



# FCS-7111

## 1-Port H.264 PoE Video Server

### User's Manual

V1.0

## ***Table of Contents***

---

<b>Overview</b>	<b>3</b>
Read Before Use	3
Package Contents	3
Physical Description	4
Network Deployment	7
Software Installation	10
Network Setting	15
PPPoE Setting	15
<b>Accessing the Video Server</b>	<b>22</b>
Using Web Browsers	22
Using RTSP Players	24
Using 3GPP-compatible Mobile Devices	25
Using LevelOne Recording Software	26
<b>Main Page</b>	<b>27</b>
<b>Client Settings</b>	<b>31</b>
<b>Configuration</b>	<b>33</b>
System	34
Security	36
HTTPS (Hypertext Transfer Protocol over SSL)	37
SNMP (Simple Network Management Protocol)	42
Network	43
DDNS	58
Access List	60
Audio and Video	63
Motion Detection	69
Camera Tampering Detection	71
Camera Control	72
Homepage Layout	77
Application	80
Recording	93
Local Storage	96
System Log	100
View Parameters	101
Maintenance	102
<b>Appendix</b>	<b>106</b>
URL Commands for the Network Camera/Video Server	106

# Overview

LevelOne FCS-7111 is a 1-CH video server supporting the high-performance H.264 compression format that drastically reduces file sizes and conserves valuable bandwidth and storage space. With MPEG-4 and MJPEG compatibility, video streams also can be transmitted in either of these formats for versatile applications. The streams can also be individually configured with separate frame rates, resolution, and image quality so as to meet different needs or bandwidth constraints. Users can receive multiple streams simultaneously in different settings for viewing on different platforms such as PCs or mobile phones.

The integrated 802.3af compliant PoE function reduces cabling problems, making the FCS-7111 a cost-effective surveillance solution. The built-in SD/SDHC card slot offers a convenient and portable storage option to prevent data loss in case of network disconnection. Since all data can be stored on a SD/SDHC card, the on-board storage design significantly reduces bandwidth consumption.

The FCS-7111 comes with LevelOne's ST7501 32-CH central management software for high scalability and easy-to-use operation. With the FCS-7111, you can upgrade to a full-featured, high-end IP surveillance solution using existing infrastructure.

## Read Before Use

The use of surveillance devices may be prohibited by law in your country. The video server 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 video server 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.

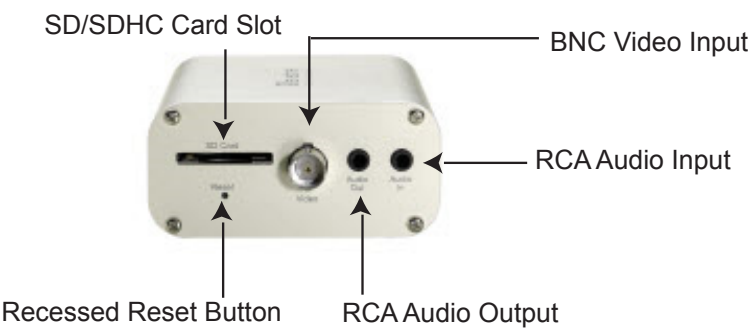
The video server is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the video server and ensure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

## Package Contents

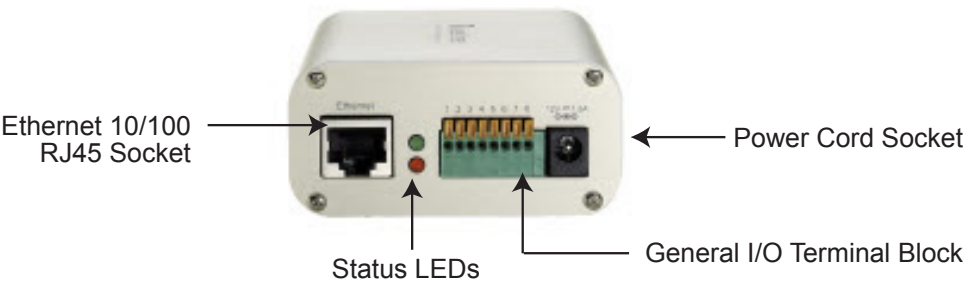
- FCS-7111
- Power Adapter
- Software CD
- Quick Installation Guide

# Physical Description

## Front Panel



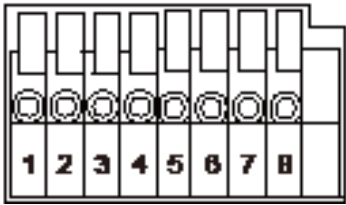
## Back Panel



## General I/O Terminal Block

This video server provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.

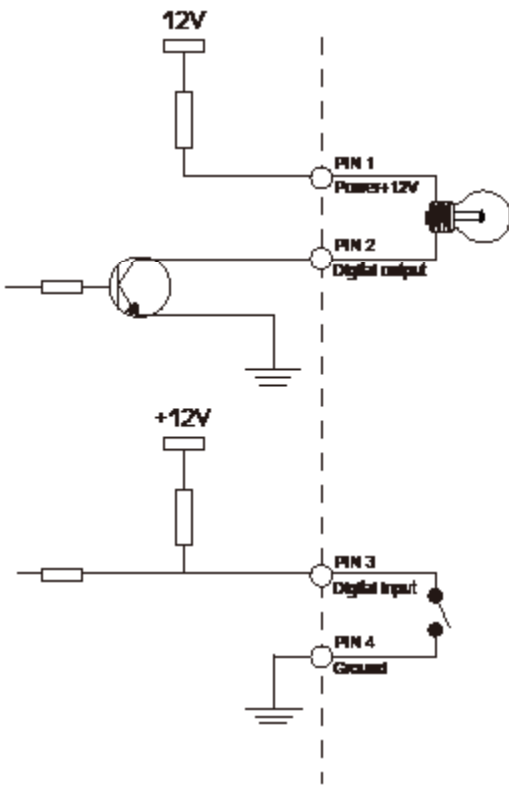
Pin	Name
1	Power +12V
2	Digital output
3	Digital input
4	Ground
5	AC 24V input
6	AC 24V input
7	RS-485 +
8	RS-485 -





## DI/DO Diagram

Please refer to the following illustration for the connection method.



## Status LED

The LED indicates the status of the video server.

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 video server 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 video server 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

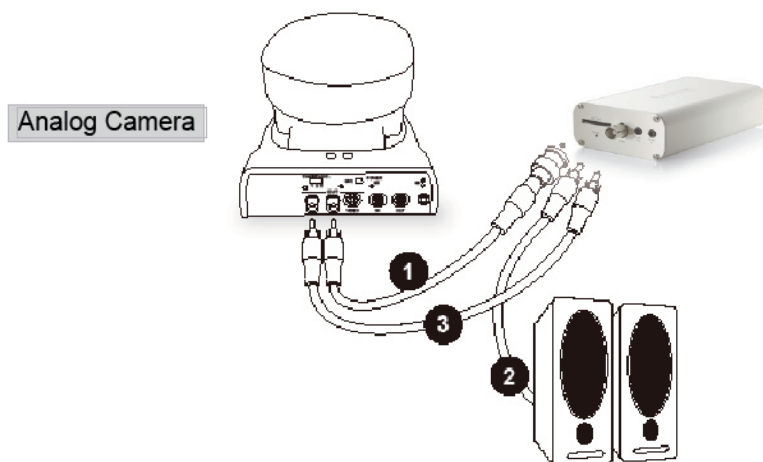
This video server is compliant with **SD/SDHC 16GB / 8GB** and other preceding standard SD cards.

## Network Deployment

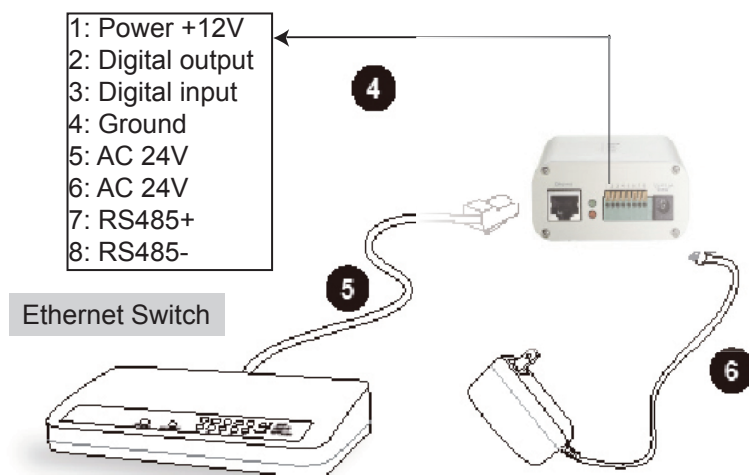
### Setting up the Video Server over the Internet

This section explains how to configure the video server to an Internet connection.

1. Make video connection from the camera to the BNC video input.
2. Make audio connection from the Line-Out audio source to the RCA audio input.
3. Make audio connection from RCA audio output to the speaker.



4. If you have external devices such as sensors and alarms, connect them to the general I/O terminal block.
5. Connect the video server to a switch via Ethernet cable.
6. Connect the power cable from the video server to a power outlet.

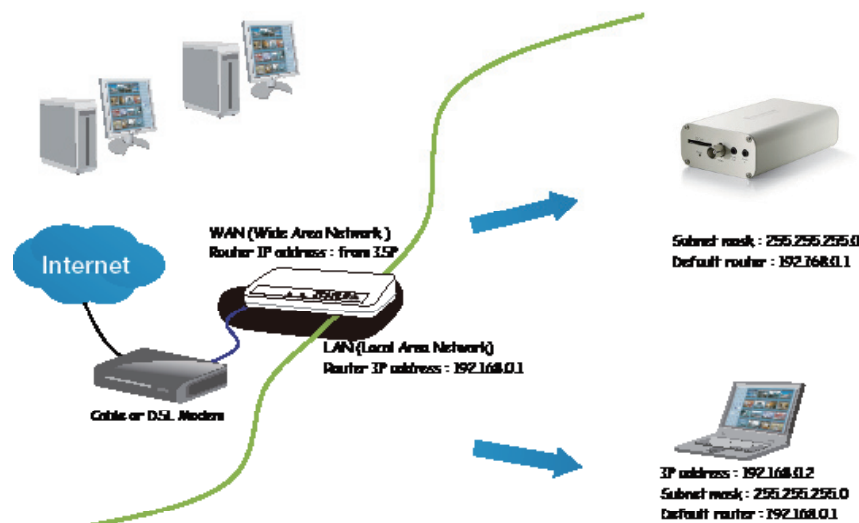


There are several ways to set up the video server over the Internet. The first way is to set up the video server behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

## Internet connection via a router

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

1. Connect your video server 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 Video server is 192.168.0.3, please forward the following ports for the Video server 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 Video server 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 Video server. Please refer to LAN on page 33 for details.

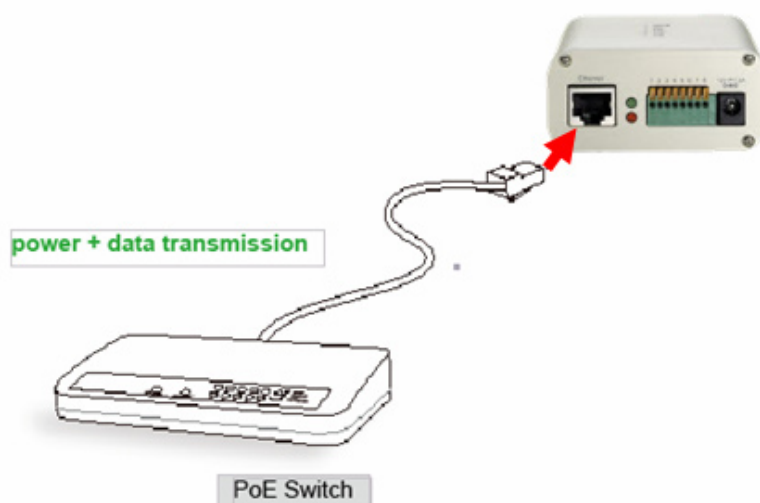
## Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 34 for details.

## Set up the Video Server through Power over Ethernet (PoE)

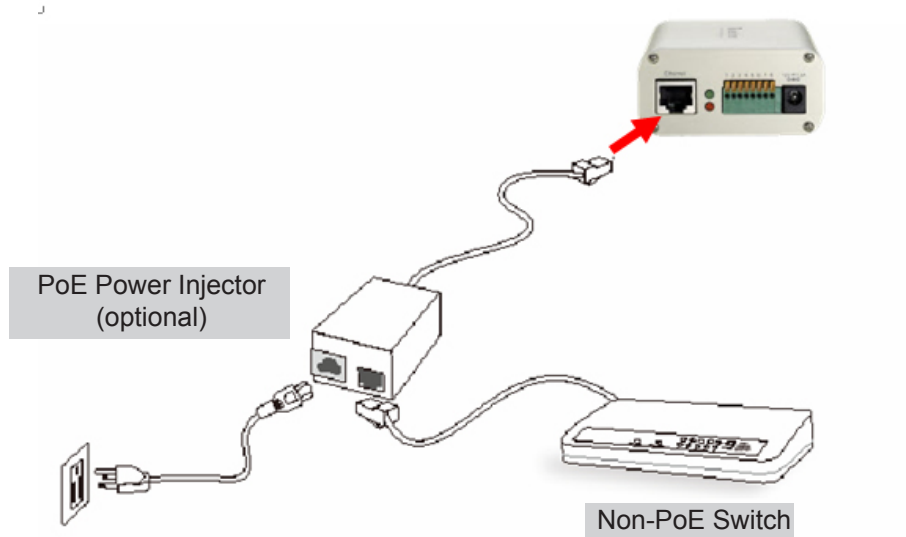
### When using a PoE-enabled switch

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



### When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the video server and a 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

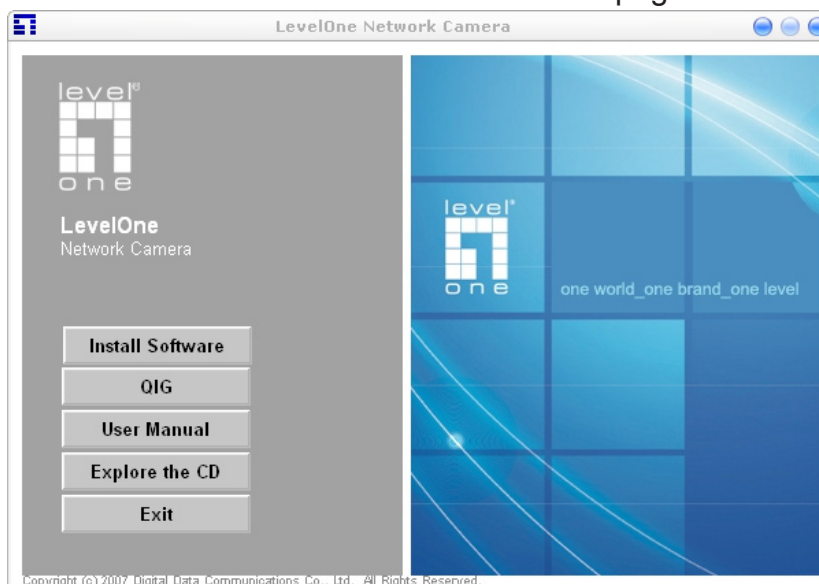
### How to Use Installation Wizard

#### **Installation**

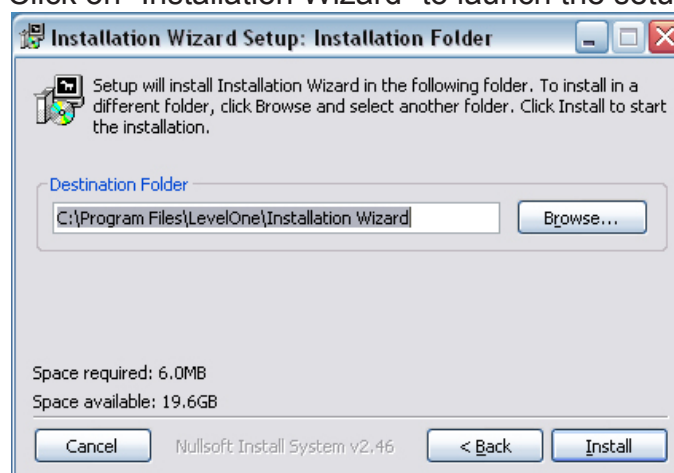
The following are steps for the software installation.

**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.

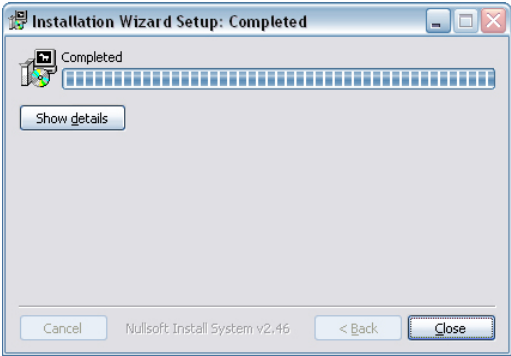


**STEP. 3** There are links on this page, including Installation Wizard, User’s Manual and Surveillance Software. Click on “Installation Wizard” to launch the setup program.



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

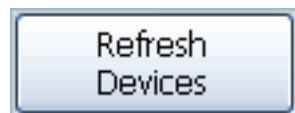
Once you run the Installation Wizard, after a short searching time, you will see the user interface as below. “**Manual Setup**” button, a “**Refresh Devices**” button and an arrow button on the left panel of your user interface. When you click on the arrow button, you will see more advanced functional 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.

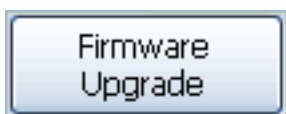
## Buttons



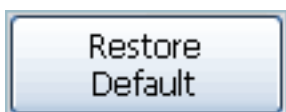
Click on this button to clean up the device list and search all devices on the within the same subnet again. It will take about 5 seconds.



Click on this button to modify the settings of the selected devices. For more detail, please refer to 0 Setup.



Click on this button to upgrade the firmware of the selected devices. For more detail, please refer to 0 Upgrade.



Click on this button to reset the selected devices to default settings.

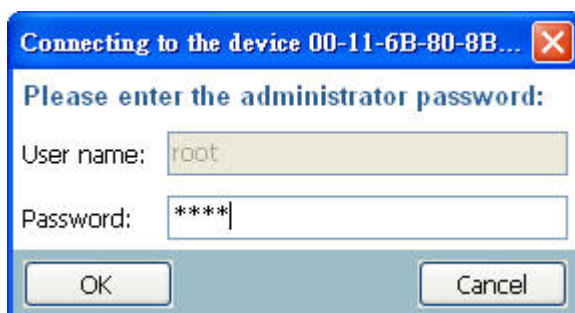


Click on this button to get information about the Installation Wizard.

## Manual Setup

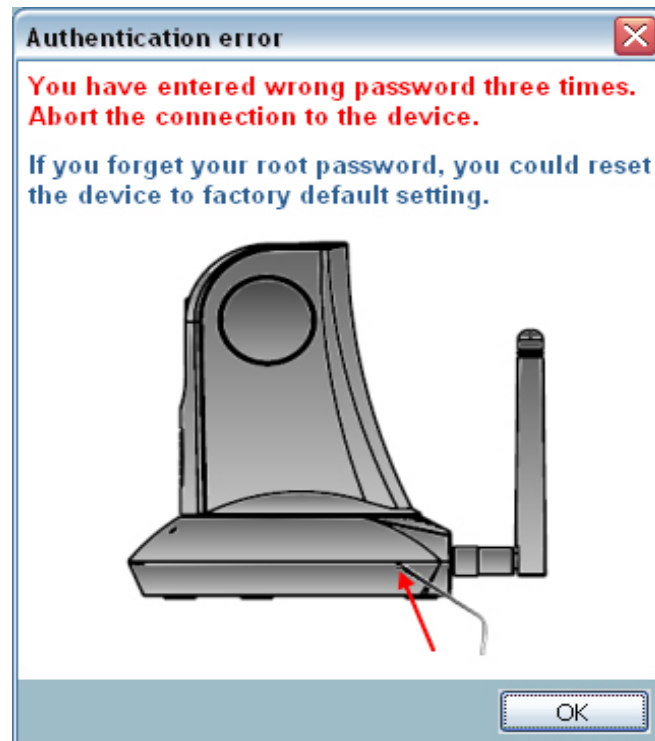
When you select one device in the selection list, the “Manual Setup” button will be enabled. Click on it to modify the settings of the selected device. After clicked on the “Manual Setup” button, Installation Wizard would try to connect to the selected device.

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

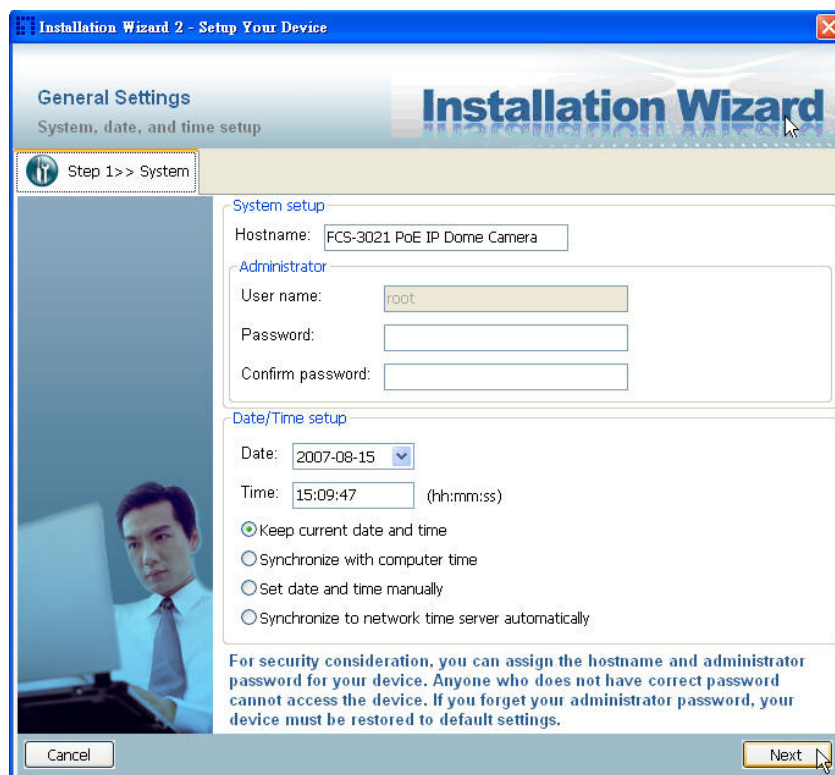




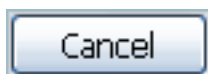
Authentication error

## 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

Date:

Time:  (hh:mm:ss)

☒ Keep current date and time

☐ Synchronize with computer time

☐ Set date and time manually

☐ Synchronize to network time server automatically

Date/Time setup

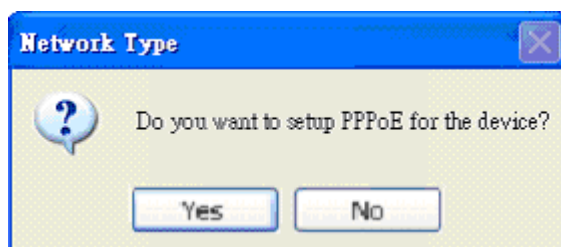
There are three ways to adjust system date and time:

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**”.

