![levelone®]

FCS-1151
2-Megapixel H.264 IP Camera
User's Manual

V1.0

Table of Contents

Overview

LevelOne FCS-1151 is a professional-series fixed network camera featuring superb image quality and exceptional bandwidth efficiency. It is especially suitable for wide open spaces such as building entrances and airports, or applications requiring accurate identification, such as human faces in banks or vehicle license plates in parking lots.

Featuring a 2-megapixel sensor, this camera is able to provide a wide field of view with exceptional detail when compared to a standard VGA camera, significantly reducing the number of camera installations. The ePTZ function enables users to focus on close-up shots of different areas in the camera's view without moving the camera physically. Users can quickly move to a target area by simply clicking on the video feed from the camera on their screen. In addition, the FCS-1151 can deliver user-defined thumbnails for viewing instead of video of an entire scene so as to optimize bandwidth and storage efficiency.

The FCS-1151 supports H.264 compression technology, drastically reducing file sizes and conserving valuable network bandwidth. With MPEG-4 and MJPEG compatibility, video streams can also be transmitted in either of these formats for versatile applications. The streams can also be individually configured to meet different needs or bandwidth constraints, thereby further reducing bandwidth and storage requirements. Users can receive multiple streams simultaneously in different resolutions, frame rates and image qualities for viewing on different platforms.

Thanks to its day and night function achieved by a built-in removable IR-cut filter, the FCS-1151 is able to maintain clear images 24 hours a day.

Additionally, the FCS-1151 camera incorporates an adjustment ring to improve lens compatibility with either C- or CS-mount lens, providing system integrators with more flexibility and hassle-free installation for different applications. The built-in SD/SDHC card slot offers a convenient and portable storage option to prevent data loss in case of network disconnection.

Data security with the FCS-1151 is further enhanced with HTTPS encryption and 802.1x authentication. Together with PoE, QoS, activity adaptive streaming, and the included 32-CH central management software, the FCS-1151 is indisputably the top choice for reliable and high performance surveillance.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.
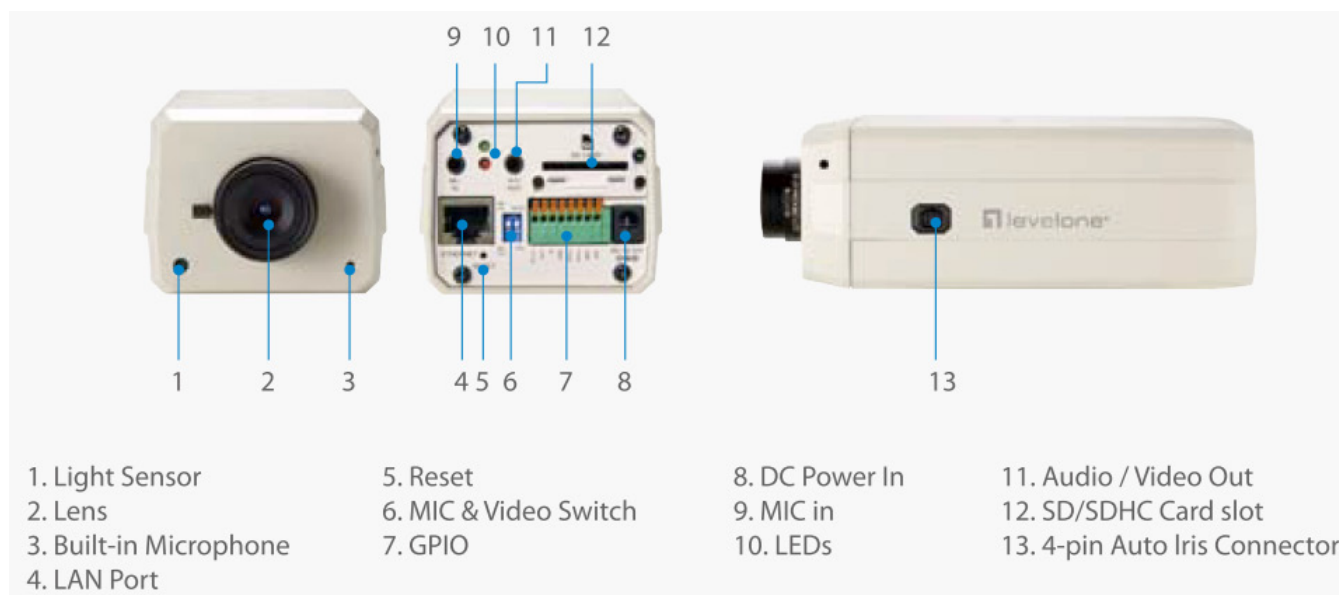
It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Package Contents

- FCS-1151
- Power Adapter
- Camera Stand
- CS-mount Lens
- Software CD
- Quick Installation Guide
- L-type Hex Key Wrench

Physical Description

1. Light Sensor	5. Reset	8. DC Power In	11. Audio / Video Out
2. Lens	6. MIC & Video Switch	9. MIC in	12. SD/SDHC Card slot
3. Built-in Microphone	7. GPIO	10. LEDs	13. 4-pin Auto Iris Connector
4. LAN Port			

General I/O Terminal Block

This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.
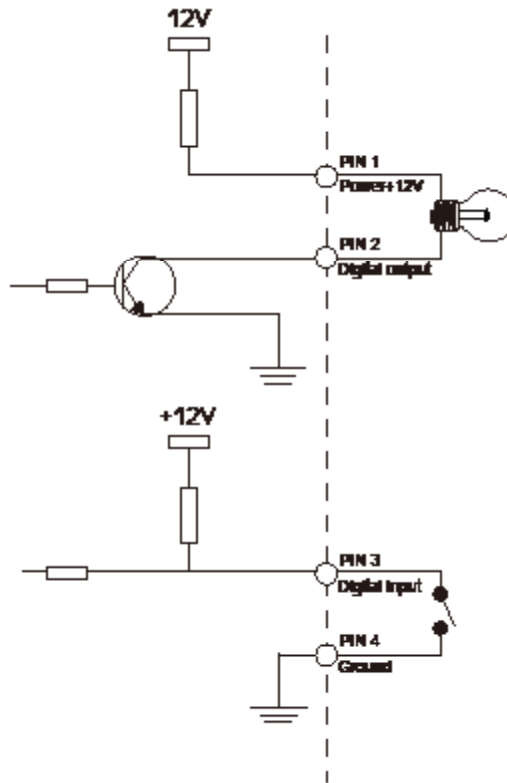
Pin	Name
1	Power +12V
2	Digital Output
3	Digital Input
4	Ground
5	AC 24V input
6	AC 24V input
7	RS-485 +
8	RS-485 -

DI/DO Diagram

Please refer to the following illustration for the connection method.

Status LED

The LED indicates the status of the Network Camera.

Item	LED status	Description
1	Steady Red	Power on and system booting
	Red LED unlighted	Power off
2	Steady Red + Blink Green every 1 sec.	Network works (heartbeat)
	Steady Red + Green LED unlighted	Network fail
3	Steady Red + Blink Green every 2 sec.	Audio mute (heartbeat)
4	Blink Red every 0.15 sec. + Blink Green every 1 sec.	Upgrading Firmware
5	Blink Red every 0.15 sec. + Blink Green every 0.15 sec.	Restore default

Hardware Reset

The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Reset: Press and release the recessed reset button with a paper clip or thin object. Wait for the Network Camera to reboot.

Restore: Press and hold the recessed reset button until the status LED rapidly blinks. It takes about 30 seconds. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

SD/SDHC Card Capacity

This network camera is compliant with **SD/SDHC 16GB / 8GB** and other preceding standard SD cards.

Installation
Hardware Installation

Follow the steps below to mount the lens to the Network Camera:
1. Mount the lens by turning it clockwise onto the camera mount until it stops. If necessary, turn the lens counterclockwise slowly until it gets the best attitude.
2. Connect the lens cable plug to the camera connector.

Network Deployment

Setting up the Network Camera over the Internet

This section explains how to configure the Network Camera to an Internet connection.
1. If you have external devices such as sensors and alarms, connect them to the general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.
3. Connect the power cable from the Network Camera to a power outlet.

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 10 for details.
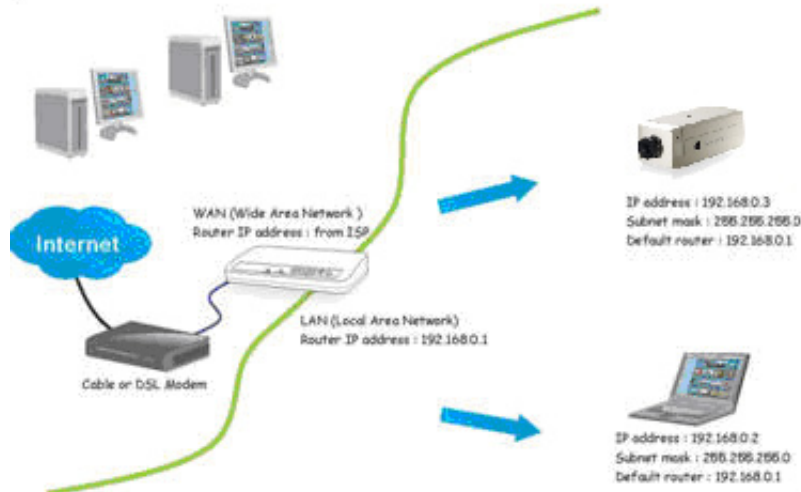
2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

■ HTTP port
■ RTSP port
■ RTP port for audio
■ RTCP port for audio
■ RTP port for video
■ RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 33 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN for details.

1. Set up the Network Camera in a LAN. Please refer to Software installation on latter pages for details.
2. Go to Configuration > Network > Network Type. Select LAN > Use fixed IP address.
3. Enter the static IP, Subnet mask, Default router, Primary DNS provided by your ISP.

Network Type

- ⊙ LAN
  - ○ Get IP address automatically
  - ⊙ Use fixed IP address
    - IP address: 60.248.39.146
    - Subnet mask: 255.255.255.240
    - Default router: 60.248.39.145
    - Primary DNS: 168.95.1.1
    - Secondary DNS: 192.168.0.20
  - Primary WINS server:
  - Secondary WINS server:
  - ☑ Enable UPnP presentation
  - ☐ Enable UPnP port forwarding
- ○ PPPoE
  - User name:
  - Password:
  - Confirm password:

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE for details.

Set up the Network Camera through Power over Ethernet (PoE)

When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via Ethernet cable.

power + data transmission
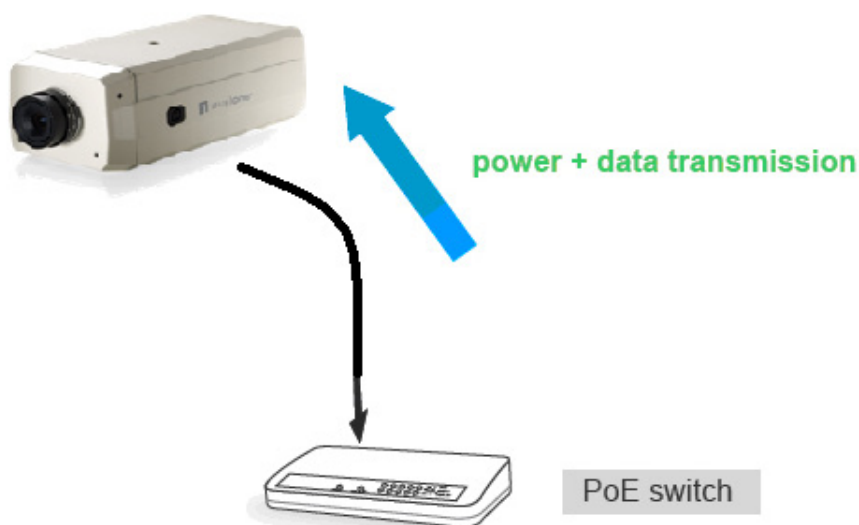
PoE switch

When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.

PoE power injector
(optional)

non-PoE switch
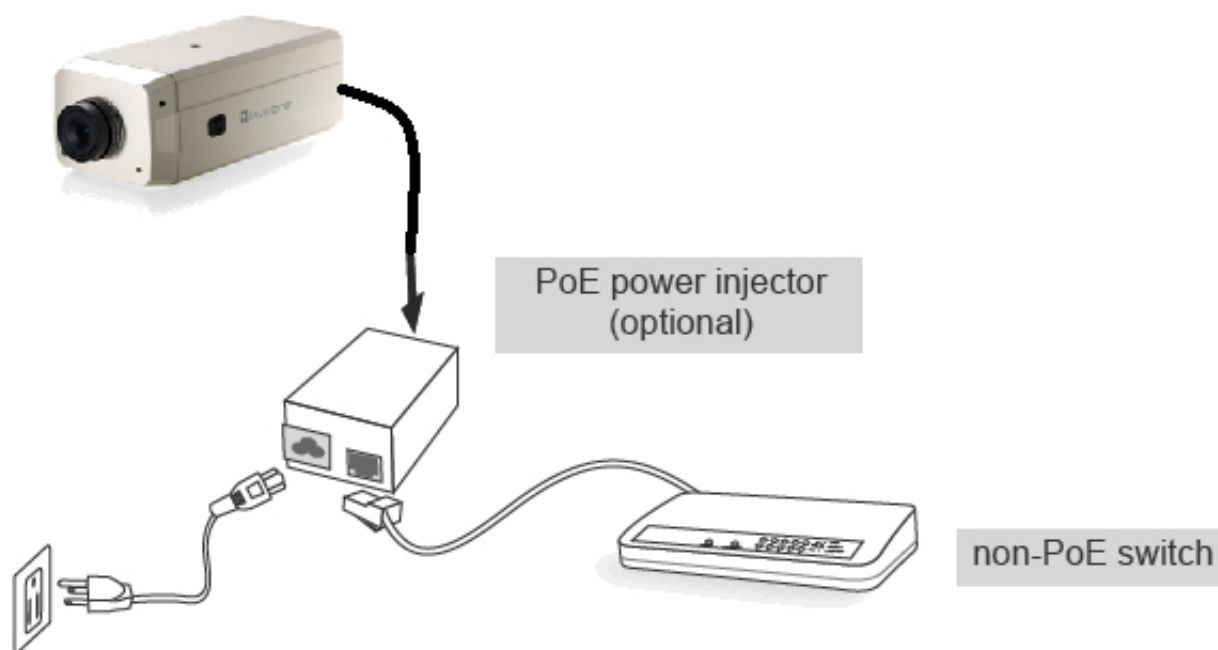
Software Installation

The following are steps for the software installation.

Note: The default user name is root and the password is blank

How to Use Installation Wizard

Installation
The following are steps for the software installation.

STEP. 1 Put the Installation disk into the CD-ROM drive, and the installation should start automatically. If the installation does not start, click on "Start" on the lower left corner of your screen, open "My Computer" and double click on the CD-ROM icon. The Installation Wizard Installation Window will appear.

STEP. 2 There are links on this page, including Install Software, User's Manual and Customer Homepage. Click on "Install Software" to enter Install Software page.
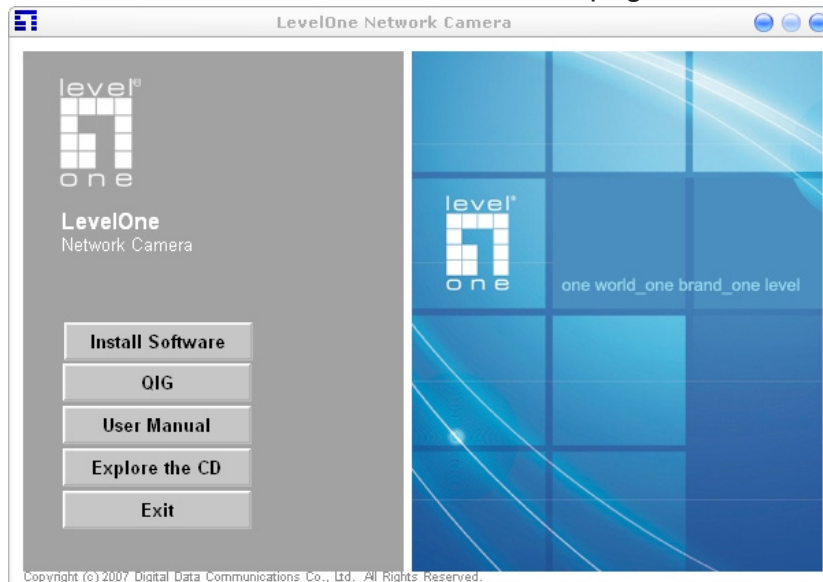
STEP. 3 There are links on this page, including Installation Wizard, User's Manual and Surveillance Software. Click on "Installation Wizard" to launch the setup program.
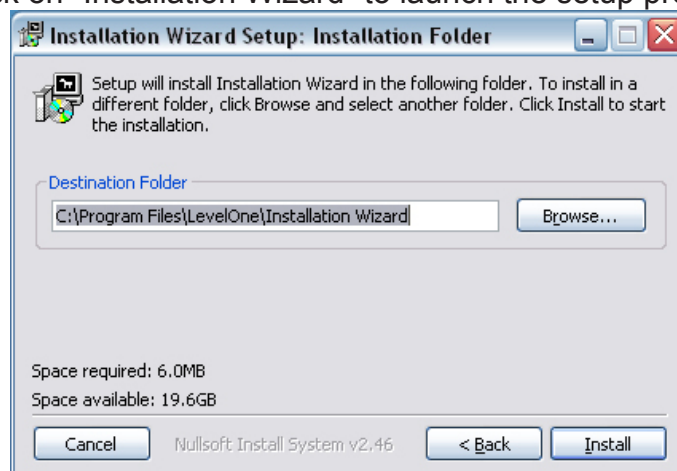
Destination Location for Installation

STEP 4: After clicking "Install" button, the install system will install the Installation Wizard to your computer, and a progress bar will display on the dialog. After completed the installation, please click on the "Close" button.
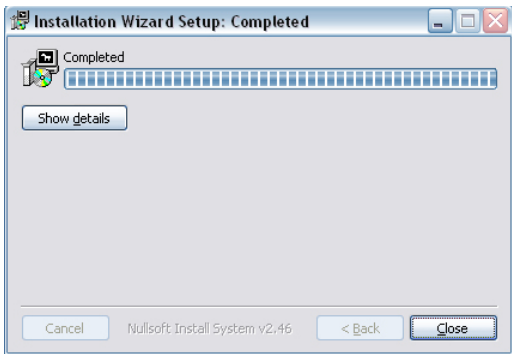
Completed

Using Installation Wizard

User Interface
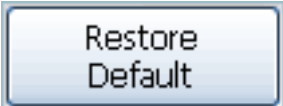
Once you run the Installation Wizard, after a short searching time, you will see the user interface as below. "**Manual Setup**" button, a "**Refresh Devices**" button and an arrow button on the left panel of your user interface. When you click on the arrow button, you will see more advanced functional buttons: "**Firmware Upgrade**", "**Restore Default**" and "**About IW**". You can select your device by double-clicking it in the device list. The left three buttons ("**Manual Setup**", "**Firmware Upgrade**", and "**Restore Default**") won't be enabled until you select at least one device.

Installation Wizard allows you to setup one device at one time and upgrade multiple devices (of the same model) at the same time. If you selected different models, then the "**Firmware Upgrade**" button would be disabled.

Installation wizard allows you to setup or upgrade multiple devices (of the same model) at the same time. If you selected different models, then the buttons will be disabled. There are five buttons on the bottom of the main page, and five buttons on the left panel of the main page.
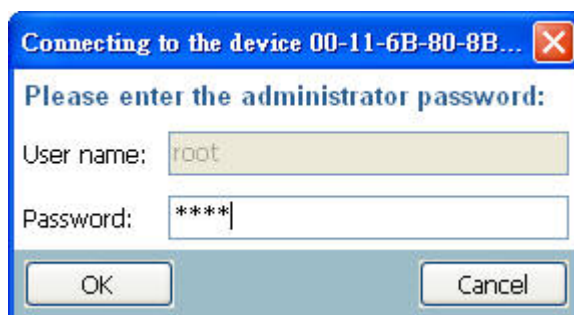
Buttons

Refresh Devices	Click on this button to clean up the device list and search all devices on the within the same subnet again. It will take about 5 seconds.
Manual Setup	Click on this button to modify the settings of the selected devices. For more detail, please refer to 0 Setup.
Firmware Upgrade	Click on this button to upgrade the firmware of the selected devices. For more detail, please refer to 0 Upgrade.
Restore Default	Click on this button to reset the selected devices to default settings.
About IW	Click on this button to get information about the Installation Wizard.

