.The Parameters function can be found under this path: System> Parameter.

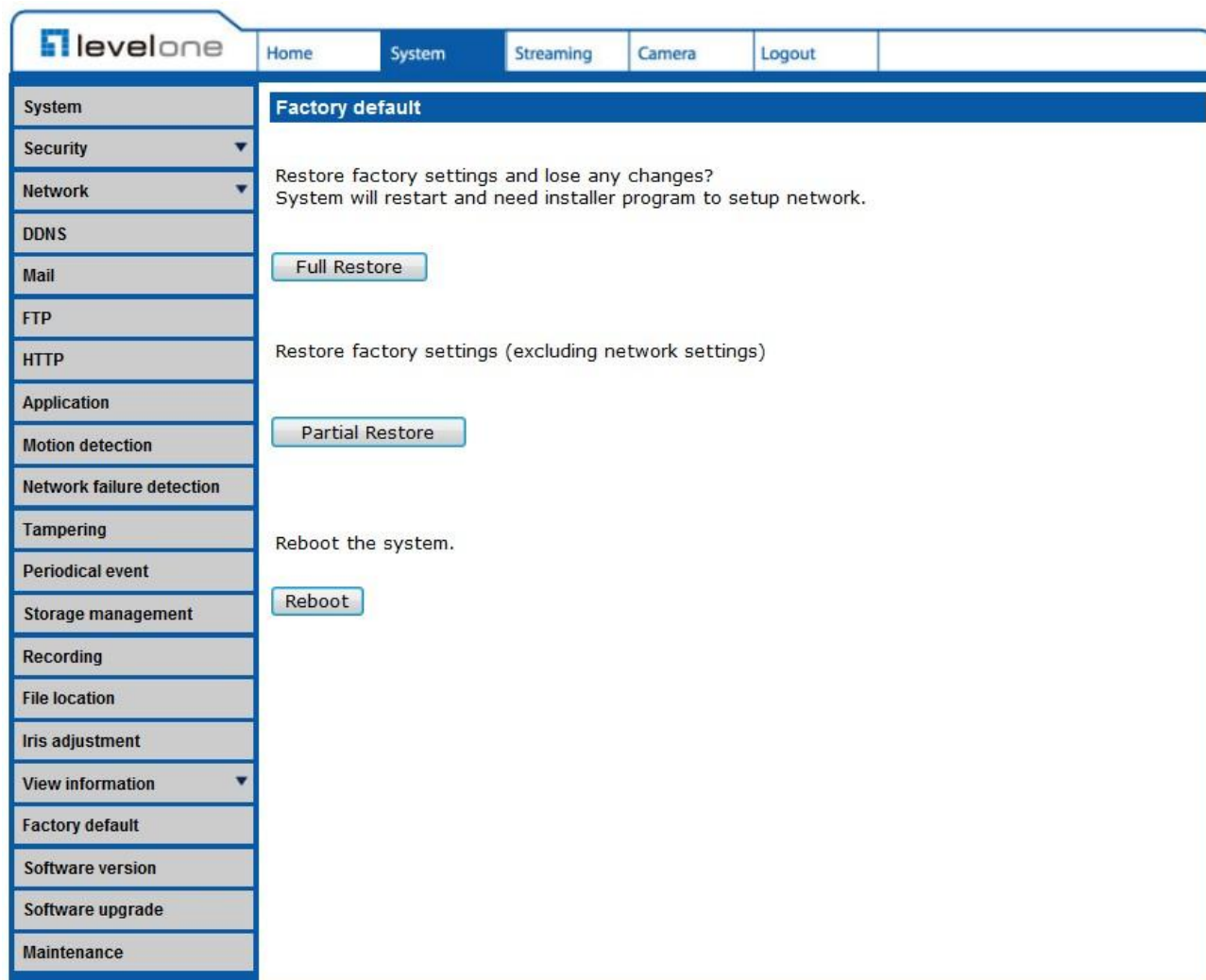
The screenshot displays the 'levelone' web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar contains a list of system functions: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Log file, User information, Parameters, and Factory default. The 'Parameters' option is highlighted. The main content area, titled 'Parameter list', shows the 'Mega Pixel Camera Initial Configuration File' settings. The settings are as follows:

Parameter	Value
exposure mode	<auto>
min shutter speed	<8>
fixed shutter speed	<56>
white balance mode	<auto>
white balance rgain	<57>
white balance bgain	<54>
brightness value	<128>
sharpness value	<4>
contrast value	<64>
saturation	<64>
hue value	<128>

Click on this item to view the entire system's parameter setting such as Camera Settings, Mask Information and Network Information.

5.3.3.18 Factory Default

The Factory Default setting can be found under this path: System> Factory Default.



The screenshot shows the LevelOne web interface. The top navigation bar includes the LevelOne logo and tabs for Home, System, Streaming, Camera, and Logout. The left sidebar contains a list of system settings: System, Security, Network, DDNS, Mail, FTP, HTTP, Application, Motion detection, Network failure detection, Tampering, Periodical event, Storage management, Recording, File location, Iris adjustment, View information, Factory default, Software version, Software upgrade, and Maintenance. The main content area is titled "Factory default" and contains the following text: "Restore factory settings and lose any changes? System will restart and need installer program to setup network." Below this text is a "Full Restore" button. Further down, the text reads "Restore factory settings (excluding network settings)" with a "Partial Restore" button. At the bottom, the text says "Reboot the system." with a "Reboot" button.

Users can follow the instructions on this page to reset the IP Camera to factory default setting if needed.

Set Default

Click on the <Set Default> button to recall the factory default settings. Then the system will restart in 30 seconds.



NOTE: The IP address will be restored to default.

Reboot

Click on the <Reboot> button, and the system will restart without changing current settings.

5.3.3.19 Software Version

The Software Version can be found under this path: System> Software Version.

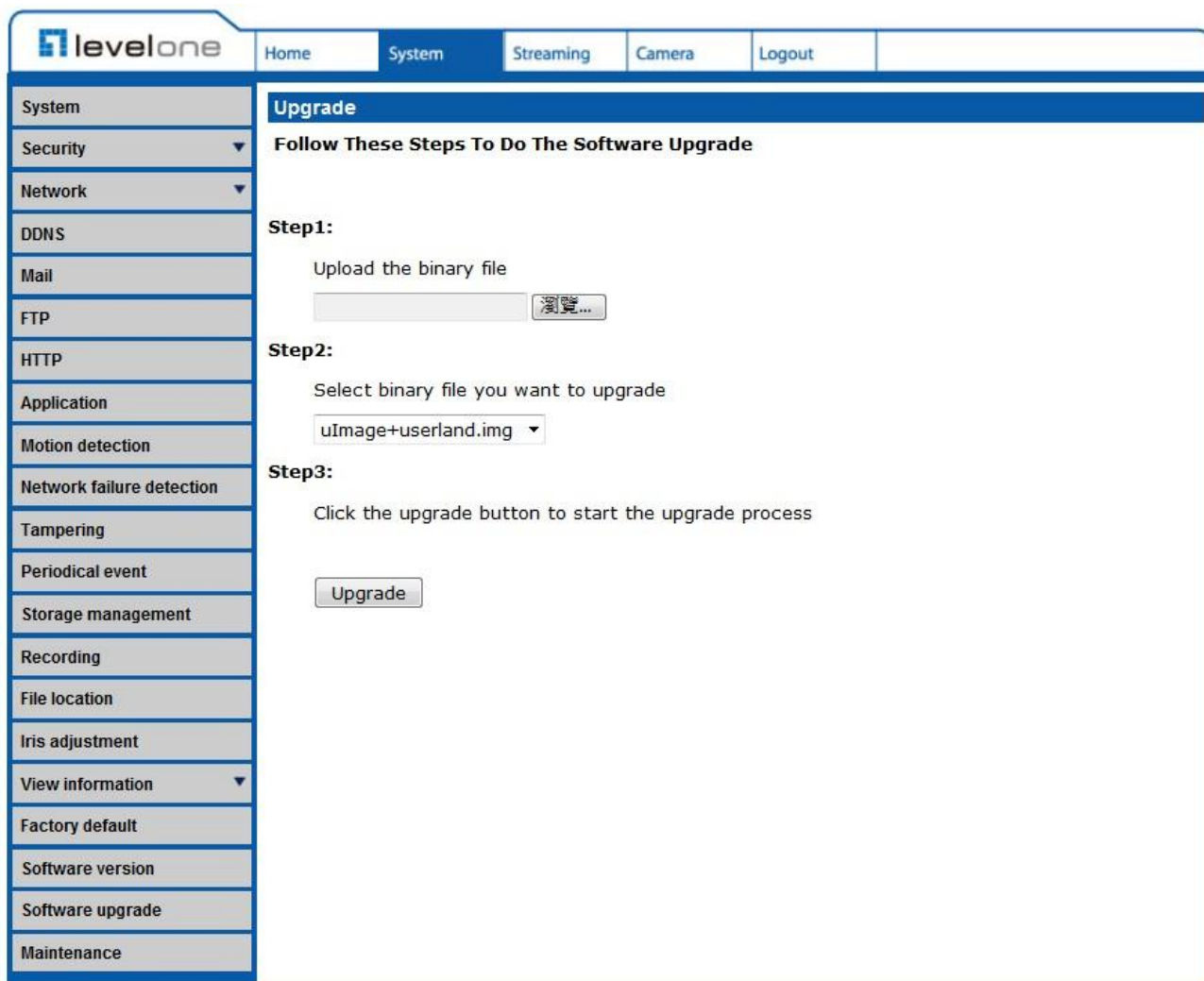
The screenshot displays the LevelOne web interface. At the top, there is a navigation bar with the LevelOne logo and several tabs: Home, System (which is the active tab), Streaming, Camera, and Logout. On the left side, there is a vertical menu with various system settings categories. The 'Software version' option is highlighted in the bottom section of this menu. The main content area on the right is titled 'Software version' and contains the text: 'The software version is **le20120821NSA**'.