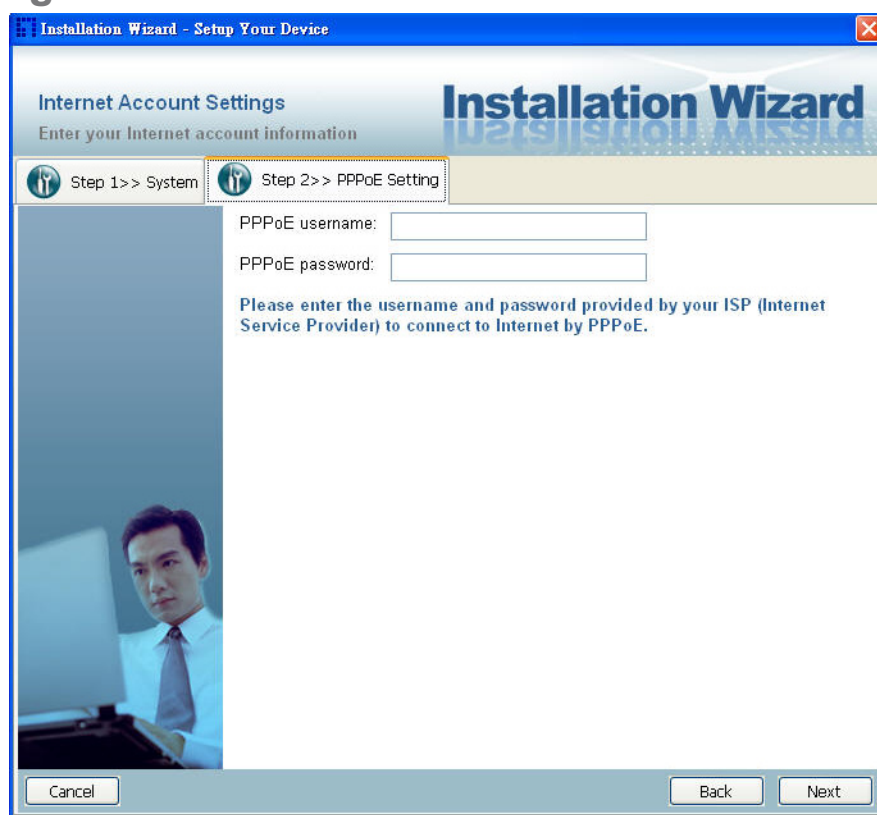
## Network Setting

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

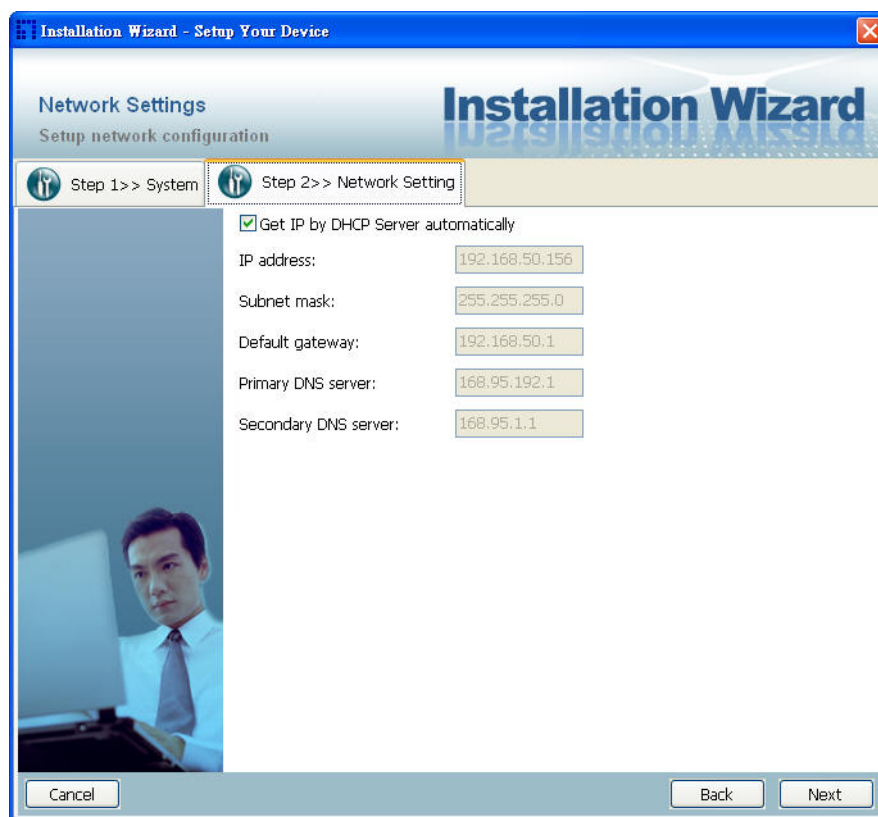


Network setting for PPPoE

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

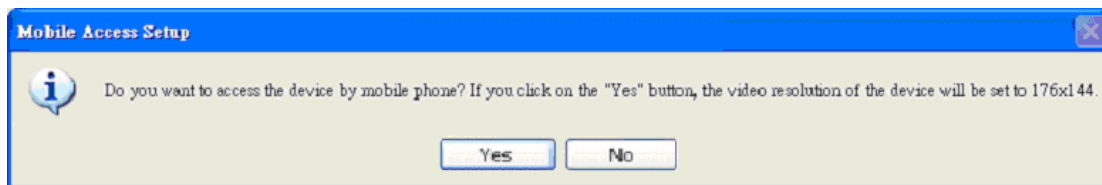
You could set up the network with DHCP or fixed IP:

- 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:

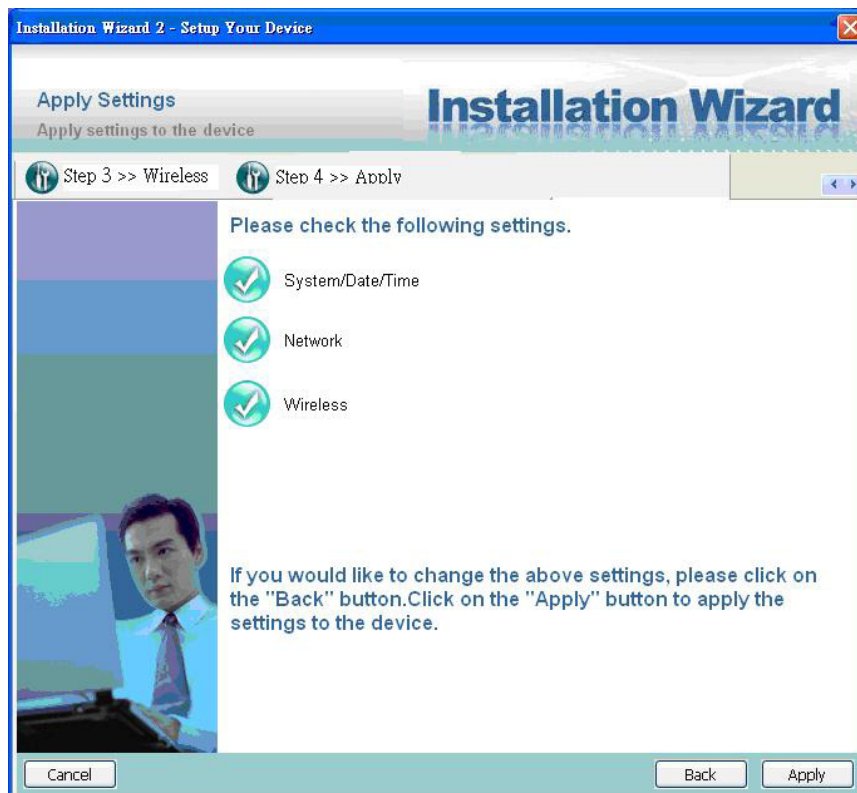
- 1.Video: The video codec will be set to MPEG-4, and the resolution will be set to 176x144 pixels.
- 2.Audio: The audio codec will be set to AAC.



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

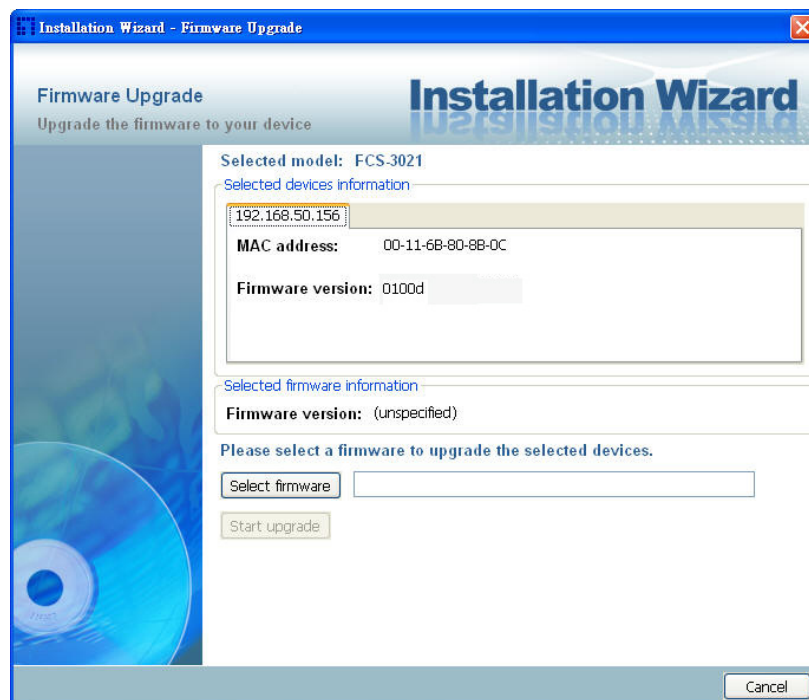
When you select one device or multiple devices (of the same model), the “**Firmware Upgrade**” button will be enabled. Click on it to upgrade the firmware of the selected device(s). After click on the “**Firmware Upgrade**” button, Installation Wizard will try to connect the selected device(s) and lead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



Click on the "Firmware Upgrade"

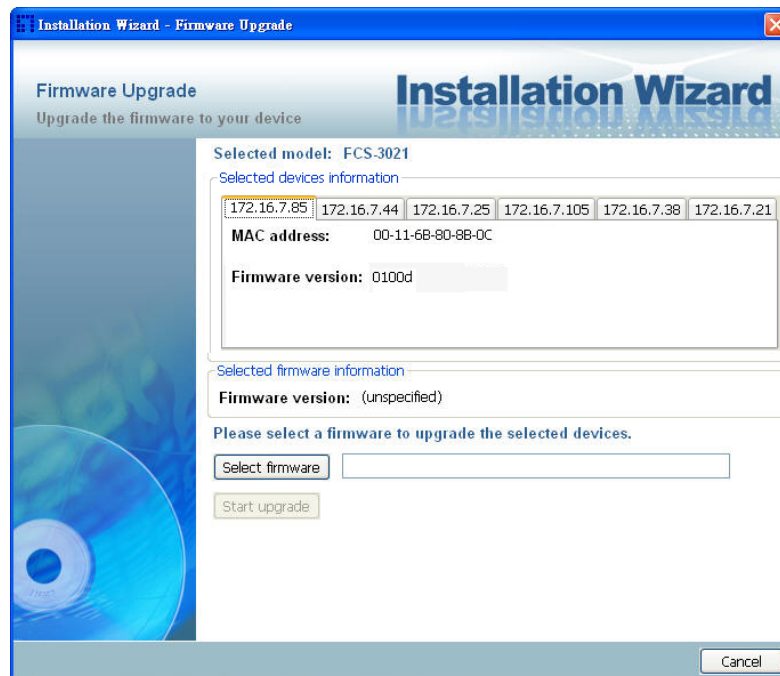
## Device Information

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

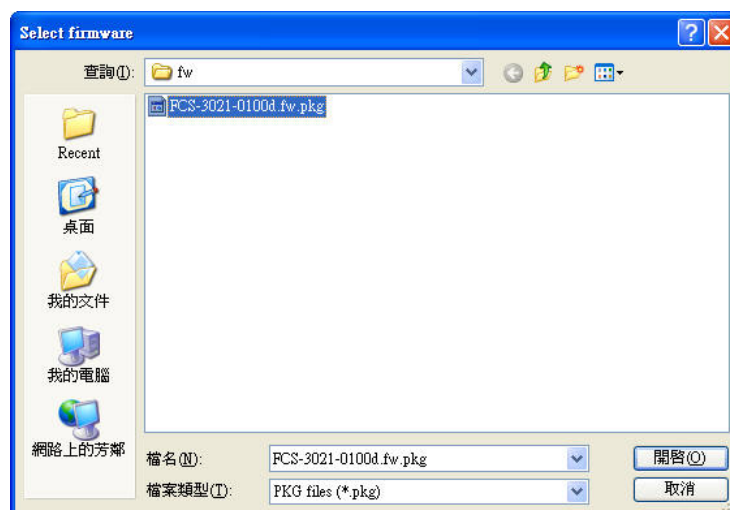
## Firmware Information

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

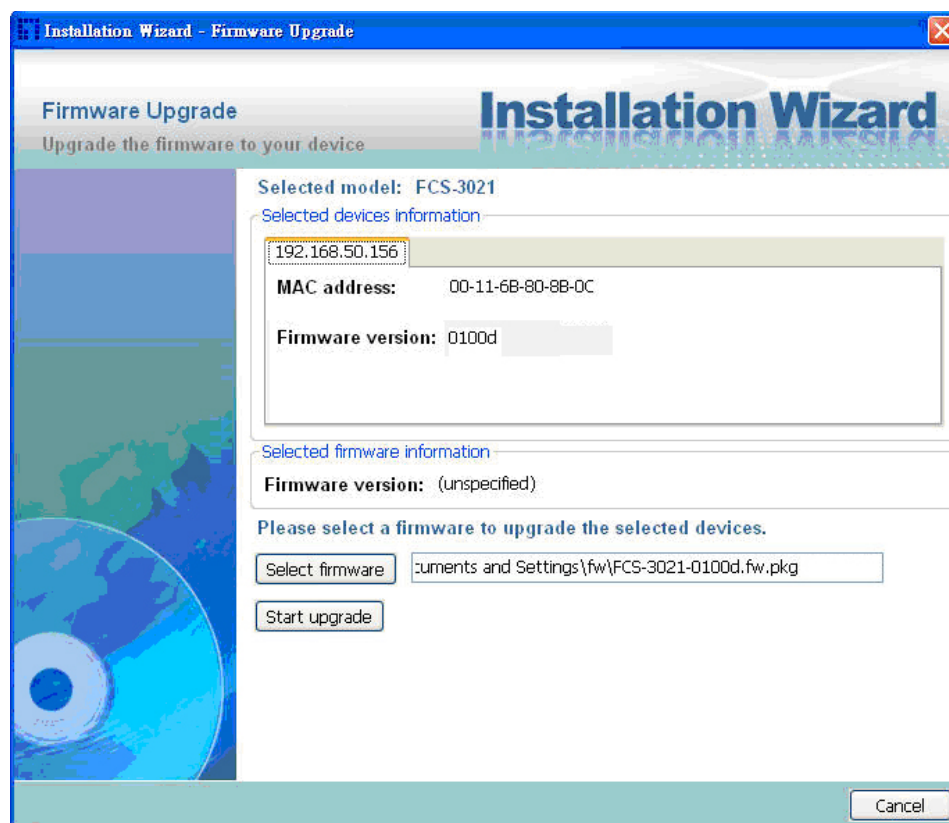
**Firmware version:** The version number of the selected firmware.

## Select Firmware

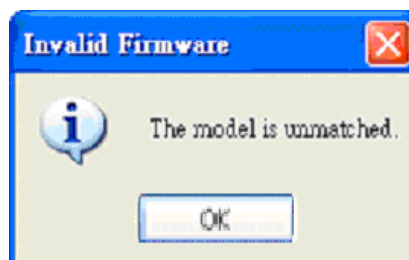
You can use the “Select firmware” button to browse the file that you want upgrade onto the selected device(s). After selected the file, Installation Wizard will check whether the file you selected is correct. If it's the correct version, then the package information will display the information about 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

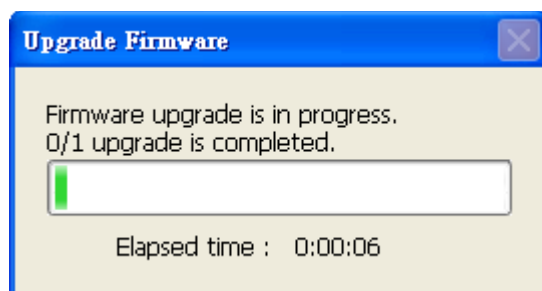


Warning message for unmatched firmware



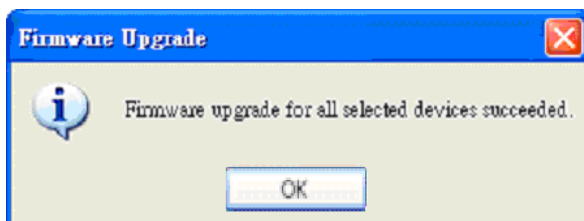
## Start Upgrade

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 Video Server

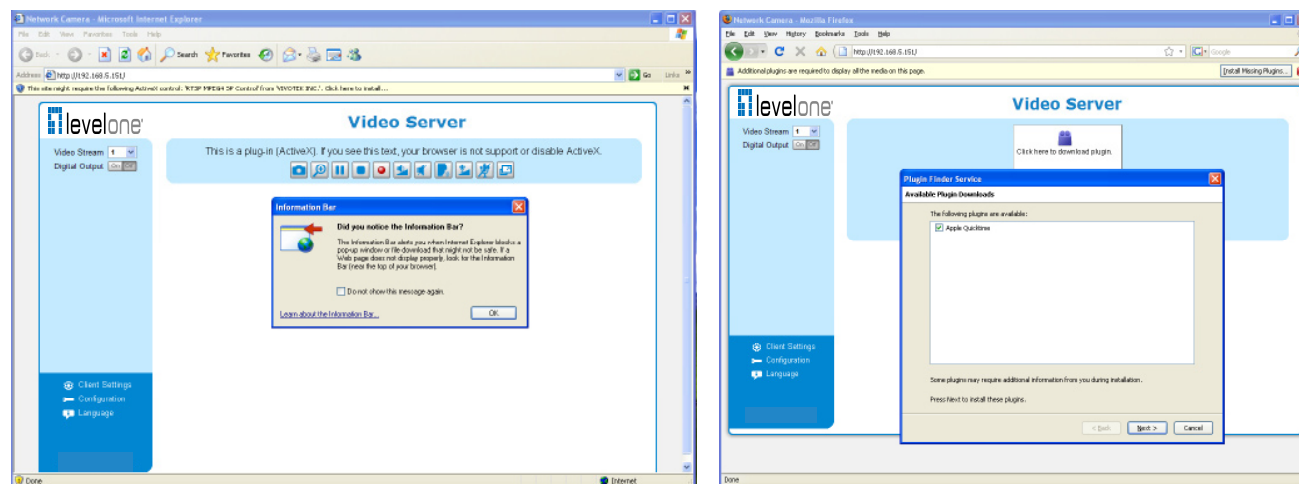
This chapter explains how to access the video server through web browsers, RTSP players, 3GPP-compatible mobile devices, and LevelOne recording software.

## Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the video servers on the LAN.

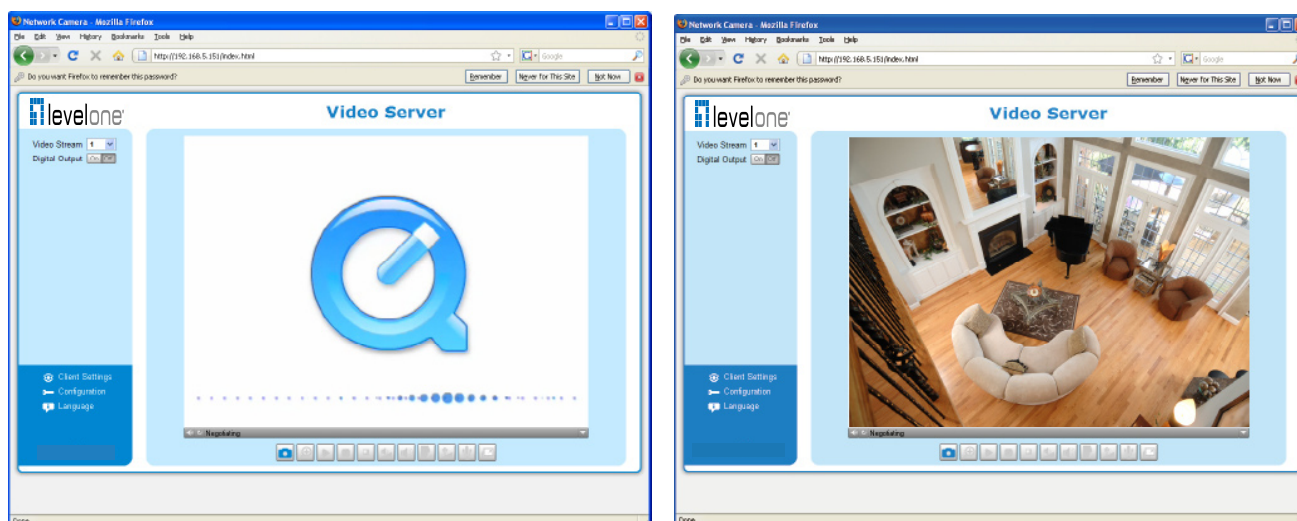
If your network environment is not a LAN, follow these steps to access the Network Camera:

1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the video server 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 video server, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.



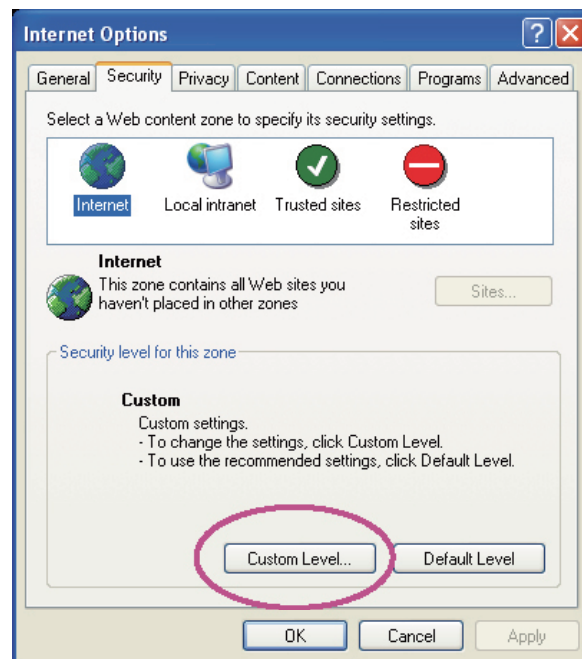
### **NOTE**

- For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.