Manual Setup

When you select one device in the selection list, the "Manual Setup" button will be enabled. Click on it to modify the settings of the selected device. After clicked on the "Manual Setup" button, Installation Wizard would try to connect to the selected device.

The default Administrator's password is blank and the Network Camera initially will not ask for any password. If the authentication is failed, there would be a pop-up dialog window to ask for correct password. If you failed three times, the Installation Wizard would show you a warning dialog window and abort the connecting to the selected device.
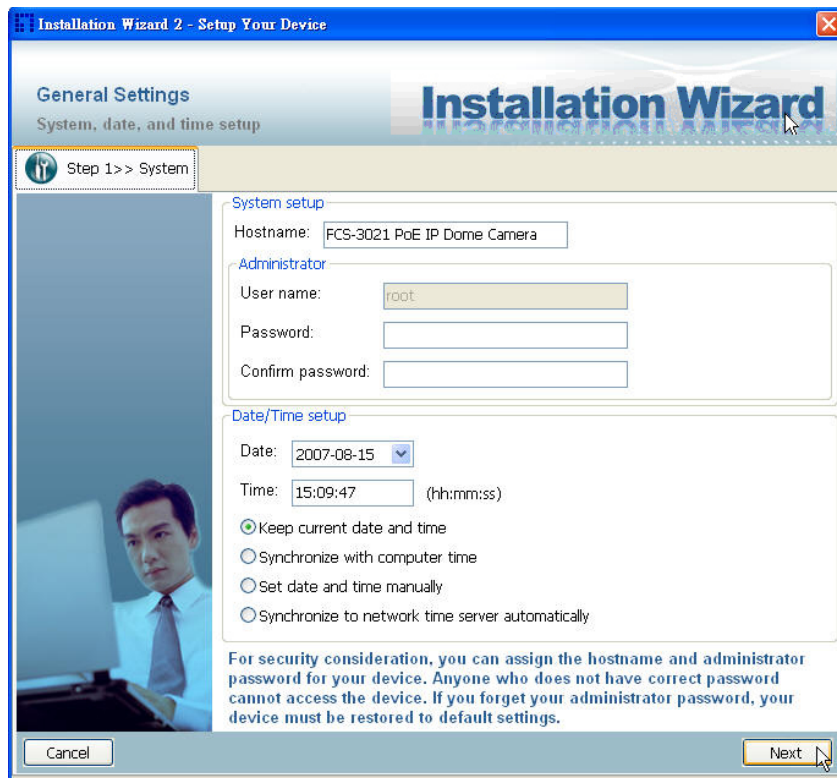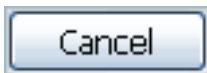
Authentication Dialog Window
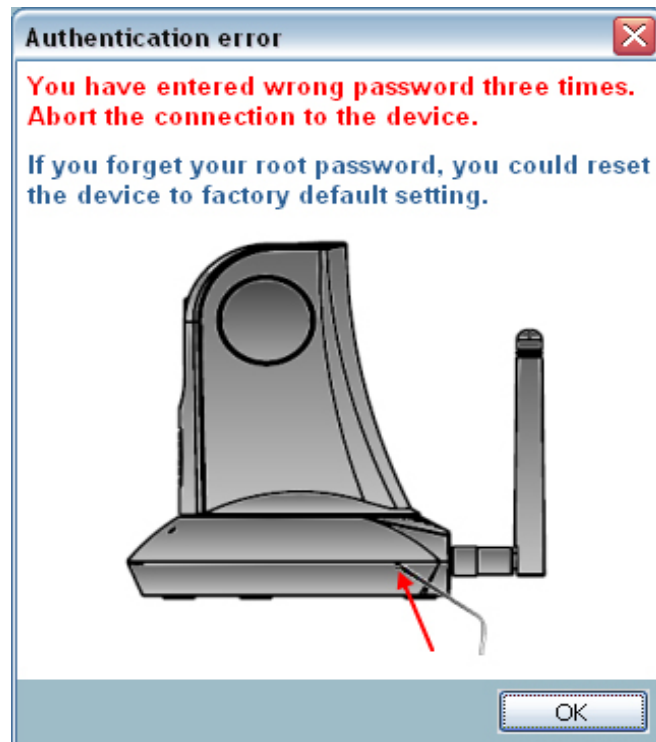
Authentication error

System Setting

After connected to the selected device, the Installation Wizard will switch to system setting page as below.

System setting page

 Click on this button to cancel the setup progress.

 Click on this button to keep the present setting and go to the next page.

Change Host Name

The "**Hostname**" is used for the homepage title of main page and is displayed as the title in the video window of the main page. The maximum string length is 40 characters or 20 characters in double-byte-character-systems like Chinese or Japanese. But for some models supported Unicode, the maximum string length depends on the characters you input, and it may less than 20 characters.

Change root password

To change the administrator's password, type the new password in both "**Password**" and "**Confirm Password**" text boxes identically. What is typed will be displayed as asterisks for security purposes. The maximum password depends on the server you connected.

Adjust date and time

Date/Time setup

There are three ways to adjust system date and time:

1.   "**Synchronize with computer time**": The easiest way is to make device synchronized with your computer time.
2.   "**Set date and time manually**": Set the date and time manually by entering new values. Notice the format in the related field while typing.
3.   "**Synchronize to network time server automatically**": Make device automatically synchronize with timeservers over the Internet every hour.

If you want to keep the current date and time, please choose "**Keep current date and time**".

Network Setting

The Installation Wizard can help you to setup the network connection with LAN or PPPoE. After you clicked on the "**Next**" button on the System page, the Installation Wizard would lead you to the PPPoE setting page. If you want to connect your server to Internet via PPPoE, please click on "Yes" to start the PPPoE setting process, or click on "**No**" to invoke the LAN setting.
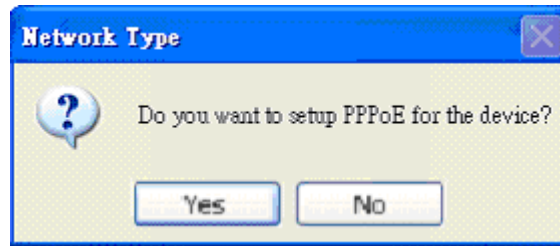

Choosing the network type

PPPoE Setting

Network setting for PPPoE

If you click on "**Yes**" in the "Network Type" dialog window, you will be led to the PPPoE setting page. In this page, you can input the "**PPPoE username**" and "**PPPoE password**" provided by your ISP, and then the server will be set to PPPoE mode rather than LAN mode when the setup is completed. If you don't know the account information, please contact your ISP. After inputting the account information, please click on the "**Next**" button to continue your next step.

LAN Setting

If you click on "No" in the "Network Type" dialog window, you will be led to the Network setting page. In this page, you can change the server's IP address, subnet mask, default gateway, primary DNS server, secondary DNS and DHCP server. Please refer to the below page.
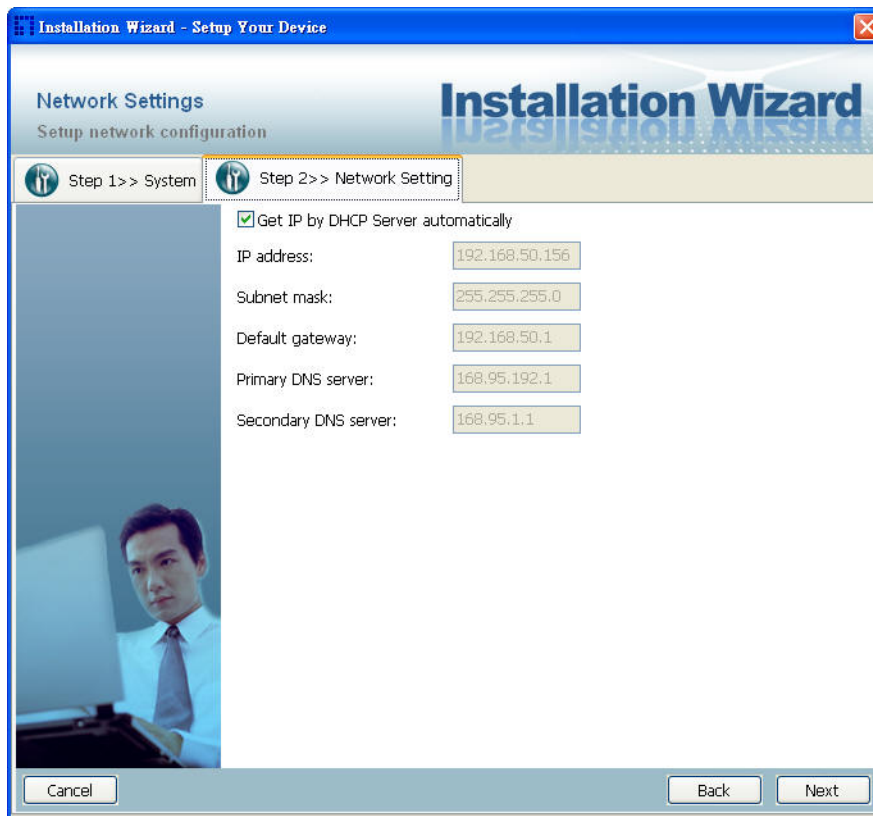
Network Setting for LAN

You could set up the network with DHCP or fixed IP:

1.DHCP: Check the "**Get IP by DHCP Server automatically**" will force the device to renew its IP address whenever it reboots, and the related network configuration is provided by the DHCP server.

2.Fixed IP: If you want the device to use a fixed IP, please uncheck the "**Get IP by DHCP Server automatically**" checkbox and assign a valid IP address, subnet mask, default gateway and DNS server for the device.

Mobile Access

After finished the DDNS setting and click on the Next button. If your device supports mobile viewer and you want to access the device by mobile phone, you can enable the "Mobile Access" by clicking on the Yes button. The Installation Wizard will do some setting for mobile viewing toward the device:

1.Video: The video codec will be set to MPEG-4, and the resolution will be set to 176x144 pixels.

2.Audio: The audio codec will be set to AAC.
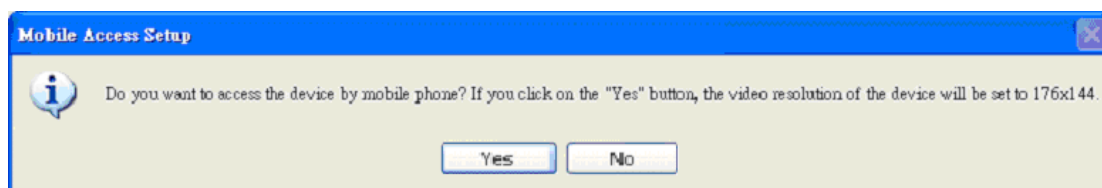
Mobile Access

Apply to selected device

After configuring all the settings, the apply page will show up. Click on "Apply" button to apply the changes to the selected device or click on "Back" button to go back to the previous page and modify the setting again.
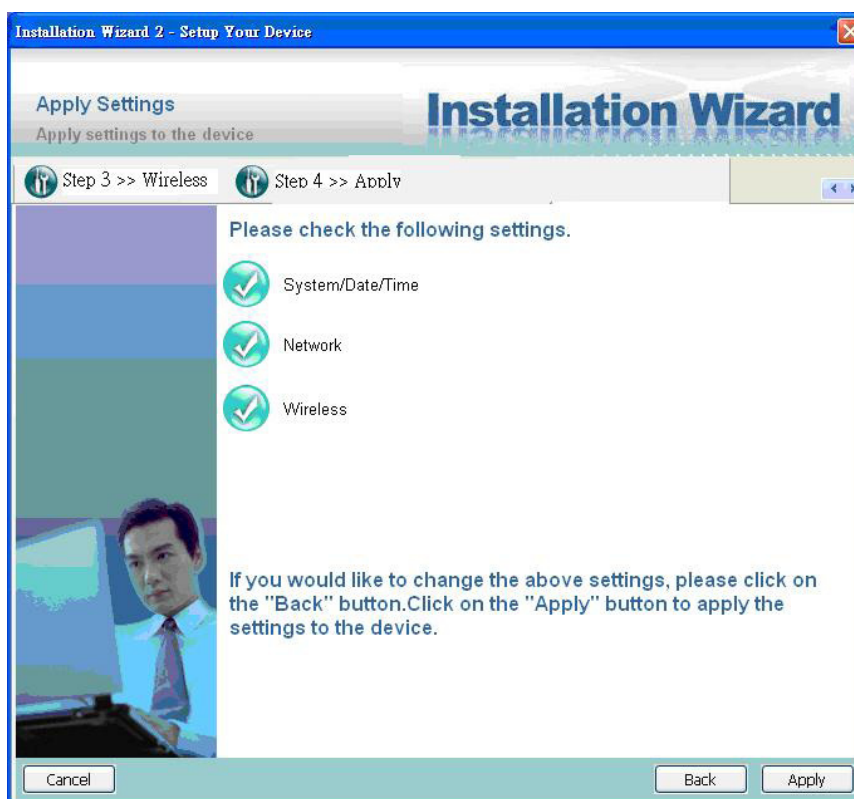
Apply page

When you click on the "Apply", it will start to update your settings to server.

Upgrade

When you select one device or multiple devices (of the same model), the "**Firmware Upgrade**" button will be enabled. Click on it to upgrade the firmware of the selected device(s). After click on the "**Firmware Upgrade**" button, Installation Wizard will try to connect the selected device(s) and lead you to the firmware upgrade page.

Click on the "Firmware Upgrade"

Device Information

After connected to the selected device(s), it would display as below. If you select more than one device, then the device information will show all the selected devices. You can switch to the server info by click on the tab control.
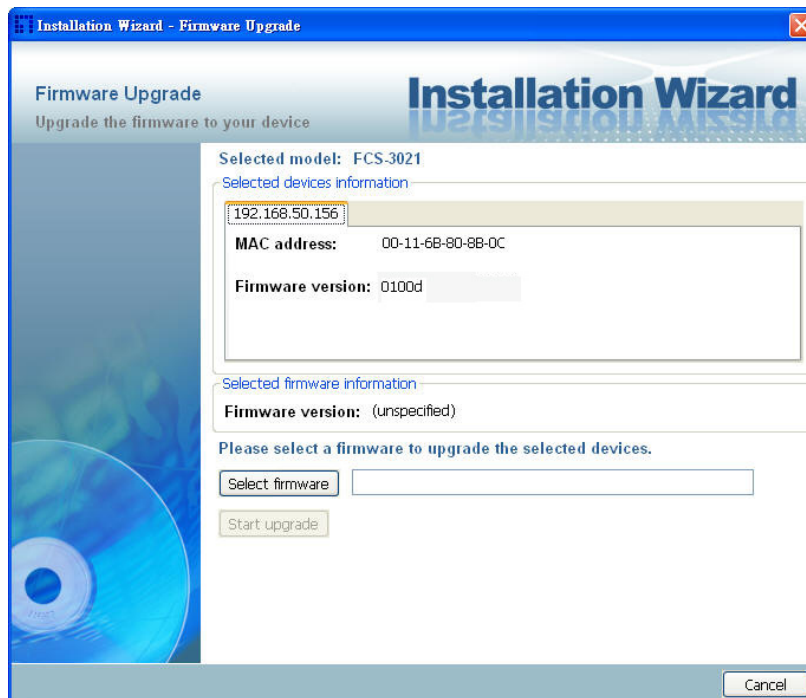
Device information
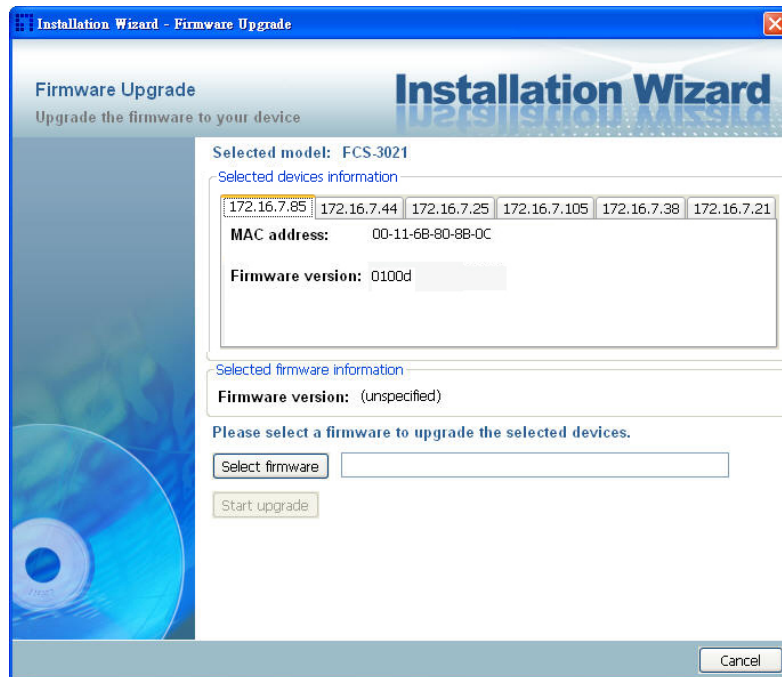
Multiple devices information

Firmware Information
The selected firmware information will show the information about the file that you selected.

Firmware version: The version number of the selected firmware.