System	Software version
System	
Security	
Network	
DDNS	
Mail	
FTP	
HTTP	
Application	The software version is le20120821NSA
Motion detection	
Network failure detection	
Tampering	
Periodical event	
Storage management	
Recording	
File location	
Iris adjustment	
View information	
Factory default	
Software version	
Software upgrade	
Maintenance	

The current software version is displayed in the software version page.

5.3.3.20 Software Upgrade

The Software Upgrade setting can be found under this path: System> Software Upgrade.



Upgrade

Follow These Steps To Do The Software Upgrade

Step1:

Upload the binary file

Step2:

Select binary file you want to upgrade

Step3:

Click the upgrade button to start the upgrade process



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

The procedure of software upgrade is as below:

Step 1. Click on “Browse” and select the binary file to be uploaded, ex. ulmage_userland.



NOTE: Do not change the upgrade file name, or the system will fail to find the file.

Step 2. Pull down the upgrade binary file list and select the file “ulmage+userland.img”

Step 3. Click on the <Upgrade> button. The system will check whether the upgrade file

exists or not first, and then begin to upload the upgrade file. Subsequently, the upgrade status bar will display on the page. When it runs to 100%, the upgrade process is finished.

After the upgrade process is finished, the viewer will return to Home page.

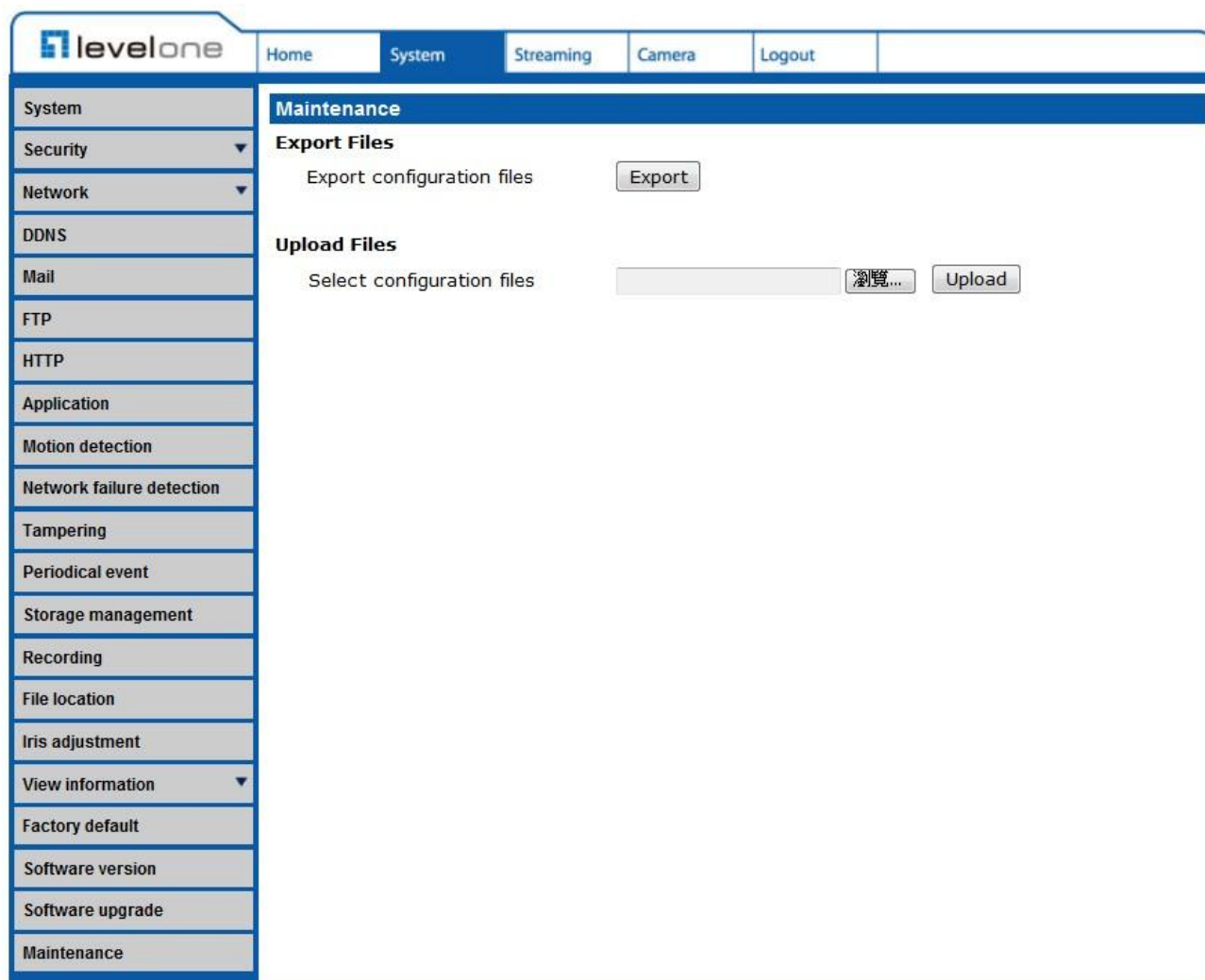
Step 4. Close the video browser.

Step 5. Start <Control Panel> on your PC, and then double click on <Add or Remove Programs>. In the <Currently install programs> list, select <DCViewer> and click on the button “Remove” to uninstall the existing DC Viewer.

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

5.3.3.21 Maintenance

The Maintenance setting can be found under this path: System> Maintenance.



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

Export

Users can save the system settings by exporting the configuration file (.bin) to a specified location for future use. Click on the <Export> button, and the popup File Download window will come out as shown below. Click on <Save> and specify a desired location for saving the configuration file.

Upload

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

5.4 Streaming

Under the tab <Streaming>, there are submenus including: <Video Format>, <Video Compression>, <Video ROI>, <Video OCX Protocol>, <Video Frame Rate>, <Video Mask>, and <Audio>.

In the Streaming submenus, the Administrator can configure specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Further details of these settings will be specified in the following sections.

5.4.1 Video Format (Video Resolution and Rotate Type)

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

The screenshot shows the 'levelone' web interface with the 'Streaming' tab selected. On the left is a sidebar menu with options: Video Format, Video Compression, Video ROI, Video OCX Protocol, Video Frame Rate, Video Mask, and Audio. The main content area is titled 'Video Format' and contains several sections:

- Video Resolution :** A dropdown menu is set to 'H.264 + H.264 + H.264 + H.264'. Below it are four rows of settings:
 - H.264-1 format : 1920 x 1080 (15 fps)
 - H.264-2 format : 1280 x 1024 (15 fps)
 - H.264-3 format : 720 x 480 (15 fps)
 - H.264-4 format : 352 x 240 (30 fps)A 'Save' button is located below these settings.
- Note :** A text note stating: 'Image attachment by FTP or E-mail will be available only while MJPEG streaming is selected.'
- Text Overlay Settings :** Three checkboxes are checked: 'Include date', 'Include time', and 'Include text string'. The 'Include text string' field contains the value '20120821'. A 'Save' button is below.
- Video Rotate Type :** A dropdown menu is set to 'Normal video'. A 'Save' button is below.
- GOV Settings :** Two rows of settings for GOV Length:
 - H.264-1 GOV Length : 60 H.264-2 GOV Length : 60
 - H.264-3 GOV Length : 30 H.264-4 GOV Length : 30A 'Save' button is below.
- H.264 Profile :** Four dropdown menus, all set to 'Main profile':
 - H.264-1 : Main profile
 - H.264-2 : Main profile
 - H.264-3 : Main profile
 - H.264-4 : Main profileA 'Save' button is below.