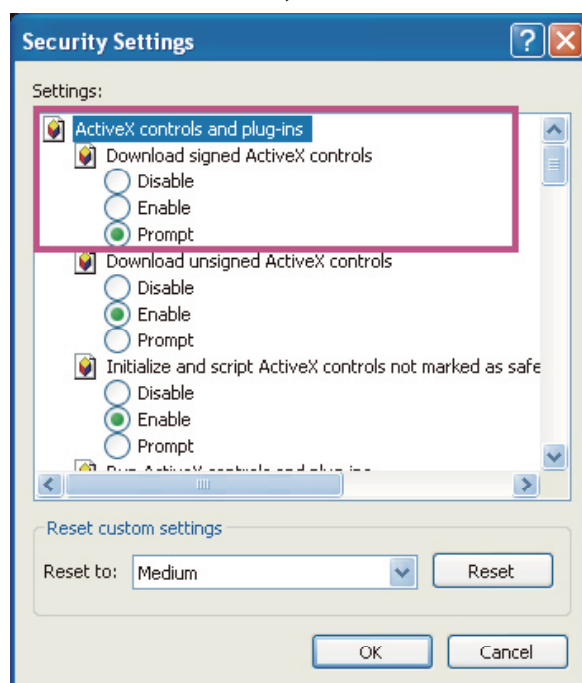


- By default, the video server is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the video server.  
For more information about how to enable password protection, please refer to Security on page 26.
- If you see a dialog box indicating that your 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

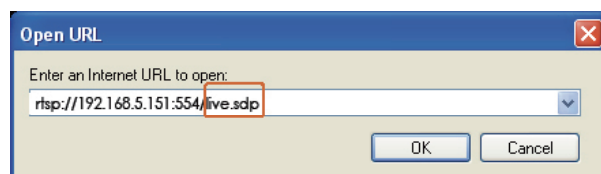


Real Player

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

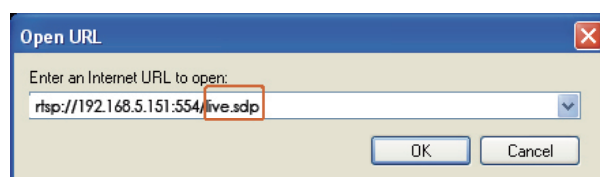
To view the streaming media through 3GPP-compatible mobile devices, make sure the video server can be accessed over the Internet. For more information on how to set up the video server over the Internet, please refer to Setup the video server over the Internet on page 7.

To utilize this feature, please check the following settings on your video server:

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.

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

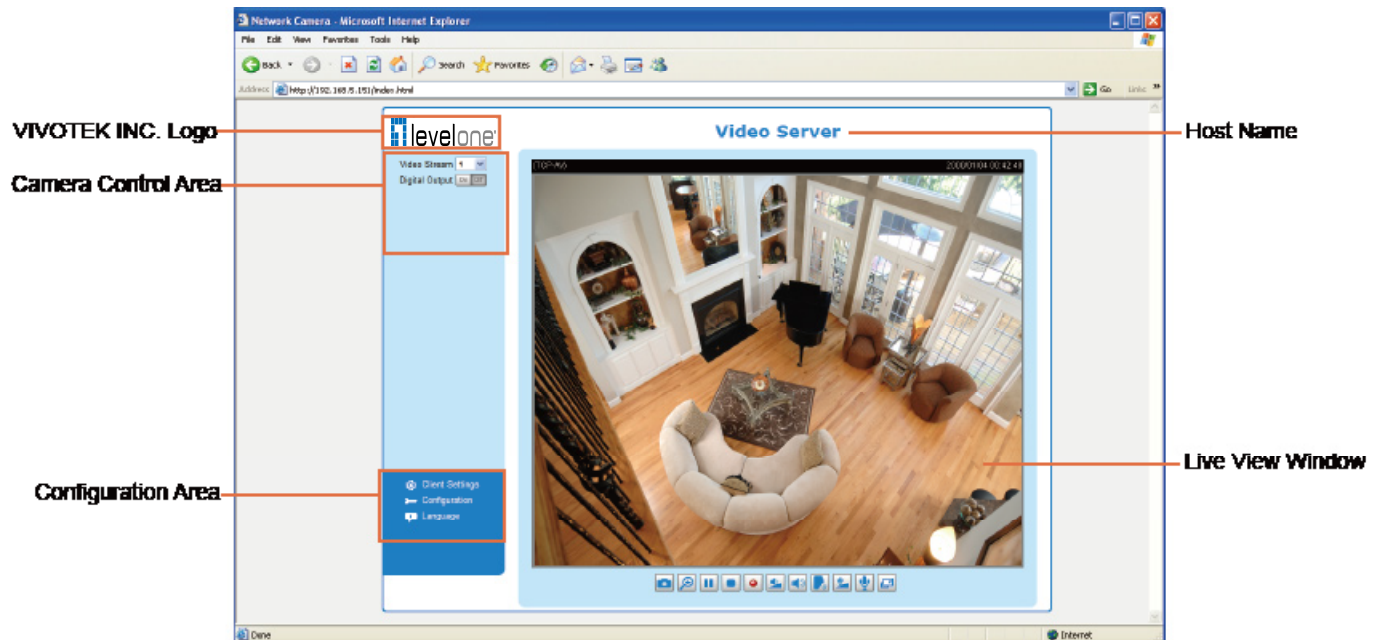
The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple video servers. Please install the recording software; then launch the program to add the video server to the Channel list. For detailed information about how to use the recording 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 video server 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 56 for detailed information.

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

## Configuration Area

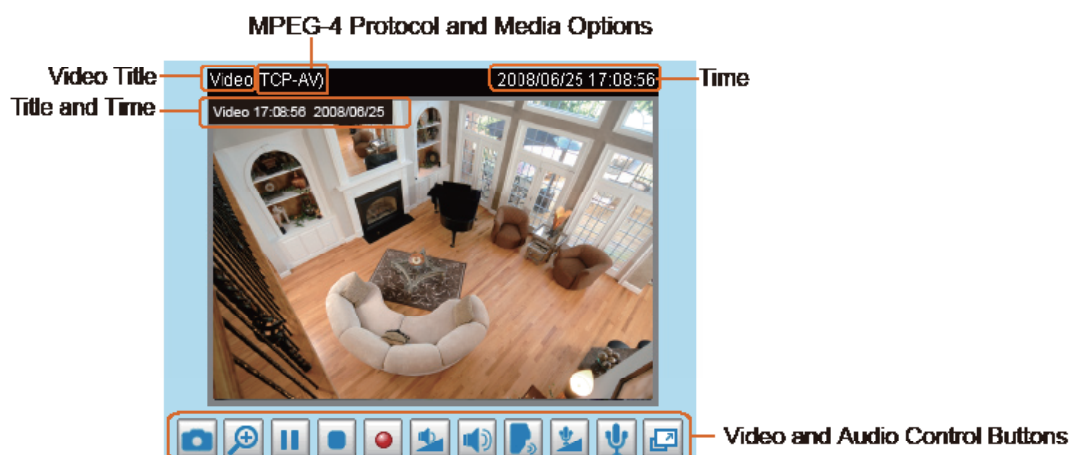
**Client Settings:** Click this button to access the client setting page. For more information, please refer to Client Settings on page 21.

**Configuration:** Click this button to access the configuration page of the video server. It is suggested that a password be applied to the video server so that only the administrator can configure the video server. 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, 簡體中文, and 繁體中文.

## Live Video Window

- The following window is displayed when the video mode is set to MPEG-4:




Video Title: The video title can be configured. For more information, please refer to Video Settings on page 53.


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

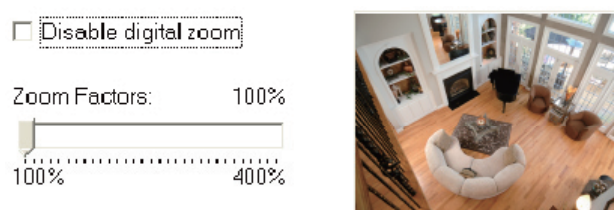
Time: Display the current time. For further configuration, please refer to Video Settings on page 53.



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 video server model and video server 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.

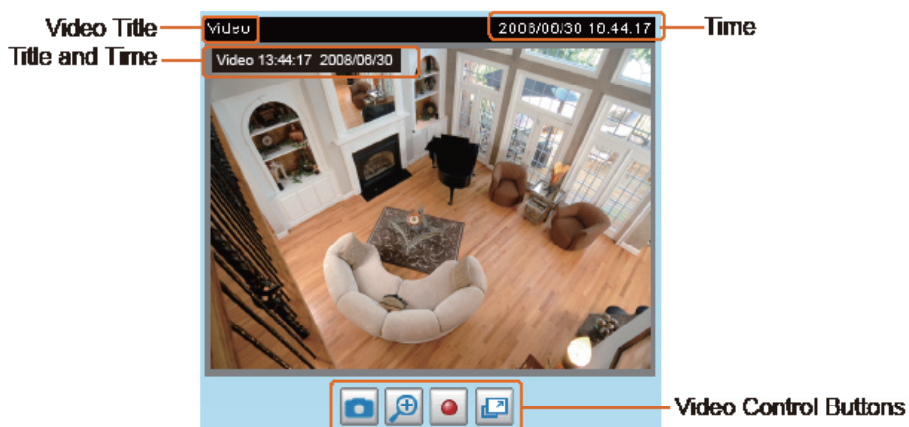
 **Talk:** Click this button to talk to people around the video server. Audio will project from the external speaker connected to the video server. Click this button  again to end talking transmission.

 **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 video server model and video server 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.

 **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.

☐ Disable digital zoom

Zoom Factors: 100%



# 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

H.264/MPEG-4 Media Options

☒ Video and Audio

☐ Video Only

☐ Audio Only

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

H.264/MPEG-4 Protocol Options

☐ UDP Unicast

☐ UDP Multicast

☒ TCP

☐ HTTP

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 video server 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 video server while serving multiple clients at the same time. Note that to utilize this feature, the video server 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

**MP4 Saving Options**

Folder:

File name prefix:

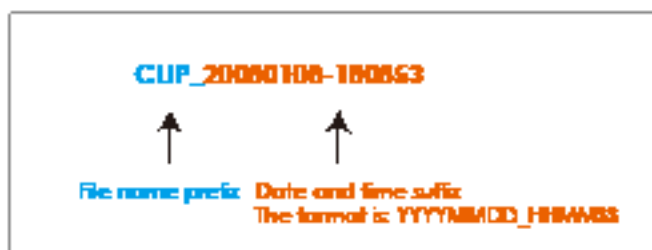
☒ Add date and time suffix to file name

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.

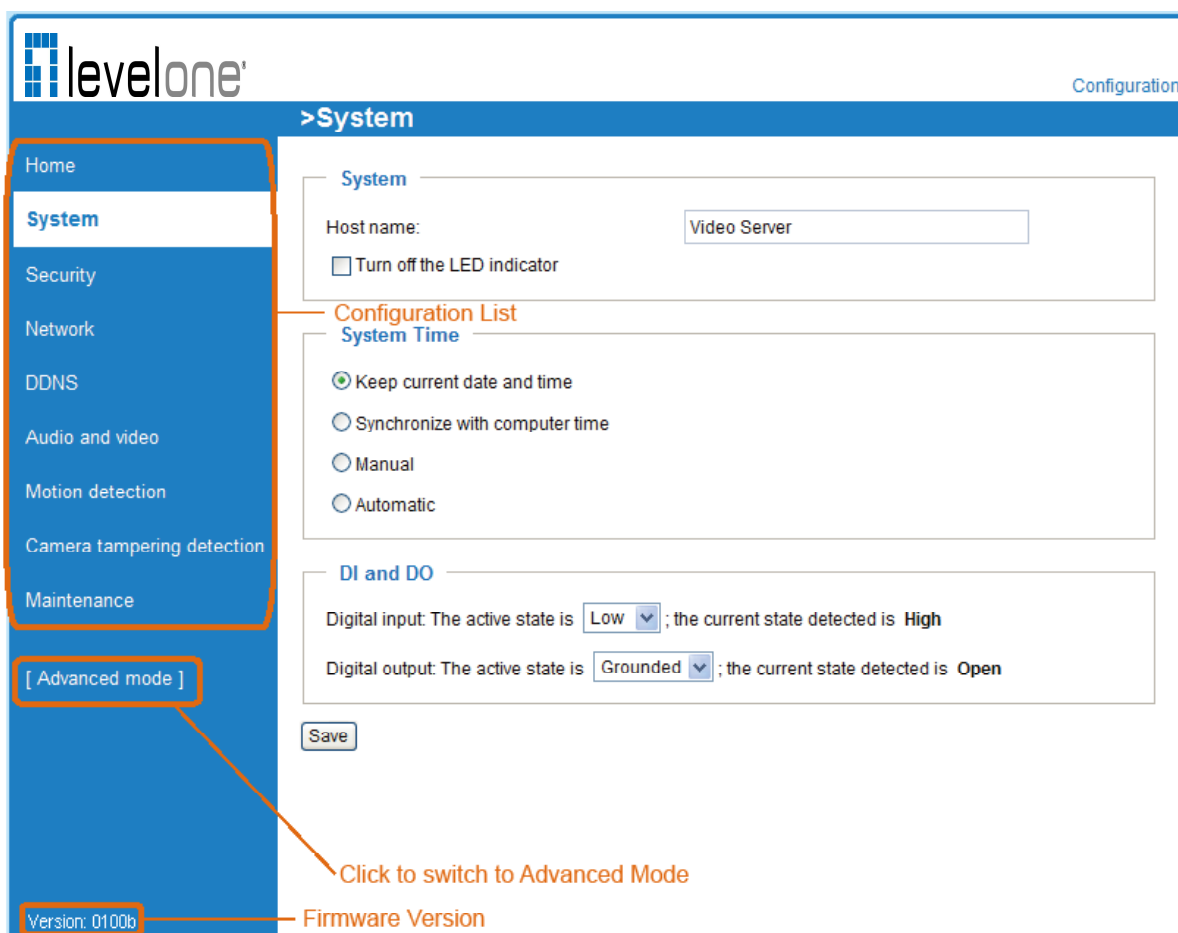
LevelOne offers an easy-to-use user interface that helps you set up your video server with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (HTTPS/ Access list/ 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.

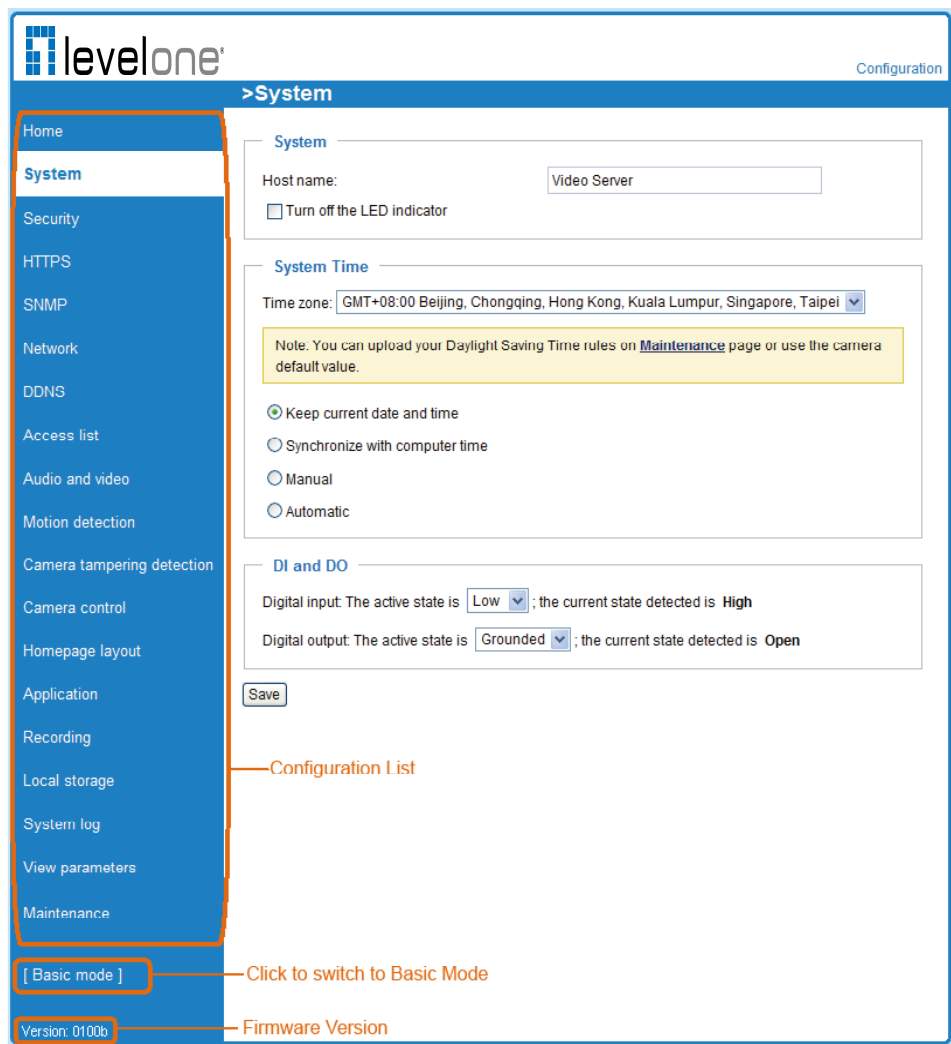
In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second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

System

Host name:

Video Server

☐ Turn off the LED indicator

**Host name:** Enter a desired name for the video server. 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 video server is in operation, you can select this option to turn off the LED indicators.

## System Time

**System Time**

Time zone: GMT+08:00 Beijing, Chongqing, 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 Video server. The video server'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 video server 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 video server 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 93 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 video server will report the current status.

**Digital output:** Select Grounded or Open to define normal status for the digital output. The video server 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 video server.

## Manage Privilege Advanced Mode

Manage Privilege

	Operator	Viewer
Digital Output:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTZ control:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow anonymous viewing		

Save

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 video server 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:

User name:

User password:

Confirm user password:

Privilege: 

Administrator  
Administrator  
Operator  
Viewer

Delete

Add

Update

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 video server on page 96. 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.

**Enable HTTPS**

\*To enable HTTPS, you have to create and install certificate first.

☒ Enable HTTPS secure connection:

☒ HTTP & HTTPS ☐ HTTPS only

**Save**

**Create and install certificate method**

☒ Create self-signed certificate automatically

☐ Create self-signed certificate manually:

☐ Create certificate request and install:

### Create and Install Certificate Method

Before using HTTPS for communication with the video server, 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.

**Enable HTTPS**

\*To enable HTTPS, you have to create and install certificate first.

☒ Enable HTTPS secure connection:

☒ HTTP & HTTPS ☐ HTTPS only

**Save**

**Create and install certificate method**

☒ Create self-signed certificate automatically

☐ Create self-signed certificate manually:

☐ Create certificate request and install:

**Certificate Information**

Status: Not installed

**Property** **Remove**

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

**Certificate Information**

Status: Active

Country:

State or province:

Locality:

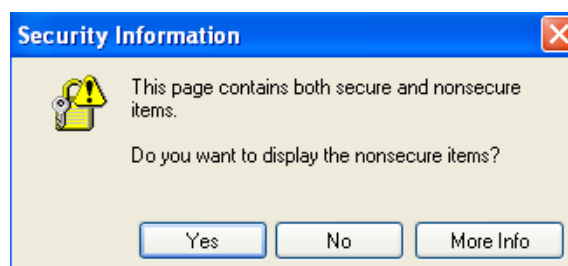
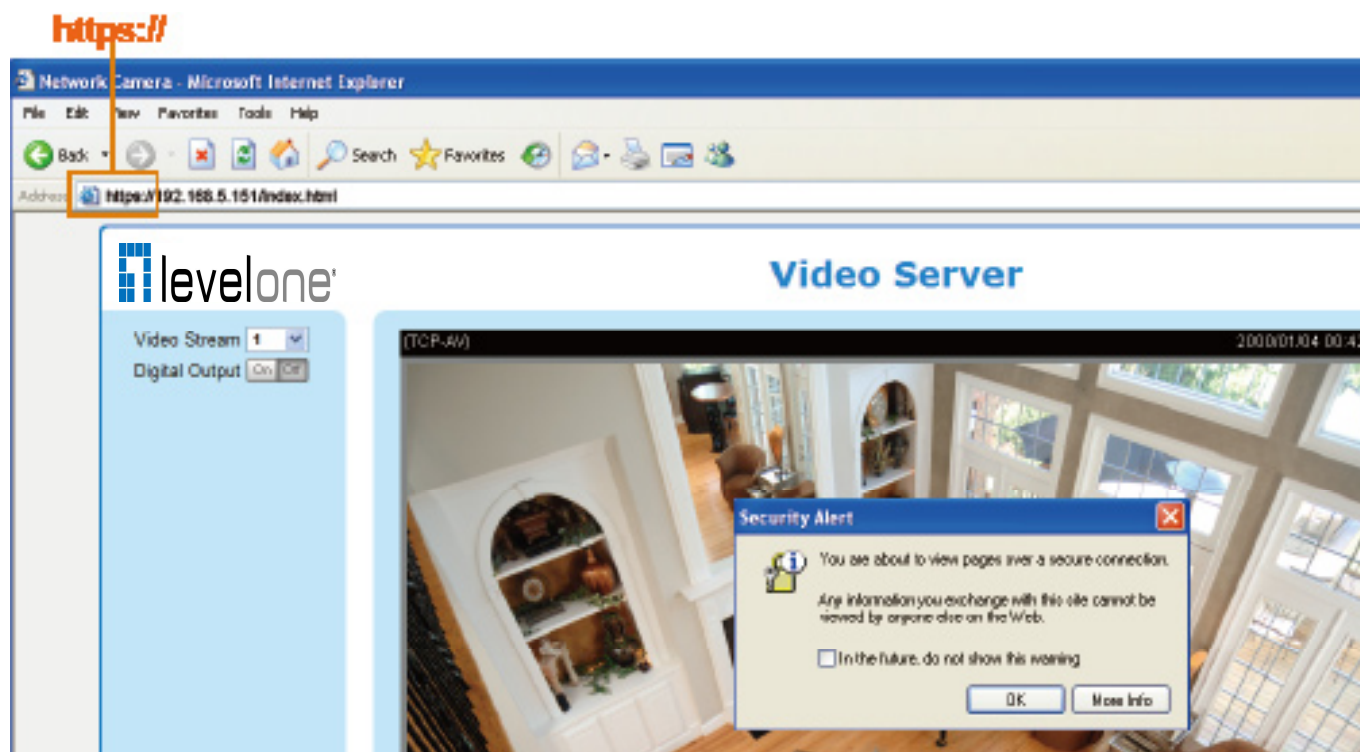
Organization:

Organization Unit:

Common Name:

**Property** Remove

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.

**Create and install certificate method**  
☐ Create self-signed certificate automatically  
☒ Create self-signed certificate manually:  
Self-signed certificate:   
☐ Create certificate request and install:

**Create Certificate**  
Country:   
State or province:   
Locality:   
Organization:   
Organization Unit:   
Common Name:   
Validity:  days

Please wait while the certificate is being generated...