Select Firmware
You can use the "Select firmware" button to browse the file that you want upgrade onto the selected device(s). After selected the file, Installation Wizard will check whether the file you selected is correct. If it's the correct version, then the package information will display the information about the file and enable the "Start Upgrade" button. Therefore you can click on the button to upgrade the firmware. If not, then it will be a pop-up warning message.
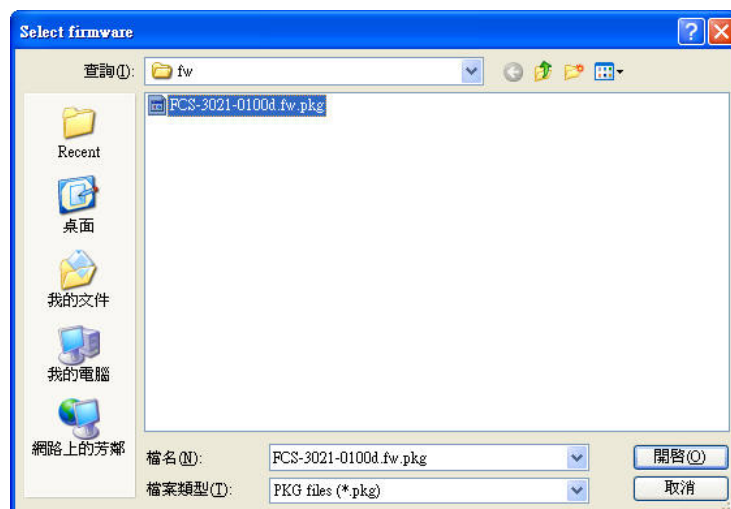
Select firmware
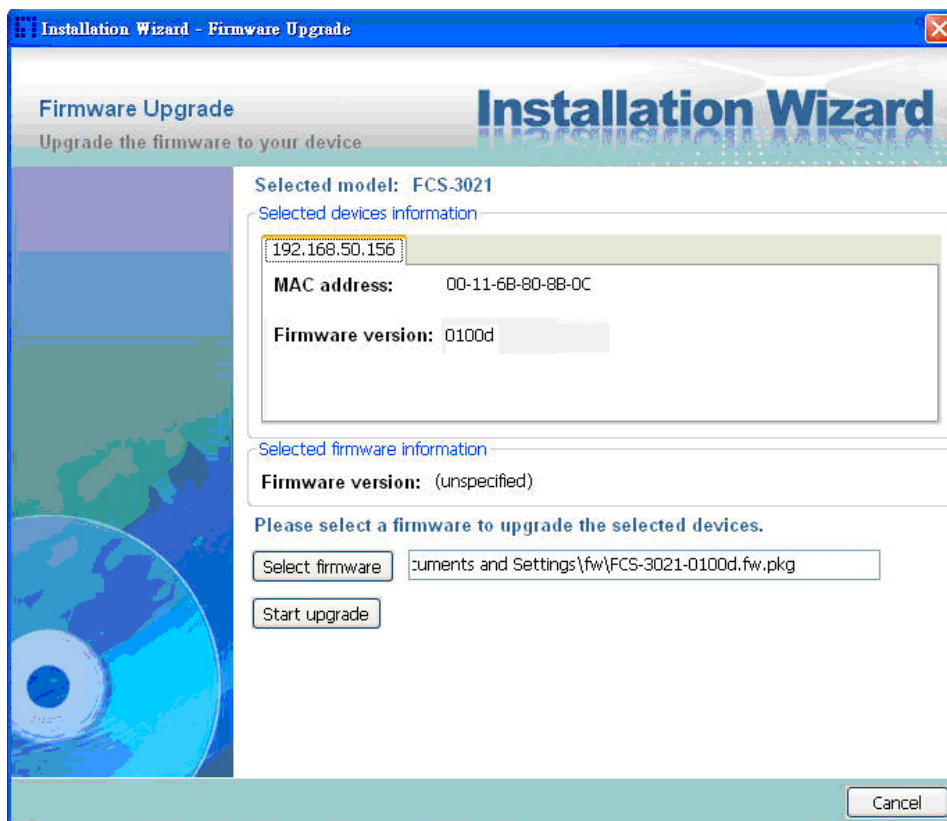
Firmware Information
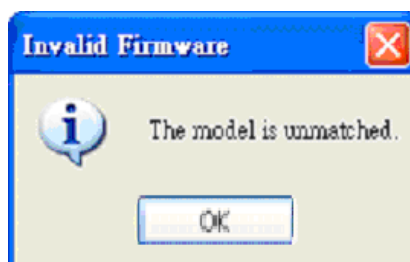
Warning message for unmatched firmware

Start Upgrade

Clicking on the "Start Upgrade" button to upgrade the firmware of the selected device(s), and it will be a pop-up dialog window to show the progress of the upgrading process. Usually, it will take about 5 to 10 minutes to finish the firmware upgrading. It depends on your server model and network bandwidth. We recommend you do the upgrade process in wired LAN environment rather than PPPoE or wireless environment.
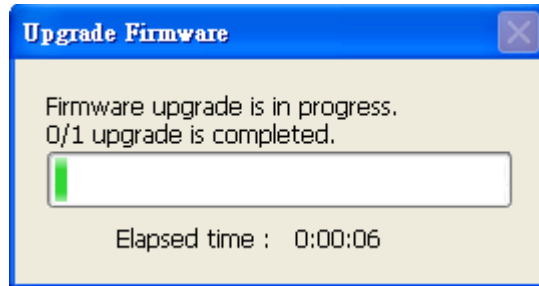
Update progress

After the upgrade process had been done, you could see the dialog window as below. Please click on the button "OK" to finish it.
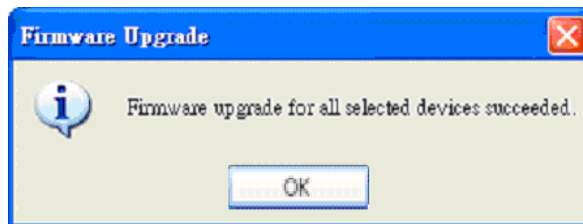
Upgrade Done

Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and LevelOne recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the LevelOne network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.
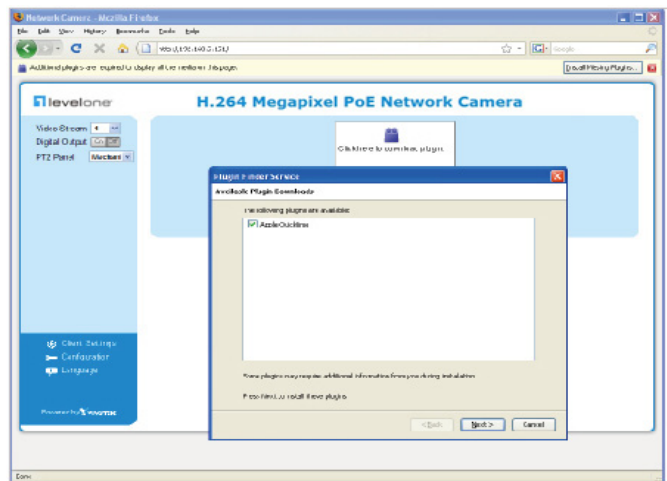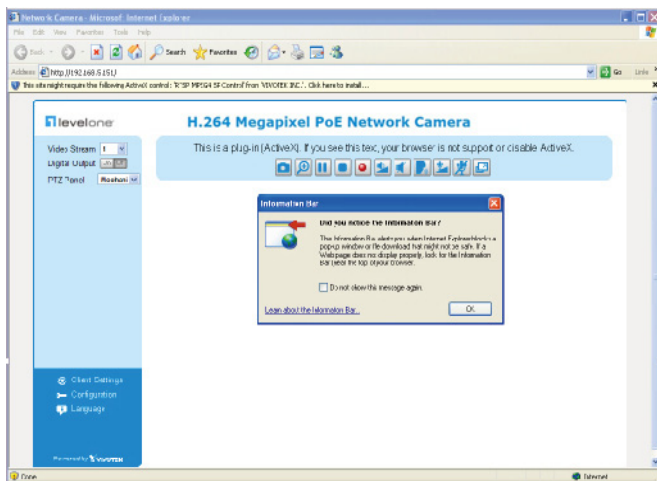
NOTE

► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you donn't have Quick Time on your computer, please download it first, then launch the web browser.*
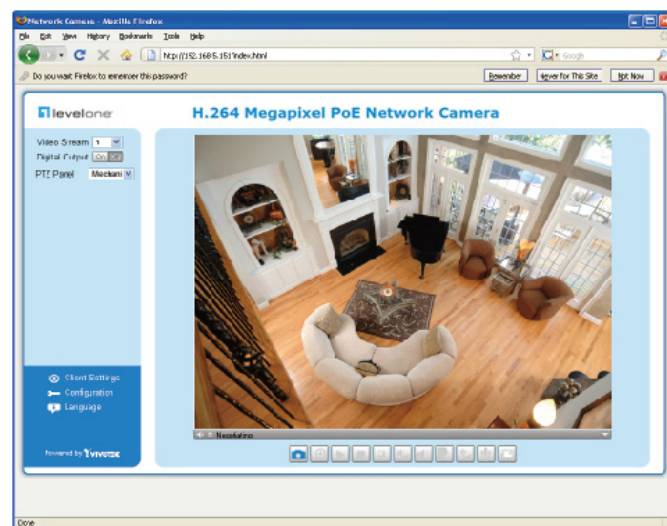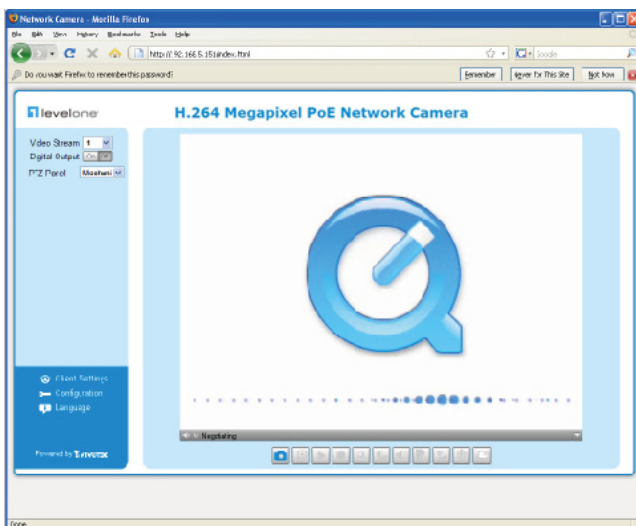
► By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.
For more information about how to enable password protection, please refer to Security on page 26.

► If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.

1. Choose Tools > Internet Options > Security > Custom Level.
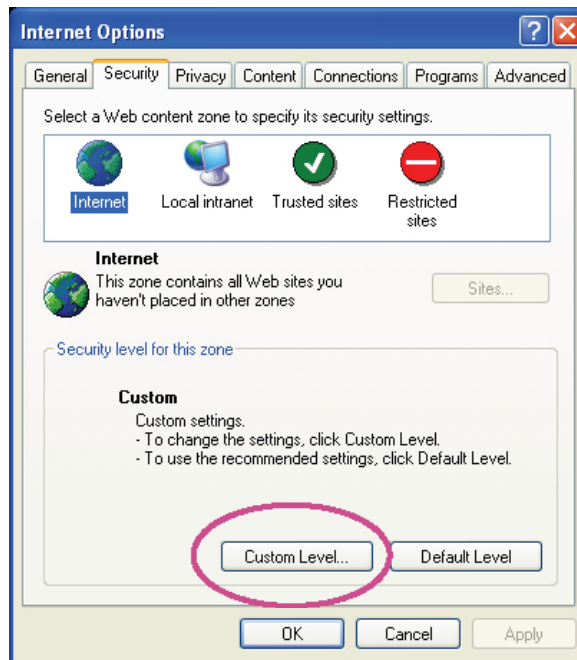
2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.
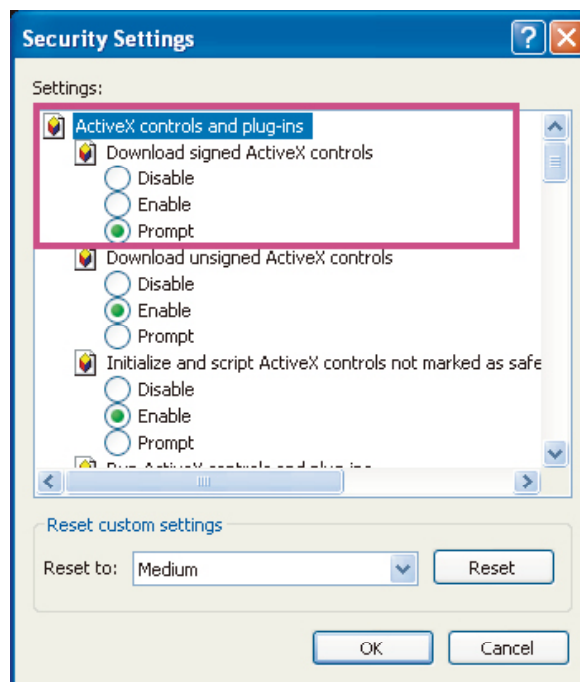
3. Refresh your web browser, then install the Active X® control. Follow the instructions to complete installation.

Using RTSP Players

To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 46.
For example:
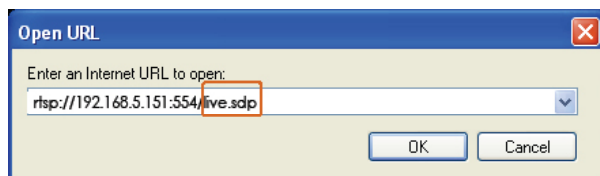
4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 46 for details.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 7.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 46.

2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Viewing Window on page 59.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 46.

4. Launch the player on the 3GPP-compatible mobile devices (ex. Real Player).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>.
   For example:
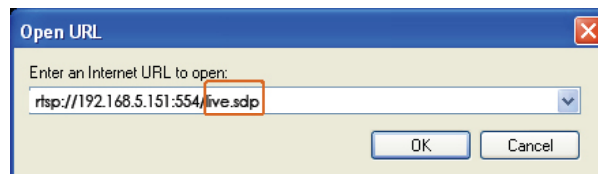
Using LevelOne Recording Software

The product software CD also contains recording software, 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 the recording software, please refer to the user's manual of the software or download it from http://www.LevelOne.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections: LevelOne INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.
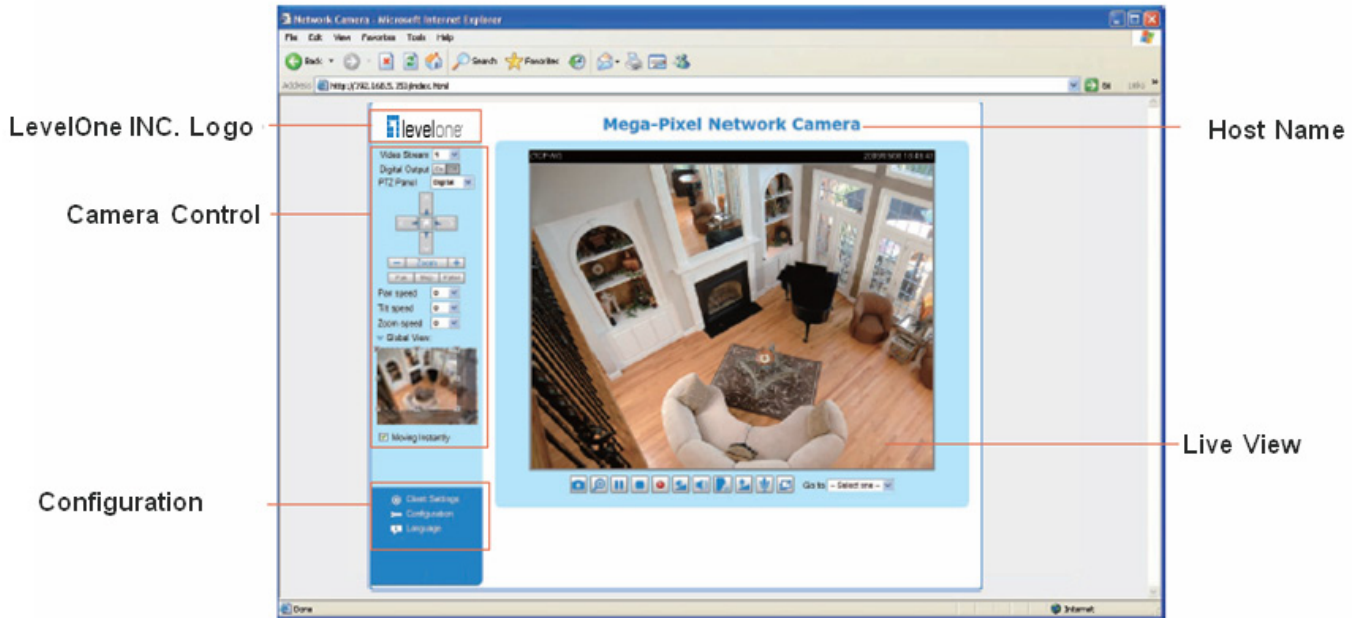
LevelOne INC. Logo

Click this logo to visit the LevelOne website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 24.

Camera Control Area

Video Stream: This Network Cmera supports multiple streams (stream 1 ~ 4) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 59 for detailed information.

Digital Output: Click to turn the digital output device on or off.

PTZ Panel: This Network Camera supports both "digital" (e-PTZ) and "mechanical" pan/tilt/zoom control. Please refer to Camera Control on page 70 for detailed information.

Global View: Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the curruent video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation, please refer to E-PTZ Operation on page 75. For more information about how to set up the viewing region of the current video stream, please refer to Viewing Windows on page 59.
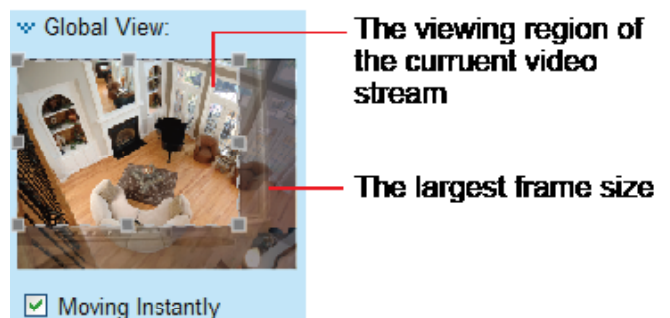
Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 21.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 23.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Live Video Window

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:
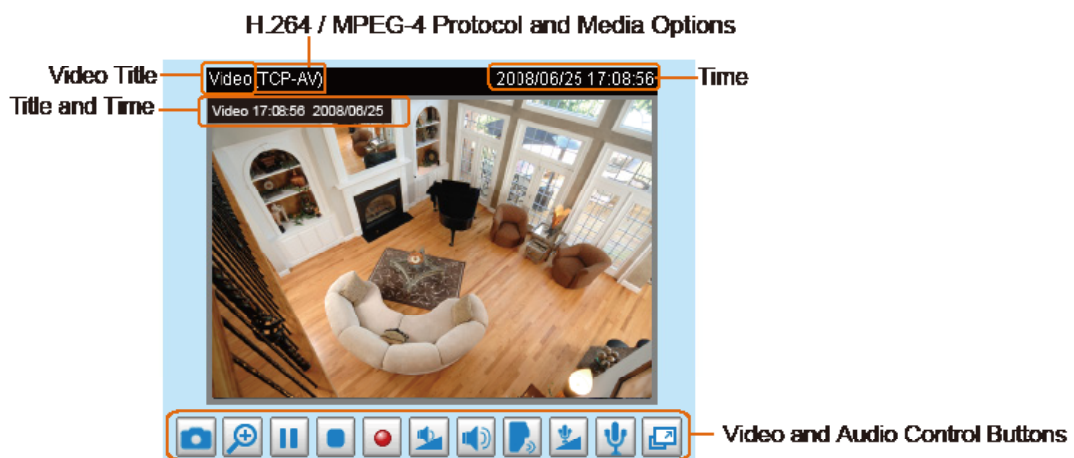
Video Title: The video title can be configured. For more information, please refer to Video Settings on page 53.

H.264 / MPEG-4 Protocol and Media Options: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 21.

Time: Display the current time. For further configuration, please refer to Video Settings on page 53.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Video Settings on page 53.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck "Disable digital zoom" to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.

Pause: Pause the transmission of the streaming media. The button becomes the ▶ Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the ▶ Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the ■ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 22 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:
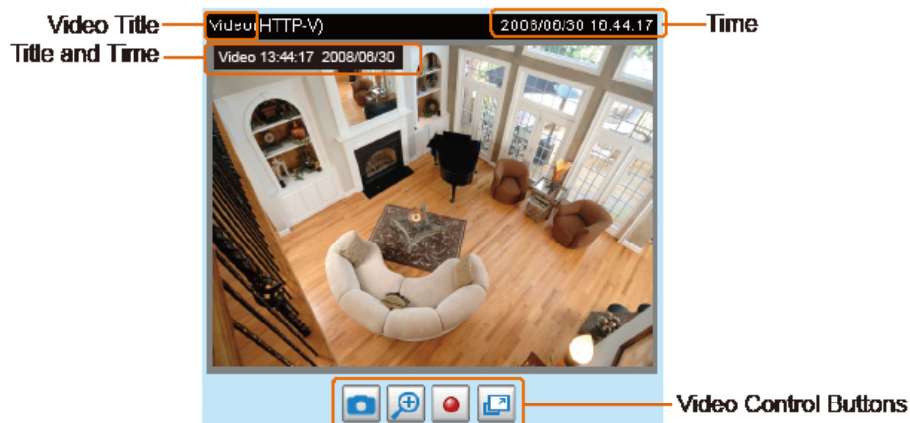
Video Title: The video title can be configured. For more information, please refer to Video Settings on page 53.

Time: Display the current time. For more information, please refer to Video Settings on page 53.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 53.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

📷 Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

🔍 Digital Zoom: Click and uncheck "Disable digital zoom" to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.

☐ Disable digital zoom

Zoom Factors: 100%

100%   400%

🔴 Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the 🟥 Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 22 for details.

🔲 Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.
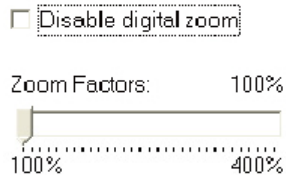
Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264 / MPEG-4 Media Options

Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

H.264 / MPEG-4 Protocol Options

Depending on your network environment, there are four transmission modes of H.264 or MPEG-4 streaming:

UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 46.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

MP4 Saving Options

Users can record live video as they are watching it by clicking 🔴 Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.

Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.
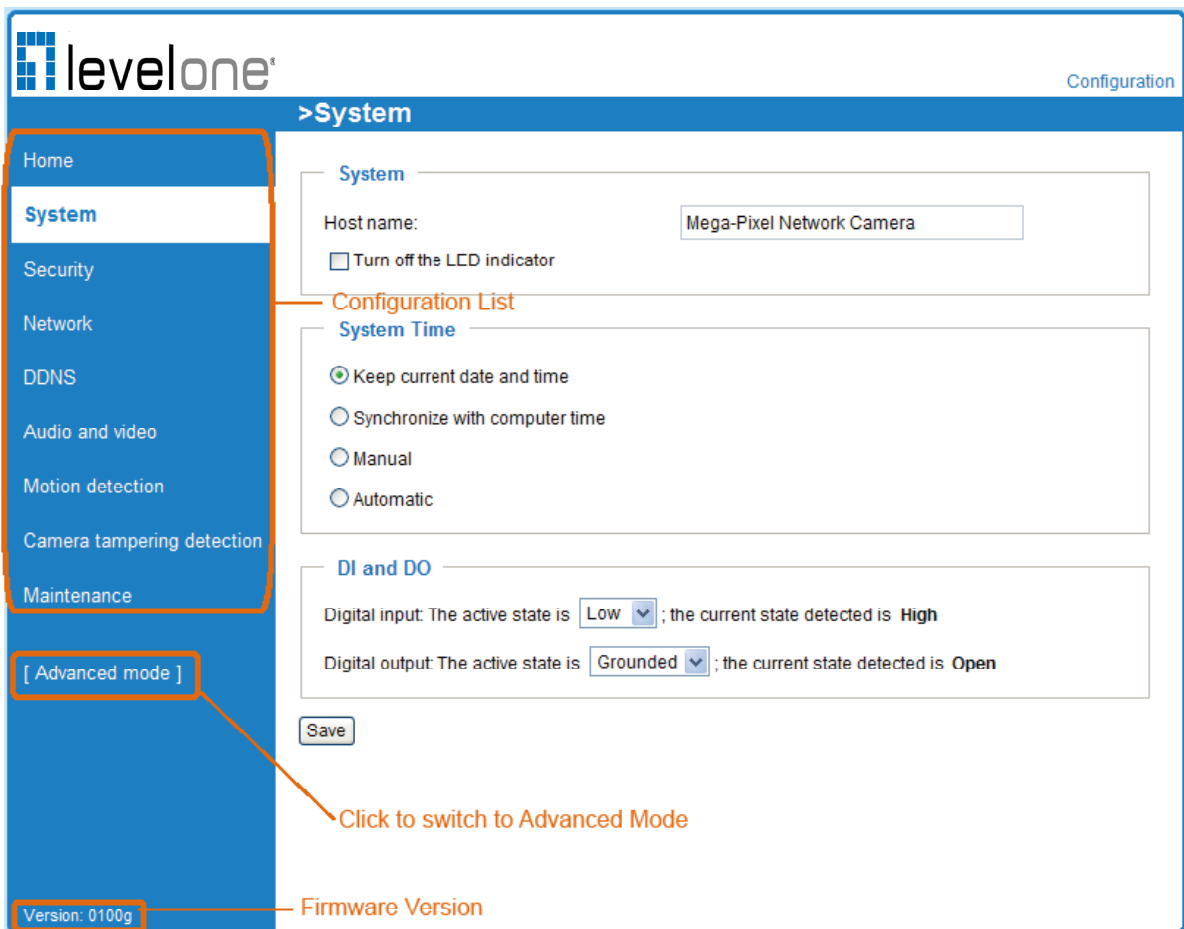
LevelOne offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (HTTPS/ Access list/ Homepage layout/ Application/ Recording/ System log/ View parameters) are not displayed in Basic Mode.

If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch to Advanced Mode.

In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the Basic Mode and the Advanced Mode:

Basic Mode

Advanced Mode

Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are marked with Advanced Mode . If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch over.

System

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page.

Turn off the LED indicators: If you do not want to let others know that the network camera is in operation, you can select this option to turn off the LED indicators.

System Time

System Time

Time zone: GMT+08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei ▾

Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.

⦿ Keep current date and time
○ Sync with computer time:
○ Manual:
○ Automatic:

Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone Advanced Mode : Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export Daylight Saving Time Configuration File on page 103 for details.

DI and DO

DI and DO

Digital input: The active state is Low ▾ ; the current state detected is High

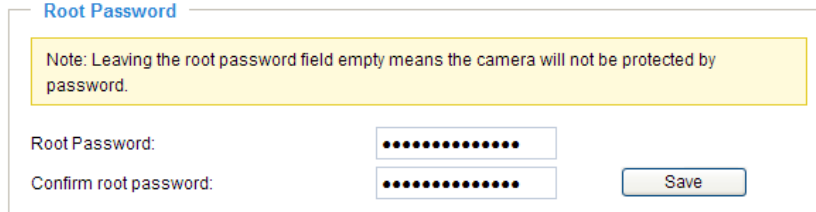Digital output: The active state is Grounded ▾ ; the current state detected is Open

Save

Digital input: Select High or Low to define normal status for the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define normal status for the digital output. The Network Camera will show whether the trigger is activated or not.

Security

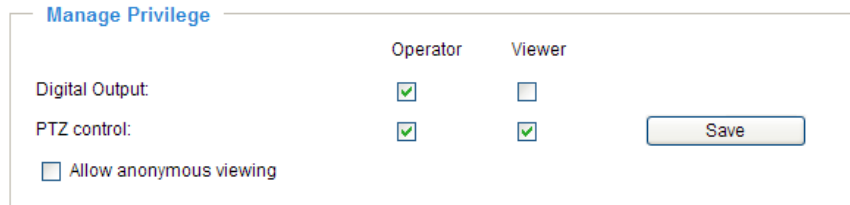This section explains how to enable password protection and create multiple accounts.

Root Password

Root Password

Note: Leaving the root password field empty means the camera will not be protected by password.

Root Password: ••••••••••••••

Confirm root password: ••••••••••••••   Save

The administrator account name is "root", which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the "root" account first.
1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user's name and password in their respective fields to access the Network Camera.
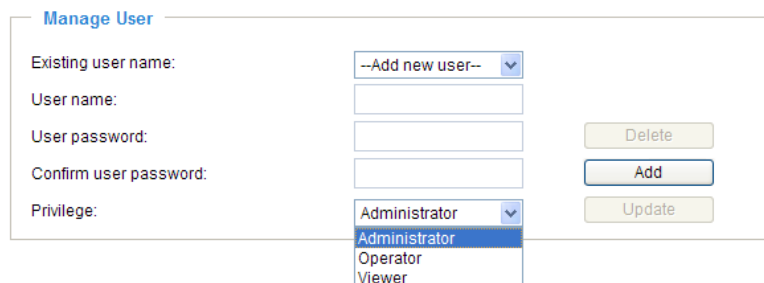
Manage Privilege `Advanced Mode`

Manage Privilege

	Operator	Viewer	
Digital Output:	☑	☐	
PTZ control:	☑	☑	Save
☐ Allow anonymous viewing			

Digital Output & PTZ control: You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Main Page on page 17.)

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password.

Manage User

Manage User

Existing user name:	--Add new user-- ▼
User name:	
User password:	Delete
Confirm user password:	Add
Privilege:	Administrator ▼ / Update

Administrator
Operator
Viewer

Administrators can add up to 20 user accounts.
1. Input the new user's name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 106. Viewers access only the main page for live viewing.

Here you also can change a user's access rights or delete user accounts.
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Enable HTTPS

Check this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS" or "HTTPS only". Note that you have to create and install a certificate first in the second column before clicking the **Save** button.

Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate automatically

1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Save** to generate a certificate.

4. The Certificate Information will automatically de displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.

5. Click **Home** to return to the main page. Change the address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.
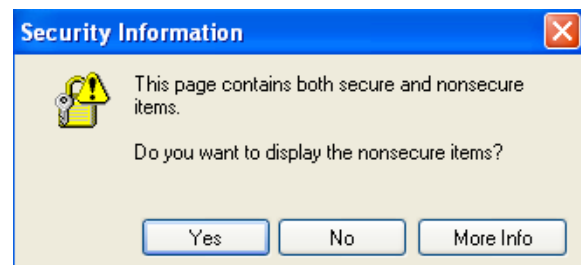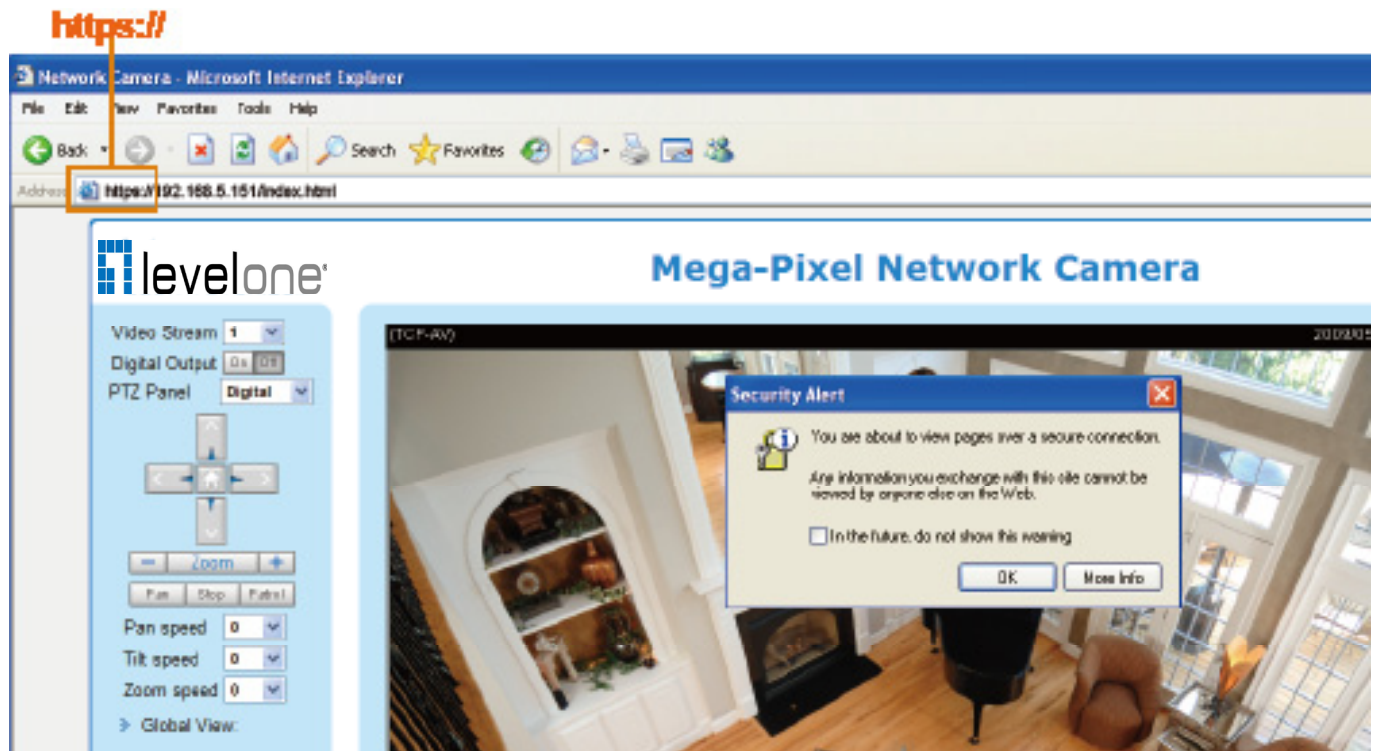
Create self-signed certificate manually

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.

3. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to see detailed information about the certificate.

Create certificate and install : Select this option if you want to create a certificate from a certificate authority.

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.

Create Certificate

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name:

Validity: 9999 days

Save   Close

Please wait while the certificate is being generated...
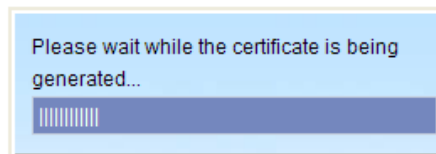
3. If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.
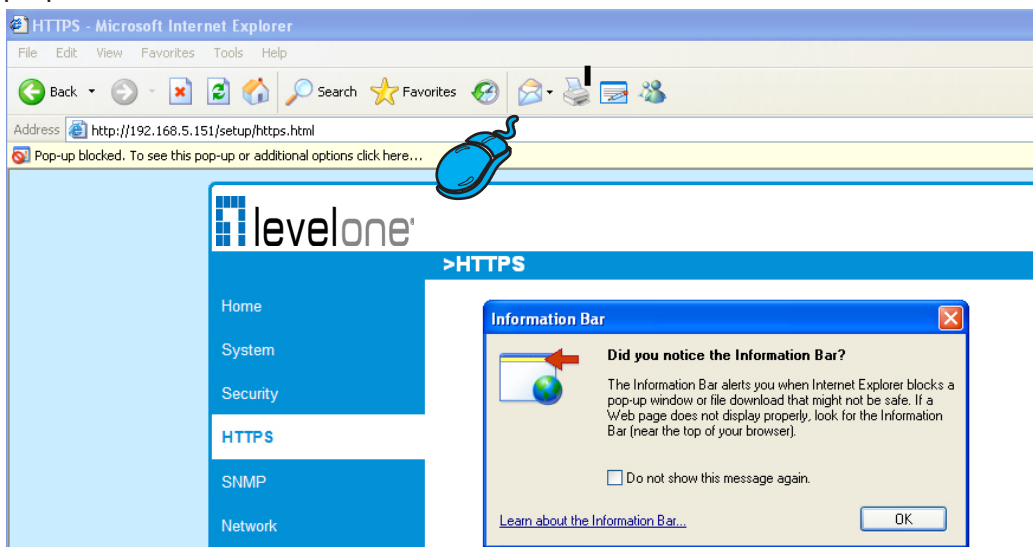
4. The pop-up window shows an example of a certificate request.

Create Certificate Request Completed

Copy the PEM format request below and send it to a CA for identify validation. After that, you have to install it by clicking the "Upload" button on HTTPS page.

Certificate Request (PEM format)

-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECADB5MQswCQYDVQQGEwJUVzERMA8GA1UECBMIUHJvdmluY2UxEjAQ
BgNVBAcTCUNpdHkgTmFtZTEaMBgGA1UEChMRT3JnYW5pemF0aW9uIE5hbWUxEjAQ
BgNVBAsTCVVuaXQgTmFtZTETMBEGA1UEAxMKSVAgQWRkcmVzczCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAuOT75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27fFSLG57bW9SoxrWuLhSvRZW
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCIeDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAAaAAMAOGCSqGSIb3DQEBBQUAA4GBAAVazWOAtftfU9dyFgTxOYO1D/zO
FOTkbnDOQG18e4ftJ3rRODlTvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqdCUqGiX
5ObLGlsubWsXr88PngaBwjYoTpG3qlzvUPJZLAVmdL3ne5urTbABXOScCHOQGtH+
PX9dw4OJWkIC8QhV
-----END CERTIFICATE REQUEST-----

5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera. Wait for the certificate authority to issue a SSL certificate; click **Browse...** to search for the issued certificate, then click Upload in the second column.

NOTE

► *How do I cancel the HTTPS settings?*
  1. Uncheck **Enable HTTPS secure connection** *in the first column and click* **Save***; a warning dialog will pop up.*
  2. Click **OK** *to disable HTTPS.*
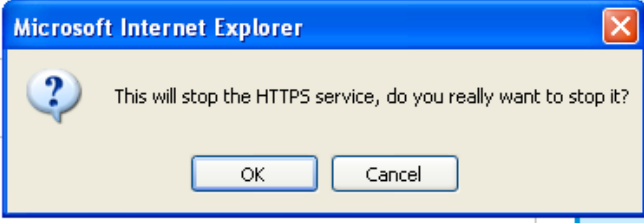
3. The webpage will redirect to a non-HTTPS page automatically.

► *If you want to create and install other certificates, please remove the existing one. To remove the signed certificate, uncheck* **Enable HTTPS secure connection** *in the first column and click* **Save***. Then click* **Remove** *to erase the certificate.*
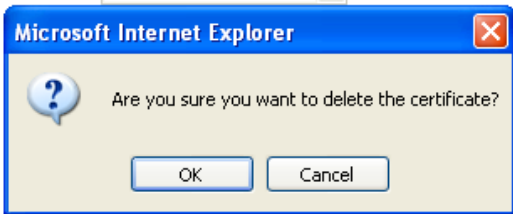
SNMP (Simple Network Management Protocol) `Advanced Mode`

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c
Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

☑ Enable SNMPv1, SNMPv2c

> SNMPv1, SNMPv2c Settings
> Read/Write community: Private
> Read only community: Public

Enable SNMPv3
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

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

■ Authentication password: Enter the password for authenrication (at least 8 characters).

■ Encryption password: Enter a password for ecryption (at least 8 characters).

☑ Enable SNMPv3

> SNMPv3 Settings
> Read/Write Security name: Private
> Authentication Type: MD5
> Authentication Password:
> Encryption Password:
> Read only Security name: Public
> Authentication Type: MD5
> Authentication Password:
> Encryption Password:

Network

This section explains how to configure a wired network connection for the Network Camera.

Network Type

LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

<u>Get IP address automatically</u>: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

<u>Use fixed IP address</u>: Select this option to manually assign a static IP address to the Network Camera.

1. You can make use of LevelOne Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 10 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

<u>Subnet mask</u>: This is used to determine if the destination is in the same subnet. The default value is "255.255.255.0".

<u>Default router</u>: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS server: The secondary WINS server that maintains the database of computer name and IP address.

Enable UPnP presentation: Select this option to enable UPnP^{TM} presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP^{TM} is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP^{TM} component is installed on your computer.
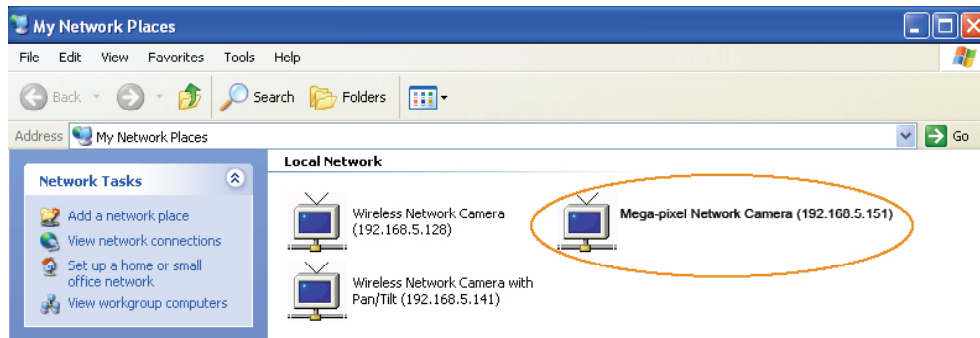
Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP^{TM} and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.
1. Set up the Network Camera on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page 86) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 89). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.


5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

NOTE

► If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.

► If UPnP^{TM} is not supported by your router, you will see the following message:
Error: Router does not support UPnP port forwarding.