Video Resolution

Under Video Resolution section, the available video resolution formats are including MJPEG and H.264. Please refer to the User's Manual for more combination details.

Click on <Save> to confirm the setting.

Text Overlay Settings

Users can select the items to display data including date/time/text on the live video panel. The maximum length of the string is 20 alphanumeric characters. Click on <Save> to confirm the Text Overlay setting.

Video Rotate Type

Users can change video display type if necessary. Selectable video rotate types include Normal, Flip, Mirror, 90 degree clockwise, 180 degree rotate and 90 degree counterclockwise.

The following is descriptions for different video rotate type.

◆ Flip

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

◆ Mirror

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

◆ 90 Degree counter-/clockwise

Selecting <90 Degree Counter-/clockwise> will make the image 90° counter-/clockwise inversed.

◆ 180 Degree Rotate

Selecting <180 Degree> will make the image 180° inversed.

Click on <Save> to confirm the setting.

GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. The setting range is from 2 to 64. Default value is 60, which means there's one I-frame every 60 frames. Longer GOV length means lower I-frame frequency. The default value for H.264-1/ H.264-2/ H.264-3/ H.264-4 is 60/ 60/ 30/ 30. Click on <Save> to confirm the GOV setting.

H.264 Profile

Users can set each H.264 Profile to <Baseline Profile>, <Main Profile> or <High Profile> according to its compression needs. With the same bit rate, the higher the compression ratio, the better the image quality is. The default setting is <Main Profile>.



NOTE: Please make sure the higher compression ratio is supported by system before setup.

5.4.2 Video Compression

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

Users can select a proper MJPEG/H.264 compression mode in the video compression page depending on the application.

MJPEG Q (Quality) factor

Higher value implies higher bit rates and higher visual quality. The default setting of MJPEG Q factor is 35; the setting range is from 1 to 70.

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

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

Display Compression Information

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

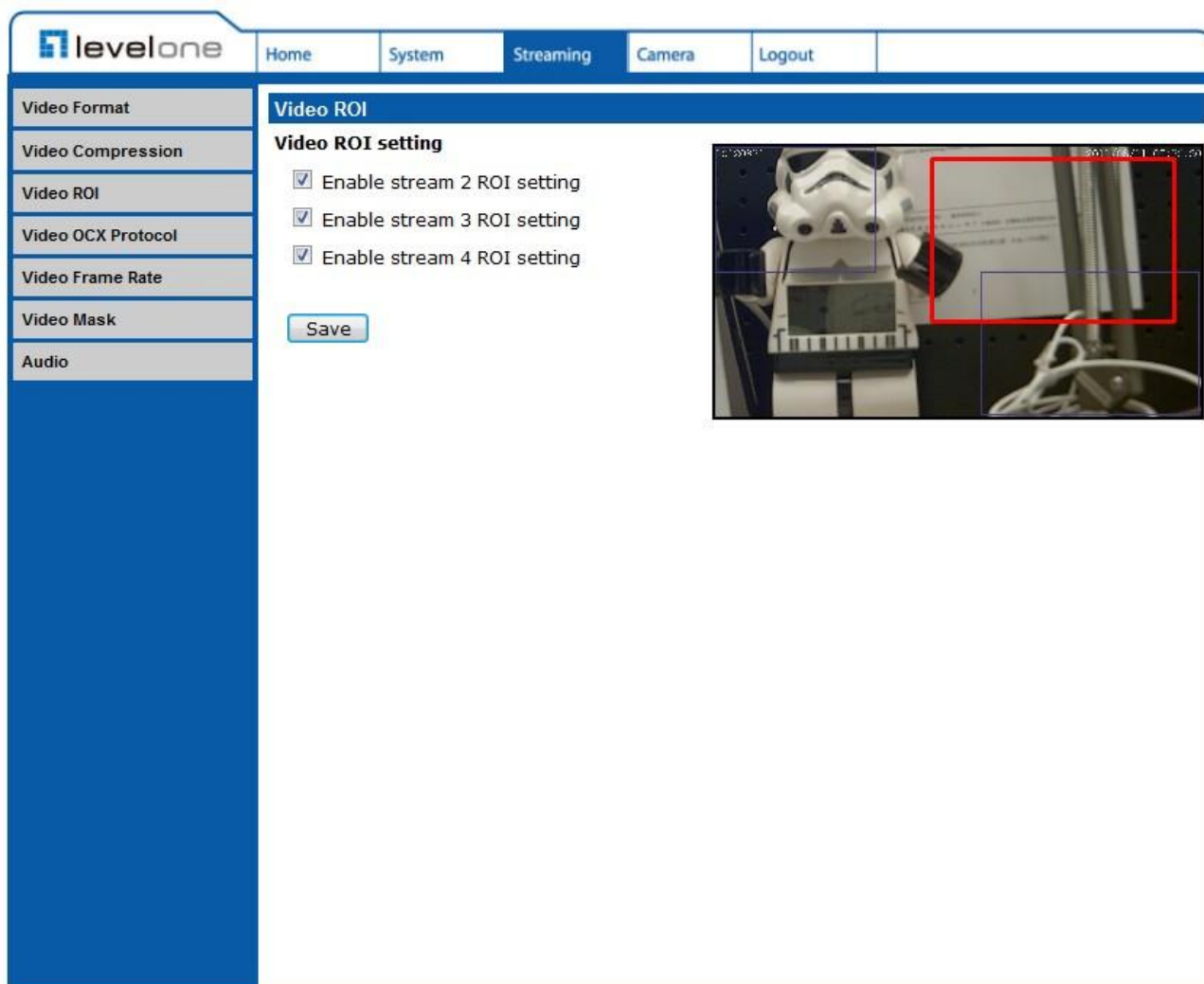
CBR Mode Setting

The CBR (Constant Bit Rate) mode could be the preferred bit rate mode if the bandwidth available is limited. It is important to take account of image quality while choosing to use CBR mode.

Click on <Save> to confirm the setting.

5.4.3 Video ROI

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



ROI stands for Region of Interest. This function allows users to select specific monitoring region for 2nd, 3rd and 4th streams, instead of showing the full image.



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

Video ROI Setting

◆ Enable Stream 2 ROI Setting

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

◆ **Enable Stream 3 ROI Setting**

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

◆ **Enable Stream 4 ROI Setting**

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

5.4.4 Video OCX Protocol

The Video OCX Protocol setting can be found under this path: Streaming> Video OCX Protocol.

The screenshot shows the 'levelone' web interface. The top navigation bar includes 'Home', 'System', 'Streaming', 'Camera', and 'Logout'. The left sidebar lists various settings: 'Video Format', 'Video Compression', 'Video ROI', 'Video OCX Protocol' (which is highlighted), 'Video Frame Rate', 'Video Mask', and 'Audio'. The main content area is titled 'Video OCX Protocol' and contains the following settings:

- Video OCX protocol setting :**
 - ☒ RTP over UDP
 - ☐ RTP over RTSP(TCP)
 - ☐ RTSP over HTTP
 - ☐ MJPEG over HTTP
 - ☐ Multicast mode
- Multicast IP Address:
- Multicast H.264-1 Video Port:
- Multicast H.264-2 Video Port:
- Multicast H.264-3 Video Port:
- Multicast H.264-4 Video Port:
- Multicast MJPEG Video Port:
- Multicast Audio Port:
- Multicast TTL:
-

Note:
This page only applies to video streams going to a DC Viewer.

In the Video OCX protocol setting page, users can select RTP over UDP, RTP over RTSP (TCP), RTSP over HTTP or MJPEG over HTTP for streaming video over the network. In the case of multicast networking, users can select the Multicast mode. Click on <Save> to confirm the setting.