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.

**Certificate Information**  
Status:   
Country:  
State or province:  
Locality:  
Organization:  
Organization Unit:  
Common Name:

**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 and install certificate method**  
☐ Create self-signed certificate automatically  
☐ Create self-signed certificate manually:  
☒ Create certificate request and install:  
Certificate request:   
Select certificate file:

Create Certificate

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name:

Validity:

9999

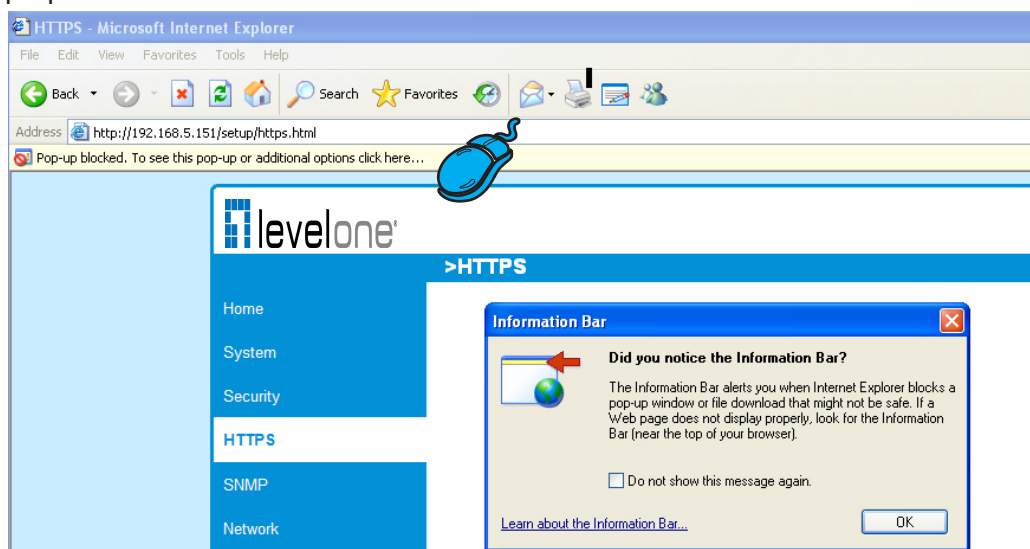
days

Save

Close

Please wait while the certificate is being generated...

- 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.