► Steps to enable the UPnP^{TM} user interface on your computer:
Note that you must log on to the computer as a system administrator to install the UPnP^{TM} components.
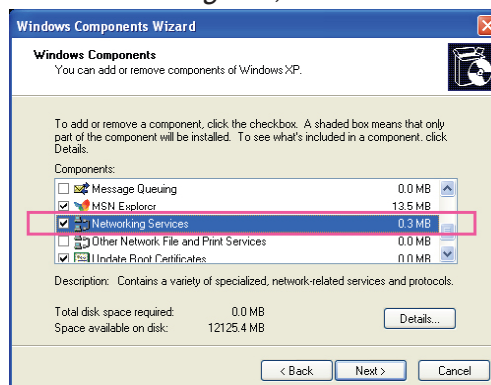
1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.
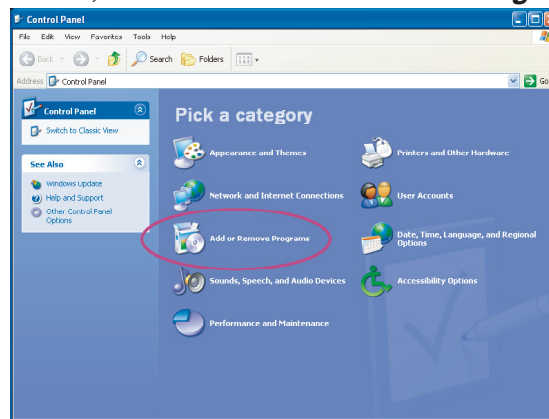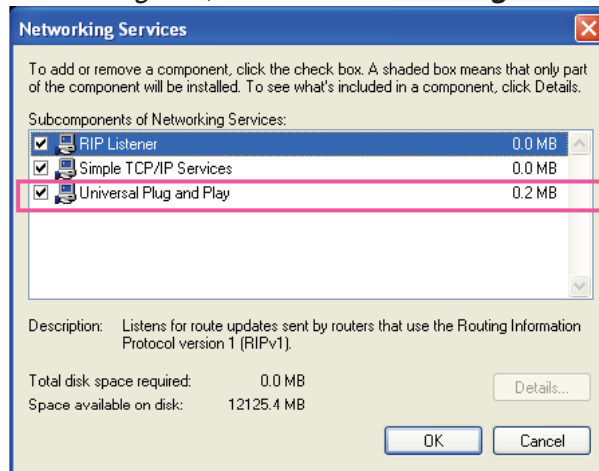

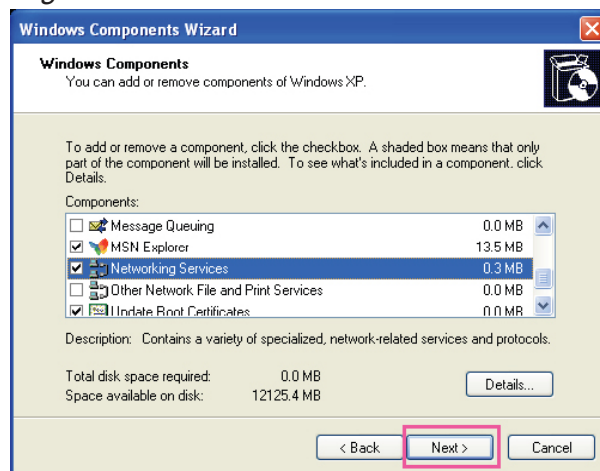2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.
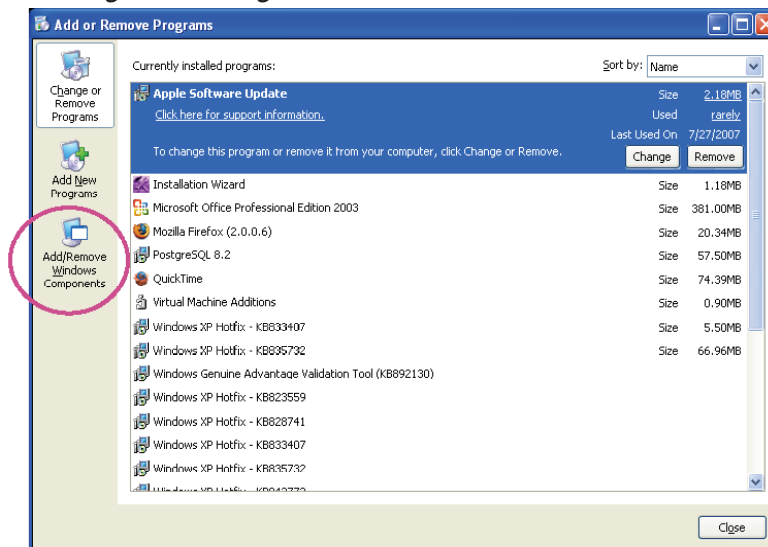
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.

4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.

5. Click **Next** in the following window.

6. Click **Finish**. UPnP^{TM} is enabled.

► How does UPnP^{TM} work?
   UPnP^{TM} networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

► Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 102 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.

Enable IPv6

Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:
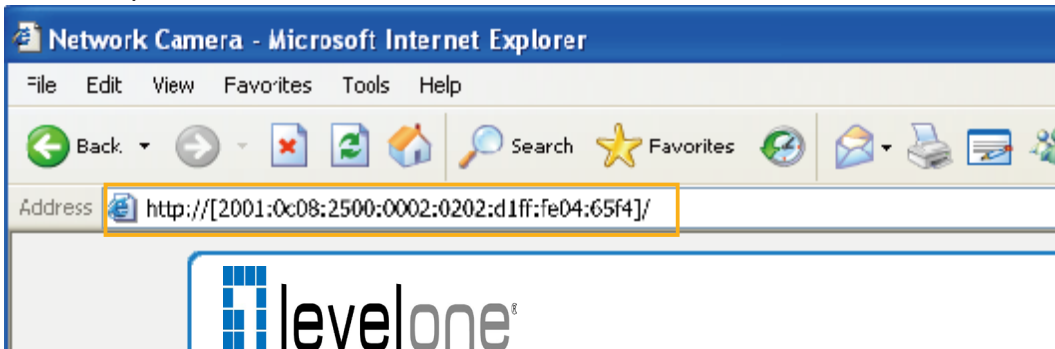
Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:

NOTE

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** on page 43 for detailed information.)*

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*

[eth0 address]

fe80:0000:0000:0000:0202:d1ff:fe11:2299/64@Link

[ppp0 address]

fe80:0000:0000:0000:0202:d1ff:fe11:2299/10@Link

2001:b100:01c0:0002:0202:d1ff:fe11:2299/64@Global

[Gateway]

fe80::90:1a00:4142:8ced

[DNS]

2001:b000::1

Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:

☑ Enable IPv6

IPv6 Information

☑ Manually setup the IP address

Optional IP address / Prefix length [   ] / 64

Optional default router [   ]

Optional primary DNS [   ]

IEEE 802.1x `Advanced Mode`

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

Supplicant
(Network Camera)

Authenticator
(Network Switch)

Authentication Server
(RADIUS Server)

1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A "go between" which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user's access request.

■ LevelOne Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:
1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (ie. MIS of your company) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE

► *The authentication process for 802.1x:*

1. The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).

2. A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.

3. The switch also forwards the RADIUS Server's certificate to the Network Camera.

4. Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.
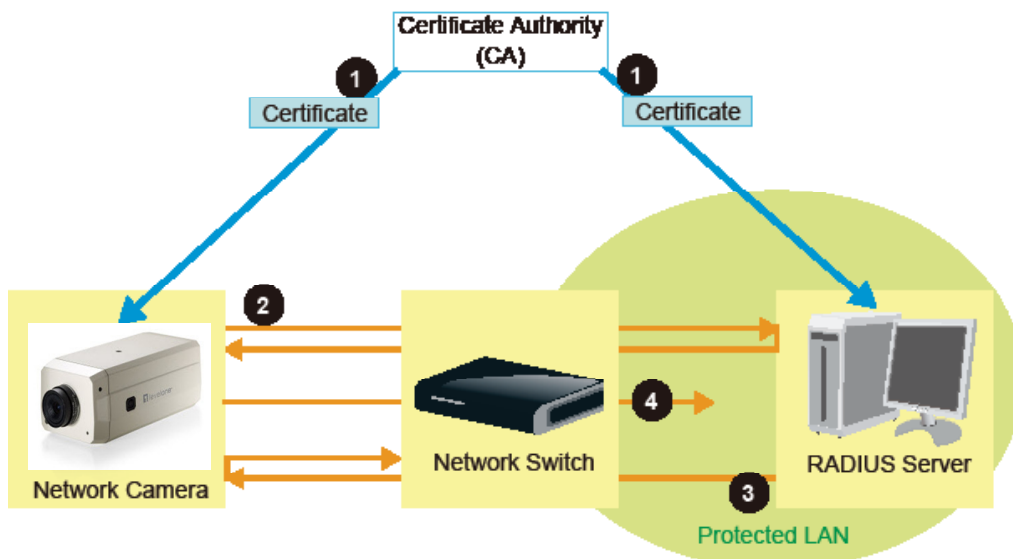
QoS (Quality of Service) `Advanced Mode`

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:
- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates prioritization from 0~7 (Eight different classes of service are available). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).

CoS	
☑ Enable CoS	
VLAN ID:	1
Live video:	0
Live audio:	0
Event/Alarm:	0
Management:	0

If you assign Video the highest level, the switch will handle video packets first.

NOTE

► *The web browsing may fail if the CoS setting is incorrect.*

► *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Though CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

HTTP `Advanced Mode`

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 26 for details.

Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.

If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:
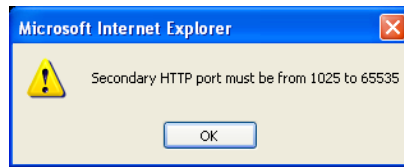
To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.


Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Configuration > Audio and Video > Video Settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Viewing Windows on page 59.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream 1 ~ 5>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.
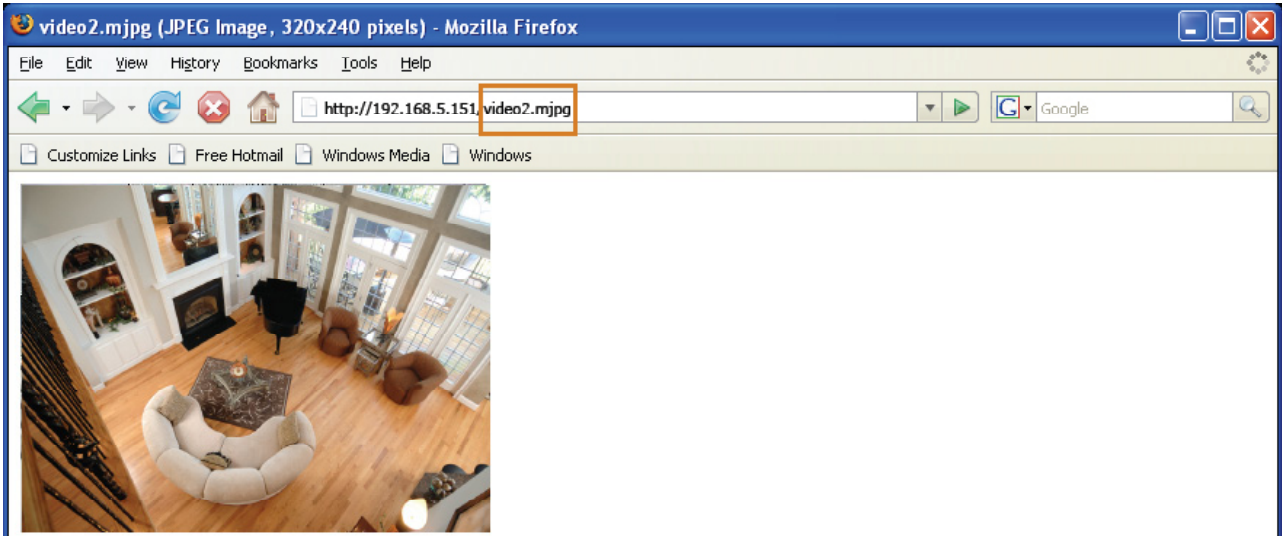
NOTE

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1 ~ 5> will fail to access the Network Camera.*

► *Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 106.*

HTTPS

By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio

By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" on the Audio and Video Settings page and the media option is set to "Video and Audio" on the Client Settings page. Please refer to Client Settings on page 21 and Audio and Video Settings on page 53.
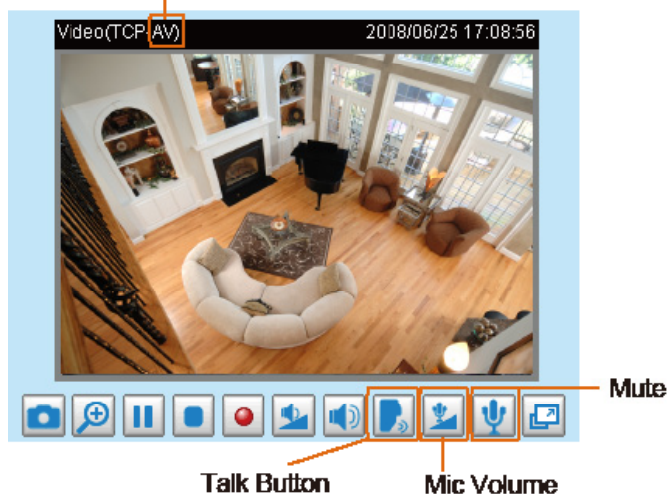
Click ![icon] to enable audio transmission to the Network Camera; click ![icon] to adjust the volume of microphone; click ![icon] to turn off the audio. To stop talking, click ![icon] again.

FTP

The FTP server allows the user to save recorded video clips. You can utilize LevelOne's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 26 for details.

Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.

If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

The availability of the RTSP streaming for the three authentication modes is listed in the following table:

|	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the Network Camera, you have to set the video mode to MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ 5>

For example, when the access name for stream 1 is set to live.sdp:

1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.
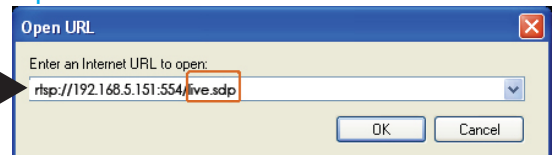
RTSP port /RTP port for video, audio/ RTCP port for video, audio
■ RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

■ The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

■ The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:
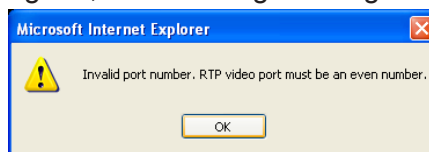
Multicast settings for stream 1 ~ 4: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 ~ 4.

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:
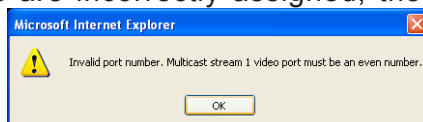
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service

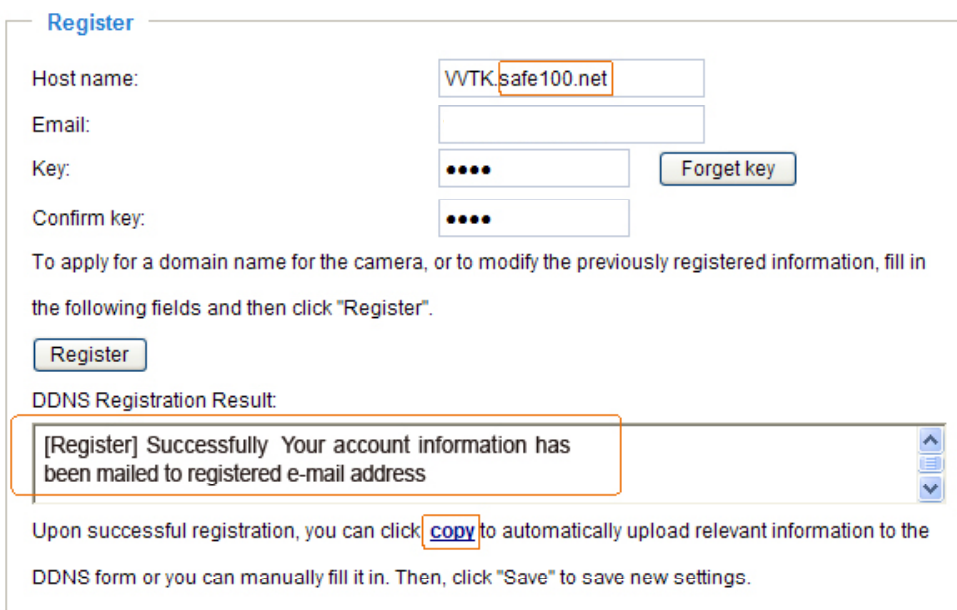Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider from the provider drop-down list.
LevelOne offers **Safe100.net**, a free dynamic domain name service, to LevelOne customers. It is recommended that you register **Safe100.net** to access LevelOne's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net
1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

LevelOne offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:
■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access List `Advanced Mode`

This section explains how to control access permission by verifying the client PC's IP address.

General Settings

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

View Information: Click this button to display the connection status window showing a list of the current connections. For example:

■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:
1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 26.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 46.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to Security on page 26.

■ Refresh: Click this button to refresh all current connections.

■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player).

<u>Enable access list filtering</u>: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are on the Allowed list and not on the Denied list can access the Network Camera. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 37 for detailed information.

■ Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list.

There are three types of rules:
<u>Single</u>: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List.

For example:

IP address 192.168.2.x will be bolcked.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. This rule is only applied to IPv4.

For example:

■ Delete Allowed/Denied list:
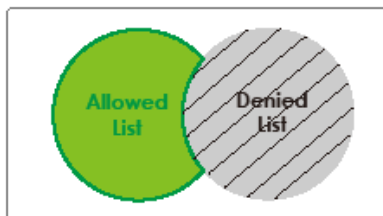In the Delete Allowed List or Delete Denied List column, make a selection and click **Delete**.

NOTE

► For example, when the range of IP addresses on the allowed list is set from 1.1.1.0 to 192.255.255.255 and the range in the denied list is set from 1.1.1.0 to 170.255.255.255, only users' IPs between 171.0.0.0 and 192.255.255.255 can access the Network Camera.

Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

Audio and Video

This section explains how to cofigure the audio and video settings of the Network Camera. It is composed of the following two columns: Video Settings and Audio Settings.

Video Settings

Video title: Enter a name that will be displayed on the title bar of the live video.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Iris mode: Select a proper iris mode for your environment.

Select caching stream: This Network Camera supports time shift cache stream on the Network Camera. Select one stream and check the below option **Enable time shift caching stream**.

Enable time shift caching stream Advanced Mode : Check this item to enable the time shift cache stream on the Network Camera, which will stores video in the camera's embedded memory for a period of time depending on the cache memory of each Network Camera. This function can work seamlessly with LevelOne's ST7501 recording software. When an event occurs, the recording software can request time shift cache stream from the camera, which allows the user to get an earlier video data.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation. Please note that the preset locations will be cleared after flip/mirror.

Overlay title and time stamp on video: Select this option to place the video title and time on the video streams.
Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be stamped on the video streams.
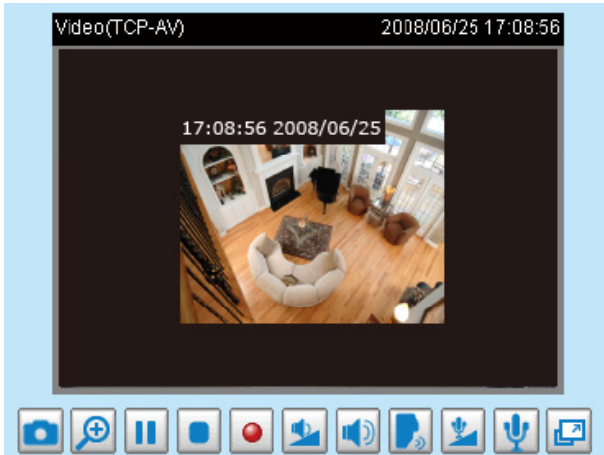
Options of Video ███ Advanced Mode ███
There are three options for you to choose: **Video quality first**, **Video frame rate first**, and **Cropping mode**. Select either one mode according to your needs.
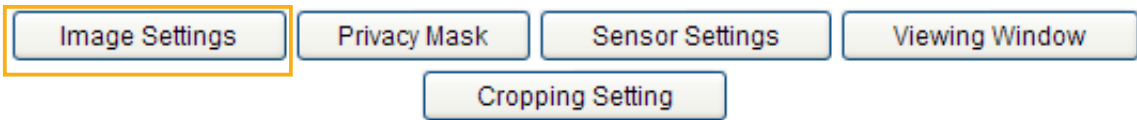

Options of Video

◉ Video quality first (MAX 15fps)

○ Video frame rate first (Maximum frame size 800x600)

○ Cropping mode

■ Video quality first: Select this option will reduce the maximum frame rate to 15fps and clear the settings in the Viewing Window.

■ Video frame rate first: Select this option will limit the frame size to 800x600 and clear the settings in the Viewing Window.

■ Cropping mode: The cropping function allows users to crop unnecessary information and simply transmit the image of the target region for live viewing or storage. With the trimming, the transmitting data size and thus, the network load is reduced and a higher frame rate is obtained. As a result, bandwidth resources and storage space can be used more efficiently.