Video OCX protocol setting options include:

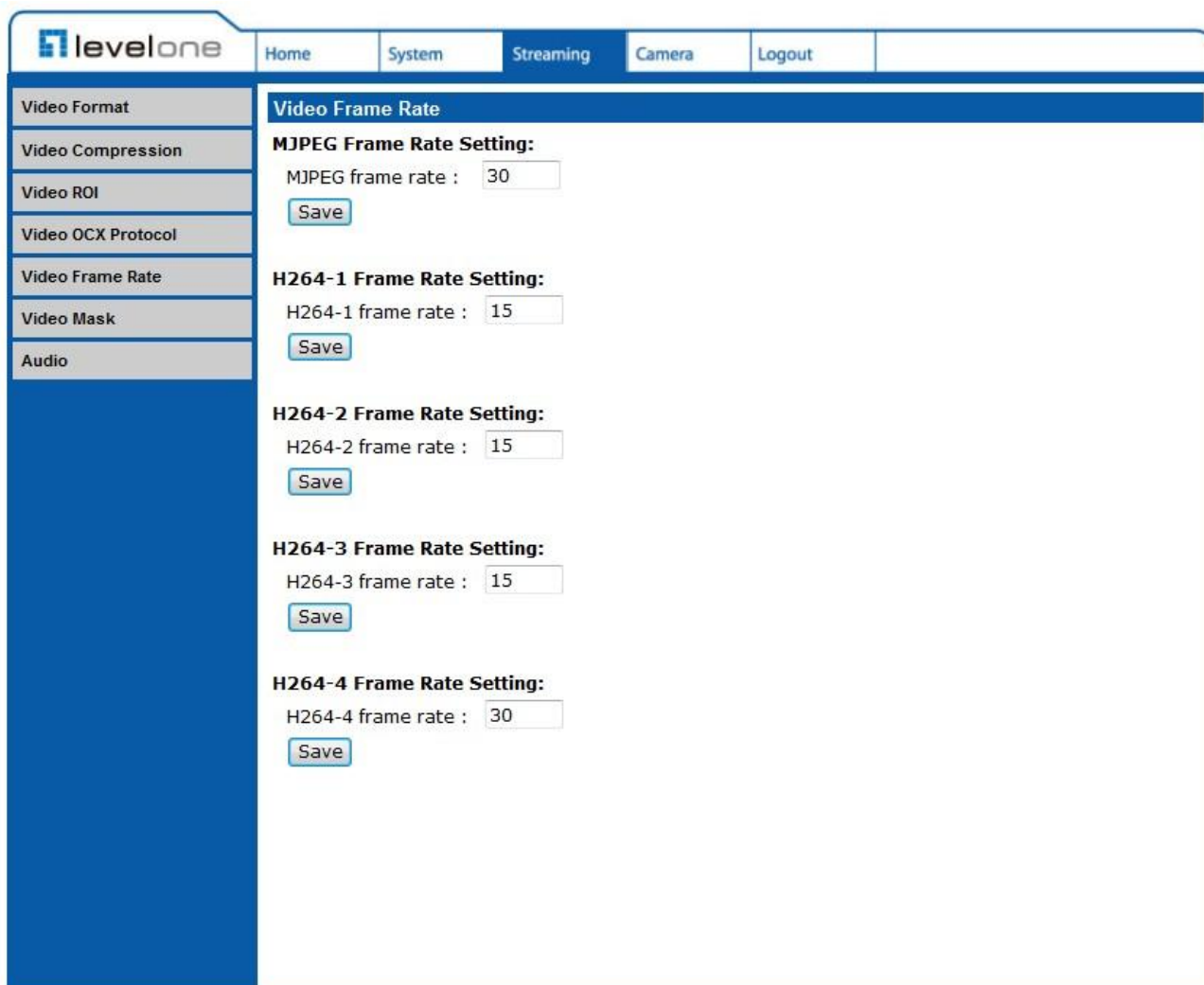
◆ **RTP over UDP / RTP over RTSP(TCP) / RTSP over HTTP / MJPEG over HTTP**

◆ **Multicast Mode**

Enter all required data, including <Multicast IP Address>, <Multicast H.264-1/ H.264-2/ H.264-3/ H.264-4 Video Port>, <Multicast MJPEG Video Port>, <Multicast Audio Port> and <Multicast TTL> into each blank.

5.4.5 Video Frame Rate

The Video Frame Rate setting can be found under this path: Streaming> Video Frame Rate.



The screenshot shows the LevelOne web interface. The top navigation bar includes links for Home, System, Streaming, Camera, and Logout. The left sidebar contains a menu with options: Video Format, Video Compression, Video ROI, Video OCX Protocol, Video Frame Rate (selected), Video Mask, and Audio. The main content area is titled "Video Frame Rate" and contains the following settings:

- MJPEG Frame Rate Setting:**
MJPEG frame rate :
- H264-1 Frame Rate Setting:**
H264-1 frame rate :
- H264-2 Frame Rate Setting:**
H264-2 frame rate :
- H264-3 Frame Rate Setting:**
H264-3 frame rate :
- H264-4 Frame Rate Setting:**
H264-4 frame rate :

Video frame rate is for setting the frames per second (fps) if necessary.

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

The default setting of MJPEG/H.264-1/H.264-2/ H.264-3/ H.264-4 Frame Rate is 30 fps; the setting range is from 1 to 30.

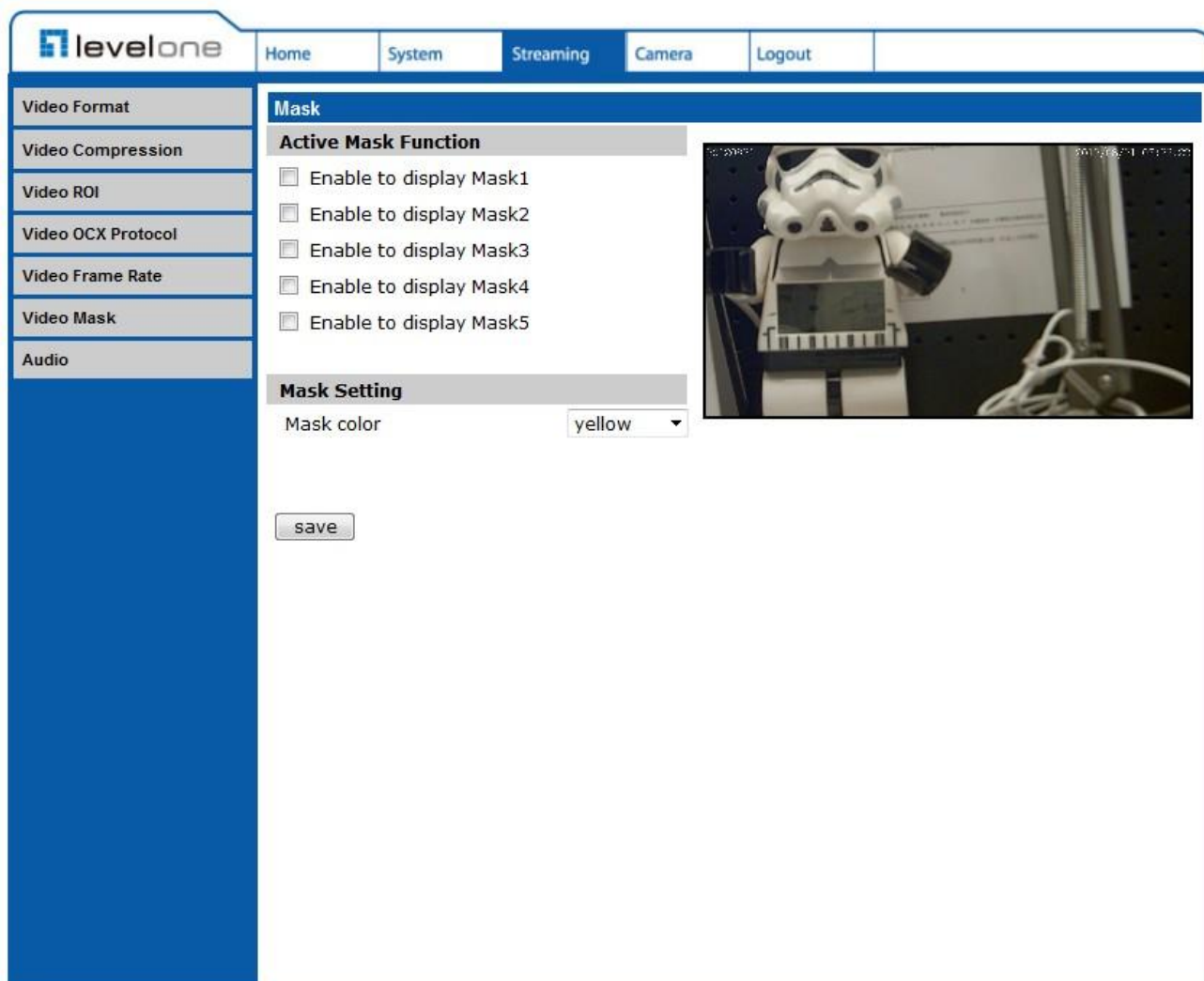
Click on <Save> to confirm the setting.



NOTE: Lower frame rate will decrease video smoothness.

5.4.6 Video Mask

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



Active Mask Function

◆ Add a Mask

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



NOTE: It is suggested to set the Video Mask twice bigger than the object.

◆ Cancel a Mask

Uncheck the checkbox of the Video Mask meant to be deleted, and the selected mask will disappear from the Live Video pane instantly.

Mask Setting

◆ Mask color

The selections of Mask color include red, black, white, yellow, green, blue, cyan, and magenta. Click on <Save> to confirm the setting.

5.4.7 Audio (Audio Mode and Bit Rate Settings)

The Audio Mode setting can be found under this path: Streaming> Audio.