- 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
BgNVBACTCUNpdHkgTmFtZTEaMBGGA1UEChMRMT3JnYW5pemF0aW9uIE5hbWUxEjAQ
BgNVBAsTCVVueXQgTmFtZTETMBEGA1UEAxMKSVAgQWRkcmlVczCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAuOT75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27ffSLG57bW9S0xrWuLhSvRZW
mCD+/ / AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCieDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAaAAaMAOGCSqGSIb3DQEBBQUAA4GBAAVazWOAtftfU9dyFgTxOY01D/ zO
FOTkbnDQG18e4ftJ3rR0D1TvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqdcUqG1X
50bLG1subWsxR88PngaBwjYoTpG3q1zvUPJZLAVmdL3neSurTbABXOScCHOQgtH+
PX9dw4OJWkIC8QhV
-----END CERTIFICATE REQUEST-----

```

- Look for a trusted certificate authority that issues digital certificates. Enroll the video server. 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.

**Create and install certificate method**

☐ Create self-signed certificate automatically  
☐ Create self-signed certificate manually:  
☒ Create certificate request and install:

Certificate request:   
 Select certificate file:

---

**Certificate Information**

Status:

## NOTE

- How do I cancel the HTTPS settings?

- Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.
- Click **OK** to disable HTTPS.

**Enable HTTPS**

\*To enable HTTPS, you have to create and install certificate first.

☐ Enable HTTPS secure connection:

**Create and install certificate method**

☒ Create self-signed certificate automatically  
☐ Create self-signed certificate manually:

**Microsoft Internet Explorer**

?

This will stop the HTTPS service, do you really want to stop it?

- 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.

**Certificate Information**

Status:

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name:

IP Address

**Microsoft Internet Explorer**

?

Are you sure you want to delete the certificate?

## SNMP (Simple Network Management Protocol) Advanced Mode

This section explains how to use the SNMP on the video server. 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, video servers, 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:	<input type="text" value="Private"/>
Read only community:	<input type="text" value="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 authentication (at least 8 characters).
- Encryption password: Enter a password for encryption (at least 8 characters).

☒ Enable SNMPv3

SNMPv3 Settings

Read/Write Security name:	<input type="text" value="Private"/>
Authentication Type:	<input type="button" value="MD5"/>
Authentication Password:	<input type="text"/>
Encryption Password:	<input type="text"/>
Read only Security name:	<input type="text" value="Public"/>
Authentication Type:	<input type="button" value="MD5"/>
Authentication Password:	<input type="text"/>
Encryption Password:	<input type="text"/>

## Network

This section explains how to configure a wired network connection for the video server.

### Network Type

Network Type

☒ LAN:

☒ Get IP address automatically

☐ Use fixed IP address:

☒ Enable UPnP presentation

☐ Enable UPnP port forwarding

☐ PPPoE:

☐ Enable IPv6

Save

### LAN

Select this option when the video server 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. Remember to click **Save** when you complete the Network setting.

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

Use fixed IP address: Select this option to manually assign a static IP address to the video server.

Network Type

☒ LAN:

☐ Get IP address automatically

☒ Use fixed IP address:

IP address: 192.168.5.109

Subnet mask: 255.255.255.0

Default router: 192.168.5.1

Primary DNS: 192.168.0.10

Secondary DNS: 192.168.0.20

Primary WINS server:

Secondary WINS server:

☒ Enable UPnP presentation

☐ Enable UPnP port forwarding

☐ PPPoE:

☐ Enable IPv6

Save

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.

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

Default router: 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.

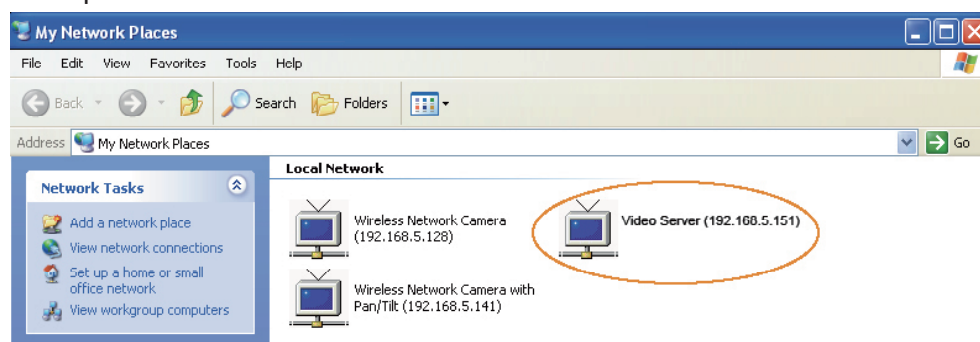
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

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™ presentation for your video server so that whenever a video server is presented to the LAN, shortcuts of connected video servers will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



Enable UPnP port forwarding: To access the video server from the Internet, select this option to allow the video server 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™ and it is activated.

### PPPoE (Point-to-point over Ethernet)

Select this option to configure your video server 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 video server's public IP address.

1. Set up the video server on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page 76) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 79). 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.

**Network Type**

☐ LAN:

☒ PPPoE:

User name:

Password:

Confirm password:

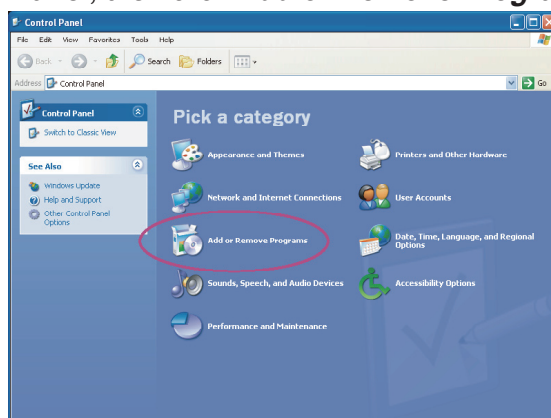
5. The video server will reboot.
6. Disconnect the power to the video server; remove it from the LAN environment.



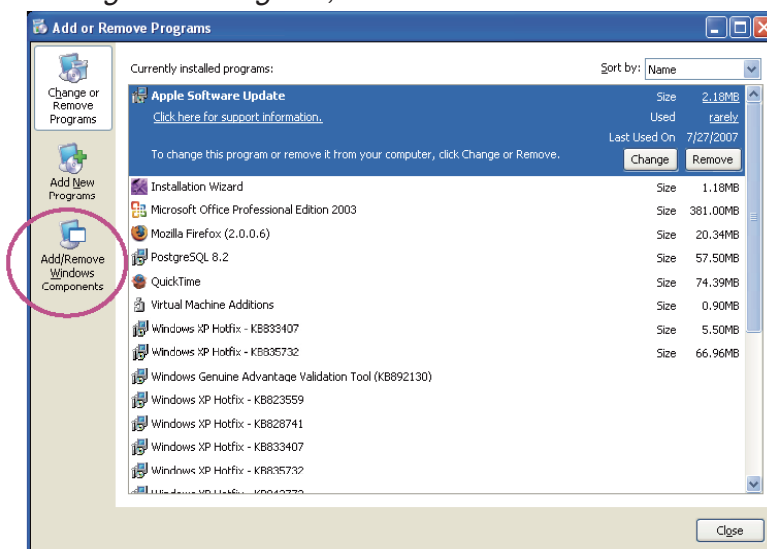
## NOTE

- ▶ If the default ports are already used by other devices connected to the same router, the video server will select other ports for the video server.
- ▶ If UPnP™ 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™ user interface on your computer:  
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

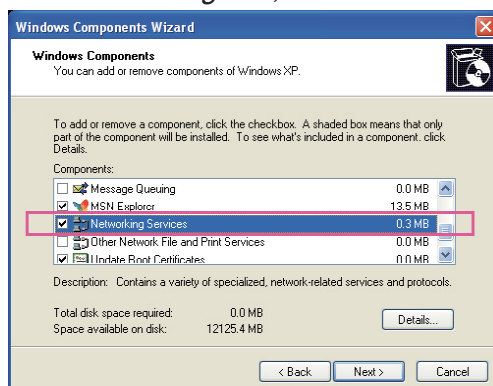
1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.



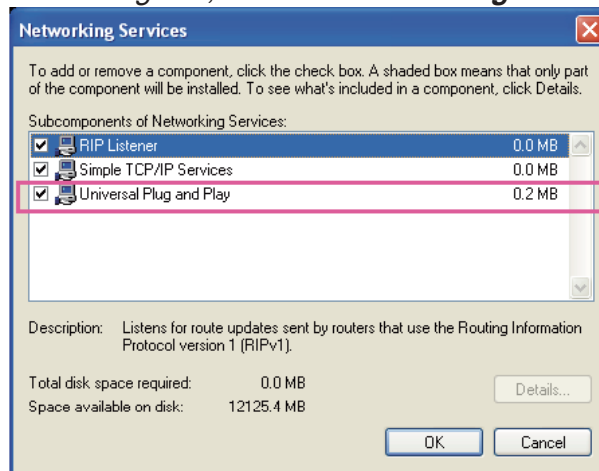
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.



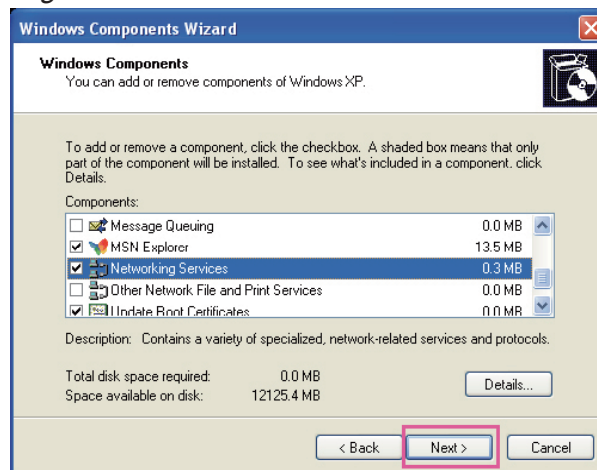
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.



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™ is enabled.

► **How does UPnP™ work?**

UPnP™ 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 video servers, you will see video server shortcuts under *My Network Places*.

► **Enabling UPnP port forwarding allows the video server 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 video server's public address in order to access the video server 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 video server'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 video server to factory default; please refer to Restore on page 92 for details. After the video server 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.

Network Type

☒ LAN:

☒ Get IP address automatically

☐ Use fixed IP address:

☒ Enable UPnP presentation

☐ Enable UPnP port forwarding

☐ PPPoE:

☒ Enable IPv6

IPv6 Information

☐ Manually setup the IP address

Save

When IPv6 is enabled, by default, the video server 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.

IPv6 NET Information

[eth0 address]

IPv6 address list of host

[Gateway]

IPv6 address list of gateway

[DNS]

IPv6 address list of DNS

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:

Refers to Ethernet

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

Link-global IPv6 address/network mask

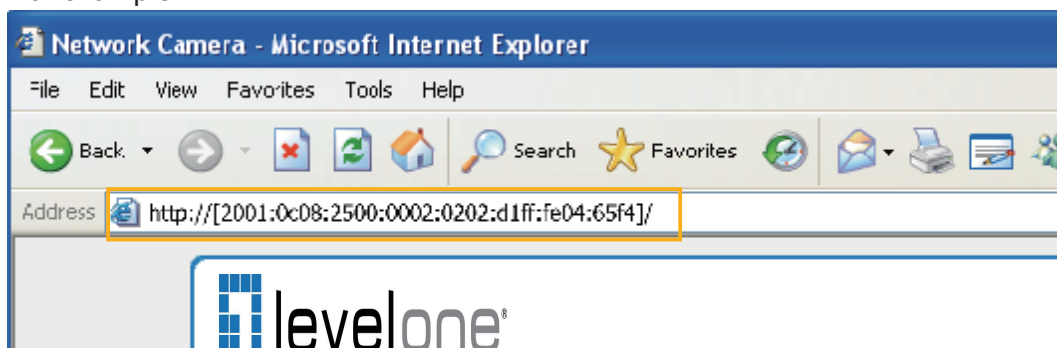
Link-local IPv6 address/network mask

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:

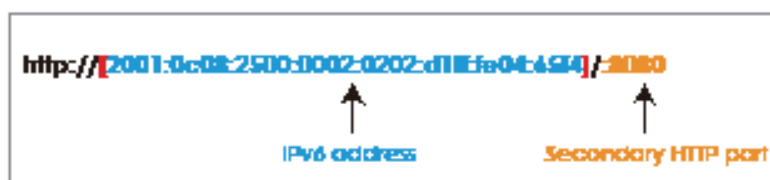


4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.  
For example:



#### 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:



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 video servers 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 video server 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 video server to a PC or notebook outside of the protected LAN. Open the configuration page of the video server 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).

**IEEE 802.1x**

☒ Enable 802.1x

EAP method: EAP-PEAP ▼

Identity:

Password:

CA certificate:

Status: no file

**IEEE 802.1x**

☒ Enable 802.1x

EAP method: EAP-TLS ▼

Identity:

Private key password:

CA certificate:  Browse... Upload

Status: no file Remove

client certificate:  Browse... Upload

Status: no file Remove

Client private key:  Browse... Upload

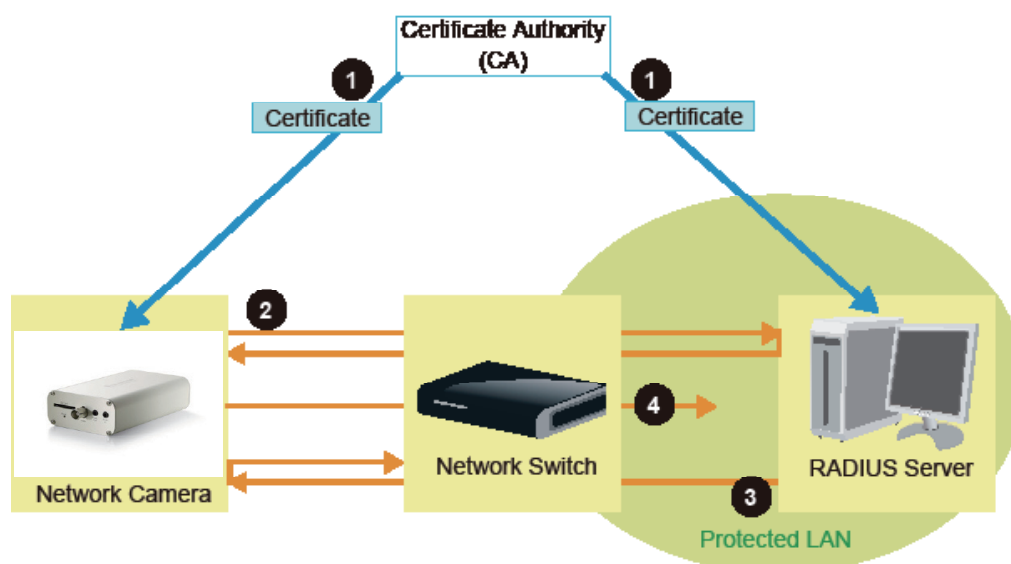
Status: no file Remove

3. When all settings are complete, move the video server 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 video server (the supplicant) and the RADIUS Server (the authentication server).*
2. *A video server 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 video server and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the video server.*
4. *Assuming all certificates are validated, the switch then changes the video server'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).

QoS/DSCP

☒ Enable QoS/DSCP

Live video:

0

Live audio:

0

Event/Alarm:

0

Management:

0



## HTTP Advanced Mode

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

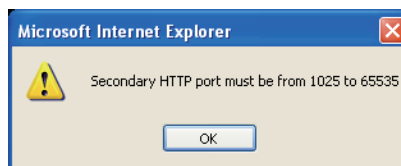
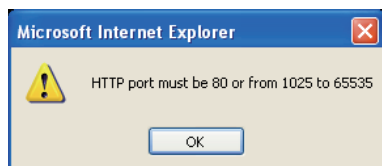
**HTTP**

Authentication:	basic
HTTP port:	80
Secondary HTTP port:	8080
Access name for stream 1:	video.mjpg
Access name for stream 2:	video2.mjpg
Access name for stream 3:	video3.mjpg
Access name for stream 4:	video4.mjpg

Authentication: Depending on your network security requirements, the video server 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 video server on the LAN, both the HTTP port and secondary HTTP port can be used to access the video server. 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 video server's IP address.

on a LAN  
http://192.168.4.160 or  
http://192.168.4.160:8080

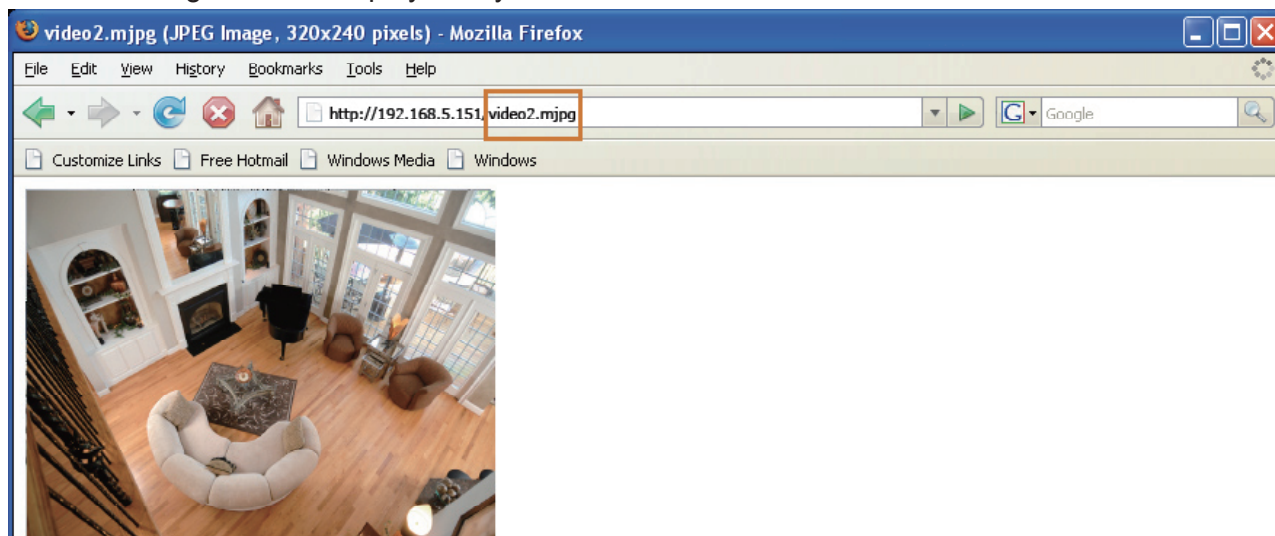
Access name for stream 1 ~ 4: This video server supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Configuration > Audio and Video > Video Settings** to set up the video quality of linked streams.

When using Mozilla Firefox or Netscape to access the video server 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 video server to feed live pictures to Mozilla Firefox and Netscape.

URL command -- <http://<ip address>:<http port>/<access name for stream 1 ~ 4>>

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 ~ 4>> will fail to access the video server.

## **HTTPS**

<b>HTTPS</b>	
HTTPS port:	<input type="text" value="443"/>

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

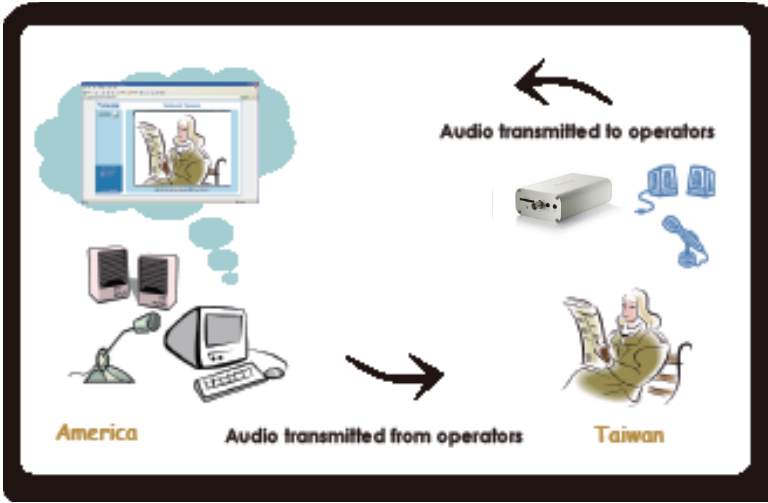
## **Two way audio**

<b>Two way audio</b>	
Two way audio port:	<input type="text" value="5060"/>

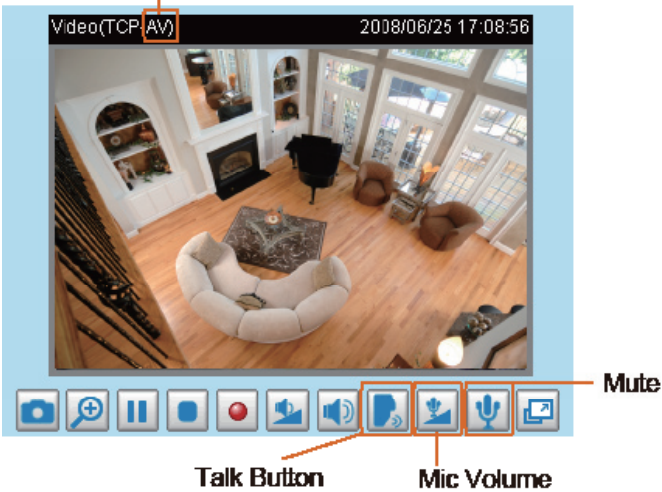
By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.





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

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.



Audio is being transmitted to the Network Camera



Click  to enable audio transmission to the video server; click  to adjust the volume of microphone; click  to turn off the audio. To stop talking, click  again.

FTP

FTP

FTP port:

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 video server first; please refer to Security on page 26 for details.

RTSP Streaming

Authentication:

disable

Access name for stream 1:

live.sdp

Access name for stream 2:

live2.sdp

Access name for stream 3:

live3.sdp

Access name for stream 4:

live4.sdp

RTSP port:

554

RTP port for video:

5556

RTCP port for video:

5557

RTP port for audio:

5558

RTCP port for audio:

5559

**Authentication:** Depending on your network security requirements, the video server 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 ~ 4:** This video server 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 video server, 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 ~ 4>`

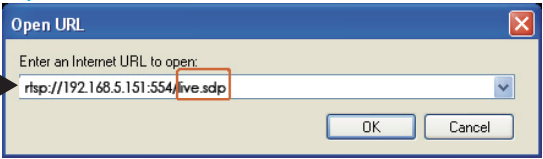
For example, when the access name for **stream 1** is set to **live.sdp**:

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.

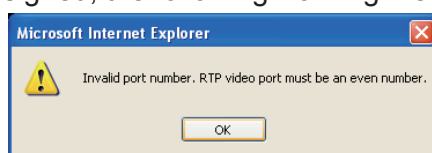


RTSP port /RTP port for video, audio/ RTCP port for video, audio

- 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 video server 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.

▼ Multicast settings for stream 1:

☐ Always multicast

Multicast group address: 239.128.1.99

Multicast video port: 5560

Multicast RTCP video port: 5561

Multicast audio port: 5562

Multicast RTCP audio port: 5563

Multicast TTL [1~255]: 15

▼ Multicast settings for stream 2:

☐ Always multicast

Multicast group address: 239.128.1.100

Multicast video port: 5564

Multicast RTCP video port: 5565

Multicast audio port: 5566

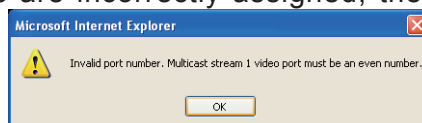
Multicast RTCP audio port: 5567

Multicast TTL [1~255]: 15

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 bandwidth.

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 video server. DDNS is a service that allows your video server, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

## DDNS: Dynamic domain name service

DDNS: Dynamic domain name service

☐ Enable DDNS:

Provider:

Dyndns.org(Dynamic) ▼

Host name:

User name:

Password:

Save

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 video servers 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.

Register

Host name:

VVTK.safe100.net

Email:

Key:

Forget key

Confirm key:

To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

Register

DDNS Registration Result:

[Register] Successfully Your account information has been mailed to registered e-mail address

▲  
▼

Upon successful registration, you can click [copy](#) to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

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.



**DDNS: Dynamic domain name service**

☒ Enable DDNS:

Provider: Safe100.net

Host name: VTK.safe100.net [\*.safe100.net]

Email:

Key:

**Save**

---

**Register**

Host name: VTK.safe100.net

Email:

Key:  **Forget key**

Confirm key:

To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

**Register**

DDNS Registration Result:

[Register] Successfully Your account information has been mailed to registered e-mail address

Upon successful registration, you can click [copy](#) to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

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\(Custom\)](http://www.dyndns.com/): visit <http://www.dyndns.com/>
- [TZO.com](http://www.tzo.com/): visit <http://www.tzo.com/>
- [DHS.org](http://www.dns.org/): visit <http://www.dns.org/>
- [dyn-interfree.it](http://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

General Settings

Maximum number of concurrent streaming connection(s) limited to: 

10

View Information

☐ Enable access list filtering

Save

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:

Connection status

	IP address	Elapsed time	User ID
<input type="checkbox"/>	192.168.1.147	12:20:34	root
<input type="checkbox"/>	61.22.15.3	00:10:09	
<input type="checkbox"/>	192.168.3.25	45:00:34	greg
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Refresh

Add to deny list

Disconnect

- IP address: Current connections to the Video server.
- 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).

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

## Filter Type

Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.

## Filter

Then you can add a rule to the following Access List. 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.

Filter

IPv4 access list

Add
Delete

IPv6 access list

Add
Delete

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

There are three types of rules:

Single: This rule allows the user to add an IP address to the Allowed/Denied list.

For example:

filter address

Rule: Single

IP address: 192.168.2.1

OK
Cancel

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

**filter address**

Rule: Network

Network address / Network mask 192.168.2.0 / 24

OK Cancel

IP address 192.168.2.x will be blocked.

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

**filter address**

Rule: Range

IP address - IP address 192.168.2.0 - 192.168.2.255

OK Cancel

### 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.

**Administrator IP address**

☐ Always allow the IP address to access this device

Save

## Audio and Video

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

### Video Settings

**Video Settings**

Video title:

Color:

Color ▾

Modulation:

Auto ▾

Select caching stream:

Stream 1 ▾

Video orientation:

☐ Flip ☐ Mirror

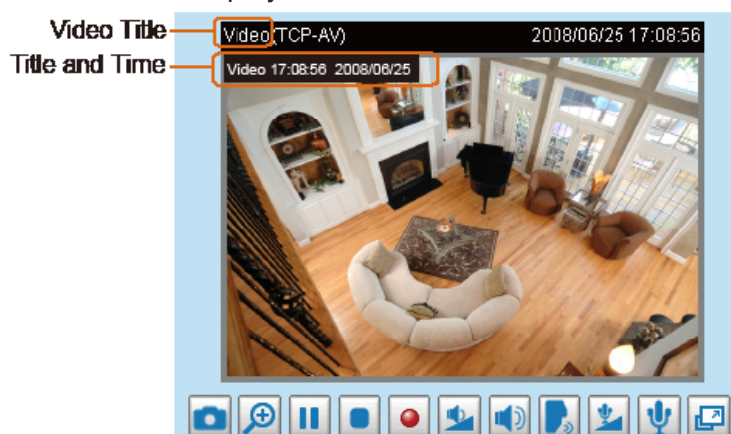
☐ Overlay title and time stamp on video and snapshot.

☐ Enable time shift caching stream

Image Settings

Privacy Mask

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.

Modulation: Select Auto, NTSC or PAL according to your linked device.

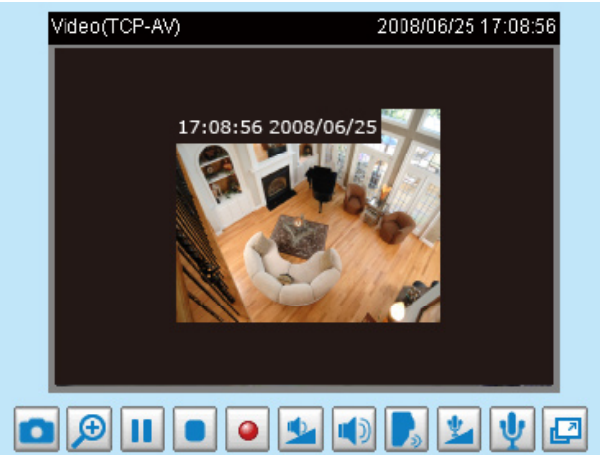
Select caching stream: This video server supports time shift cache stream on the video server. Select one stream and check the below option **Enable time shift caching stream**.

Enable time shift caching stream **Advanced Mode**: Check this item to enable the time shift cache stream on the video server, which will stores video in the video server's embedded memory for a period of time depending on the cache memory of each video server. 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 linked device is installed upside-down (ex. on the ceiling) to correct the image orientation.

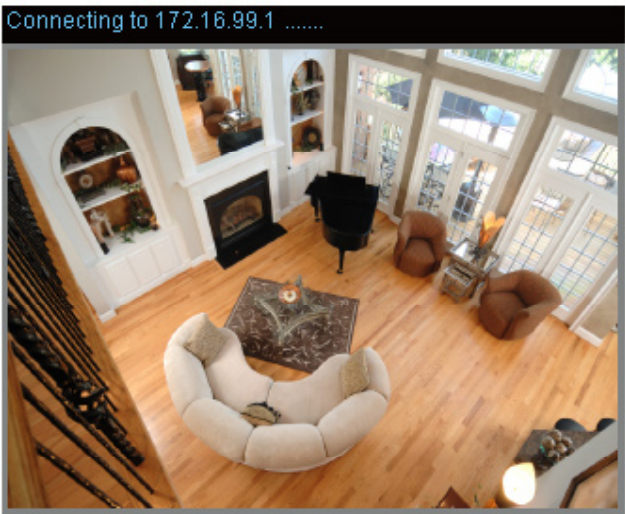
Overlay title and time stamp on video: Select this option to place the video title and time on the video streams.

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.



[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.



**Image Adjustment**

Brightness:	<input type="text" value="+0"/>	Saturation:	<input type="text" value="+0"/>
Contrast:	<input type="text" value="+0"/>	Sharpness:	<input type="text" value="+0"/>

Preview

Restore

Save

Close

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 -3 to +3.

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.

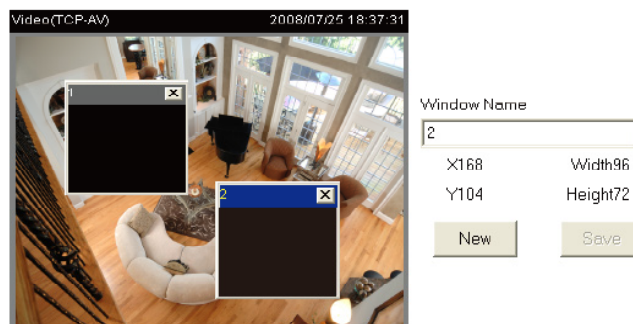
## Privacy Mask **Advanced Mode**

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.

☐ Enable privacy mask



☒ Enable privacy mask



■ 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.

## Video quality settings for stream 1 ~ 4 Advanced Mode

Click the items to display the detailed video quality settings.

Video quality settings for stream 1:

☐ MPEG-4:

☒ H.264:

Frame size:

D1

Maximum frame rate:

30 fps

Intra frame period:

1 S

Video quality:

☐ Constant bit rate:

512 Kbps

☒ Fixed quality:

Good

☐ JPEG:

Video quality settings for stream 2:

☒ MPEG-4:

☐ H.264:

Frame size:

D1

Maximum frame rate:

30 fps

Intra frame period:

1 S

Video quality:

☐ Constant bit rate:

512 Kbps

☒ Fixed quality:

Good

☐ H.264:

Video quality settings for stream 3:

☐ MPEG-4:

☐ H.264:

☒ JPEG:

Frame size:

D1

Maximum frame rate:

30 fps

Video quality:

Good

Video quality settings for stream 4:

☒ MPEG-4:

☐ H.264:

☐ JPEG:

Frame size:

QCIF

Maximum frame rate:

30 fps

Intra frame period:

1 S

Video quality:

☐ Constant bit rate:

512 Kbps

☒ Fixed quality:

Good

fixed

### NOTE

- ▶ The frame size of stream 4 is fixed to QCIF. If you want to stream out the video to a mobile device, please select stream 4.

This video server offers real-time H.264, MPEG-4, and MJPEG 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:

☒ H.264:

Frame size:

D1

Maximum frame rate:

15 fps

Intra frame period:

1/2 S

Video quality:

☐ Constant bit rate:

Customize

2048 Kbps [1~4000]

☒ Fixed quality:

Customize

7 [0~51]

#### ■ 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. The frame sizes are selectable in the following resolutions: QCIF, CIF, 4CIF, and D1.

#### ■ 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

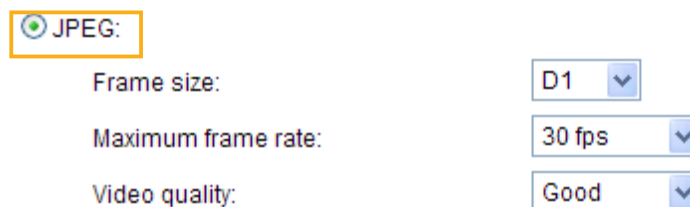
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

#### ■ 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, and 4Mbps. 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 video server 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:



☒ JPEG:

Frame size: D1

Maximum frame rate: 30 fps

Video quality: Good

#### ■ 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. The frame sizes are selectable in the following resolutions: QCIF, CIF, 4CIF, and D1.

#### ■ 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.



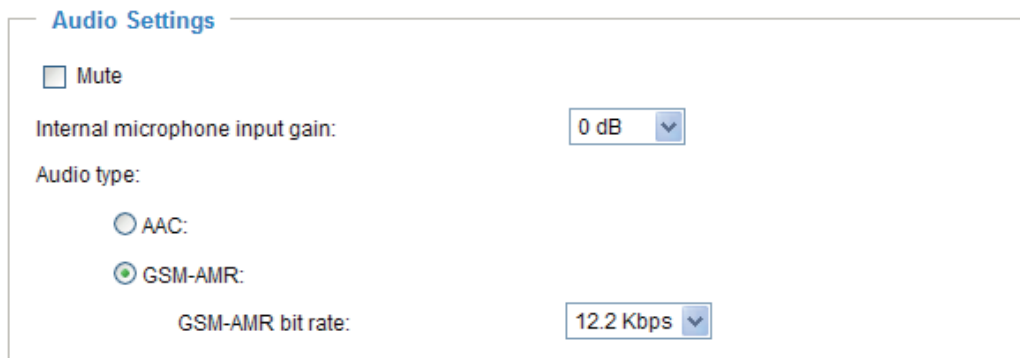
#### ■ Video quality

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 occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

### Audio Settings



**Audio Settings**

☐ Mute

Internal microphone input gain: 0 dB

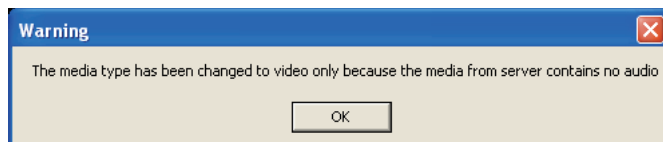
Audio type:

☐ AAC:

☒ GSM-AMR:

GSM-AMR bit rate: 12.2 Kbps

**Mute:** Select this option to disable audio transmission from the video server 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).

**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.



## Motion Detection

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

☒ Enable motion detection



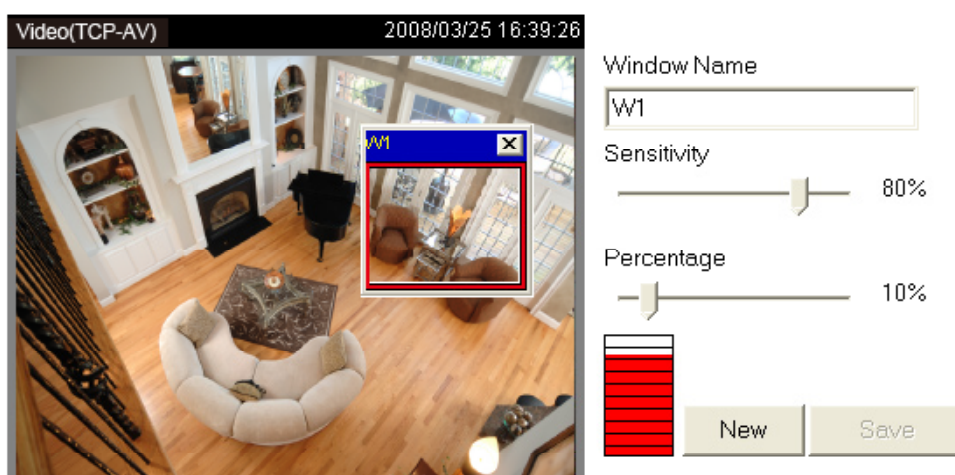
Follow the steps below to enable motion detection:

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.

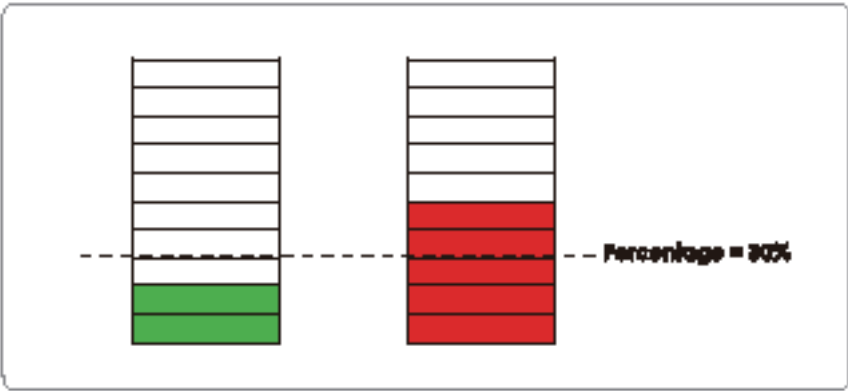
For example:

☒ Enable motion detection



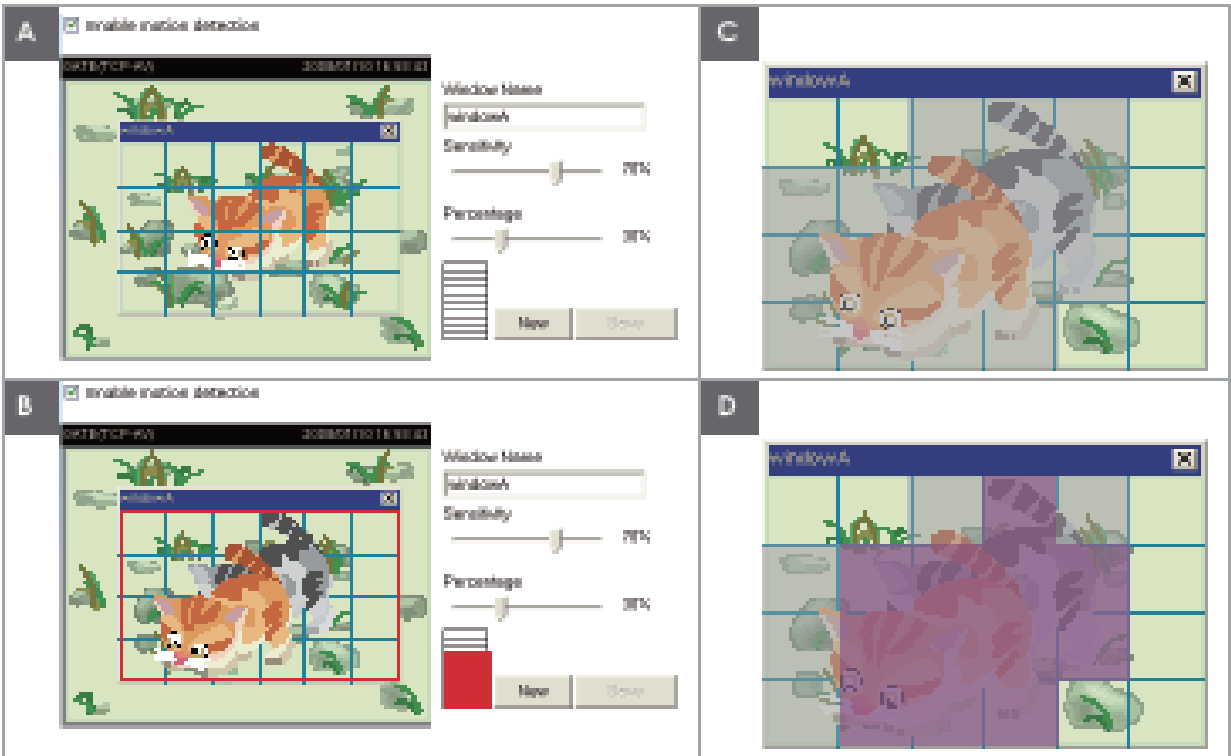
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the video server and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured 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 70.

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.



**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 video server 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**.

**Camera tampering detection**

☒ Enable camera tampering detection

Trigger duration:  seconds [10~600]

Save

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 79 for detailed information.

# Camera Control

This section explains how to control the Network Camera’s Pan/Tilt/Zoom operation by connecting to a PTZ driver or scanner via RS485 interface.

## RS485 Settings

RS485 Settings

☒ Disable

☐ PTZ camera

☐ Transparent HTTP Tunnel

Save

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.

☒ PTZ camera

☐ Transparent HTTP Tunnel

Camera ID

1

PTZ driver:

None

Port settings:

Baud rate:

9600

Data bits:

8

Stop bits:

1

Parity bit:

none

Preset Position

Custom Command

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 64.

Transparent HTTP Tunnel: 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 96 or [http://www.LevelOne.com/downloadfiles/faq/videoserver/UART\\_HTTP\\_Tunnel.pdf](http://www.LevelOne.com/downloadfiles/faq/videoserver/UART_HTTP_Tunnel.pdf).

☒ Transparent HTTP Tunnel

Port settings:

Baud rate:

9600

Data bits:

8

Stop bits:

1

Parity bit:

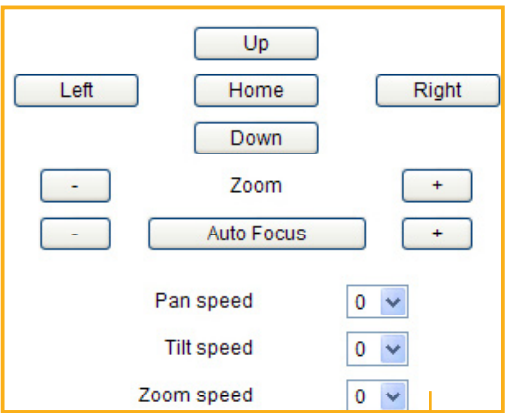
none

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.



1 Functions are the same as the Control Panel on the home page

Patrol selection:

2

Preset locations	Selected locations	
	Source	Dwelling time (sec):

6

Save

Select Remove Up Down 0 Update

2

Preset position name:

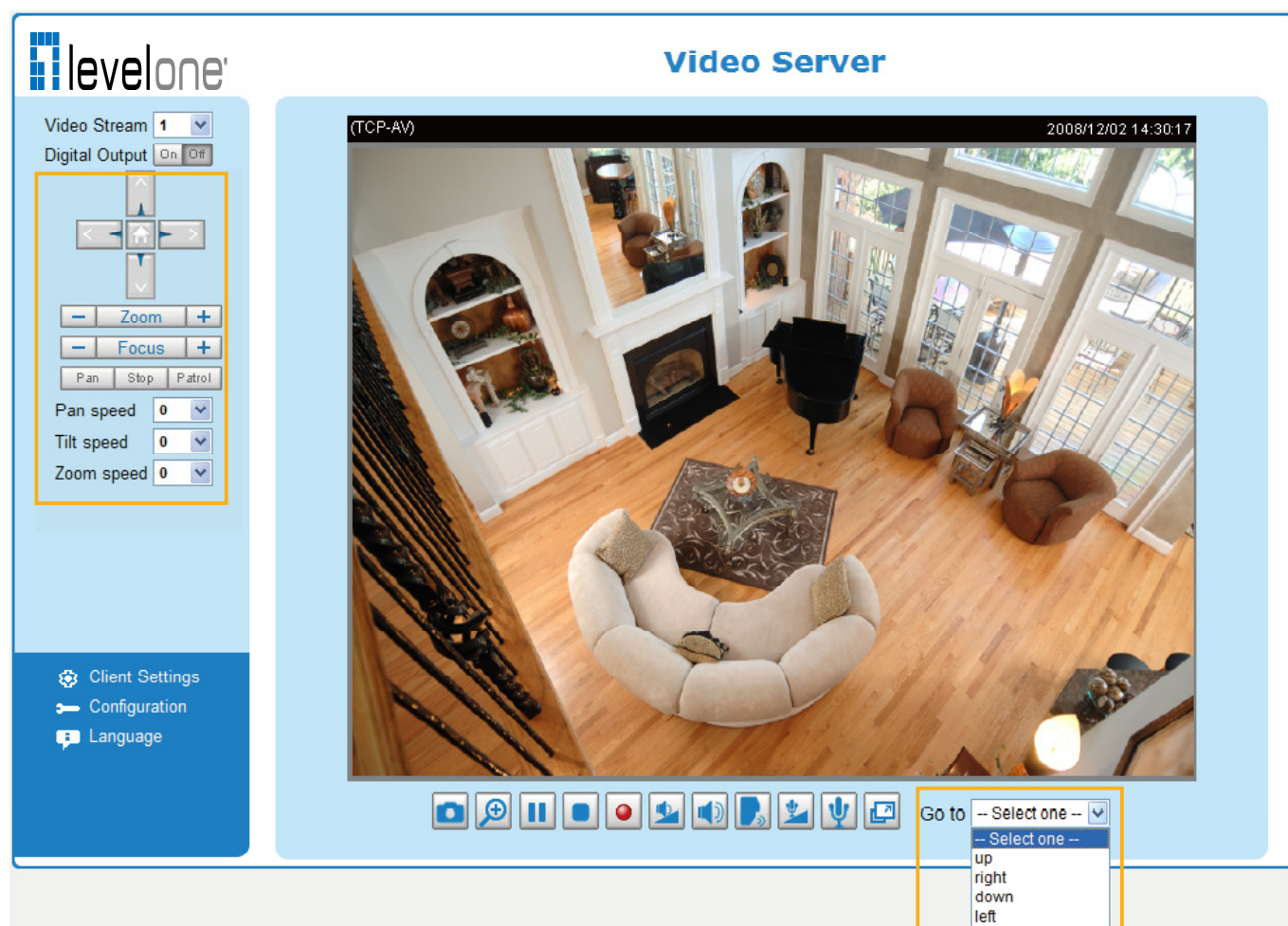
Add

4

Preset Position:

Go to Delete

- The Camera Control Panel and Preset Positions will be displayed on the home page:
- Click Go to: 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.



Left

Up

Home

Right

Down

-

Zoom

+

-

Auto Focus

+

Pan speed

0

▼

Tilt speed

0

▼

Zoom speed

0

▼

Patrol selection:

1

Preset locations

up  
right  
down  
left

Select

2

Source

right  
left

Remove

Up

Down

5

3

Dwelling time (sec):

10  
10

10

Update

6

7

Save

Close

Preset position name:

Add

Preset Position:

up

▼

Go to

Delete



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	<input type="text"/>
Down	<input type="text"/>
Left	<input type="text"/>
Right	<input type="text"/>
Home	<input type="text"/>
Zoom in	<input type="text"/>
Zoom out	<input type="text"/>
Closer focus	<input type="text"/>
More distant focus	<input type="text"/>
Auto Focus	<input type="text"/>

**NOTE**

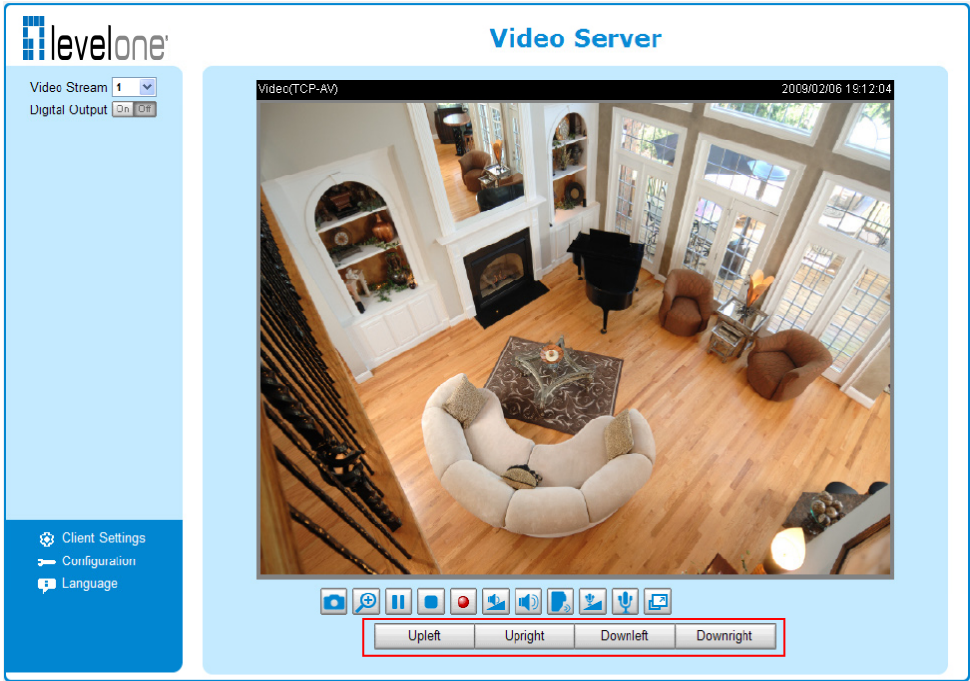
► If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver, the Control Settings column will not be displayed.

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

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

	Button name	Command
Command 1:	<input type="text" value="Upleft"/>	<input type="text"/>
Command 2:	<input type="text" value="Upright"/>	<input type="text"/>
Command 3:	<input type="text" value="Downleft"/>	<input type="text"/>
Command 4:	<input type="text" value="Downright"/>	<input type="text"/>
Command 5:	<input type="text"/>	<input type="text"/>

► The command buttons will be displayed on the main page:



## Homepage Layout Advanced Mode

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

### Preview

This column shows the settings of your homepage 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:



- Hide Powered by LevelOne: If you check this item, it will be removed from the homepage.



### Logo

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

**Logo graph**

You can upload a small logo(Gif, JPG or PNG), which will be resized to 160x50 pixels (if it is not already that size) and which will be visible on the main page. Upload a new logo will replace the old custom logo (if there was one uploaded)

☐ Default ☒ Custom

Logo link:

Follow the steps below to upload a new logo:

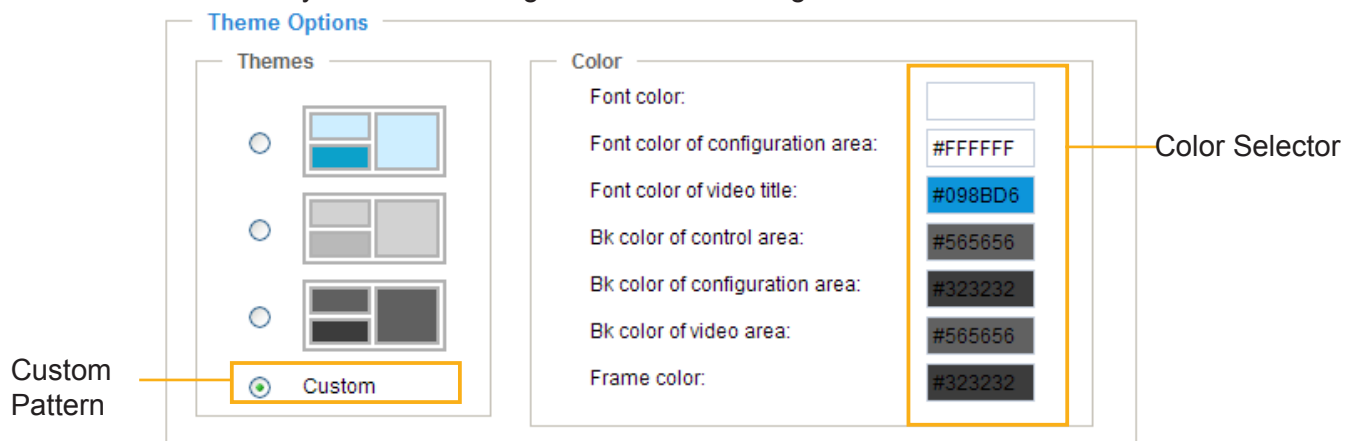
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

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.

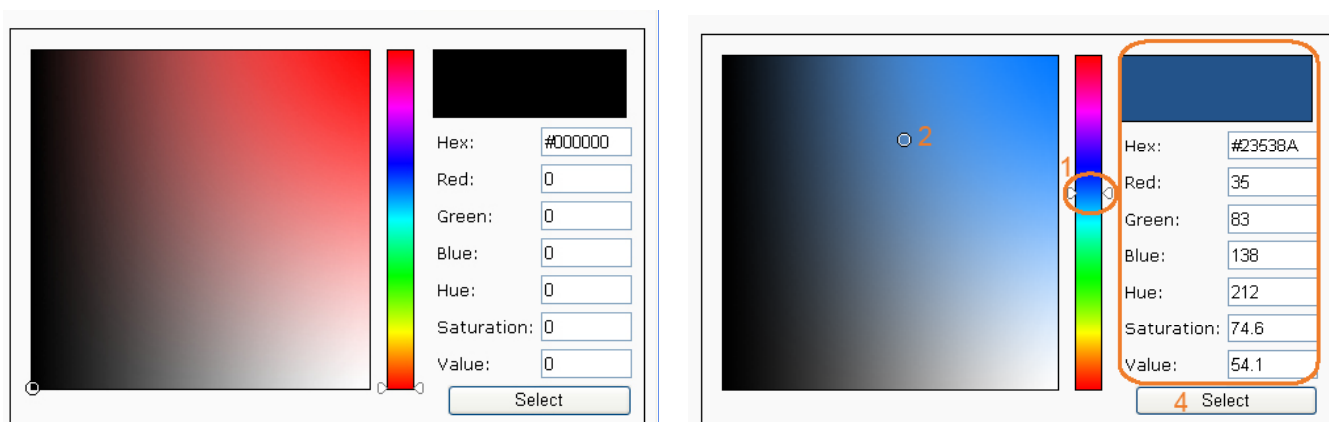
78 - User's Manual

■ Follow the steps below to set up the customized homepage:

1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



3. The palette window will pop up as shown below.

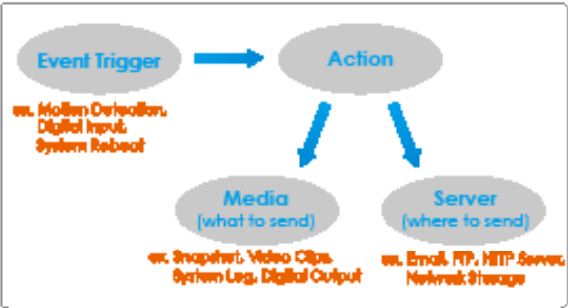


4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

# Application Advanced Mode

This section explains how to configure the video server to responds to particular situations (event). A typical application is that when a motion is detected, the video server 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 video server to send snapshots or videos to your email address or FTP site.



Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
------	--------	-----	-----	-----	-----	-----	-----	-----	------	---------

Add

Help

Customized Script

Name	Date	Time
------	------	------

Add

Delete

## 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.

Customized Script

Name	Date	Time
User1	20081113	18:13:46
User2	20081113	18:11:32

Click to upload a file

Add

User1

Delete

Click to modify the script online