Image Settings ███ Advanced Mode ███
Click **Image Settings** to open the Image Settings page. On this page, you can tune the White balance, Brightness, Saturation, Contrast, and Sharpness settings for the video.

White balance: Adjust the value for the best color temperature.

■ Auto
The Network Camera automatically adjusts the color temperature of the light in response to different light sources. The white balance setting defaults to **Auto** and works well in most situations.

■ Keep current value
Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions.
1. Set the White balance to **Auto** and click **Save**.
2. Place a sheet of white paper in front of the lens, then allow the Network Camera to adjust the color temperature automatically.
3. Select Keep Current Value to confirm the setting while the white balance is being measured.
4. Click **Save** to enable the new setting.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5.

■ Saturation: Adjust the image saturation level, which ranges from -5 to +5.

■ Contrast: Adjust the image contrast level, which ranges from -5 to +5.

■ Sharpness: Adjust the image sharpness level, which ranges from -5 to +5.

You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting and click **Close** to exit the page.

Privacy Mask **Advanced Mode**

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.
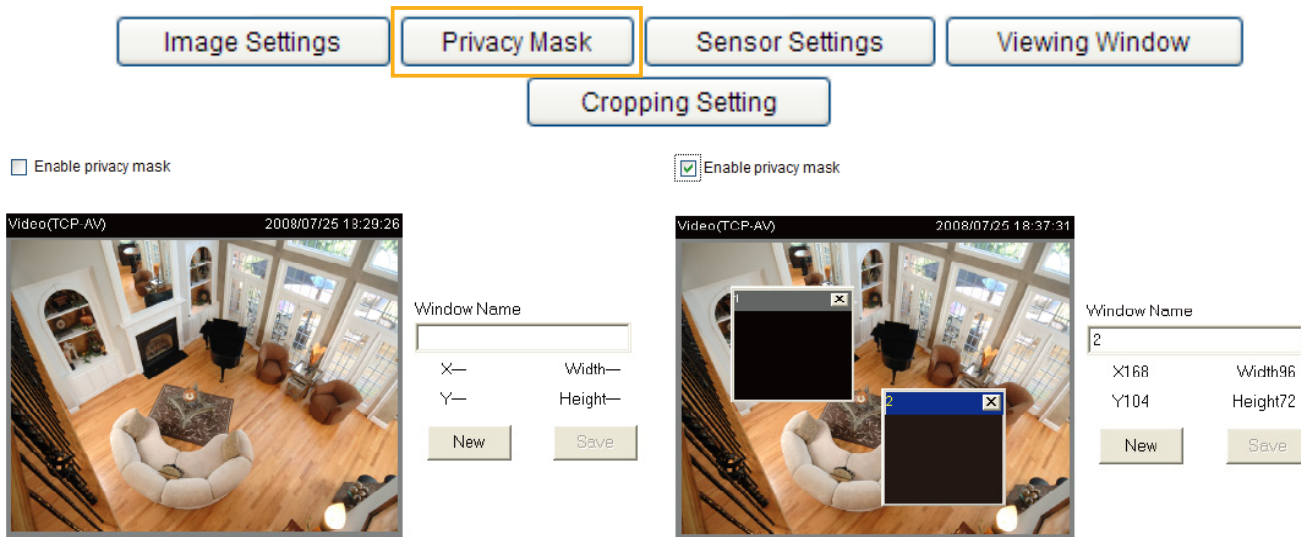
■ To set the privacy mask windows, follow the steps below:
1. Click **New** to add a new window.
2. Use the mouse to size and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Select **Enable privacy mask** to enable this function.

NOTE

► *Up to 5 privacy mask windows can be set up on the same screen.*

► *If you want to delete the privacy mask window, please click the 'x' on the upper right-hand corner of the window.*

Sensor Settings `Advanced Mode`

Click **Sensor Settings** to open the Sensor Settings page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) settings.

You can configure two sets of sensor settings: one for normal situations, the other for special situations, such as day/night/schedule mode.

Exposure

■ Maximum Exposure Time: Select a proper maximum exposure time according to the light source of the surroundings. The exposure times are selectable for the following durations: 1/480, 1/240, 1/120 second, 1/60 second, 1/30 second, 1/15 second, and 1/5 second. Shorter exposure times result in less light.

■ Exposure level: You can manually set the Exposure level, which ranges from 1 to 8 (dark to bright).The default value is 4.

■ Enable AGC (Auto Gain Control): You can manually set the AGC level (2X 4X, or 8X). The default value is 4X.

■ Enable BLC (Back Light Compensation): Enable this option when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings and click **Close** to exit the page.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Sensor Settings Profile Settings page as shown below.


Please follow the steps beolw to setup a profile:
1. Check **Enable this profile**.
2. Select the applied mode: Day mode, Night mode, or schedule mode. Please manually enter a range of time if you choose Schedule mode.
3. Configure Exposure settings in the second column. Please refer to last page for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.

Viewing Window `Advanced Mode`
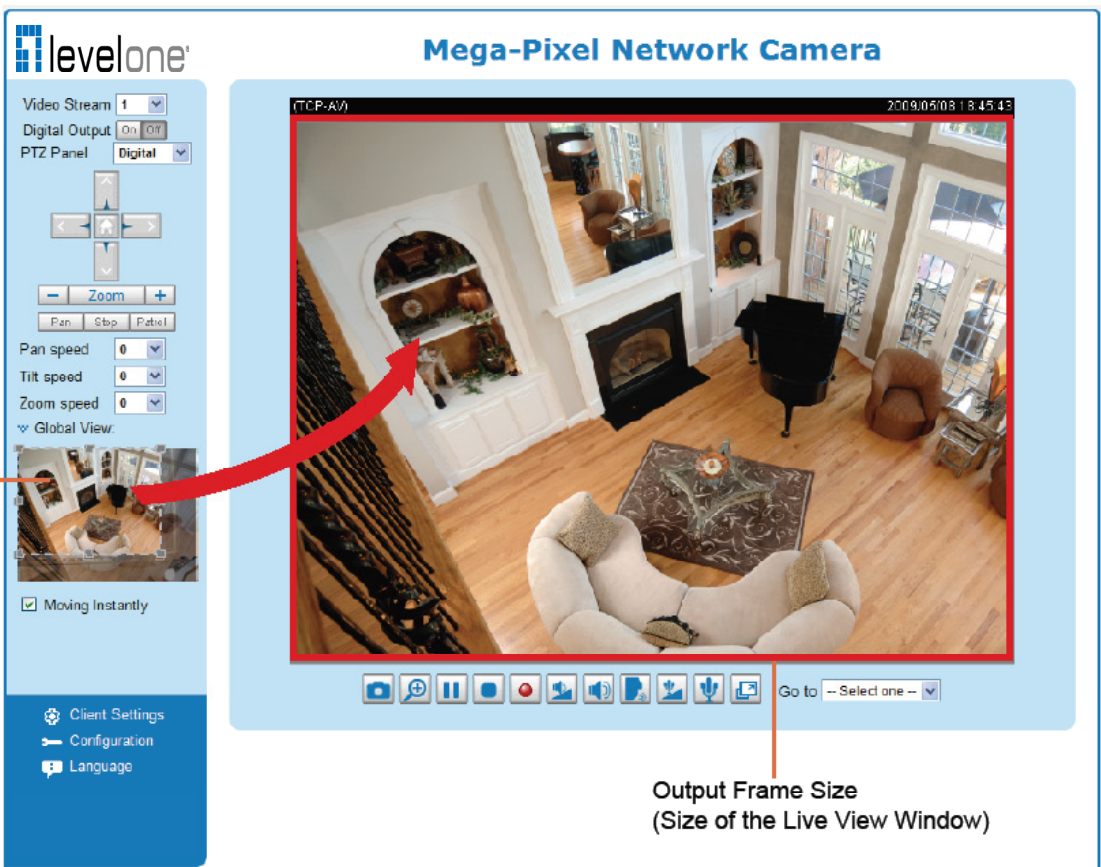
Click **Viewing Window** to open the Viewing Window Settings page.

Image Settings	Privacy Mask	Sensor Settings	Viewing Window

Cropping Setting
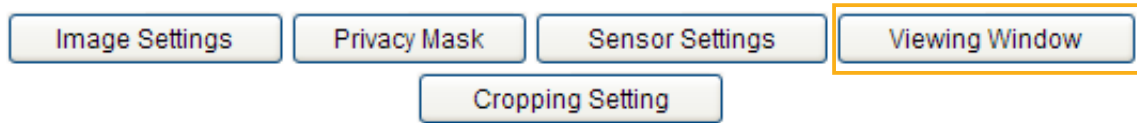
This Network Camera supports multiple streams with frame size ranging from 176 x 144 to 1600 x 1200.

The definition of multiple streams:
■ Stream 1: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

■ Stream 2: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

■ Stream 3 (Mobile stream): Users can define the "Region of Interest" (viewing region), but the "Output Frame Rate" (size of the live view window) is fixed at 176 x 144.

■ Stream 4 (Global view stream): This stream captures the full view of the video and streams out at the maximum resolution (1600 x 1200).

NOTE

► *All the items in the "Region of Interest" should not be greater than the "Output Frame Size" (current maximum resolution).*

Click **Viewing Window** to open the viewing region settings page. On this page, you can set the **Region of Interest** and the **Output Frame Size** for stream 1 ~ 3.

Please follow the steps below to set up those settings for a stream:

1. Select a stream which you want to set up the viewing region. If you want to stream out the video to a mobile device, please select stream 3.
2. Select a **Region of Interest** from the drop-down list. The floating frame, the same as the one in the Gloabl View window on the home page, will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.
3. Choose a proper **Output Frame Size** from the drop-down list according to the size of your monitoring device.

■ The parameters of the multiple streams:

	Region of Interest	Output frame size
Stream 1	1600 X 1200 ~ 176 x 144 (Selectable)	1600 X 1200 ~ 176 x 144 (Selectable)
Stream 2	1600 X 1200 ~ 176 x 144 (Selectable)	1600 X 1200 ~ 176 x 144 (Selectable)
Stream 3	1468 x 1200 ~ 176 x 144 (Selectable)	176 x 144 (Fixed)
Stream 4	1600 X 1200 (Fixed)	1600 X 1200 (Fixed)

■ The maximum **Region of Interest** of stream 3 is 1468 x 1200. You can also check the item "Set region to full view" to extend the region to full view (1600 x 1200). However, the image will be distorted a little bit.

When completed with the settings in the Viewing Window, click **Save** to enable the settings and click **Close** to exit the window. The selected **Output Frame Size** will immediately be applied to the **Frame size** of each video stream as shown on the next page. Then you can go back to the home page to test the e-PTZ function. For more information about the e-PTZ function, please refer to page 75.

Cropping Setting `Advanced Mode`

Click **Cropping Setting** to open the Cropping Settings page.
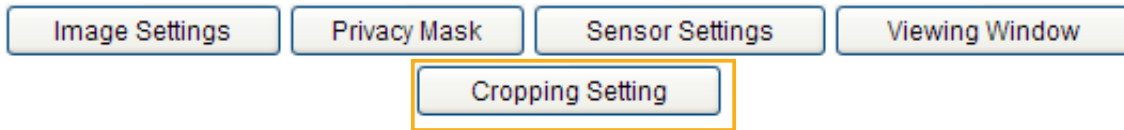
Please follow the steps below to set up cropping mode for mutiple streams:
1. Click **Cropping Setting** to open the window as shown below.
2. Select a **Captured area** from the drop-down list. The floating frame, the same as the one in the Global View window on the home page, will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.
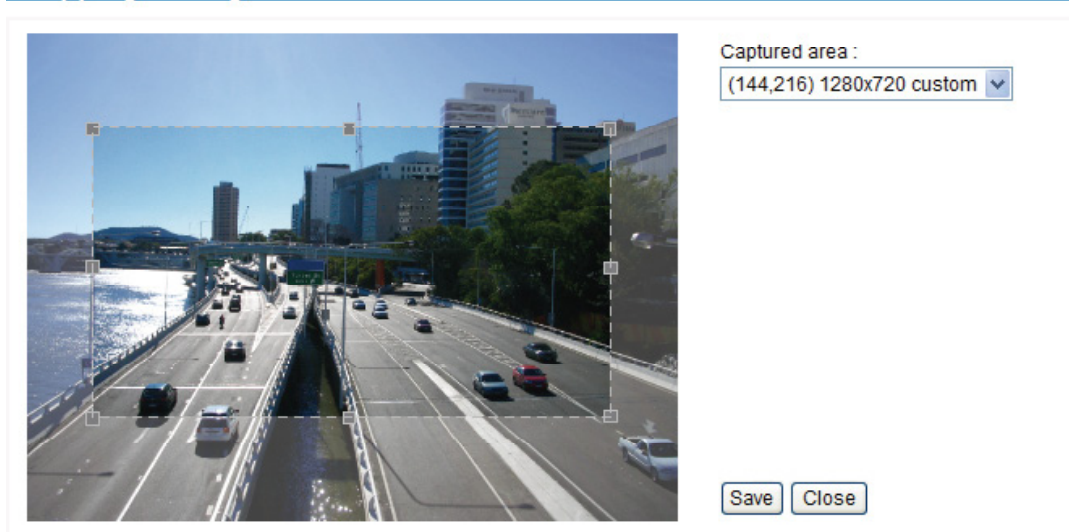
3. Click **Save** to enable the settings and click **Close** to exit the window. Below is the illustration of cropped image:
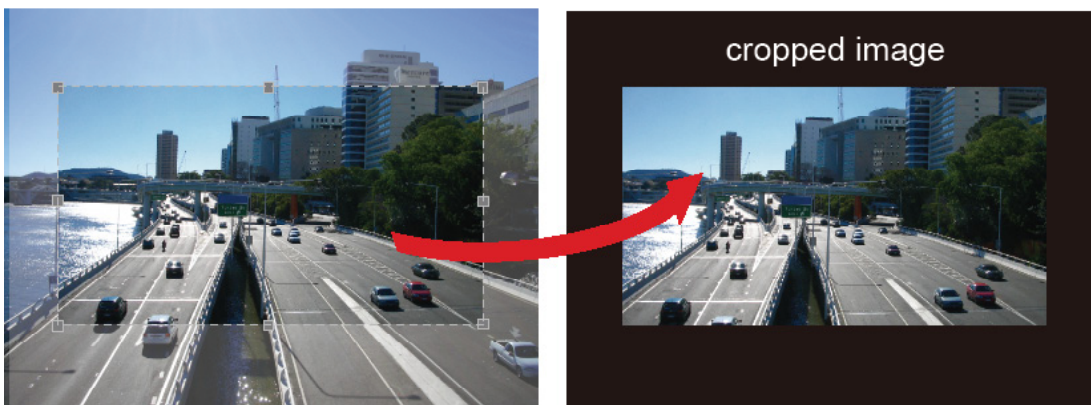
NOTE

► *In cropping mdoe, the maximum frame rate will be up to 30fps if the width is under 1280 and the height is under 720; otherwise, the maximum frame rate may be reduced to 15fps.*

► *Select cropping mode will clear the settings in the Viewing Window and disable Motion Detection, Privacy Mask, and Preset Position.*

Video Quality Settings Advanced Mode

Click the stream item to display the detailed information. The maximum frame size will follow your settings in above sections.

This Network Camera offers real-time H.264, MPEG-4 and MJEPG compression standards (Triple Codec) for real-time viewing.

If **H.264 / MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are four parameters for you to adjust the video performance:

■ Frame size
   You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
   This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.
   If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality
A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, and 8Mbps. You can also select **Customize** and manually enter a value.

On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:

■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Video quality
The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

NOTE

► _Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality._

► _Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video._

[Day/Night Settings]{.underline}

Switch to B/W in night mode
Select this to enable the Network Camera to automatically switch to B/W during night mode.

IR cut filter
With a removable IR-cut filter, this Network Camera can automatically remove the filter to let IR light into the sensor during low light conditions.

■ Auto mode
   The Network Camera automatically removes the filter by judging the level of ambient light.

■ Day mode
   In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

■ Night mode
   In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

■ Synchronize with digital input
   The Network Camera automatically removes the IR cut filter when DI triggers.

■ Schedule mode
   The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

Light sensor sensitivity
Select Low, Normal, or High sensitivity for the light sensor.

Audio Settings

Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:
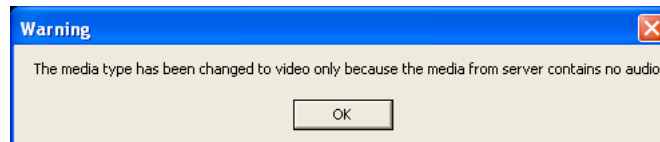
Internal microphone input gain: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) ~ -33 db (least sensitive).

External microphone input: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) or -33 db (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate Advanced Mode .
■ AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.

■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.

When completed with the settings on this page, click **Save** to enable the settings.

NOTE

► *The Network Camera offers two inputs to capture audio - internal microphone or external microphone. The internal/external microphone switch is located on the back panel of the Network Camera.*

Motion Detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.

Motion Detection Setting 1:
For normal situations
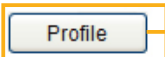
Motion Detection Setting 2:
For special situations

Follow the steps below to enable motion detection:

1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   ■ To move and resize the window, drag and drop your mouse on the window.
   ■ To delete window, click X on the top right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:
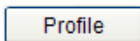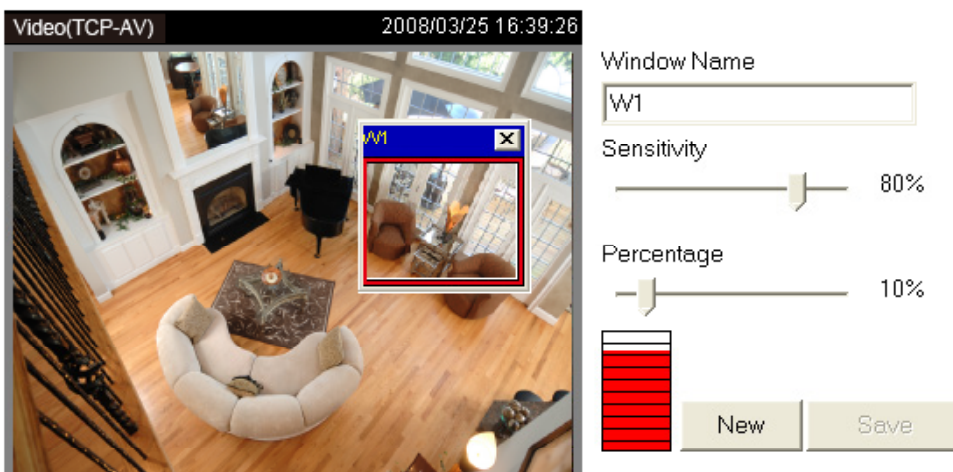
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Application on page 80.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.
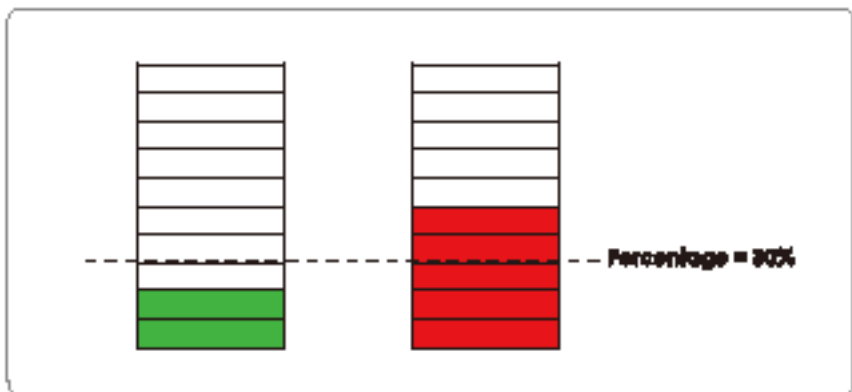
If you want to configure other motion detection settings for day/night/schedule mode, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.

Please follow the steps beolw to set up a profile:
1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you choose Schedule mode.
4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to Application > Event Settings > Trigger to choose it as a trigger source. Please refer to page 82 for detailed information.