The screenshot shows the 'levelone' web interface. The top navigation bar includes the logo and links for Home, System, Streaming, Camera, and Logout. The left sidebar lists various settings: Video Format, Video Compression, Video ROI, Video OCX Protocol, Video Frame Rate, Video Mask, and Audio. The 'Audio' section is selected, displaying the following configuration options:

- Transmission Mode:** Radio buttons for Full-duplex (Talk and listen simultaneously), Half-duplex (Talk or listen, not at the same time), Simplex (Talk only), Simplex (Listen only), and Disable (selected).
- Server Gain Setting:** Input gain and Output gain, both set to 3 via dropdown menus.
- Bit Rate:** Set to uLAW via a dropdown menu.
- A **Save** button is located at the bottom of the settings area.

In the Audio page, the Administrator can select one transmission mode and audio bit rate.

Transmission Mode

◆ Full-duplex (Talk and Listen simultaneously)

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

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

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

◆ Simplex (Talk only)

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

◆ **Simplex (Listen only)**

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

◆ **Disable**

Select the item to turn off the audio transmission function.

Server Gain Setting

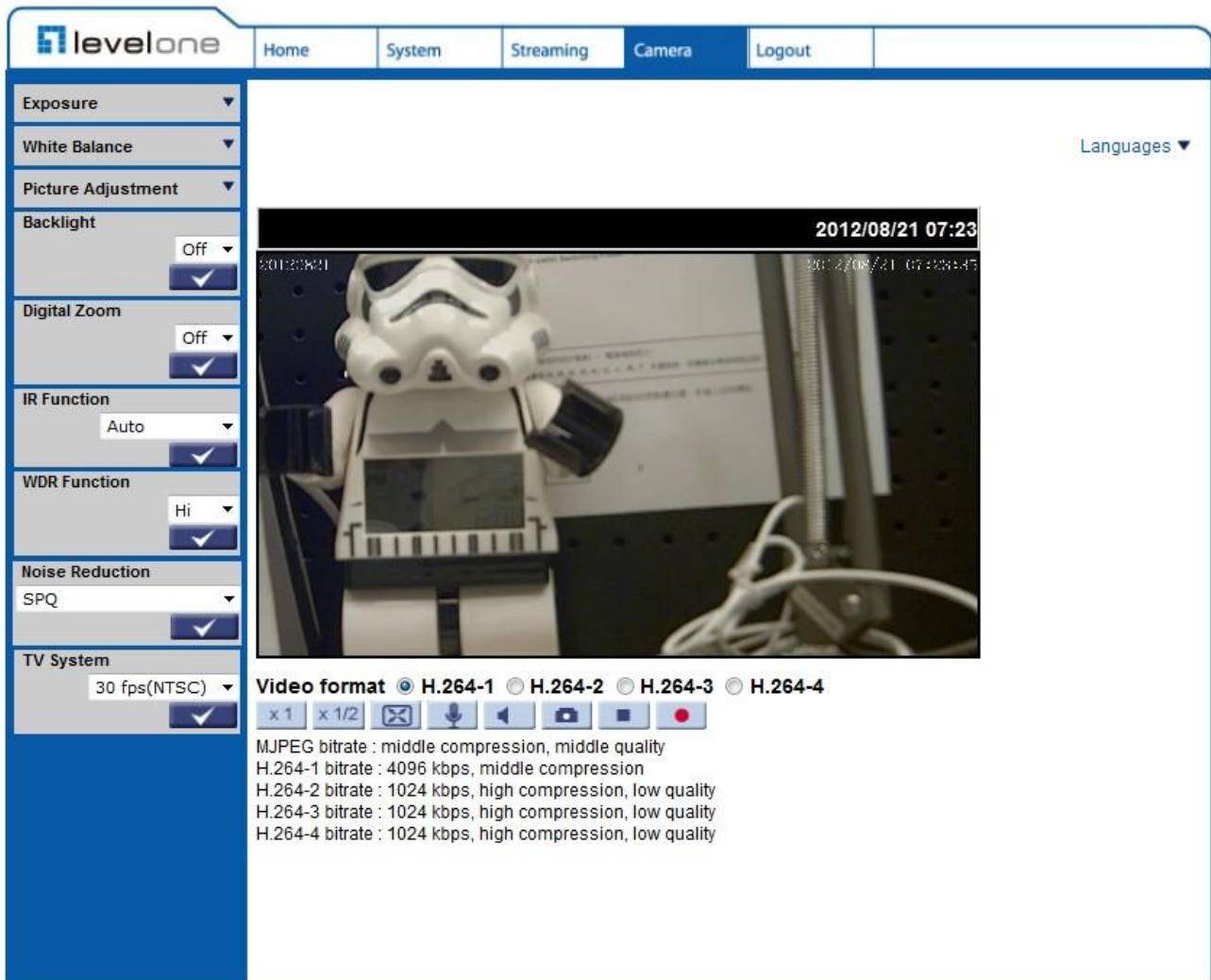
Set the audio input/output gain levels for sound amplification. The audio gain values are adjustable from 1 to 6. The sound will be turned off if the audio gain is set to "Mute".

Bit Rate

Selectable audio transmission bit rate include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), uLAW (G.711) and ALAW (G.711). Both uLAW and ALAW signify 64 kbps but in different compression formats. Higher bit rate will let higher audio quality and require bigger bandwidth. Click on <Save> to confirm the setting.

5.5 Camera

Under the tab <Camera>, there are submenus including: <Exposure>, <White Balance>, <Picture Adjustment>, <Backlight>, <Digital Zoom>, <IR Function>, <WDR Function>, <Noise Reduction>, and <TV System>.



The screenshot displays the LevelOne camera web interface. The top navigation bar includes links for Home, System, Streaming, Camera (selected), and Logout. A left sidebar contains a list of camera settings: Exposure, White Balance, Picture Adjustment, Backlight (set to Off), Digital Zoom (set to Off), IR Function (set to Auto), WDR Function (set to Hi), Noise Reduction (set to SPQ), and TV System (set to 30 fps(NTSC)). The main content area shows a live video feed of a Stormtrooper figure. Above the feed is a timestamp '2012/08/21 07:23'. Below the feed, there are video format options: H.264-1 (selected), H.264-2, H.264-3, and H.264-4. Below these are icons for zoom (x1, x1/2), pan, tilt, and other controls. At the bottom, there is a list of video formats and their corresponding bitrates and qualities.

2012/08/21 07:23

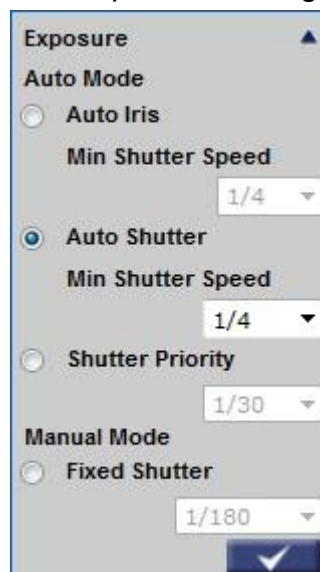
Video format ☒ H.264-1 ☐ H.264-2 ☐ H.264-3 ☐ H.264-4

x1 x1/2

MJPEG bitrate : middle compression, middle quality
H.264-1 bitrate : 4096 kbps, middle compression
H.264-2 bitrate : 1024 kbps, high compression, low quality
H.264-3 bitrate : 1024 kbps, high compression, low quality
H.264-4 bitrate : 1024 kbps, high compression, low quality

5.5.1 Exposure Setting

The Exposure Setting can be found under this path: Camera> Exposure.



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

Each exposure mode is specified as follows:

Auto Mode

◆ **Auto Iris (Fixed Focal Lens Excluded)**

In this mode, the exposure gives priority to the auto iris. The minimum shutter speed can be set from 1 (1/1.5) to 1/30 (1/25) sec. AGC (Auto Gain Control) will function automatically according to the light conditions of the subject.



NOTE: This function is not available for Fixed Focal Lens Models.

◆ **Auto Shutter Mode**

This function is to control the shutter speed and adjust the iris automatically according to the light intensity. It is also effective if a fixed iris lens is being used. The minimum shutter speed range is configurable from 1 (1/1.5) to 1/500 (1/425) sec.

◆ **Shutter Priority Mode**

This function is to set the shutter speed at a specified speed. The range is configurable from 1/30 (1/25) to 1/500 (1/425) sec.

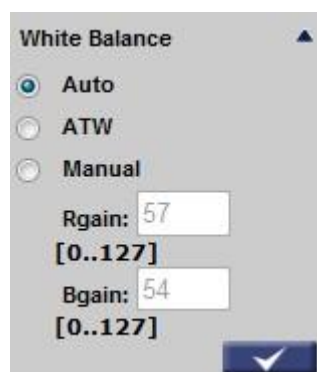
Manual Mode

◆ Fixed Shutter Mode

In this mode, fixed shutter speed could be selected from the dropdown menu. The shutter speed range is from 1/10000 to 1 (1/1.5) sec. with 19 (18) options. Users could select suitable shutter speed according to the environmental illumination.