```
<?xml version="1.0" encoding="UTF-8"?>
<eventmgr version="0102">
  <maxprocess>1</maxprocess>
  <!-- from 08:30:00-20:30:00 on Monday to Friday every week -->
  <schedule id="0">
    <duration>
      <weekday>1-5</weekday>
      <time>08:30:00-20:30:00</time>
    </duration>
  </schedule>
  <!-- Motion -->
  <motion condition="0">
    <status id="0">trigger</status>
    <status id="1">trigger</status>
  </motion>
  <event id="0">
    <description>Mail system log to email address</description>
    <condition>0</condition>
    <scheduleno>0</scheduleno>
    <delay>10</delay>
  </event>
</eventmgr>
```

Upload

## 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  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
- ☐ Video loss
- ☐ Video restore

### Event Schedule

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

#### Time

- ☒ Always
- ☐ From  to  [hh:mm]

### Action

- ☐ Trigger digital output for  seconds
- ☐ Move to preset location: Up

Note: Please configure [Preset locations](#) first

Server	Media	Extra parameter
<input type="checkbox"/> SD	<span>-----None-----</span> <input type="button" value="v"/>	<input type="button" value="SD Test"/> <input type="button" value="View"/>

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 video server. The trigger source can be configured to use the video server’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 59 for details.

Trigger

☒ Video motion detection:

Normal: ☐ 1 ☐ 2 ☐ 3

Note: Please configure [Motion detection](#) first

☐ Periodically:

☐ Digital input

☐ System boot

☐ Recording notify

☐ Camera tampering detection

☐ Video loss

☐ Video restore

- Periodically  
This option allows the video server to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

Trigger

☐ Video motion detection:

☒ Periodically:

Trigger every other  minutes

☐ Digital input

☐ System boot

☐ Recording notify

☐ Camera tampering detection

☐ Video loss

☐ Video restore

- Digital input  
This option allows the video server 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 video server when the power to the video server is disconnected.
- Recording notify  
This option allows the video server to trigger when the recording disk is full or when recording starts to rewrite older data.



#### ■ Camera tampering detection

This option allows the video server to trigger when the camera detects that it is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 61 for detailed information.

Trigger

☐ Video motion detection:  
☐ Periodically:  
☐ Digital input  
☐ System boot  
☐ Recording notify  
☒ Camera tampering detection:  

Note: Please configure [Camera tampering detection](#) first

☐ Video loss  
☐ Video restore

#### ■ Video loss

This option triggers the video server when the transmitted media files are missing.

#### ■ Video restore

This option triggers the video server when the camera starts to transmit video files.

### Event Schedule

Specify the period for the event.

Event Schedule

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time

☒ Always  
☐ From  to  [hh:mm]

#### ■ Select the days of the week.

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

### Action

Define the actions to be performed by the video server when a trigger is activated.

Action

☐ Trigger digital output for  seconds  
☐ Move to preset location:

Note: Please configure [Preset locations](#) first

Add Server Add Media

Server	Media	Extra parameter
<input type="checkbox"/> SD	<input type="text" value="None"/>	<input type="button" value="SD Test"/> <input type="button" value="View"/>

#### ■ 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.

#### ■ Move to preset location

Select this option, the Network Camera will move to the preset location when a trigger is activated. Please setup the preset locations on camera configuration page first.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the video server 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 76.

Click **Add Media** to configure [Media Settings](#). For more information, please refer to Media Settings on page 79.

Here is an example of the Event Settings page:

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

☐ Video loss

☐ Video restore

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

☐ Move to preset location: 

Up

Note: Please configure [Preset locations](#) first

Add Server

Add Media

	Server	Media	Extra parameter	
<input type="checkbox"/>	SD	<div>-----None-----</div>	<div>SD Test</div>	<div>View</div>
<input type="checkbox"/>	FTP	<div>-----None-----</div>		
<input type="checkbox"/>	NAS	<div>-----None-----</div>	<div><input type="checkbox"/> Create folders by date time and hour automatically</div>	<div>View</div>
<input type="checkbox"/>	Email	<div>-----None-----</div>		
<input type="checkbox"/>	HTTP	<div>-----None-----</div>		

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
<a href="#">Event1</a>	<a href="#">ON</a>	V	V	V	V	V	V	V	00:00~24:00	di

Add
Event1
Delete
Help

### Server Settings

Name	Type	Address/Location
<a href="#">FTP</a>	ftp	
<a href="#">NAS</a>	ns	\\192.168.5.122\nas
<a href="#">Email</a>	email	
<a href="#">HTTP</a>	http	http://192.168.5.10/cgi-bin/upload.cgi

Add
FTP
Delete

### Media Settings

Available memory space: 8000KB

Name	Type
<a href="#">Snapshot</a>	snapshot
<a href="#">Video Clip</a>	videoclip
<a href="#">System log</a>	systemlog

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 video server 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.

Server name:

**Server Type**

☒ Email:

Sender email address:

Recipient email address:

Server address:

User name:

Password:

Server port:

☐ This server requires a secure connection (SSL)

☐ FTP:

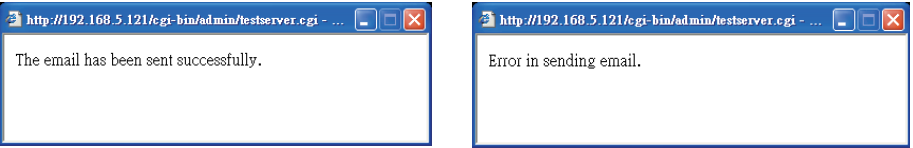
☐ HTTP:

☐ Network storage:

- 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 name:

**Server Type**

☐ Email:

☒ **FTP:**

Server address:

Server port:

User name:

Password:

FTP folder name:

☒ Passive mode

☐ HTTP:

☐ Network storage:

■ **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.

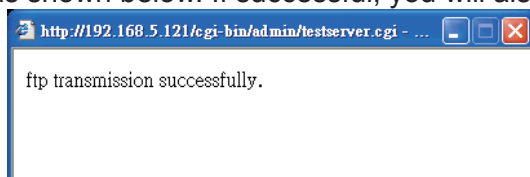
■ **FTP folder name**

Enter the folder where the media file will be placed. If the folder name does not exist, the video server 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.

Server name:

**Server Type**

☐ Email:

☐ FTP:

☒ HTTP:

URL:

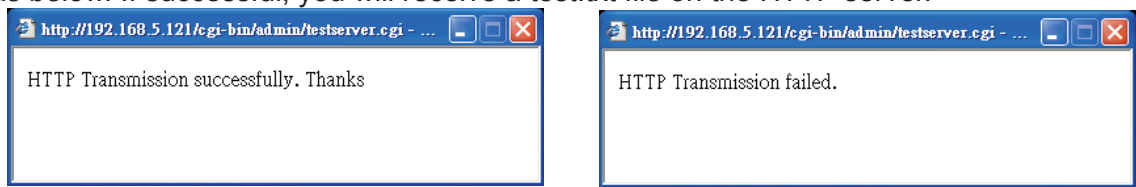
User name:

Password:

☐ Network storage:

- 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 83 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:

Server	Media	Extra parameter
<input type="checkbox"/> SD	<input type="text" value="----None-----"/>	<input type="button" value="SD Test"/> <input type="button" value="View"/>
<input type="checkbox"/> FTP	<input type="text" value="----None-----"/>	
<input type="checkbox"/> NAS	<input type="text" value="----None-----"/>	<input type="checkbox"/> Create folders by date time and hour automatically <input type="button" value="View"/>
<input type="checkbox"/> Email	<input type="text" value="----None-----"/>	
<input type="checkbox"/> HTTP	<input type="text" value="----None-----"/>	

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.

Media name:

Media Type

☒ Snapshot

Source:

Send  pre-event image(s) [0~7]

Send  post-event image(s) [0~7]

File name prefix:

☒ Add date and time suffix to file name

☐ Video Clip

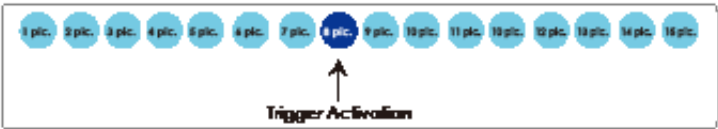
☐ System log

Save

Close

- Source: Select to take snapshots from stream 1 ~ 4.
- Send ☐ pre-event images  
The video server 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.

Media name:

**Media Type**

☐ Snapshot

☒ Video Clip

Source:

Pre-event recording:  seconds [0~9]

Maximum duration:  seconds [1~10]

Maximum file size:  Kbytes [50~800]

File name prefix:

☐ System log

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

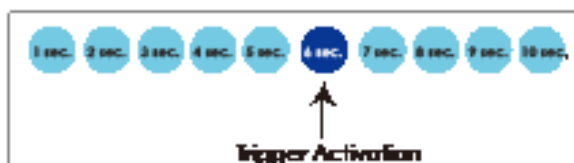
■ **Pre-event recording**

The video server 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 video server 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.

Add Server

Add Media

	Server	Media	Extra parameter	
<input type="checkbox"/>	SD	<div>-----None-----<div>-----None----- Snapshot Video Clip System log</div></div>	<div>SD Test</div>	<div>View</div>
<input type="checkbox"/>	FTP		<input type="checkbox"/> Create folders by date time and hour automatically	
<input type="checkbox"/>	NAS	<div>-----None-----<div></div></div>	<div>View</div>	
<input type="checkbox"/>	Email	<div>-----None-----<div></div></div>		
<input type="checkbox"/>	HTTP	<div>-----None-----<div></div></div>		

- 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 83 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 86 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.

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

☐

→

20081120

☐

→

20081121

☐

→

20081122

Click to delete selected items

Delete

Delete all

Click to delete all recorded data

The format is: YYYYMMDD

Click to open the directory

Click [20081120](#) to open the directory:

The format is: HH (24r)

Click to open the file list for that hour

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

	file name	size	date	time
<input type="checkbox"/>	<a href="#">Recording1 58.mp4</a>	2526004	2008/11/20	07:58:28
<input type="checkbox"/>	<a href="#">Recording1 59.mp4</a>	2563536	2008/11/20	07:59:28

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
<input type="checkbox"/>	<a href="#">Recording1 58.mp4</a>	2526004	2008/11/20	07:58:28
<input type="checkbox"/>	<a href="#">Recording1 59.mp4</a>	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 79 for detailed information.

## Recording Advanced Mode

This section explains how to configure the recording settings for the video server.

### Recording Settings

Recording Settings

Note: Before setup recording, you have to setup network storage first via [Server](#) page

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
<div style="display: flex; justify-content: space-between; align-items: center;"><span>Add</span><span>SD Test</span><span>▼</span><span>Delete</span></div>											

Insert your SD card and click here to test

#### **NOTE**

- ▶ 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 86 for detailed information.

### Network Storage Setting

Click [Server](#) to open the Server Settings page and follow the steps below to set up:

1. Fill in the information for your server.

For example:

>Server Settings

Server name: NAS 3

**Server Type**

☐ Email:

☐ FTP:

☐ HTTP:

1 ☒ Network storage:

Network storage location: \\192.168.5.122\\nas Network storage path  
(\\server name or IP address\\folder name)

(For example:  
\\my\_nas\\disk\\folder)

Workgroup:  

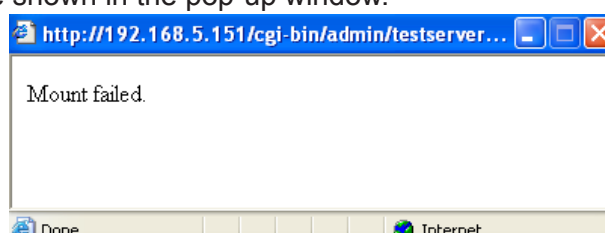
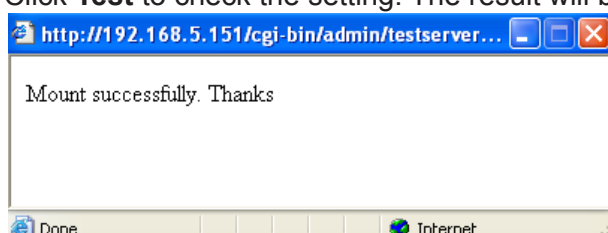
User name: ritali

Password: ●●●●●● User name and password for your server

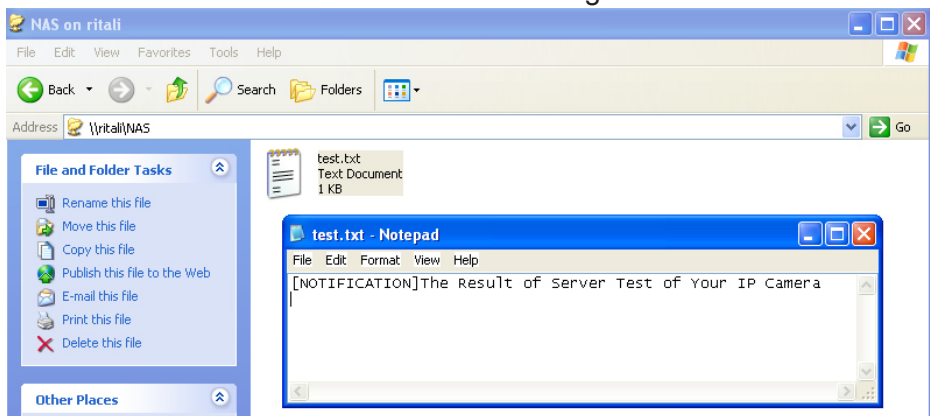
Test Save Close

2 4

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**

Recording name:

☐ Enable this recording

Priority: 

Normal

Source: 

Stream1

Trigger

☒ Schedule

☐ Network fail

Recording Schedule

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time

☒ Always

☐ From 

00:00

 to 

24:00

 [hh:mm]

Destination

SD

SD

NAS

Capacity:

☐ Entire free space

☒ Limit recording size in 

100

 Mbytes

File name prefix: 

Video\_

☒ Enable cyclic recording

Reserved amount 

15

 Mbytes

Note: To enable recording notification please configure [Application](#) first

Save

Close

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).

94 - User's Manual

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 recording size. 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 72 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**.

Recording Settings

Note: Before setup recording, you have to setup network storage first via [Server](#) page

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
<a href="#">Video</a>	<a href="#">ON</a>	V	V	V	V	V	V	V	00:00~24:00	stream1	<a href="#">NAS</a>

Add

SD Test

Video

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 82 for details.

☐

☒

[20081120](#)

☐

☒

[20081121](#)

☐

☒

[20081122](#)

Delete

Delete all

# Local Storage Advanced Mode

This section explains how to manage the local storage on the video server. 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

**SD card status:** 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.

▼ SD card control:

☐ Enable cyclic storage

☐ Enable automatic disk cleanup

Maximum duration for keeping files:  days

- **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** column.

Searching and viewing the records

▼ File attributes:

Trigger type:	<input type="checkbox"/> Digital input	<input type="checkbox"/> Video loss	<input type="checkbox"/> Video restore
	<input type="checkbox"/> System boot	<input type="checkbox"/> Recording notify	<input type="checkbox"/> Motion
	<input type="checkbox"/> Periodically	<input type="checkbox"/> Network fail	<input type="checkbox"/> Tampering
Media Type:	<input type="checkbox"/> Video Clip	<input type="checkbox"/> Snapshot	<input type="checkbox"/> Text
Locked:	<input type="checkbox"/> Locked	<input type="checkbox"/> Unlocked	

▼ Trigger time:


From:	Date	<input type="text" value="2009-03-05"/>	Time	<input type="text" value="00:00:00"/>
To:	Date	<input type="text" value="2009-03-05"/>	Time	<input type="text" value="23:59:59"/>
		(yyyy-mm-dd)		(hh:mm:ss)

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

Highlight an item

Click to switch pages

Search results

Search:

Show 10 entries

	Trigger time	Media type	Trigger type	Locked
<input checked="" type="checkbox"/>	2009-03-05 10:47:57	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:48:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:49:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:50:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:51:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:52:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:53:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:54:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:55:57	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:56:57	Videoclip	Periodically	No

Showing 11 to 20 of 32 entries

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 recording. You can click again to unlock the selections. For example:

Search results

Show 10 entries

Search:

	Trigger time	Media type	Trigger type	Locked
<input checked="" type="checkbox"/>	2009-03-05 10:47:57	Videoclip	Periodically	Yes
<input checked="" type="checkbox"/>	2009-03-05 10:48:58	Videoclip	Periodically	Yes
<input checked="" type="checkbox"/>	2009-03-05 10:49:58	Videoclip	Periodically	Yes
<input type="checkbox"/>	2009-03-05 10:50:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:51:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:52:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:53:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:54:58	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:55:57	Videoclip	Periodically	No
<input type="checkbox"/>	2009-03-05 10:56:57	Videoclip	Periodically	No

Showing 11 to 20 of 32 entries

View

Download

Uncheck All

JPEGs to AVI

Lock/Unlock

Remove

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 video server to send the system log to the remote server as backup.

## Remote Log

Remote Log

☐ Enable remote log

Log server settings

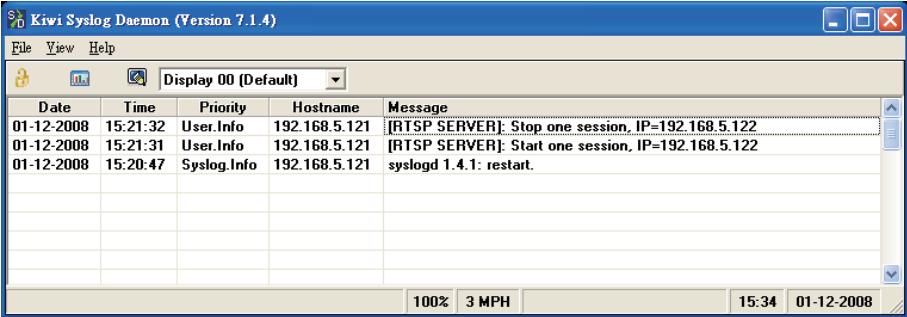
IP address:

port:

514

Save

You can configure the video server 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 video server. 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

Current Log

Sep 18 10:28:43 syslogd 1.5.0: restart.

Sep 18 10:28:45 [swatchdog][308]: Ready to watch httpd.

Sep 18 10:28:46 [EVENT MGR]: Starting eventmgr with support for EcTun

Sep 18 10:28:46 [EVENT MGR]: Task conf file: there is no valid event in recording\_task.xml, skip it

Sep 18 10:28:46 [EVENT MGR]: Task conf file: there is no valid event in event\_task.xml, skip it

Sep 18 10:28:51 [DRM Service]: Starting DRM service.

Sep 18 10:28:55 automount[651]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address

Sep 18 10:28:55 automount[651]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF

Sep 18 10:28:55 automount[660]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address

Sep 18 10:28:55 automount[660]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF

Sep 18 10:28:56 [SYS]: Serial number = 0002D109C260

Sep 18 10:28:56 [SYS]: System starts at Fri Sep 18 10:28:56 UTC 2009

Sep 18 10:28:56 [NET]: === NET INFO ===

This column displays the system log in chronological order. The system log is stored in the video server’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='Video Server'
system_ledoff='0'
system_date='2009/09/21'
system_time='11:02:13'
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='VS8102'
system_info_extendedmodelname='VS8102'
system_info_serialnumber='0002D109C260'
system_info_firmwareversion='VS8102-VVTK-0100b'
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=''
system_info_language_i17=''
```