NOTE

► *How does motion detection work?*
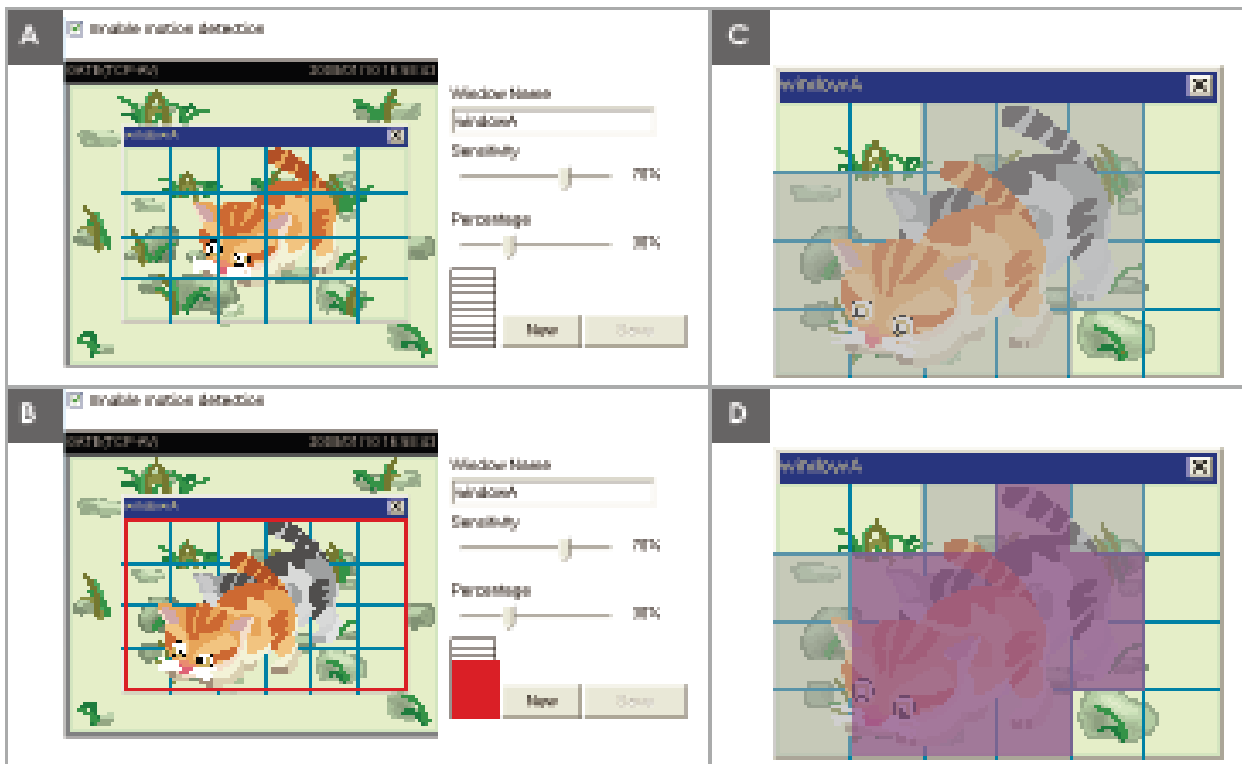
There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

Camera Tampering Detection

This section explains how to set up camera temper detection. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.

Please follow the steps below to set up the camera tamper detection function:
1. Check **Enable camera tampering detection**.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Application page** > **Event Settings / Server Settings (how to send alarm message) / Media Settings (send what type of alarm message)**. Please refer to page 82 for detailed information.

Camera Control

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.
There are two ways to enable the camera control function:
1. Mechanical: Connect the Network Camera to a PTZ driver or scanner via RS485 interface.
2. Digital: Control the e-PTZ operation. It allows users to quickly move the focus to a target area for close-up viewing without moving the camera physically. Please refer to page 75 for detailed instruction.

Mechanical PTZ Operation

If you select "Mechanical", the RS485 Settings section will be displayed as shown below:

RS485 Settings

Disable: Select this option to disable this function.

PTZ camera: Select this option to enable PTZ operation.
To utilize this feature, please connect the Network Camera to a PTZ driver or scanner via RS485 interface first. Then you can configure the PTZ driver and RS485 port with the following settings.

LevelOne offers three PTZ drivers: DynaDome/SmartDOME, Lilin PIH-7x00, and Pelco D protocol. If none of the above PTZ drivers is supported by your PTZ scanner, please select **Custom camera** (scanner). Please refer to the user's manual of your PTZ scanner to determine the Camera ID, PTZ driver, and Port settings. The Camera ID is necessary to control multiple cameras. If you click **Save** to enable this function, the camera control panel will be displayed on the main page. Please refer to the illustration on page 72.

<u>Transparent HTTP Tunnel</u>: If you want to use your own RS-485 device, you can use UART commands to build a Transparent HTTP Tunnel. The UART commands will be sent through HTTP tunnel established between the RS-485 device and the linked camera. For detailed application notes, please refer to URL Commands on page 106 or http://www.LevelOne.com/downloadfiles/faq/videoserver/UART_HTTP_Tunnel.pdf.

Preset Positions

If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver and click the **Save** button, the **Preset Position** button will be enabled. Click **Preset Position** to open the settings page. You can also select preset positions for the camera to patrol. A total of 20 preset positions can be configured.

Please follow the steps below to preset a position:
1. Adjust the shooting area to the desired position using the buttons on the right side of the window.
2. Enter a name for the preset position, which allows for up to forty characters. Click **Add** to enable the settings. The preset positions will be displayed under the Preset Location list on the left-hand side.
3. To add additional preset positions, please repeat steps 1~2.
4. To remove a preset position from the list, select it from the drop-down list and click **Delete**.
5. The preset positions will also displayed on the main page. Please refer to the illustration on the next page.
6. Click **Save** to enable the settings.
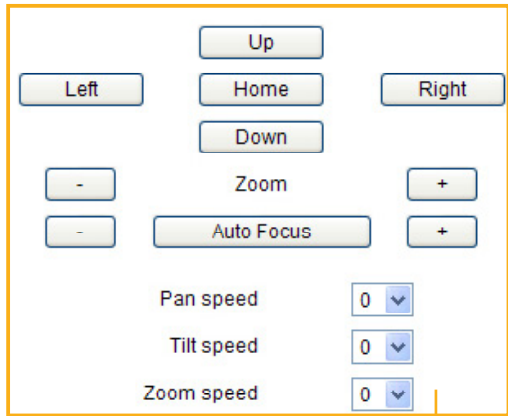
Home page in Mechanical PTZ Mode

■ The Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected preset position.

Patrol Settings

You can select some preset positions for the Network Camera to patrol.

Please follow the steps below to set up a patrol schedule:

1. Click a preset location on the list and click **Select**.
2. The selected preset location will be displayed on the **Source** list.
3. Set the **Dwelling time** for the preset location during auto patrol. You can also manually enter a value in the blank and click **Update**.
4. Repeat step 1 and 3 to select additional preset locations.
5. If you want to delete a selected location, select it from the Source list and click **Remove**.
6. Select a location and click **Up** or **Down** to rearrange the patrol order.
7. Click **Save** to enable the settings.

Custom Command

If **Custom Camera (scanner)** is selected as the PTZ driver, the **Preset Position** and **PTZ Control Panel** on the main page will be disabled. You will need to configure command buttons to control the PTZ scanner. Click **Custom Command** to open the Custom Command page to set the commands in the Control Settings session. Please refer to your PTZ scanner user's manual to enter the commands in the following fields. Click **Save** to enable the settings and click **Close** to exit the page.

Control settings:

Up	
Down	
Left	
Right	
Home	
Zoom in	
Zoom out	
Closer focus	
More distant focus	
Auto Focus	

Leaving the "Button name" field empty means the command button will not be displayed in the homepage.

	Button name	Command
Command 1:	Upleft	
Command 2:	Upright	
Command 3:	Downleft	
Command 4:	Downright	
Command 5:		

Save   Close

NOTE

►*If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver, the Control Settings column will not be displayed.*

►*For all PTZ drivers, a total of five additional command buttons can be configured.*

►*The command buttons will be displayed on the main page:*
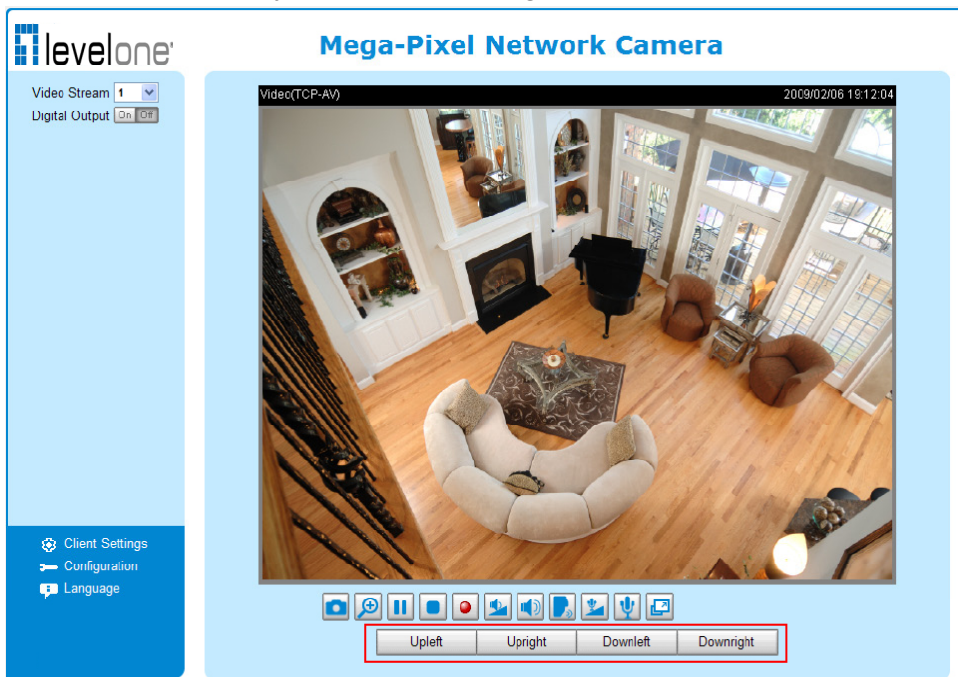
E-PTZ Operation

If you select "Digital", the e-PTZ control settings section will be displayed as shown below:

Select Stream: Select one of the stream 1~3 to set up the e-PTZ control. Please note that **each stream can be set up with its own e-preset positions and e-patrol settings**. For detailed information about how to set up **Preset Positions** and **Patrol Settings**, please refer to page 71~73.

Zoom Times Display
If you check this item, the zoom indicator will be displayed on the home page when you zoom in/out the live viewing window as the picture shown on the next page.

When completed with the settings of e-PTZ, click **Save** to enable the settings on this page.

Home page in E-PTZ Mode

■ The e-Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected e-preset position.

■ If you have set up different e-preset positions for stream 1~3, you can select one of the video streams to display its separate e-preset positions.

Global View
In addition to using the e-PTZ control panel, you can also use the mouse to drag or resize the floating frame to pan/tilt/zoom the viewing region. The live view window will also move to the viewing region accordingly.

Moving Instantly
If you check this item, the live view window will switch to the new viewing region instantly after you move the floating frame.

Click on Image
The e-PTZ function also supports "Click on Image". When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point.

Homepage Layout Advanced Mode

This section explains how to set up your own customized homepage layout.

Preview

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the third column on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

Logo

Here you can change the logo at the top of your homepage.

Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.

Preset Patterns
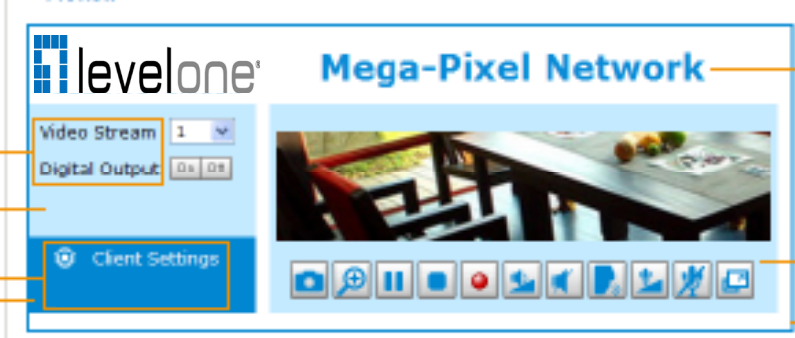
■ Follow the steps below to set up the customed homepage:
1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.

Custom Pattern — Color Selector
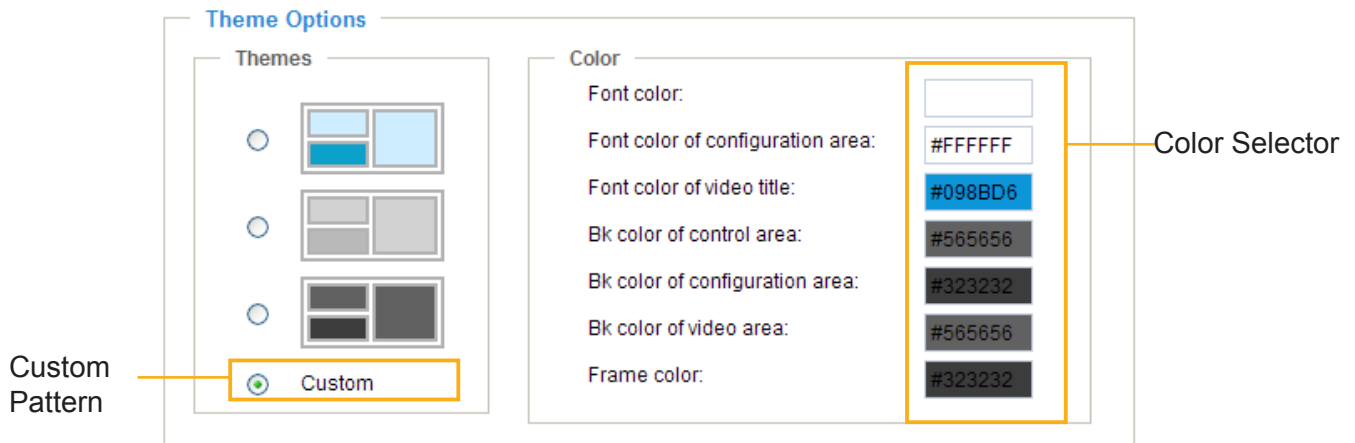
3. The palette window will pop up as shown below.
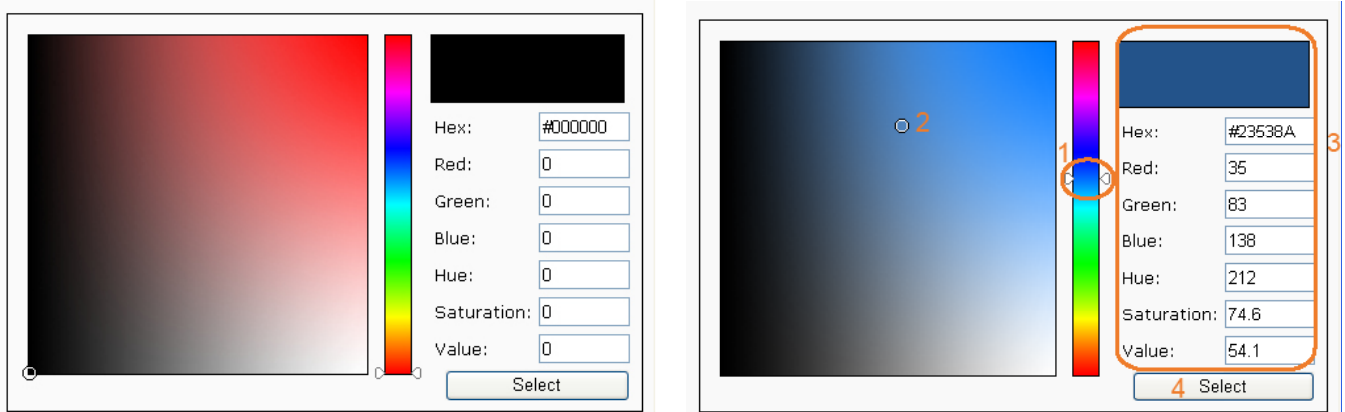
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced Mode

This section explains how to configure the Network Camera to responds to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications.

In the illustration on the right, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.
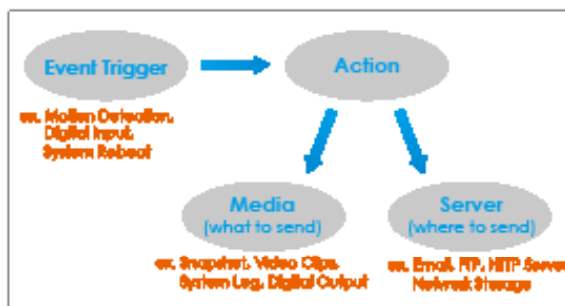
Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will pop up. If you need more information, please ask for LevelOne technical support.

Click to upload a file

Click to modify the script online

Event Settings

In the **Event Settings** column, click **Add** to open the **Event Settings** page. On this page, you can arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be configured.

Event name: [   ]

☐ Enable this event

Priority: [Normal ▾]

Detect next event after [10] second(s).

Note: This can only applied to motion detection and digital input

Trigger

- ○ Video motion detection:
- ○ Periodically:
- ○ Digital input
- ◉ System boot
- ○ Recording notify
- ○ Camera tampering detection:

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

- ◉ Always
- ○ From [00:00] to [24:00] [hh:mm]

Action

☐ Trigger digital output for [1] seconds

[Add Server] [Add Media]

	Server	Media	Extra parameter
☐	SD	[-----None----- ▾] [SD Test] [View]	

[Save] [Close]

Event name: Enter a name for the event setting.

Enable this event: Select this option to enable the event setting.

Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

Detect next event after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

An event is an action initiated by a user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger
This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.
There are several choices of trigger sources as shown below. Select the item to display the detailed configuration options.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 66 for details.

■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

■ System boot
This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify
 This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data.

■ Camera tampering detection
 This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 69 for detailed information.

Event Schedule
Specify the period for the event.

■ Select the days of the week.

■ Select the recording schedule in 24-hr time format.

Action
Define the actions to be performed by the Network Camera when a trigger is activated.

■ Trigger digital output for ☐ seconds
 Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated.

■ Add Server / Add Media
Click **Add Server** to configure Server Settings. For more information, please refer to Server Settings on page 86.
Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on page 89.

Here is an example of the Event Settings page:

Event name: Event1

☑ Enable this event

Priority: Normal ▼

Detect next event after 10 second(s).

Note: This can only applied to motion detection and digital input

Trigger

○ Video motion detection

○ Periodically

◉ Digital input

○ System boot

○ Recording notify

○ Camera tampering detection

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

◉ Always

○ From 00:00 To 24:00 [hh:mm]

Action

☐ Trigger digital output for 1 seconds

[Add Server] [Add Media]

Server	Media	Extra parameter
☐ SD	-----None----- ▼	[SD Test] [View]
☐ FTP	-----None----- ▼	
☐ NAS	-----None----- ▼	☐ Create folders by date time and hour automatically [View]
☐ Email	-----None----- ▼	
☐ HTTP	-----None----- ▼	

[Save] [Close]

When completed, click **Save** to enable the settings and click **Close** to exit Event Settings page. The new event settings / server settings / media settings will appear in the event drop-down list on the Application page.

Here is an example of the Application page with an event setting:

Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
Event1	ON	V	V	V	V	V	V	V	00:00~24:00	di

Add [Event1 ▼] Delete Help

Server Settings

Name	Type	Address/Location
FTP	ftp	
NAS	ns	\\192.168.5.122\nas
Email	email	
HTTP	http	http://192.168.5.10/cgi-bin/upload.cgi

Add [FTP ▼] Delete

Media Settings

Available memory space: 8000KB

Name	Type
Snapshot	snapshot
Video Clip	videoclip
System log	systemlog
Recording notify	recordmsg

Add [Snapshot ▼] Delete

Customized Script

Name	Date	Time

Add [▼] Delete

When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

Server name: Enter a name for the server setting.

Server Type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Email: Select to send the media files via email when a trigger is activated.