5.5.2 White Balance Setting

The White Balance Setting can be found under this path: Camera> White Balance.



A camera needs to find reference color temperature, which is a way of measuring the quality of a light source, for calculating all the other colors. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance Control modes according to the operating environment. The following table shows the color temperature of some light sources for reference. Click on \checkmark to confirm the new setting.

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

Auto Mode (Auto White Balance)

The Auto White Balance mode is suitable for environment with light source having color temperature in the range roughly from 2700 ~ 7800K.

ATW Mode (Auto Tracking White Balance)

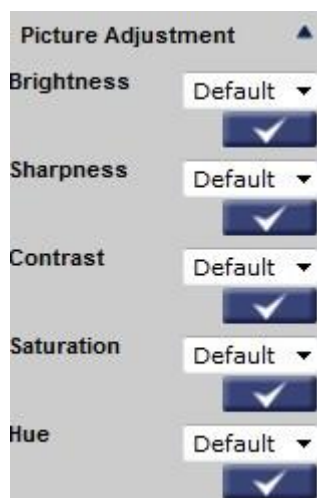
With Auto Tracking White Balance function, the white balance in a scene will be automatically adjusted while temperature color is changing. The ATW Mode is suitable for environment with light source having color temperature in the range roughly from 2500 ~ 10000K.

Manual Mode

In this mode, users can change the White Balance value manually. Users can select a number between 0 ~127 of “Rgain/ Bgain” item to gain the red/ blue illuminant on the Live Video Panel.

5.5.3 Picture Adjustment

The Picture Adjustment can be found under this path: Camera> Picture Adjustment.



Brightness

Users can adjust the image's brightness by adjusting the item. Please select ranging from -12 to +13. To increase video brightness, select a bigger number. Click on <√> to confirm the new setting.

Sharpness

Increasing the sharpness level can make the image looked sharper; especially enhance the object's edge. Please select ranging from +0 to +15. Click on <√> to confirm the new setting.

Contrast

Camera image contrast level is adjustable; please select ranging from -6 to +19. Click on <√> to confirm the new setting.

Saturation

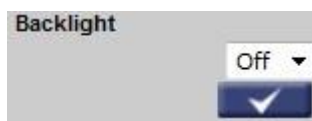
Camera image saturation level is adjustable; please select ranging from -6 to +19. Click on <√> to confirm the new setting.

Hue

Camera image hue level is adjustable; please select ranging from -12 to +13. Click on <√> to confirm the new setting.

5.3.4 Backlight

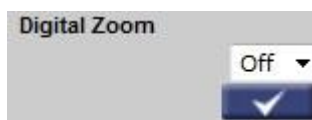
The Backlight Setting can be found under this path: Camera> Backlight.



The Backlight Compensation function prevents the center object from being too dark in surroundings where excessive light is behind the center object. Click on < √ > to confirm the new setting.

5.3.5 Digital Zoom

The Digital Zoom Setting can be found under this path: Camera> Digital Zoom.



The camera's digital zoom is adjustable from x2 to x8. Click on < √ > to confirm the new setting.

5.3.6 IR Function

The IR Function Setting can be found under this path: Camera> IR Function.



Auto/On/Off Mode

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

5.3.7 WDR Function

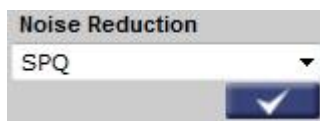
The WDR Function Setting can be found under this path: Camera> WDR Function.



The Wide Dynamic Range (WDR) function is for solving high contrast or changing light issues so that enhances better video display. The WDR is adjustable from Low, Mid to Hi. Higher level of WDR represents wider dynamic range, so that the IP Camera can catch a greater scale of brightness. Click on < √ > to confirm the new setting.

5.3.8 Noise Reduction

The Noise Reduction Setting can be found under this path: Camera> Noise Reduction.



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

Different level options for 3D Noise Reduction (3DNR) include Low, Mid and High. Higher level of 3DNR generates relatively enhanced noise reduction.

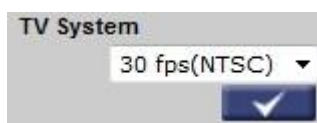
The proprietary Smart Picture Quality (SPQ) video processing method could drastically minimum motion blur and reduce noise especially in low-light environment. The combination of SPQ and 3DNR at different level further yields exceptional video performance in various conditions.

The Noise Reduction function is configurable with the following options: 3DNR Low, 3DNR Mid, 3DNR Hi, SPQ, SPQ + 3DNR Low, SPQ + 3DNR Mid, to SPQ + 3DNR Hi.

Click on < ✓ > to confirm the new setting.

5.3.9 TV System Setting

The TV System Setting can be found under this path: Camera> TV System.



Select the video format that matches the present TV system. Click on < ✓ > to confirm the new setting.

5.4 Logout

Click on the tab <Logout> on the top of the page, and the login window will pop up. This enables log in with another user name.

Appendix A: Specifications

Camera		FCS-1131-V2
Image Sensor		1/2.7" Progressive CMOS
Effective Pixels		1920(H) x 1080(V)
Minimum Illumination		0.2 lux (Color) 0.02 lux (B/W)
White Balance		Manual / AWB/ ATW
Shutter Speed		1~ 1/10000 sec.
Lens		
Lens		C / CS Mount
Operation		
Multiple Languages		English / French / German / Italian / Korean / Simplified Chinese / Traditional Chinese / Russian
Image Setting	Backlight Compensation	On / Off
	White Balance	Auto / Manual
	Noise Reduction (3D)	On / Off
	Wide Dynamic Range	On / Off
	Privacy Mask	On / Off
	Brightness	Manual
	Exposure	Auto / Manual
	Sharpness	Manual
	Contrast	Manual
	Saturation	Manual
	Hue	Manual
	Digital Zoom	Support
	Motion Detection	On / Off
	Privacy Mask Type	Color
	ICR*	Auto / On / Off / Smart
	Tampering Alarm	On / Off
Audio	Two-way Audio	Line out, Line in / Mic in
	Compression	G.711 / G.726
Network		
Interface		RJ-45, 10/100 Mbps Ethernet
Video Compression		H.264 / MJPEG
Video Streaming		Dual Streams- H.264 + H.264 / MJPEG

		Quad Streams- H.264 + H.264 + H.264 + H.264/ MJPEG
Video Resolution		H.264- Full HD 1080P / SXGA / HD 720P / XGA / SVGA / D1 / VGA / CIF MJPEG- Full HD 1080P / SXGA / HD 720P / XGA / SVGA / D1 / VGA / CIF
Protocol		IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
Security		HTTPS / IP Filter / IEEE 802.1x
Alarm	Input	1 Set 5V 10kΩ pull up
	Output	1 Set Photo Relay Output 300V DC/AC
Event Notification		HTTP / FTP / SMTP
Micro SD		microSDHC 32GB support
Supported Web Browser		Internet Explorer (6.0+) / Chrome / Firefox / Safari
User Account		20
Password Levels		User and Administrator
Mechanical		
Lens Mounting		C / CS Mount
LED Indicator		Power / Link / ACT
Connectors	Auto Iris	DC Drive
	Alarm	4 Pin Terminal Block, Pitch 3.5 mm
	Power	DC jack
	Ethernet	RJ-45
	Analog Video	1.0 Vp-p / 75 Ω, BNC
	Audio	3.5mm Stereo Phone Jack
General		
Operating Temperature		-10°C ~ 50°C (14°F ~ 122°F)
Humidity		10% ~ 90%, No Condensation
Dimension		125 x 82 x 52 mm (L x W x H) w/o Lens
Weight		330 g (0.73 lb)
Power Source		DC 12V / PoE
Power Consumption		4W
Regulatory		CE / FCC / RoHS

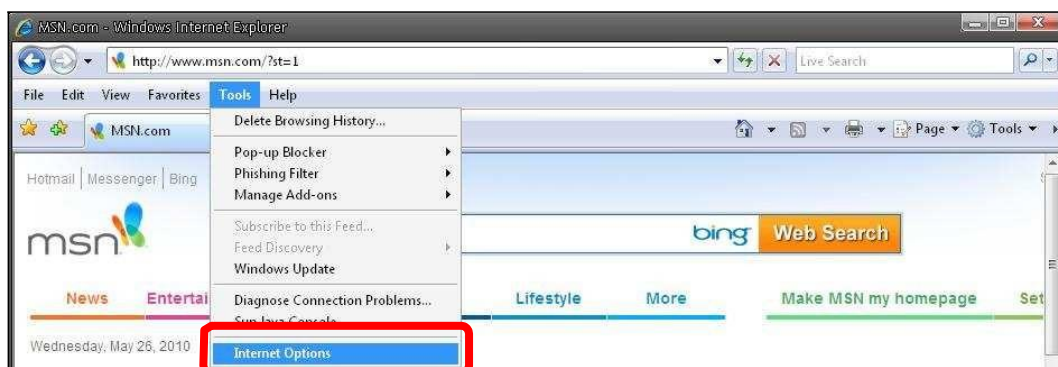
Appendix B: Internet Security Settings

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

Internet Security Level: Default

Step 1: Start the Internet Explorer (IE).

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



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



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

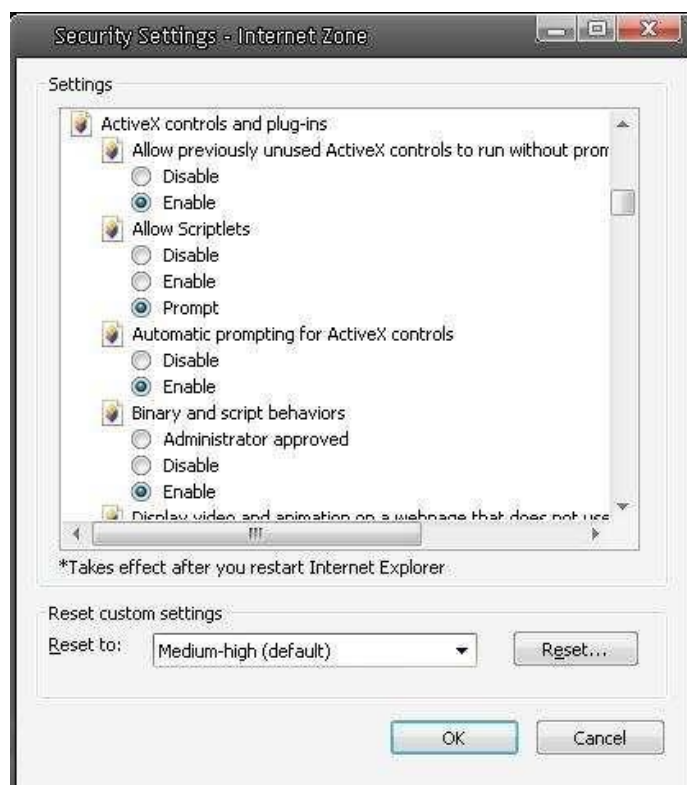
ActiveX Controls and Plug-ins Settings

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

Step 4: Down the page, press “Custom Level” (see the figure below) to change ActiveX controls and plug-ins settings.



The Security Settings screen is displayed as below:



Step 5: Under “ActiveX controls and plug-ins”, set ALL items (as listed below) to <Enable> or <Prompt>.

ActiveX controls and plug-in settings:

1. Automatic prompting for ActiveX controls
2. Binary and scrip behaviors
3. Download signed ActiveX controls
4. Download using ActiveX controls
5. Initialize and script ActiveX not marked as safe
6. Run ActiveX controls and plug-ins
7. Script ActiveX controls marked safe for scripting

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

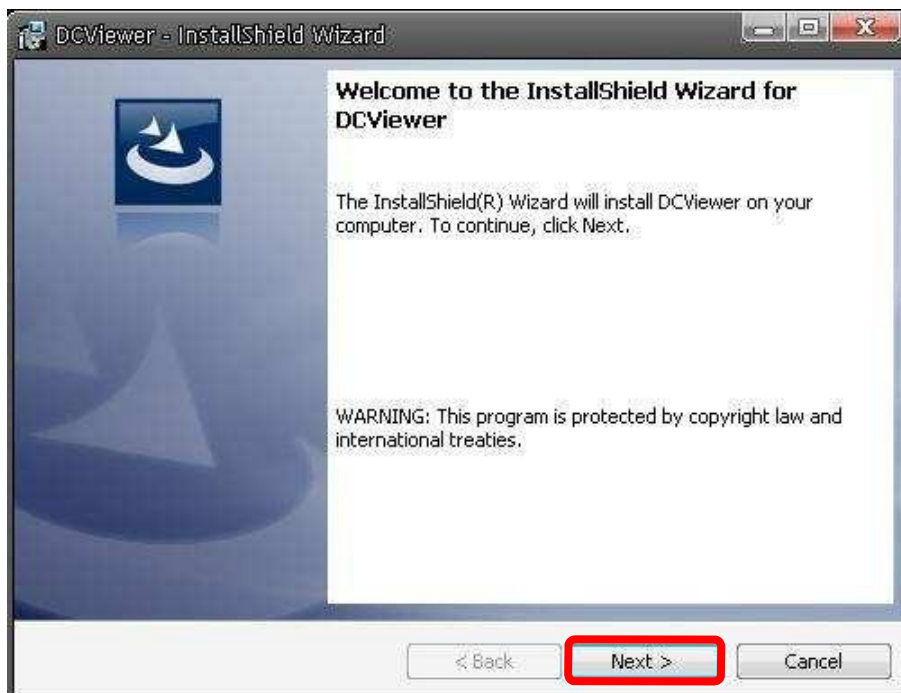
Step 7: Click <OK> to close the Internet Options screen.

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

Appendix C: DC Viewer Download Procedure

The procedure of DC Viewer software download is specified as follows.

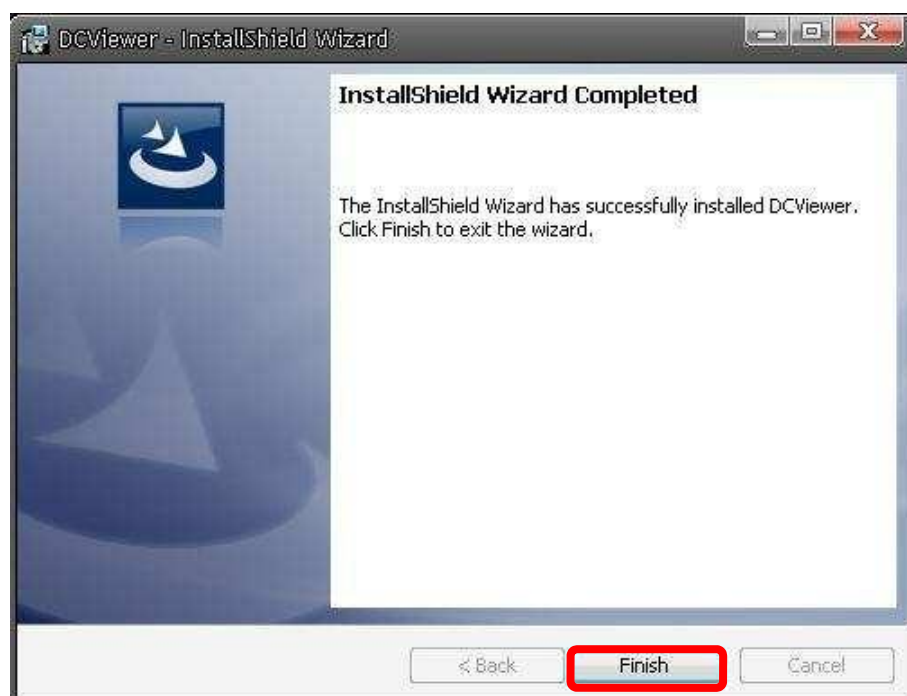
Step 1: In the DC Viewer installation page, click “Next” for starting installing.



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



Step 3: Click “Finish” to close the DC Viewer installation page.



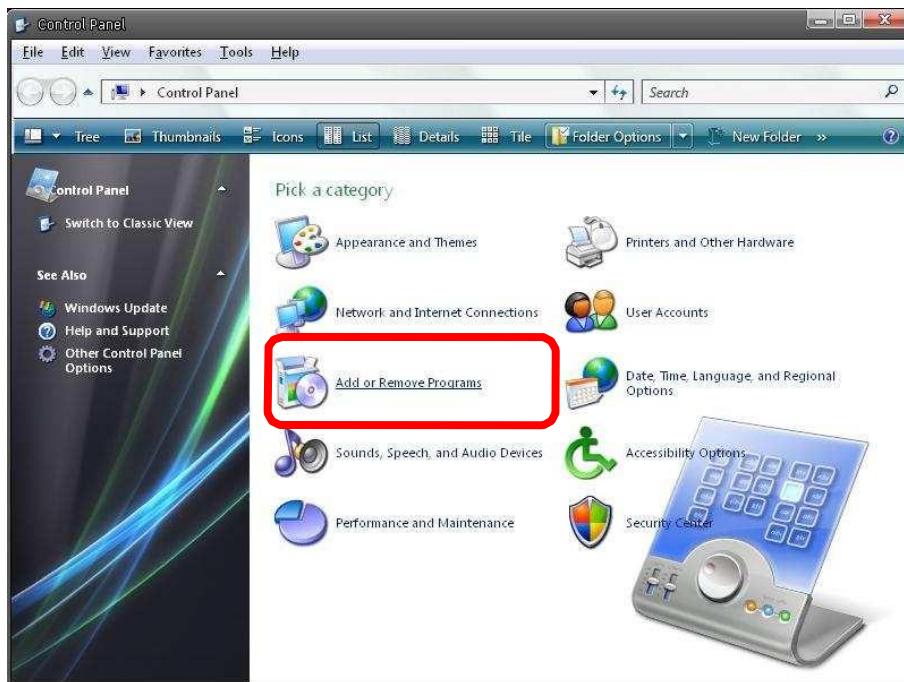
Then, the IP Camera's Home page will display as follows:



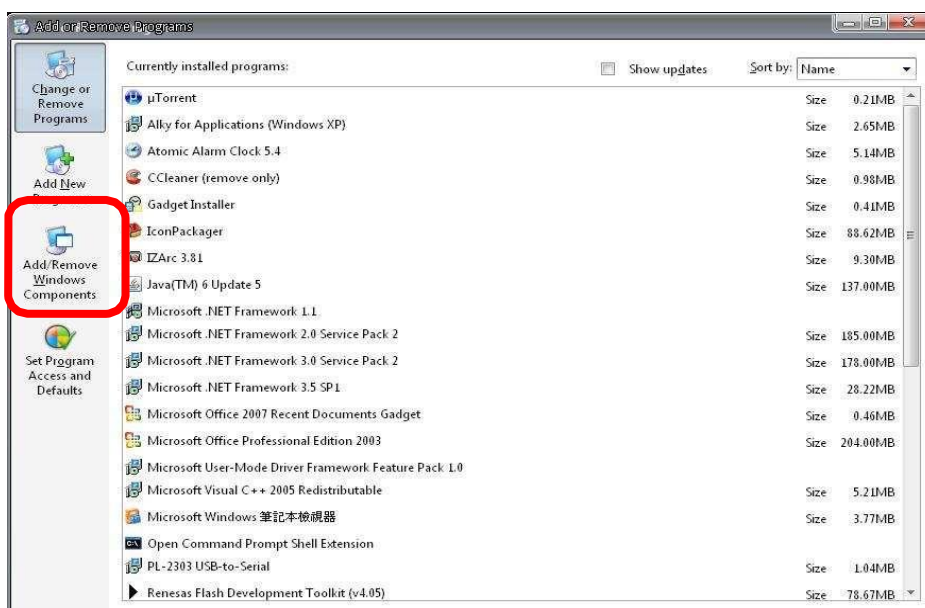
Appendix D: Install UPnP Components

Please follow the instructions below to install UPnP components.

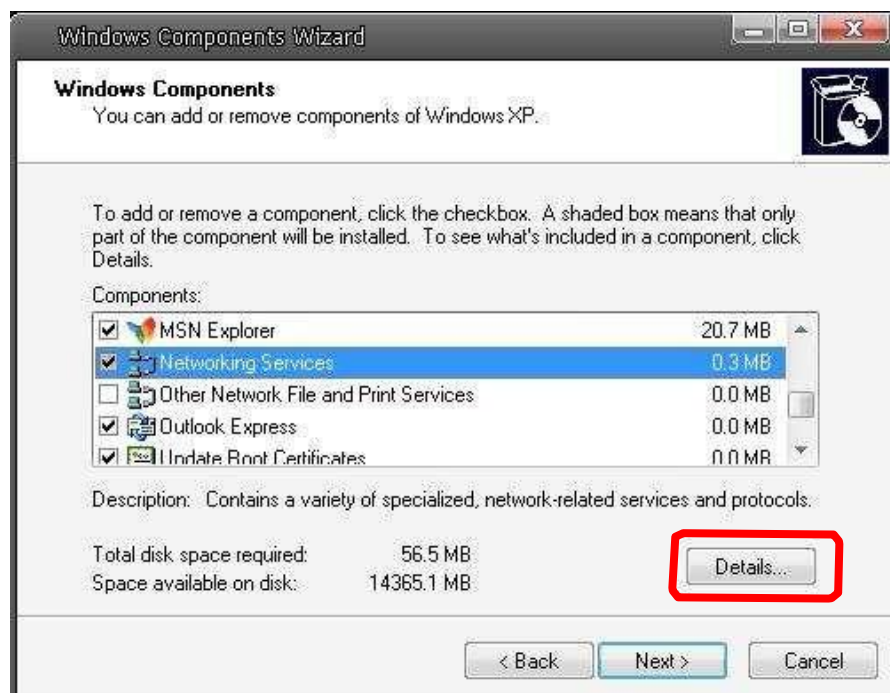
Step 1: Go to “Start”, click on “Control Panel”, and then double click “Add or Remove Programs”.



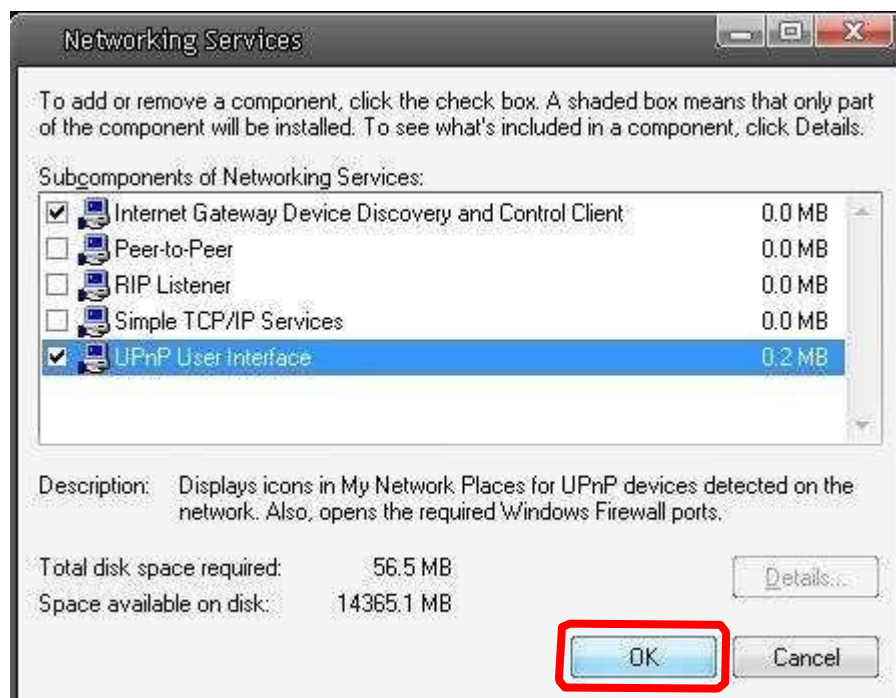
Step 2: Click on “Add/Remove Windows Components” in the Add or Remove Programs page..



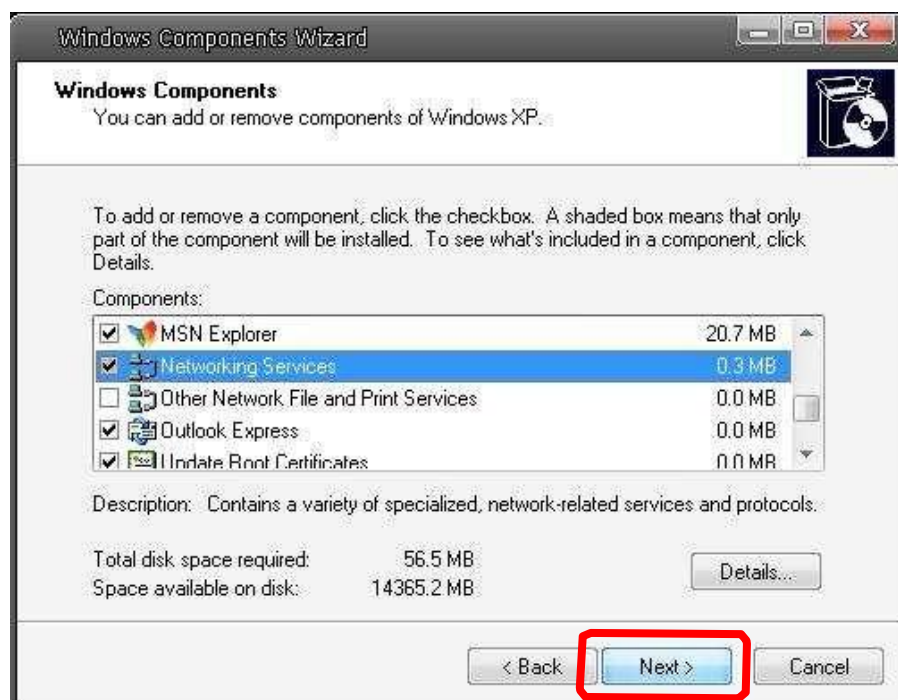
Step 3: Select “Networking Services” from the Components list in the Windows Components Wizard window, and then click “Details”.



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



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



Step 6: Click “Finish” to complete installation.