# Maintenance

This chapter explains how to restore the video server to factory default, upgrade firmware version, etc.

## Reboot

Reboot

Reboot the device

Reboot

This feature allows you to reboot the video server, 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 video server 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 video server 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 files**

Export daylight saving time configuration file

Export

Export language file

Export

Export setting backup file

Export

**Upload files**

Update daylight saving time rules

Browse...

Upload

Update custom language file

Browse...

Upload

Upload setting backup file

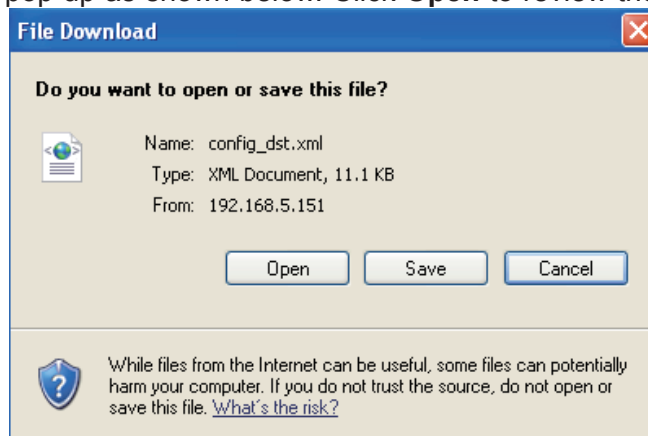
Browse...

Upload

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

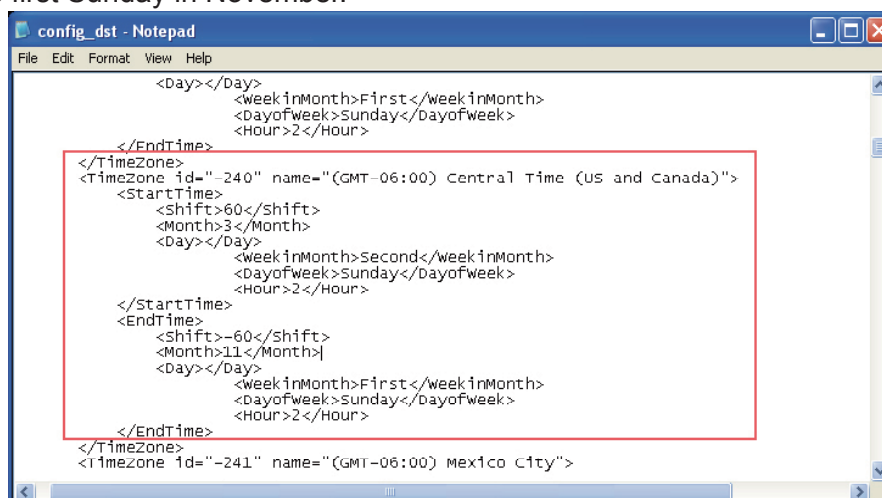
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the video server.
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.

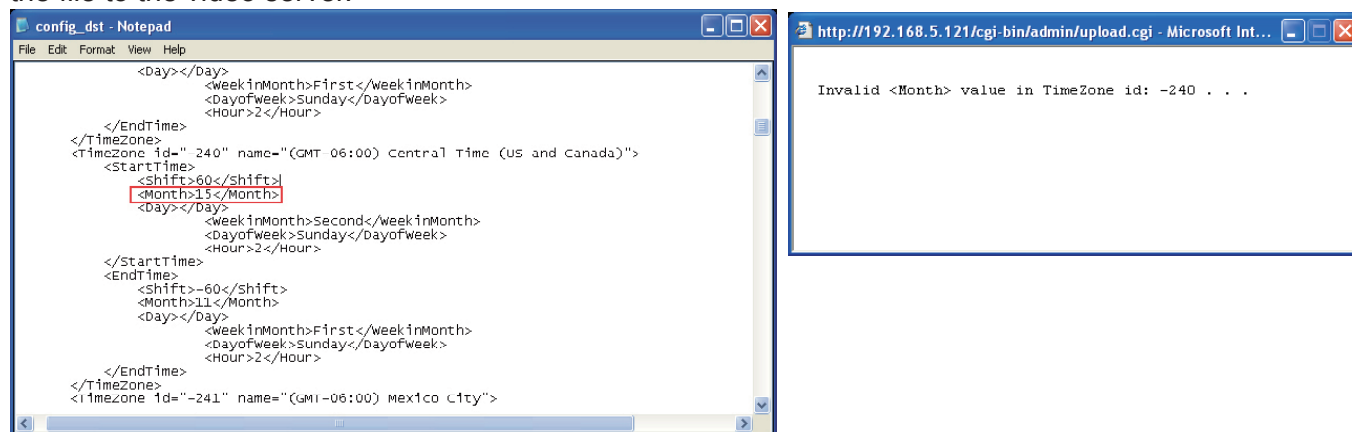
In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



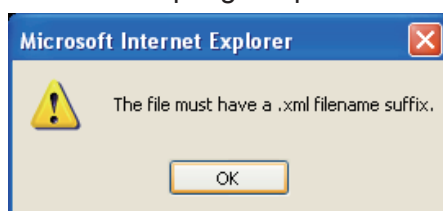


Upload daylight saving time rule: Click **Browse...** and specify the XML file to upload.

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



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



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

Upload custom language file: Click **Browse...** and specify your own custom language file to upload.

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

Upload setting backup file: 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

Upgrade firmware

Select firmware file

This feature allows you to upgrade the firmware of your video server. It takes a few minutes to complete the process.

**Note: Do not power off the video server 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 video server 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 video server.



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**

# Appendix

## URL Commands for the Network Camera/Video Server

### Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

### Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

**Example:** request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

## General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>  
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Examples: Set digital output #1 to active

<http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1>

## Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

## Get Server Parameter Values

Notes: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/<anonymous>/getparam.cgi? [<parameter>]  
[&<parameter>...]  
  
http://<servername>/cgi-bin/<viewer>/getparam.cgi? [<parameter>]
```

[&<parameter>...]

http://<servername>/cgi-bin/[operator](#)/getparam.cgi?<parameter>]

[&<parameter>...]

http://<servername>/cgi-bin/[admin](#)/getparam.cgi?<parameter>]

[&<parameter>...]

Where the <parameter> should be <group>[\_<name>] or <group>[.<name>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <group>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Content-Length: <length>\r\n

\r\n

<parameter pair>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

**Example: Request IP address and its response**

Request:

http://192.168.0.123/cgi-bin/admin/getparam.cgi?network\_ipaddress

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Content-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

## Set Server Parameter Values

**Notes:** The access right depends on the URL directory.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
```

```
[&<parameter>=<value>...][&update=<value>][&return=<return page>]
```

```
http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
```

```
[&<parameter>=<value>...][&update=<value>][&return=<return page>]
```

```
http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
```

```
[&<parameter>=<value>...][&update=<value>][&return=<return page>]
```

```
http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
```

```
[&<parameter>=<value>...][&update=<value>][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <value> to the parameter <group>_<name>.
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list.

**Return:**

```
HTTP/1.0 200 OK\r\n
```

```
Content-Type: text/html\r\n
```

```
Content-Length: <length>\r\n
```

```
\r\n
```

```
<parameter pair>
```

where <parameter pair> is

```
<parameter>=<value>\r\n
```

```
[<parameter pair>]
```

Only the parameters that you set and are readable will be returned.

**Example: Set the IP address of server to 192.168.0.123:**

Request:

[http://myserver/cgi-bin/admin/setparam.cgi?network\\_ipaddress=192.168.0.123](http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123)

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Content-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

## Available Parameters on the Server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters ";, <, >, &" are invalid.
string[n-m]	Text strings longer than 'n' characters and shorter than 'm' characters. The characters ";, <, >, &" are invalid.
password[<n>]	The same as string but displays "*" instead.
integer	Any number between $(-2^{31} - 1)$ and $(2^{31} - 1)$ .
positive integer	Any number between 0 and $(2^{31} - 1)$ .
<m> - <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [ <n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, ...	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding

	(UTF-8, UTF-16BE or UTF-16LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

**NOTE:** The camera should not be restarted when parameters are changed.

#### Group: system

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	6/6	Turn on (0) or turn off (1) all led indicators.
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYY YY.ss>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ -529	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Times Dublin,

			<p>Edinburgh, Lisbon, London</p> <p>40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris</p> <p>41: GMT 01:00 Warsaw, Budapest, Bern</p> <p>80: GMT 02:00 Athens, Helsinki, Istanbul, Riga</p> <p>81: GMT 02:00 Cairo</p> <p>82: GMT 02:00 Lebanon, Minsk</p> <p>83: GMT 02:00 Israel</p> <p>120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi</p> <p>121: GMT 03:00 Iraq</p> <p>140: GMT 03:30 Tehran</p> <p>160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan</p> <p>180: GMT 04:30 Kabul</p> <p>200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent</p> <p>220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi</p> <p>230: GMT 05:45 Kathmandu</p> <p>240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura</p> <p>260: GMT 06:30 Rangoon</p> <p>280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk</p> <p>320: GMT 08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei</p> <p>360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk</p> <p>380: GMT 09:30 Adelaide, Darwin</p> <p>400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok</p> <p>440: GMT 11:00 Magadan, Solomon Is., New Caledonia</p> <p>480: GMT 12:00 Auckland, Wellington, Fiji, Kamchatka, Marshall Is.</p> <p>520: GMT 13:00 Nuku'alofa</p>
daylight_enable	<boolean>	6/6	Enable <b>automatic</b> daylight saving time in time zone.
daylight_dst_actualmode	<boolean>	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving start time. (product dependent)
daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end time. (product dependent)



daylight_timezones	string	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 048000, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptptnet	<Any value>	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptptdst	<Any value>	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptptlang	<Any Value>	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

Subgroup of system: info (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	0/7	ODM specific model name of server (eg. DCS-S610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>

language_count	<integer>	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	0/7	Available language lists.
customlanguage_maxcount	<integer>	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	0/6	Custom language name.

#### Group: status

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~(ndo-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	6/7	Current number of HTTP push server connections.
eth_j0	<string>	1/99	Get network information from mii-tool.

#### Group: di\_i<0~(ndi-1)> (capability.ndi > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	Indicates open circuit or closed circuit (inactive status)

#### Group: do\_i<0~(ndo-1)> (capability.ndo > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	Indicate open circuit or closed circuit (inactive status)

#### Group: security

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	6/6	Indicate which privileges and above can control digital output
privilege_camctrl	view, operator, admin	6/6	Indicate which privileges and above can control PTZ
user_j0_name	string[64]	6/7	User name of root

user_i<1-20>_name	string[64]	6/7	User name
user_i0_pass	password[64]	6/6	Root password
user_i<1-20>_pass	password[64]	7/6	User password
user_i0_privilege	viewer, operator, admin	6/7	Root privilege
user_i<1-20>_privilege	viewer, operator, admin	6/6	User privilege

#### Group: network

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type.
preprocess	0-15	6/6	Stop related process before setting port value.
resetip	<boolean>	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, router, dns1, and dns2.
ipaddress	<ip address>	6/6	IP address of server.
subnet	<ip address>	6/6	Subnet mask.
router	<ip address>	6/6	Default gateway.
dns1	<ip address>	6/6	Primary DNS server.
dns2	<ip address>	6/6	Secondary DNS server.
wins1	<ip address>	6/6	Primary WINS server.
wins2	<ip address>	6/6	Secondary WINS server.

#### Subgroup of network: ieee8021x

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	6/6	Selected EAP method
identity_peap	String[64]	6/6	PEAP identity
identity_tls	String[64]	6/6	TLS identity
password	String[254]	6/6	Password for TLS
privatekeypassword	String[254]	6/6	Password for PEAP
ca_exist	<boolean>	6/6	CA installed flag
ca_time	<integer>	6/7	CA installed time. Represented in EPOCH
ca_size	<integer>	6/7	CA file size (in bytes)
certificate_exist	<boolean>	6/6	Certificate installed flag (for TLS)
certificate_time	<integer>	6/7	Certificate installed time. Represented in EPOCH
certificate_size	<integer>	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	6/6	Private key installed flag (for TLS)
privatekey_time	<integer>	6/7	Private key installed time. Represented in EPOCH

privatekey_size	<integer>	6/7	Private key file size (in bytes)
-----------------	-----------	-----	----------------------------------

#### Subgroup of network: qos

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cos_enable	<boolean>	6/6	Enable/disable CoS (IEEE 802.1p)
cos_vlanid	1~4095	6/6	VLAN ID
cos_video	0~7	6/6	Video channel for CoS
cos_audio	0~7	6/6	Audio channel for CoS
cos_eventalarm	0~7	6/6	Event/alarm channel for CoS
cos_management	0~7	6/6	Management channel for CoS
cos_eventtunnel	0~7	6/6	Event/Control channel for CoS
dscp_enable	<boolean>	6/6	Enable/disable DSCP
dscp_video	0~63	6/6	Video channel for DSCP
dscp_audio	0~63	6/6	Audio channel for DSCP
dscp_eventalarm	0~63	6/6	Event/alarm channel for DSCP
dscp_management	0~63	6/6	Management channel for DSCP

#### Subgroup of network: ipv6

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable IPv6.
addnipaddress	<ip address>	6/6	IPv6 IP address.
addonprefixlen	0~128	6/6	IPv6 prefix length.
addrouter	<ip address>	6/6	IPv6 router address.
adddns	<ip address>	6/6	IPv6 DNS address.
allowoptional	<boolean>	6/6	Allow manually setup of IP address setting.

#### Subgroup of network: ftp

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	6/6	Local ftp server port.

#### Subgroup of network: http

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port.
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic, digest	1/6	HTTP authentication mode.

s0_accessname	string[32]	1/6	HTTP server push access name for stream 1. (capability.protocol.push_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	1/6	HTTP server push access name for stream 2. (capability.protocol.push_mjpeg =1 and video.stream.count>1)
s2_accessname	string[32]	1/6	Http server push access name for stream 3 (capability.protocol.push_mjpeg =1 and video.stream.count>2)
s3_accessname	string[32]	1/6	Http server push access name for stream 4 (capability.protocol.push_mjpeg =1 and video.stream.count>3)
s4_accessname	string[32]	1/6	Http server push access name for stream 5 (capability.protocol.push_mjpeg =1 and video.stream.count>4)
anonymousviewing	<boolean>	1/6	Enable anonymous streaming viewing.

#### Subgroup of network: https

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	443, 1025 – 65535	6/6	HTTPS port.

#### Subgroup of network: rtsp

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	1/6	Enable anonymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[32]	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and video.stream.count>1)
s2_accessname	string[32]	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and video.stream.count>2)
s3_accessname	string[32]	1/6	RTSP access name for stream4 (capability.protocol.rtsp=1 and video.stream.count>3)
s0_audiotrac	<integer>	6/6	The current audio track for stream1.

k			-1 => audio mute
s1_audiotrac k	<integer>	6/6	The current audio track for stream2. -1 => audio mute
s2_audiotrac k	<integer>	6/6	The current audio track for stream2. -1 => audio mute
s3_audiotrac k	<integer>	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of network\_rtp\_s<0~(n-1)>: multicast, n is stream count

(capability.protocol.rtp\_multicast=1)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast.
ipaddress	<ip address>	4/4	Multicast IP address.
videoport	1025 ~ 65535	4/4	Multicast video port.
audioport	1025 ~ 65535	4/4	Multicast audio port.
ttd	1 ~ 255	4/4	Multicast time to live value.

Subgroup of network: sip

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	1/6	SIP port. (capability.protocol.sip=1)

Subgroup of network: rtp

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	Video channel port for RTP (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	6/6	Audio channel port for RTP (capability.protocol.rtp_unicast=1)

Subgroup of network: pppoe

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name.
pass	password[64]	6/6	PPPoE account password.

Group: ipfilter

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable access list filtering.

admin_enable	<boolean>	6/6	Enable administrator IP address.
admin_ip	String[44]	6/6	Administrator IP address.
maxconnection	1-10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	6/6	Ipfiler policy : 0 => allow 1 => deny
ipv4list_j<0-9>	Single address: <ip address> Network address: <ip address / network mask> Range address: <start ip address - end ip address>	6/6	IPv4 address list.
ipv6list_j<0-9>	String[44]	6/6	IPv6 address list.

Group: videoin\_c<0~(n-1)> for n channel products, and n is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modulation	ntsc, pal, auto	4/4	Set video input modulation type. (videoin.type=0) {product dependent}
color	0, 1	4/4	0 => monochrome 1 => color
flip	<boolean>	4/4	Flip the image.
mirror	<boolean>	4/4	Mirror the image.
ptzstatus	<integer>	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation; 0(not support), 1(support) Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support),

			1(support)
text	string[16]	1/4	Enclose caption.
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
s<0-(m-1)>_codec type	h264, mpeg4, mjpeg	1/4	Video codec type.
s<0-(m-1)>_resolu tion	QCIF, 176x120, 176x144, CIF, 352x240, 352x288, 4CIF, 704x480, 704x576 D1, 720x480 720x576	1/4	Video resolution in pixels.
s<0-(m-1)>_h264 _intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	Intra frame period in milliseconds.
s<0-(m-1)>_h264 _ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0-(m-1)>_h264 _quant	99, 1-5	4/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0-(m-1)>_h264 _qvalue	0-51	7/4	The specific quality parameter of the H264 encoder. 0 = best quality, 51 = worst quality.
s<0-(m-1)>_h264 _bitrate	1000-4000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0-(m-1)>_h264 _maxframe	1-30	1/4	Set maximum frame rate in fps (for H.264).
s<0-(m-1)>_h264 _profile	0-2	4/4	0 => Baseline profile 1 => Main profile 2 => High profile
s<0-(m-1)>_mpeg 4_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	Intra frame period in milliseconds.
s<0-(m-1)>_mpeg 4_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0-(m-1)>_mpeg 4_quant	0, 1-5	4/4	Quality of video when choosing vbr in "ratecontrolmode". 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0-(m-1)>_mpeg	1-31	7/4	The specific quality parameter of the Mpeg4



4_quantlevel			encoder. 1 = best quality, 31 = worst quality.
s<0-(m-1)>_mpeg 4_bitrate	1000-4000000	4/4	Set bit rate in bps when choosing chr in "ratecontrolmode".
s<0-(m-1)>_mpeg 4_maxframe	1-30	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0-(m-1)>_mpeg 4_qvalue	1-31	4/4	Manual video quality level input - choose customize input "mpeg4_quant = 0" (for MPEG-4).
s<0-(m-1)>_mjpe g_quant	1 - 5	4/4	Quality of JPEG video. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0-(m-1)>_mjpe g_quantlevel	2-97	7/4	The specific quality parameter of the JPEG encoder. 2 = best quality, 97 = worst quality.
s<0-(m-1)>_mjpe g_maxframe	1-30	1/4	Set maximum frame rate in fps (for JPEG).
s<0-(m-1)>_mjpe g_qvalue	2-97	4/4	Manual video quality level input - choose customize input "mjpeg_quant = 0" (for MJPEG).
s<0-(m-1)>_forcei	1	7/6	Force 1 frame.
enablewdr	<boolean>	6/6	Enable/disable WDR

Group: audioin\_c<0-(n-1)> for n channel products (capability.audioin>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
source	linein	4/4	Linein => use line input.
mute	0, 1	4/4	Enable audio mute.
gain	0-37	4/4	Gain of input.
boostmic	0-37	4/4	Gain of input.
s<0-(m-1)>_codectype	aac4, gamr	4/4	Set audio codec type for input.
s<0-(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	Set AAC4 bitrate in bps.
s<0-(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	Set AMR bitrate in bps.

Group: image\_c<0-(n-1)> for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	<product dependent>	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	<product dependent>	4/4	Adjust sharpness of image according to mode settings.

Group: **imagepreview\_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	<product dependent>	4/4	Preview of brightness adjustment of image according to mode settings.
saturation	-5 ~ 5	4/4	Preview of saturation adjustment of image according to mode settings.
contrast	-5 ~ 5	4/4	Preview of contrast adjustment of image according to mode settings.
sharpness	<product dependent>	4/4	Preview of sharpness adjustment of image according to mode settings.

Group: **timeshift\_c** for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	4/4	Enable time shift streaming for specific stream. (product dependent)

Group: **motion\_c<0~(n-1)>** for m profile and n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	4/4	Enable motion window 1-3.
win_i<0~2>_name	string[14]	4/4	Name of motion window 1-3.
win_i<0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: **tampering\_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	4/4	Threshold of tamper detection.
duration	10 ~ 600	4/4	If tampering value exceeds the 'threshold' for more than 'duration', then tamper detection is triggered.

Group: **ddes**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic DNS.
provider	Safe100, DynDNSDynamic, DynDNSCustom, TZO, DHS, DynInterfree, PeanutHull, CustomSafe100	6/6	Safe100 => safe100.net DynDNSDynamic => dyndns.org (dynamic) DynDNSCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree => dyn-interfree.it PeanutHull => PeanutHull CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_username email	string[64]	6/6	Your user or email to login to the DDNS service provider
<provider>_password key	string[64]	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

#### Group: upnpresentation

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

#### Group: upnpportforwarding

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0-3	6/7	The status of UpnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no XGD router, 3 = no need for port forwarding

#### Group: syslog

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	Enable remote log.
serverip	<IP address>	6/6	Log server IP address.
serverport	514, 1025-65535	6/6	Server port used for log.
level	0-7	6/6	Levels used to distinguish the importance of the

			information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG
--	--	--	---

Group: `camctrl_c<0~(n-1)>` for n channel product (*capability.ptzenabled*)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	1/4	Pan speed
tiltspeed	-5 ~ 5	1/4	Tilt speed
zoomspeed	-5 ~ 5	1/4	Zoom speed
autospeed	-5 ~ 5	1/4	Auto pan speed
focusspeed	-5 ~ 5	1/4	Auto focus speed
patrolseq	string[64]	1/4	(For external device) The indexes of patrol points, separated by ","
patroldwelli ng	string[128]	1/4	(For external device) The dwelling time of each patrol point, separated by ","

Group: `snmp` (*capability.snmp*) (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
v2	0~1	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	6/6	Read/write security name
secnamero	string[31]	6/6	Read only security name
authpwrw	string[8~128]	6/6	Read/write authentication password
authpwro	string[8~128]	6/6	Read only authentication password
authtypew	MIX,SHA	6/6	Read/write authentication type
authtypero	MIX,SHA	6/6	Read only authentication type
encryptpwrw	string[8~128]	6/6	Read/write password
encryptpwro	string[8~128]	6/6	Read only password
encryptypew	DES	6/6	Read/write encryption type
encryptypero	DES	6/6	Read only encryption type
rwcommunity	string[31]	6/6	Read/write community
rocommunity	string[31]	6/6	Ready only community

syslocation	string[128]	6/6	Description of Camera location (Ex. Address)
syscontact	string[128]	6/6	Description of Camera contactor (Ex. E-mail)

Group: privacymask\_c<0~(n-1)> for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean>	4/4	Enable privacy mask window.
win_i<0~4>_name	string[14]	4/4	Name of the privacy mask window.
win_i<0~4>_left	0 ~ 320/352	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	4/4	Width of privacy mask window.
win_i<0~4>_height	0 ~ 240/288	4/4	Height of privacy mask window.

Group: capability

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	Server bootup time.
nir	0, <positive integer>	0/7	Number of IR interfaces.
npir	0, <positive integer>	0/7	Number of PIRs.
ndi	0, <positive integer>	0/7	Number of digital inputs.
ndo	0, <positive integer>	0/7	Number of digital outputs.
naudioin	0, <positive integer>	0/7	Number of audio inputs.
naudioout	0, <positive integer>	0/7	Number of audio outputs.
nvideoin	<positive integer>	0/7	Number of video inputs.
nmediastream	<positive integer>	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0/7	Number of UART interfaces.
nvideoinprofile	<positive integer>	0/7	Number of videoin profiles.
nmotionprofile	<positive integer>	0/7	Number of motion profiles.
ptzenabled	<positive integer>	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation, 0(not

			<p>support}, 1{support}</p> <p>Bit 3 =&gt; Support tilt operation; 0{not support}, 1{support}</p> <p>Bit 4 =&gt; Support zoom operation; 0{not support}, 1{support}</p> <p>Bit 5 =&gt; Support focus operation; 0{not support}, 1{support}</p> <p>Bit 6 =&gt; Support iris operation; 0{not support}, 1{support}</p> <p>Bit 7 =&gt; External or built-in PT; 0{built-in}, 1{external}</p> <p>Bit 8 =&gt; Invalidate bit 1 - 7; 0{bit 1 - 7 are valid}, 1{bit 1 - 7 are invalid}</p> <p>Bit 9 =&gt; Reserved bit; Invalidate lens_pan, lens_tilt, lens_zoom, lens_focus, len_iris. 0{fields are valid}, 1{fields are invalid}</p>
npreset	<positive integer>	0/7	Number of preset locations.
eptz	<positive integer>	0/7	<p>A 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 =&gt; stream 1 supports ePTZ or not.</p> <p>Bit 1 =&gt; stream 2 supports ePTZ or not.</p> <p>The rest may be deduced by analogy</p>
protocol_https	<boolean>	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	<boolean>	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0/7	Indicate whether to support SIP.
protocol_maxconn ection	<positive integer>	0/7	The maximum allowed simultaneous connections.
protocol_maxgenc onnection	<positive integer>	0/7	The maximum general streaming connections .
protocol_maxmeg aconnection	<positive integer>	0/7	The maximum megapixel streaming connections.
protocol_rtp_multi cast_scalable	<boolean>	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multi cast_backchannel	<boolean>	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mj peg	<boolean>	0/7	Indicate whether to support server push MPEGS.
protocol_snmp	<boolean>	0/7	Indicate whether to support SNMP.

protocol_ipv6	<boolean>	0/7	Indicate whether to support IPv6.
videoin_type	0, 1, 2	0/7	0 ==> Interlaced CCD 1 ==> Progressive CCD 2 ==> CMOS
videoin_resolution	<a list of available resolution separated by commas>	0/7	Available resolutions list.
videoin_maxframe rate	<a list of available maximum frame rate separated by commas>	0/7	Available maximum frame list.
videoin_codec	<a list of available codec types separated by commas>	0/7	Available codec list.
videoout_codec	<a list of the available codec types separated by commas>	0/7	Available codec list.
audio_aec	<boolean>	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0/7	Indicate whether to support external line input.
audio_lineout	<boolean>	0/7	Indicate whether to support line output.
audio_headphoneoutput	<boolean>	0/7	Indicate whether to support headphone output.
audioin_codec	<a list of the available codec types separated by commas>	0/7	Available codec list.
audioout_codec	<a list of the available codec types separated by commas>	0/7	Available codec list.
uart_httpunnel	<boolean>	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_privilege	<boolean>	0/7	Indicate whether to support "Manage Privilege" of PTZ control in the Security page.
transmission_mode	Tx, Rx, Both	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0/7	Indicate whether to support wireless.
wireless_802dot11	<boolean>	0/7	Indicate whether to support wireless

1b			802.11b+.
wireless_802dot11g	<boolean>	0/7	Indicate whether to support wireless 802.11g.
wireless_beginchannel	1 – 14	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 – 14	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support wireless WPA2.
derivative_brand	<boolean>	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to WXX. (TCVW<->TCXX is excepted)
eventchannel	<boolean>	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0/7	Indicate whether to support joystick control.
storage_dbenabled	<boolean>	0/7	Media files are indexed in database.
namestream	<positive integer>	0/7	number of any media stream per channel
iva	<boolean>	0/7	Indicate whether to support Intelligent Video analysis

**Group: event\_customtaskfile\_i<0~2>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[41]	6/6	Custom script identification of this entry.
date	string[17]	6/6	Date of custom script.
time	string[17]	6/6	Time of custom script.

**Group: event\_i<0~2>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
enable	0, 1	6/6	Enable or disable this event.



priority	0, 1, 2	6/6	Indicate the priority of this events: "0" = low priority "1" = normal priority "2" = high priority
delay	1–999	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, visignal, virestore, pir, reconfity, tampering,	6/6	Indicate the trigger condition: "boot" = System boot "di" = Digital input "motion" = Video motion detection "seq" = Periodic condition "visignal" = Video input signal loss. "virestore" = Video input signal restore "pir" = PIR detection. "reconfity" = Recording notification. "tampering" = Tamper detection.
triggerstatus	String[40]	6/6	The status for event trigger
di	<integer>	6/6	Indicate which DI detects. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detect. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1 <sup>st</sup> window. For example, to detect the 1 <sup>st</sup> and 3 <sup>rd</sup> windows, set mdwin as 5.
inter	1–999	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".
weekday	0–127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
beginTime	hh:mm	6/6	Begin time of the weekly schedule.
endTime	hh:mm	6/6	End time of the weekly schedule. (00:00 – 24:00 sets schedule as always on)

action_do_i<0-(ndo-1)>_enable	0, 1	6/6	Enable or disable trigger digital output.
action_do_i<0-(ndo-1)>_duration	1-999	6/6	Duration of the digital output trigger in seconds.
action_cf_enable	0, 1	6/6	Enable media write on CF.
action_cf_folder	string[128]	6/6	Path to store media.
action_cf_media	NULL, 0-4	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.
action_server_i<0-4>_enable	0, 1	6/6	Enable or disable this server action. The default value is 0.
action_server_i<0-4>_media	NULL, 0-4	6/6	Index of the attached media.
action_server_i<0-4>_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.
action_goto_enable	<Boolean>	6/6	Enable/disable ptz goto preset on event triggered.
action_goto_name	string[40]	6/6	Preset name that ptz goto on event triggered.

**Group: server\_i<0-4>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	6/6	URL of the HTTP server to upload.
http_username	string[64]	6/6	Username to log in to the server.
http_passwd	string[64]	6/6	Password of the user.
ftp_address	string[128]	6/6	FTP server address.
ftp_username	string[64]	6/6	Username to log in to the server.
ftp_passwd	string[64]	6/6	Password of the user.
ftp_port	0-65535	6/6	Port to connect to the server.
ftp_location	string[128]	6/6	Location to upload or store the media.
ftp_passive	0, 1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	6/6	Email server address.
email_sslmode	0, 1	6/6	Enable support SSL.
email_port	0-65535	6/6	Port to connect to the server.

email_username	string[64]	6/6	Username to log in to the server.
email_passwd	string[64]	6/6	Password of the user.
email_senderemail	string[128]	6/6	Email address of the sender.
email_recipientemail	string[128]	6/6	Email address of the recipient.
ns_location	string[128]	6/6	Location to upload or store the media.
ns_username	string[64]	6/6	Username to log in to the server.
ns_passwd	string[64]	6/6	Password of the user.
ns_workgroup	string[64]	6/6	Workgroup for network storage.

Group: **media\_i<0~4>** (media\_freespace is used internally.)

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	snapshot, systemlog, videoclip	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 – 7	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 – 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 – 9	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 – 10	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 – 1500	6/6	Maximum size of one video clip file in Kbytes.

Group: **recording\_i<0~1>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.

trigger	schedule, networkfail	6/6	Trigger type of this entry.
enable	0, 1	6/6	Enable or disable this recording.
priority	0, 1, 2	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
limitsize	0,1	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	6/6	0: Disable recording notification 1: Enable recording notification
notifyserver	0–31	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0–i4). bit0 (LSB) = server_i0. bit1 = server_i1. bit2 = server_i2. bit3 = server_i3. bit4 = server_i4. For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.
weekday	0–127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begin time	hh:mm	6/6	Start time of the weekly schedule.
end time	hh:mm	6/6	End time of the weekly schedule. (00:00–24:00 indicates schedule always on)
prefix	string[16]	6/6	Indicate the prefix of the filename.

cyclesize	20~	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	15~	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	6/6	The destination to store the recorded data. "cf" means CF card. "0~4" means the index of the network storage.
cfolder	string[128]	6/6	Folder name.

Group: https (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	To enable or disable secure HTTP
policy	<Boolean>	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-3 ~ 1	6/6	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	6/6	Country name in the certificate information.
stateorprovincename	string[128]	6/6	State or province name in the certificate information.
localityname	string[128]	6/6	The locality name in the certificate information.
organizationname	string[64]	6/6	Organization name in the certificate information.
unit	string[32]	6/6	Organizational unit name in the certificate information.
commonname	string[64]	6/6	Common name in the certificate information.
validdays	0 ~ 9999	6/6	Valid period for the certification.

Group: disk\_i<0~(n-1)> n is the total number of storage devices.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
cyclic_enabled	<boolean>	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive integer>	6/6	To specify the expired days for automatic clean up.

## Drive the Digital Output

**Notes:** This request requires Viewer privileges.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]  
[&do3=<state>][&do4=<state>][&return=<return page>]
```

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

**Examples:** Drive the digital output 1 to triggered state and redirect to an empty page.

<http://myserver/cgi-bin/dido/setdo.cgi?do1=1>

## Query Status of the Digital Input

**Notes:** This request requires Viewer privileges.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

**Return:**

```
HTTP/1.0 200 OK\r\n  
Content-Type: text/plain\r\n  
Content-Length: <length>\r\n  
\r\n  
[di0=<state>]\r\n  
[di1=<state>]\r\n  
[di2=<state>]\r\n
```

```
[do3=<state>]\r\n
```

where <state> can be 0 or 1.

**Example:** Query the status of digital input 1.

Request:

<http://myserver/cgi-bin/dido/getdi.cgi?di1>

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

di1=1\r\n

## Query Status of the Digital Output

**Note:** This request requires Viewer privileges.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the digital output statuses will be returned.

**Return:**

```
HTTP/1.0 200 OK\r\n
```

```
Content-Type: text/plain\r\n
```

```
Content-Length: <length>\r\n
```

```
\r\n
```

```
[do0=<state>]\r\n
```

```
[do1=<state>]\r\n
```

```
[do2=<state>]\r\n
```

```
[do3=<state>]\r\n
```

where <state> can be 0 or 1.

**Example:** Query the status of digital output 1.

Request:

<http://myserver/cgi-bin/dido/getdo.cgi?do1>

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

do1=1\r\n

## Capture Single Snapshot

**Note:** This request requires Normal User privileges.

**Method:** GET/POST

**Syntax:**

http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]  
[&quality=<value>][&streamid=<value>]

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DESCRIPTION
channel	0-{n-1}	The channel number of the video source.
resolution	<available resolution>	The resolution of the image.
quality	1-5	The quality of the image.
streamed <product dependent>	0-{m-1}	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

**Return:**

HTTP/1.0 200 OK\r\n

Content-Type: image/jpeg\r\n

[Content-Length: <image size>\r\n]

<binary JPEG image data>

## Account Management

**Note:** This request requires Administrator privileges.

**Method:** GET/POST



Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?  
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]  
[&privilege=<value>][_][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## System Logs

**Note:** This request requires Administrator privileges.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n  
Content-Type: text/plain\r\n  
Content-Length: <syslog length>\r\n
```

```
\n
<system log information>\n
```

## Upgrade Firmware

**Notes:** This request requires Administrator privileges.

**Method:** POST

**Syntax:**

```
http://<servername>/cgi-bin/admin/upgrade.cgi
```

**Post data:**

```
fimage=<file name>[&return=<return page>]\n
\n
<multipart encoded form data>
```

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

## System Information

**Notes:** This request requires Normal User privileges. **(obsolete)**

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/sysinfo.cgi
```

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All fields in the previous version (0100) are obsolete. Please use "getparam.cgi?capability" instead.

**Return:**

```
HTTP/1.0 200 OK\n
Content-Type: text/plain\n
Content-Length: <system information length>\n
\n
Model=<model name of server>\n
CapVersion=0200\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of the server. Ex: IP3133-VVTK-0100a
CapVersion	<i>MMmm</i> , <i>MM</i> is major version from 00 ~ 99 <i>mm</i> is minor version from 00 ~ 99 ex: 0100	Capability field version.

## IP Filtering

**Note:** This request requires Administrator access privileges.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<servername>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<ipaddress>[&index=<value>]
[&return=<return page>]
http://<servername>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP Filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<ip address>	Single address: <ip address> Network address: <ip address / network mask> Range address: <start ip address - end ip address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## Get SDP of Streams

**Notes:** This request requires Viewer access privileges.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

"m" is the stream number.

"network\_accessname\_<0~{m-1}>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

## Open the Network Stream

**Notes:** This request requires Viewer access privileges.

**Syntax:**

For HTTP push server (MPEG):

```
http://<servername>/<network_http_s<0~m-1>_accessname>
```

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player:

```
rtsp://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

## Senddata (capability.nuart>0)

**Notes:** This request requires Viewer privileges.

**Method:** GET/POST

**Syntax:**

```
http://<servername>/cgi-bin/viewer/senddata.cgi?  
[com=<value>][&data=<value>][&flush=<value>][&wait=<value>][&read=<value>]
```

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[, <hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	1 ~ 65535	Wait time in milliseconds before read data.
read	1 ~ 128	The data length in bytes to read. The read data will be in the return page.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
<hex decimal data>\r\n
```

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

## Storage managements (capability.storage.dbenabled=1)

**Note:** This request requires **administrator** privileges.

**Method:** GET and POST

**Syntax:**

```
http://<servername>/cgi-bin/admin/ctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>_]
```

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including <i>search</i> , <i>insert</i> , <i>delete</i> , <i>update</i> , and <i>queryStatus</i> .

**Command: search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes.

		Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auts/CF/MCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'
isLocked	<boolean>	Optional. Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is "YYYY-MM-DD HH:MM:SS" Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply "TO" operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1 <sup>st</sup> 2008 to the end of Jan 1 <sup>st</sup> 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

#### Command: delete

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=delete&label=1&label=4&label=8

**Command: update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=update&isLocked=1&label=1&label=5

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=update&isLocked=0&label=2&label=3

**Command: queryStatus**

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. rettype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=queryStatus&retType=javascript