■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.
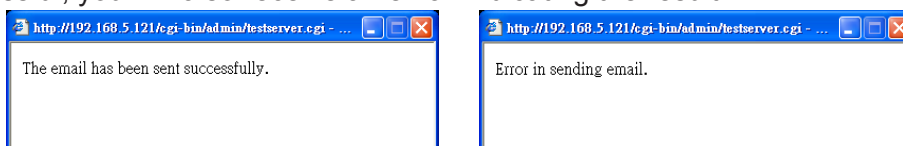
Click **Save** to enable the settings, then click **Close** to exit the page.

FTP: Select to send the media files to an FTP server when a trigger is activated.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
  By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
  Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive mode
  Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.

Click **Save** to enable the settings, then click **Close** to exit the page.

HTTP: Select to send the media files to an HTTP server when a trigger is activated.

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.

Click **Save** to enable the settings, then click **Close** to exit the page.

Network storage: Select to send the media files to a network storage location when a trigger is activated. Please refer to **Network Storage Setting** on page 93 for details.

Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, the new server settings will automatically be displayed on the Event Settings page. For example:

Media Settings

Click **Add Media** on the Event Settings page to open the Media Settings page. On this page, you can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured.

Media name: Enter a name for the media setting.

Media Type
There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.

■ Source: Select to take snapshots from stream 1 ~ 4.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.
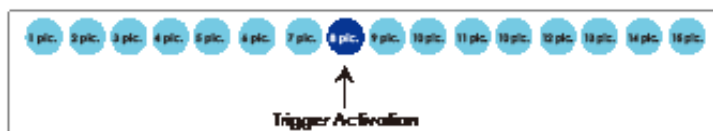
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:

Click **Save** to enable the settings, then click **Close** to exit the page.

Video clip: Select to send video clips when a trigger is activated.

■ Source: The source of video clip, which will be identical to the time shift caching stream. For more information about time shift caching stream, please refer to page 53.

■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.
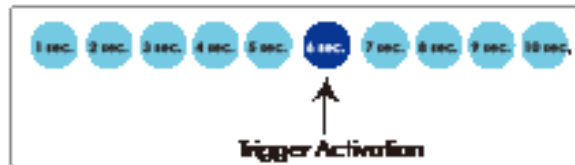
■ Maximum file size
Specify the maximum file size allowed.

■ File name prefix
Enter the text that will be appended to the front of the file name.
For example:

Click **Save** to enable the settings, then click **Close** to exit the page.

System log: Select to send a system log when a trigger is activated.
Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, click **Save** to enable the settings and click **Close** to exit this page. The new media settings will appear on the Event Settings page.

You can continue to select a server and media type for the event. Please go back to page 66 for detailed information.

■ SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 93 for detailed information.

■ Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

■ View: Click this button to open a file list window. This function is only for **SD card** and **Network Storage**.

If you click **View** button of SD card, a **Local storage** page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 96 for illustration.

If you click **View** button of Network storage, a **file directory window** will pop up for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.

The following is an example of a file destination with video clips:

☐ → **20081120** ──── The format is: YYYYMMDD
☐ → **20081121**   Click to open the directory
☐ → **20081122**

Click to delete selected items ──── [Delete] [Delete all] ──── Click to delete all recorded data

Click **20081120** to open the directory:

The format is: HH (24r)
Click to open the file list for that hour

	file name	size	date	time
☐	**Recording1_58.mp4**	2526004	2008/11/20	07:58:28
☐	**Recording1_59.mp4**	2563536	2008/11/20	07:59:28

< 07 08 09 10 11 12 13 14 15 16 17 >

[Delete] [Delete all] [Back]

Click to delete selected items

Click to delete all recorded data

Click to go back to the previous level of the directory

< 07 08 09 10 11 12 13 14 15 16 17 >

	file name	size	date	time
☐	**Recording1_58**.mp4	2526004	2008/11/20	07:58:28
☐	**Recording1_59**.mp4	2563536	2008/11/20	07:59:28

[Delete] [Delete all] [Back]

The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Media Settings page.
Please refer to page 89 for detailed information.

Recording Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

Insert your SD card and click here to test

<u>NOTE</u>

► *Before setting up this page, please set up the Network Storage on the Server Settings page first.*
► *Please remember to format your SD card when using for the first time. Please refer to page 96 for detailed information.*

Network Storage Setting
Click <u>Server</u> to open the Server Settings page and follow the steps below to set up:
1. Fill in the information for your server.
   For example:

2. Click **Test** to check the setting. The result will be shown in the pop-up window.
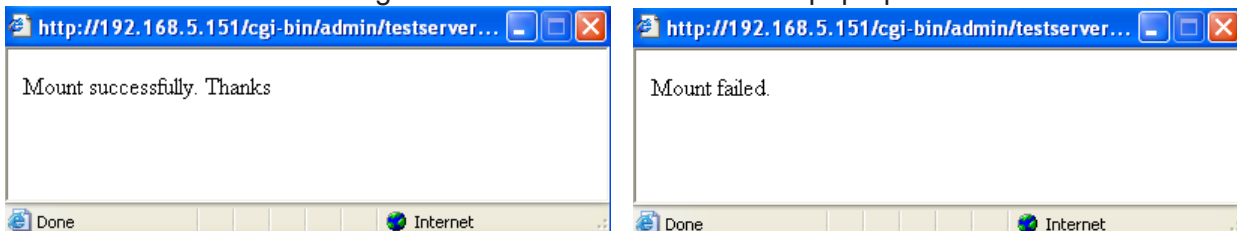
If successful, you will receive a test.txt file on the network storage server.
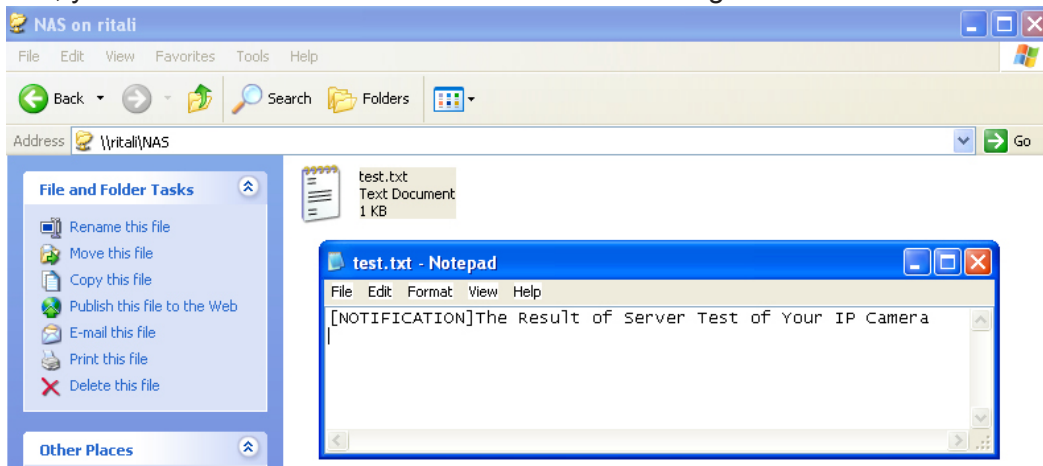
3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.

Recording Settings

Click **Add** to open the recording setting page. In this page, you can define the recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

Recording name: Enter a name for the recording setting.

Enable this recording: Select this option to enable video recording.

Priority: Select the relative importance of this recording setting (High, Normal, and Low).

Source: Select the recording source (stream 1 ~ 4).

Trigger: Select a trigger source.

■ Schedule: The server will start to record files on the local storage or network storage (NAS).

■ Network fail: Since network fail, the server will start to record files on the local storage (SD card).

Recording Schedule: Specify the recording duration.

■ Select the days of the week.

■ Select the recording start and end times in 24-hr time format.

Destination: You can select the SD card or network storage that was set up for the recorded video files.

Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

File name prefix: Enter the text that will be appended to the front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent malfunction. This value must be larger than 15 MBytes.

If you want to enable recording notification, please click **Application** to set up. Please refer to **Trigger > Recording notify** on page 83 for detailed information.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the Network Storage.
The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.

■ Click **Video** (Name): Opens the Recording Settings page to modify.

■ Click **ON** (Status): The Status will become **OFF** and stop recording.

■ Click **NAS** (Destination): Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 92 for details.

Local Storage `Advanced Mode`

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, search for recorded files to playback, download, etc.

SD card management

➤ SD card status: Detached ——————no SD card

➤ SD card control:

Searching and viewing the records

➤ File attributes:

➤ Trigger time:

[Search]

Search results

Show [10 ▾] entries   Search: [   ]

	Trigger time	Media type	Trigger type	Locked
	No matching records found			

Showing 0 to 0 of 0 entries   ◄ ►

[View] [Download] [Uncheck All] [JPEGs to AVI] [Lock/Unlock] [Remove]

Note: "View" and "Download" only apply to the highlight item

SD Card Management

<u>SD card status</u>: This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.

SD card management

➤ SD card status: Ready

Total size:	7810152 KBytes	Free size:	7602048 KBytes
Used size:	208104 KBytes	Use (%):	2.665 %

[Format]

SD card control
- ■ Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

- ■ Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter "7 days", the recorded files will be stored on the SD card for 7 days.

Click **Save** to enable your settings.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** cloumn.

File attributes: Select one or more items as your search criteria.

Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⬍ to sort the search results in either direction.

Numbers of entries displayed on one page

Enter a key word to filter the search results

Search results

Show [10 ▾] entries   Search: [＿＿＿＿＿＿＿]

	Trigger time ⬍	Media type ⬍	Trigger type ⬍	Locked ⬍
☐	2009-03-05 10:47:57	Videoclip	Periodically	No
☐	2009-03-05 10:48:58	Videoclip	Periodically	No
☐	2009-03-05 10:49:58	Videoclip	Periodically	No
☐	2009-03-05 10:50:58	Videoclip	Periodically	No
☐	2009-03-05 10:51:58	Videoclip	Periodically	No
☐	2009-03-05 10:52:58	Videoclip	Periodically	No
☐	2009-03-05 10:53:58	Videoclip	Periodically	No
☐	2009-03-05 10:54:58	Videoclip	Periodically	No
☐	2009-03-05 10:55:57	Videoclip	Periodically	No
☐	2009-03-05 10:56:57	Videoclip	Periodically	No

Highlight an item

Showing 11 to 20 of 32 entries   ◀ ▶

Click to switch pages

[View] [Download] [Uncheck All] [JPEGs to AVI] [Lock/Unlock] [Remove]

Note: "View" and "Download" only apply to the highlight item

View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file.
For example:

(Playback-V)   2009/3/5 10:47:31

[Small] [Medium] [Primary] [Close]

Click to adjust the image size

Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

JPEGs to AVI: This functions only applies to "JPEG" format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recoroding. You can click again to unlock the selections. For example:

Remove: Select the desired search results, then click this button to delete the files.

System Log `Advanced Mode`

This section explains how to configure the Network Camera to send the system log to the remote server as backup.

Remote Log

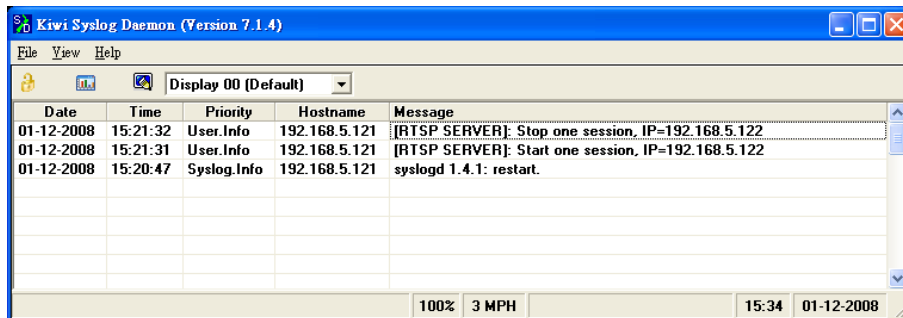You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

Follow the steps below to set up the remote log:
1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select **Enable remote log** and click **Save** to enable the setting.

Current Log

This column displays the system log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

View Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed on this page.

```
Parameter List

system_hostname='Mega-Pixel Network Camera'
system_ledoff='0'
system_lowlight='1'
system_date='2009/09/23'
system_time='09:41:28'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-1
system_updateinterval='0'
system_info_modelname='IP8161'
system_info_extendedmodelname='IP8161'
system_info_serialnumber='0002D10994F0'
system_info_firmwareversion='IP8161-VVTK-0100g'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''
system_info_language_i15=''
system_info_language_i16=''
```
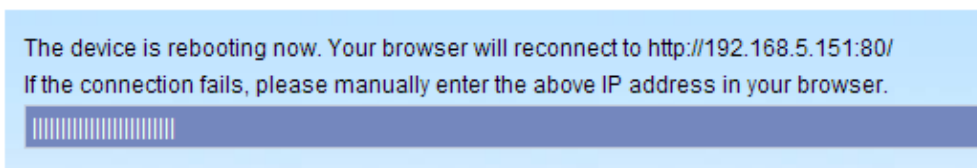
Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.
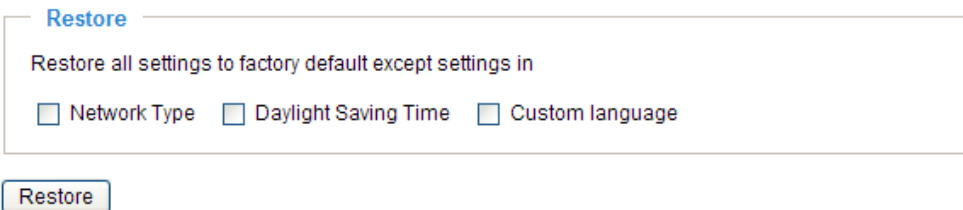
Reboot

Reboot

Reboot the device

[Reboot]

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.

The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

Restore

Restore

Restore all settings to factory default except settings in

☐ Network Type   ☐ Daylight Saving Time   ☐ Custom language

[Restore]

This feature allows you to restore the Network Camera to factory default settings.
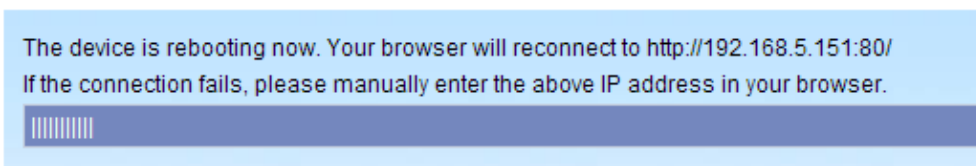
Network Type: Select this option to retain the Network Type settings (please refer to Network Type on page 33).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to System on page 24)

Custom Language: Select this option to retain the Custom Language settings.

If none of the options is selected, all settings will be restored to factory default.

The following message is displayed during the restoring process.

The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

Export / Upload Files Advanced Mode

This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting backup files.

Export daylight saving time configuration file: Click to set the start and end time of DST.

Follow the steps below to export:
1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.
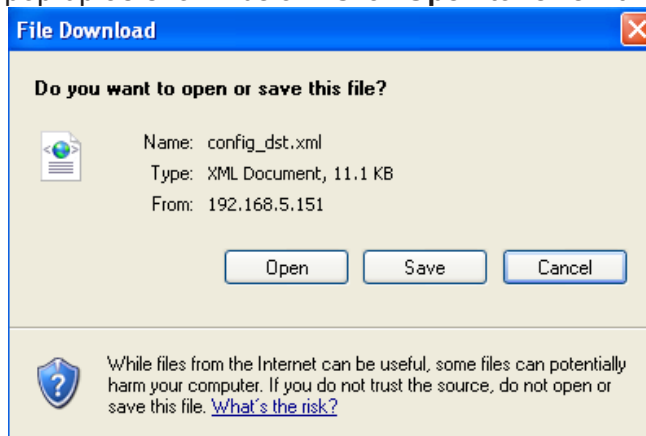
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.
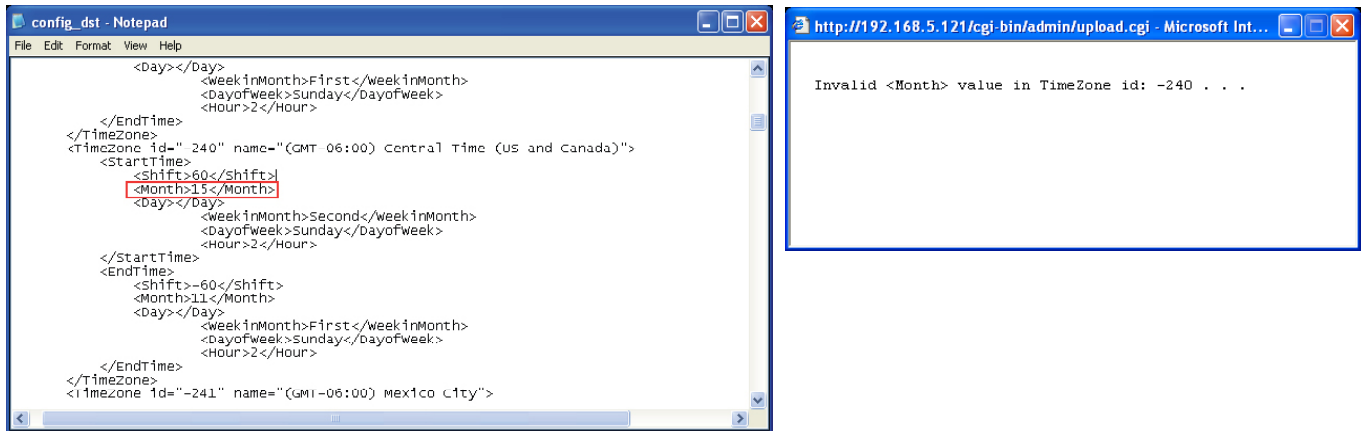
   In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.
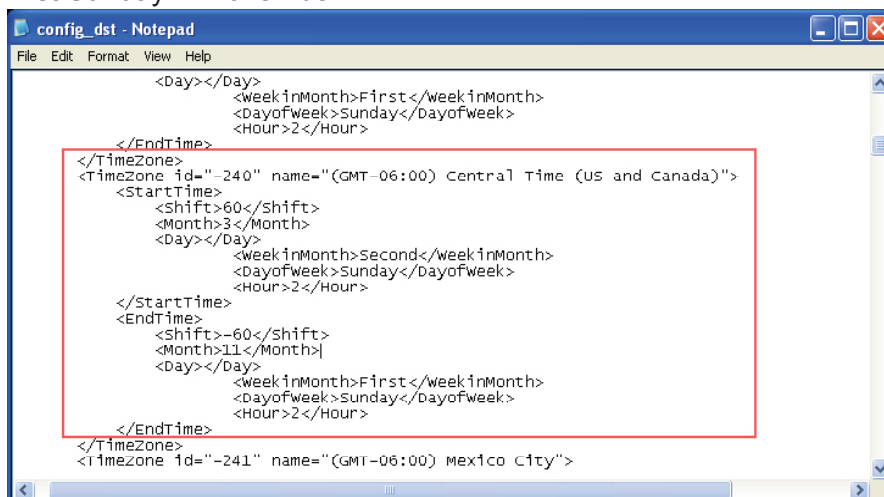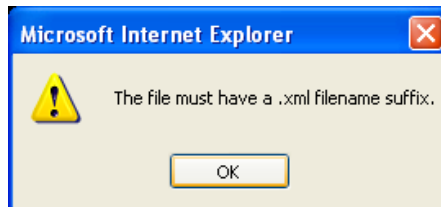
<u>Upload daylight saving time rule</u>: Click **Browse…** and specify the XML file to upload.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.

The following message is displayed when attempting to upload an incorrect file format.

<u>Export language file</u>: Click to export language strings. LevelOne provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

<u>Upload custom language file</u>: Click **Browse…** and specify your own custom language file to upload.

<u>Export setting backup file</u>: Click to export all parameters for the device and user-defined scripts.

<u>Upload setting backup file</u>: Click **Browse…** to upload a setting backup file. Please note that the model and firmware version of the device should be the same as the setting backup file. If you have set up a fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Upgrade Firmware

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the LevelOne website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see "Reboot system now!! This connection will close". After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.

Reboot system now!!
This connection will close.

The following message is displayed when you have selected an incorrect firmware file.

Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail