LevelOne

FCS-5011

Outdoor WDR PoE Network Camera w/ IR LEDs

User's Manual

Ver 1.0.0 – 0811

Table of Contents

Overview

LevelOne’s outdoor day/night network camera FCS-5011 is equipped with a wide dynamic range CMOS sensor to cope with any challenging lighting conditions.
Designed for outdoor 24-hour surveillance, FCS-5011 features the basics of day and night and vandal-proof functions that users can easily build up a cost-effective IP surveillance system without additional accessories. With a removable IR-cut filter and built-in IR illuminators, up to 15m, it can automatically remove the filter and turn on the IR illuminators during the night time to accept IR illumination for low light sensitivity. Meanwhile, the IP66-rated integrated housing shields this camera from dust and water, allowing it to be applied in harsh weather conditions of outdoor environments.
FCS-5011 with WDR (Wide dynamic range) feature can be very helpful to cope with very challenging lighting conditions. It is capable of capturing both of the dark part and bright part and combining the differences into a scene to generate a highly realistic image as the original scene. Because it preserves as much information in the video as possible, FCS-5011 helps provide video quality closer to the capabilities of the human eye. Consequently, it is largely applied in highly contrast environments such as lobby entrances, parking lots, ATM, loading areas and much more.
Incorporating numbers of advanced features including simultaneous dual streams, 3GPP mobile surveillance, 802.3af compliant PoE, two-way audio by SIP protocol, RS-485 interface for scanners or pan/tilts driver connection, and HTTPS encrypted data transmission, LEVELONE FCS-5011 allows users to boost your robust IP surveillance system by reproducing clear images in proper color in extreme high-contrast environments for your indoor/outdoor security and monitoring applications.

Read before use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but also can 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.

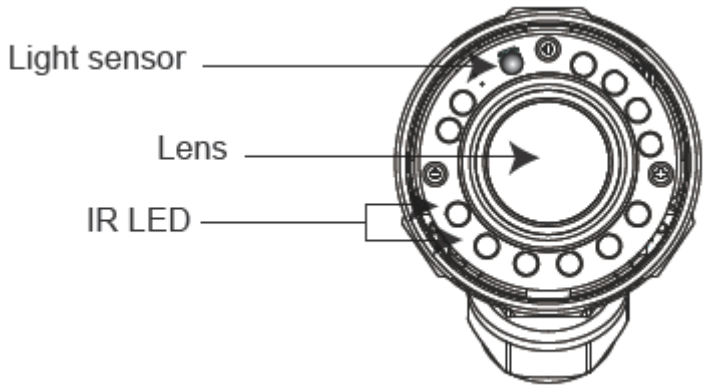
It is important to first verify that all contents received are complete according to the Package contents listed below. Take notice of the warnings in Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used properly as intended.
The Network Camera is a network device and its use should be straightforward for those who have basic network knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the URL Commands of the Network Camera section serves to be a helpful reference to customize existing homepages or integrating with the current web server.

Package contents

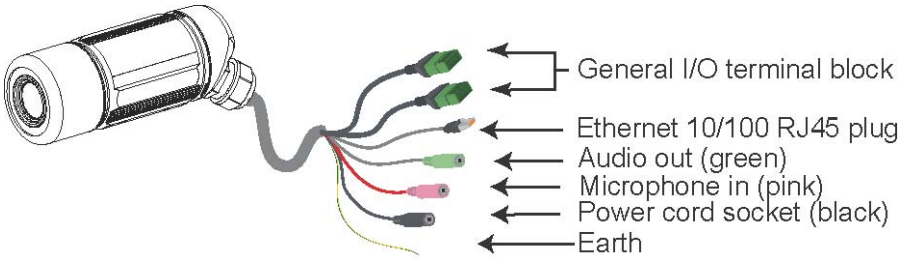
[1] FCS-5011
[2] Power Adapter
[3] Sun Shield
[4] Camera Stand
[5] Silica Gel
[6] Screws
[7] RJ45 Female/Female Coupler
[8] CD Manual/Utility
[9] Quick Installation Guide

Physical description

Front panel



Connectors



General I/O Terminal Block

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

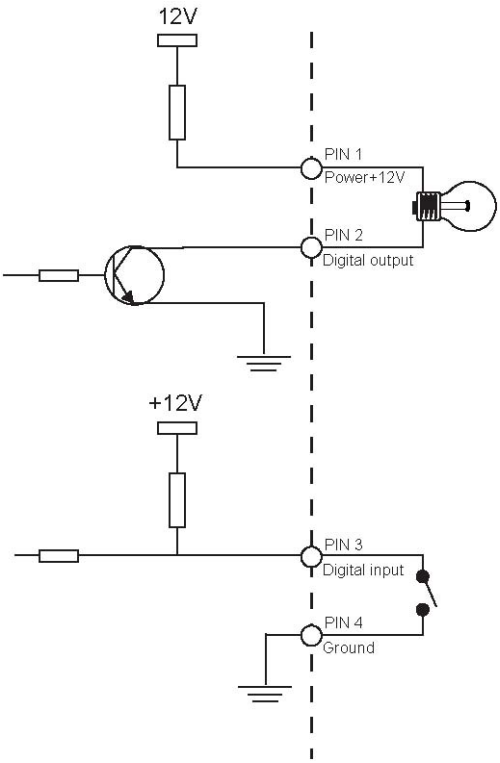
N.C.: No Connector
485B: RS485-
485A: RS485+
AC24V: Power in AC 24V
AC24V: Power in AC 24V

GND: Ground
DI : Digital Input
DO : Digital Output
+12V : Power, 12V DC

Pin	Name	Specification
N.C.	No Connector	
485B	RS485-	3.3V
485A	RS485+	3.3V
AC24V	Power in AC 24V	AC 24V ± 5%
AC24V	Power in AC 24V	AC 24V ± 5%
GND	Ground	
DI	Digital Iutput	OPEN/Short-to-GND, isolation 2kV
DO	Digital Output	Max. 40VDC, max. 400mA, isolation 2kV
+12V	Power +12V	12VDC ± 10%, max. 0.4A

DI/DO Diagram

Refer to the following illustration for connection method.

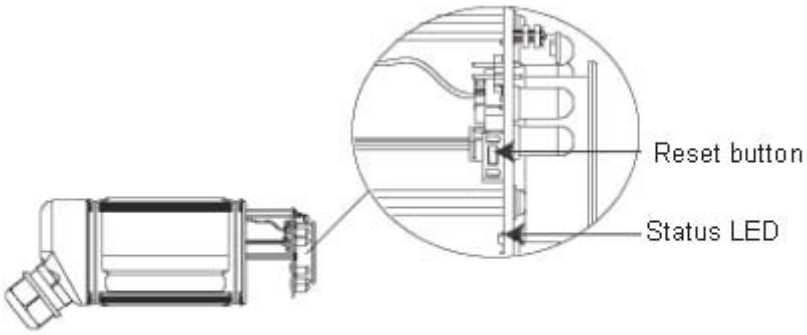


Status LED

The LED indicates the status of the Network Camera.

Status LED	Description
Blinking red (two short, one long)	1. Power is being supplied to the Network Camera 2. Restore, or reboot the Network Camera

Hardware Reset



There is a reset button on the inner side of the Network Camera. It is used to reboot the Network Camera or restore the Network Camera to factory default. Sometimes rebooting the Network Camera could set the Network Camera back to normal state. If the problems remain after rebooted, restore the Network Camera to factory default and install again.

Reboot: Press and release the reset button. The status LED will blinks two short one long in red.

Restore: Press the reset button continuously for over 5 seconds until the status LED blinks two short one long in red. Note that all settings will be restored to factory default.

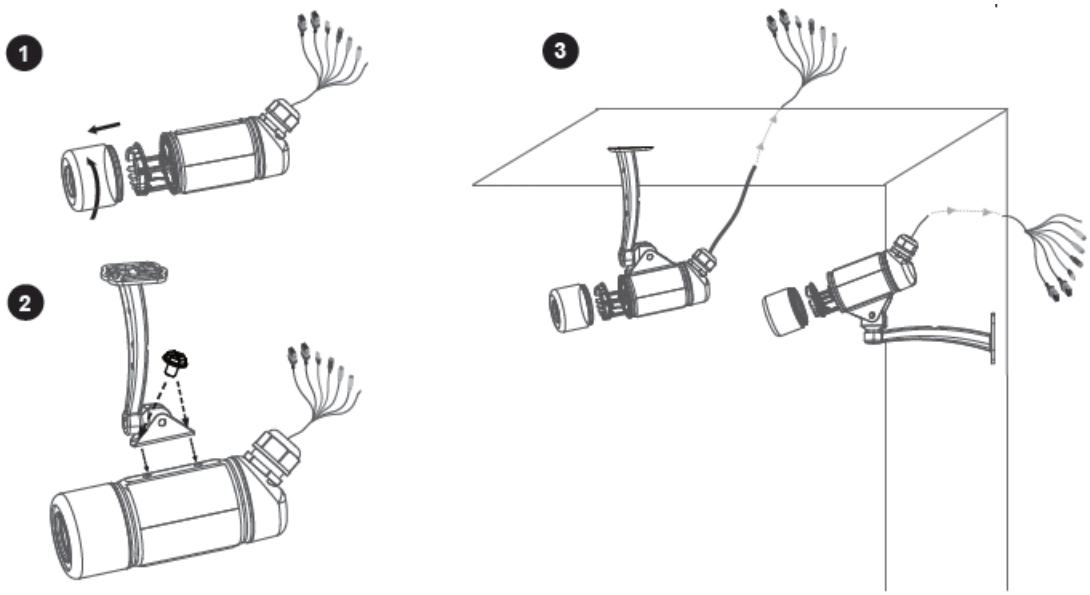
Installation

Hardware installation

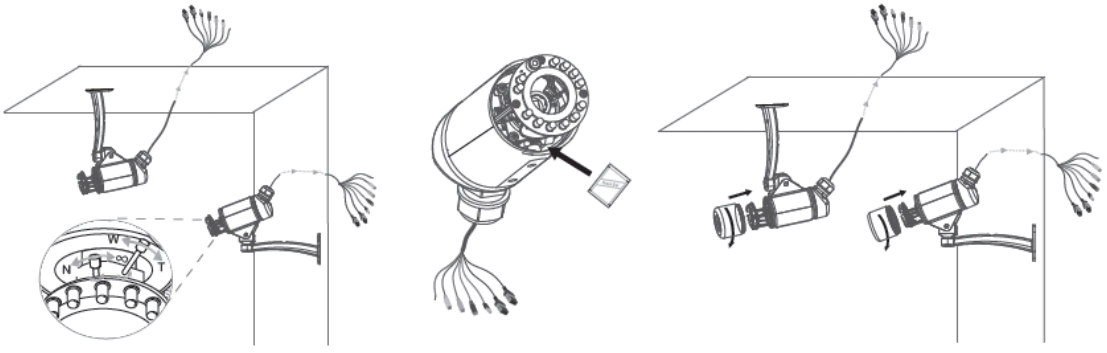
Follow the steps below to install the Network Camera:

1. Open the lens cover.

2. Secure the Network Camera to the supplied camera stand as the illustration shows.
3. Secure the Network Camera to the wall/ceiling by the supplied camera stand.



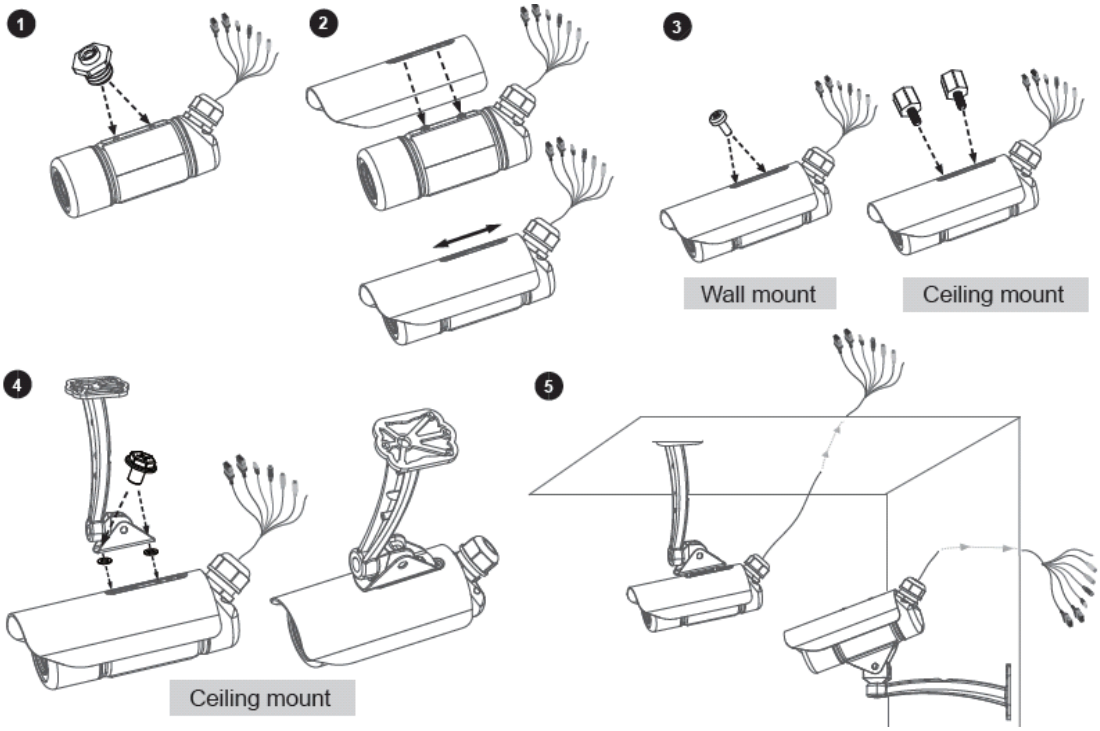
4. Feed power to the Network Camera and connect it to the Internet. For more information, please refer to Network deployment section for details.
5. Install the “Installation Wizard“ to assign IP address to the Network Camera. For more information, please refer to Software installation section for details.
6. Access to the Network Camera from the Internet. For more information, please refer to Accessing the Network Camera section for details.
7. Unscrew the zoom controller to adjust the zoom factor. Upon completion, tighten the zoom controller. Unscrew the focus controller to adjust the focus range. Upon completion, tighten the focus controller.
8. Put the supplied silica gel into the Network Camera and tighten the lens cover. (Please replace the silica gel with a new one if you open the lens cover after installation.)



Note

If you want to use the supplied sun shield for outdoor environments, please follow the steps below to install:

1. Tighten the supplied two screws.
2. Attach the supplied sun shield to the Network Camera and slide it to the desired position.
3. Fix the sun shield with supplied two screws. (Please use different screws for ceiling mount.)
4. For ceiling mount, please add the two supplied washers as the illustration to secure the camera stand.

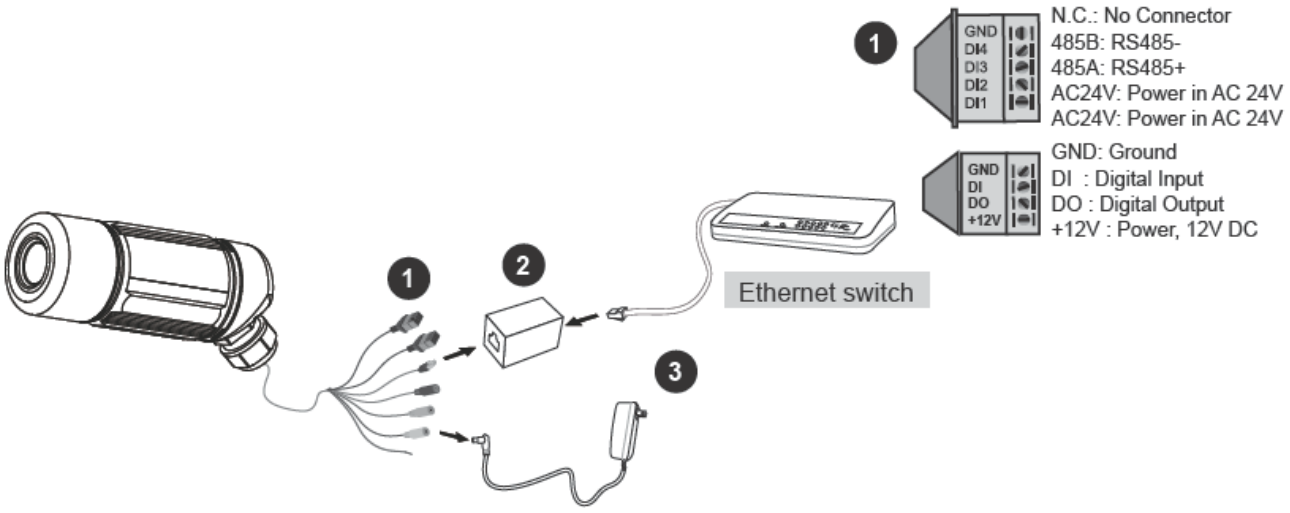


Network deployment

Setup the Network Camera over the Internet

This section explains how to configure the Network Camera to Internet connection.

1. If you have external devices such as sensors and alarms, make connection from general I/O terminal block.
2. Use the supplied RJ45 female/female coupler to connect the Network Camera to a switch. Use Category 5 Cross Cable when Network Camera is directly connected to PC.
3. Connect the power cable from the Network Camera to a power outlet.

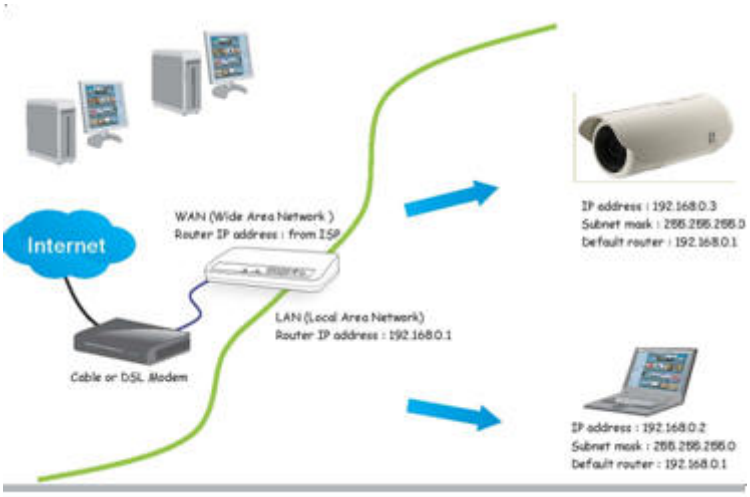


There are several ways to setup the Network Camera over the Internet. The first way is to setup the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

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

1. Connect your Network Camera behind a router, the Internet environment is illustrated as below. About how to get your IP address, please refer to Software installation on latter pages for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

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

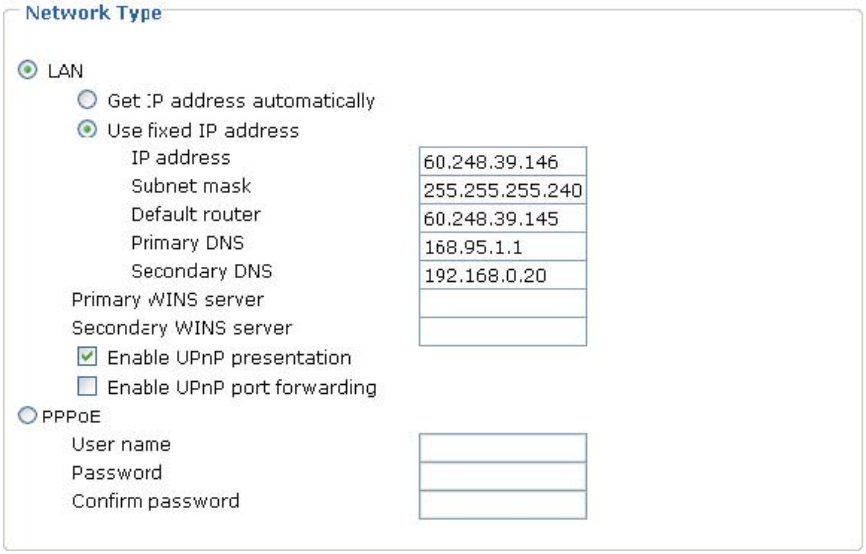
If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to the user's manual of your router.

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

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera and follow the steps below.

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



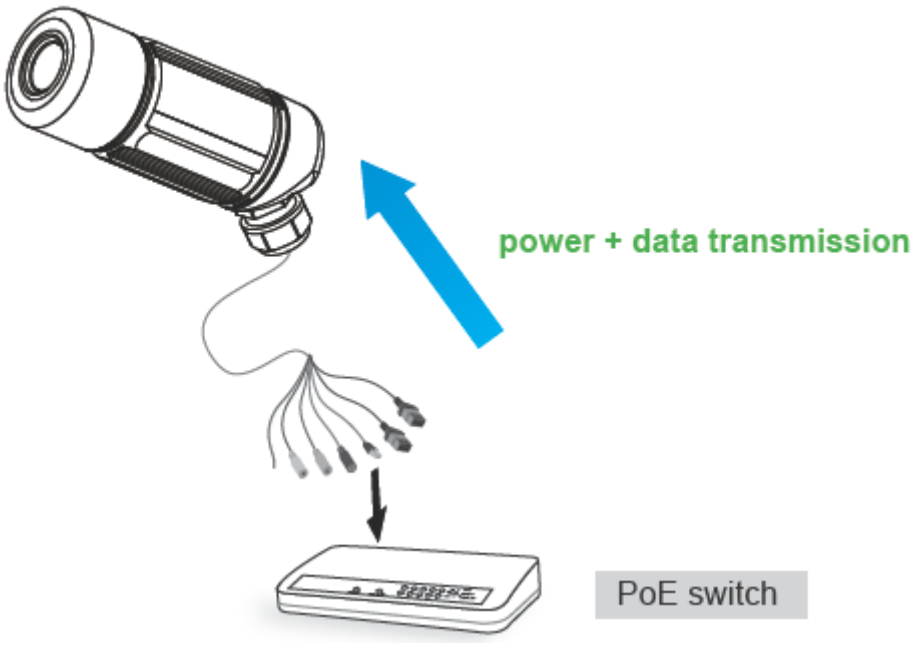
Internet connection via PPPoE (Point-to-Point over Ethernet)

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

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

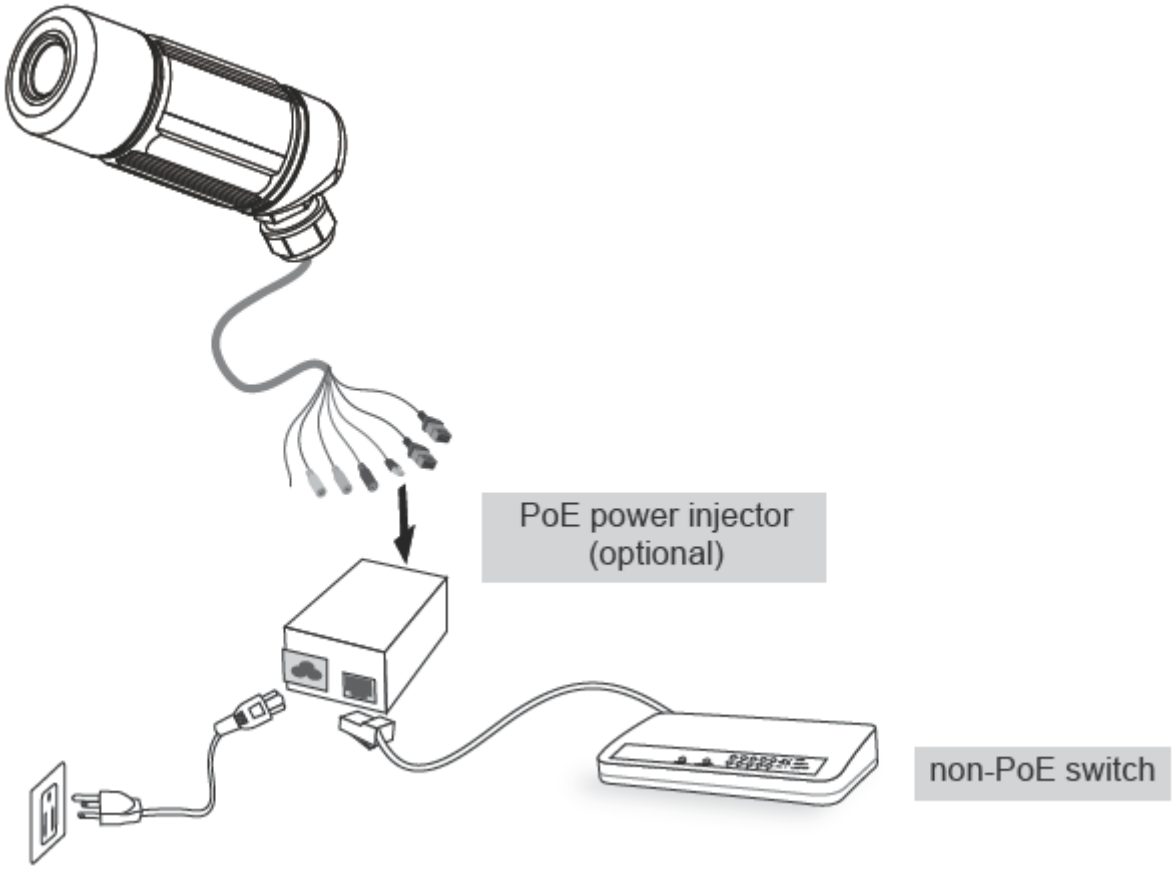
When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet cable. If your switch/router supports PoE, refer to the following illustration to connect the Network Camera to a PoE-enabled switch/router via an 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 Network Camera and a non-PoE switch/router.



Software installation

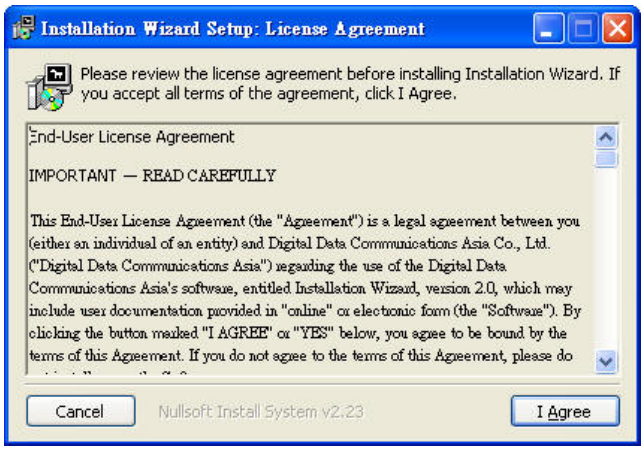
At the end of the hardware installation, users can use Installation Wizard program included in the product CDROM to find the location of the Network Camera. There may be many Network Cameras in the local network. Users can differentiate the Network Cameras with the MAC address . **The MAC address is printed on the label which is on the bottom of the Network Camera body.**

How to Use Installation Wizard

Installation

The following are steps for the software installation.

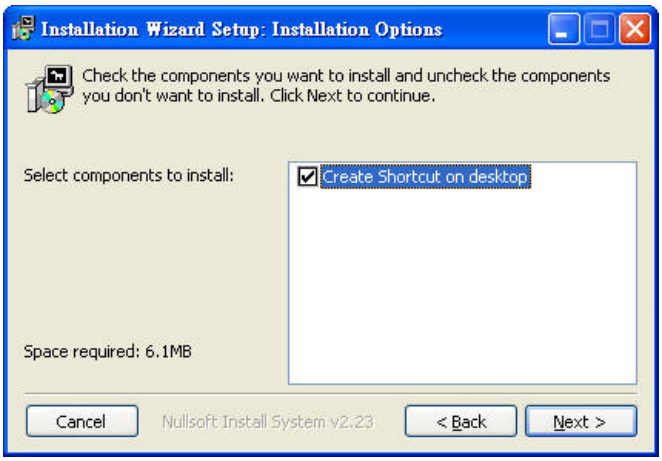
STEP 1: Put the Installation disk into the CD-ROM drive, and the installation should start automatically. If the installation does not start, click on “Start” on the lower left corner of your screen, open “My Computer” and double click on the CD-ROM->Installation_Wizard.exe. The Installation Wizard Installation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



Installation Wizard Installation Window

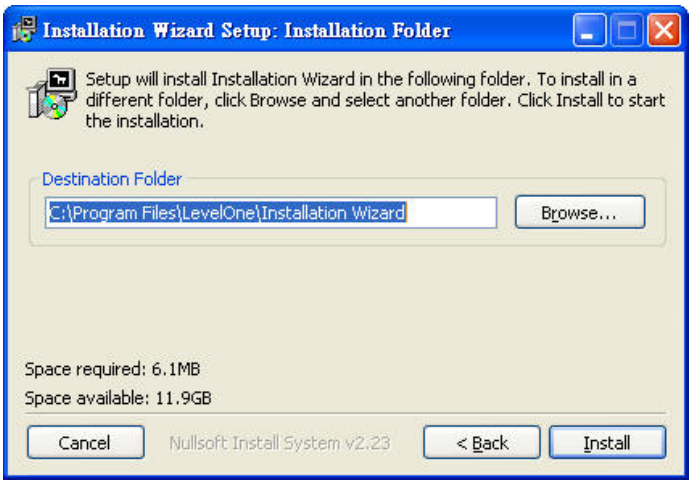
STEP 2: Please read the license agreement first, and then click on “I Agree” to continue the installation process. The install process will go on and then the below window will appear. This page is for you to select the additional

component you want to install. The component “Create shortcut on desktop” will create a shortcut on the desktop. It is more convenient for you to launch Install Wizard 2. After selecting the components, please click on the **“Next”** Button to continue.



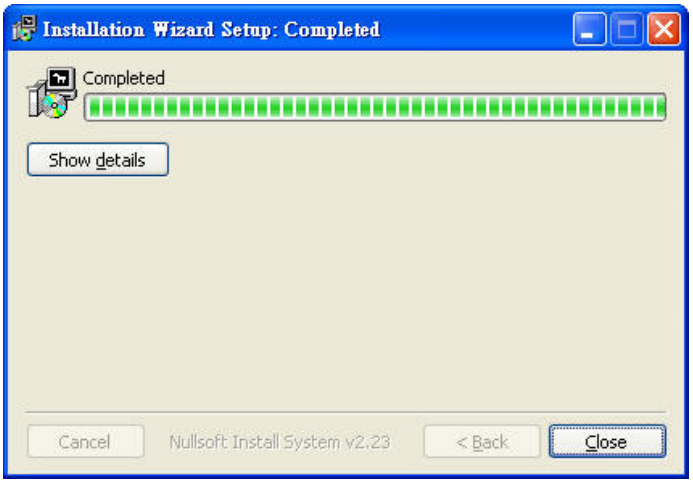
Select components to install for the Installation Wizard

STEP 3: Select the installation directory for this application software and click on “Install” button. You can also change the installation directory by clicking on “Browse…” button. After the proper directory chose, please click on the “Install” button to continue.



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.

User interface of Installation Wizard

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.

User interface of Installation Wizard after clicking on the arrow button

Action buttons

Refresh devices

Clicking on the **"Refresh Devices"** button will refresh the device list and search all devices on the LAN again. Refreshing the device list will take several seconds.

If you want to link to your device, double-clicking it on your device list will lead you to the browser for operating your device.

Function buttons

Function buttons

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

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

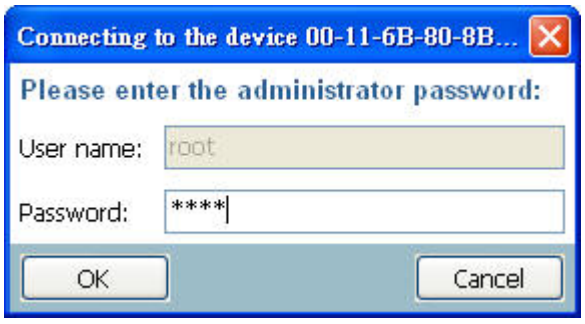
Click on this button to restore the selected device to factory default.

Click on this button to get version information of the Installation Wizard .

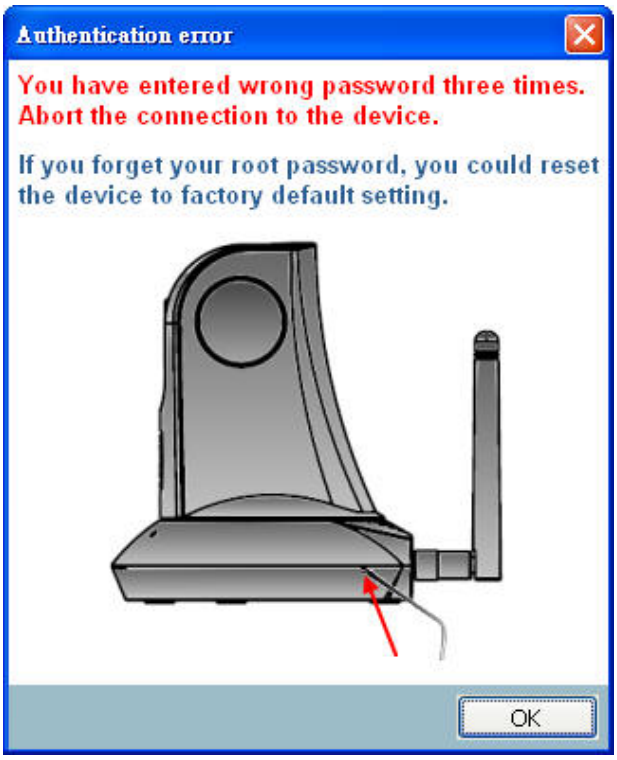
Manual Setup

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.



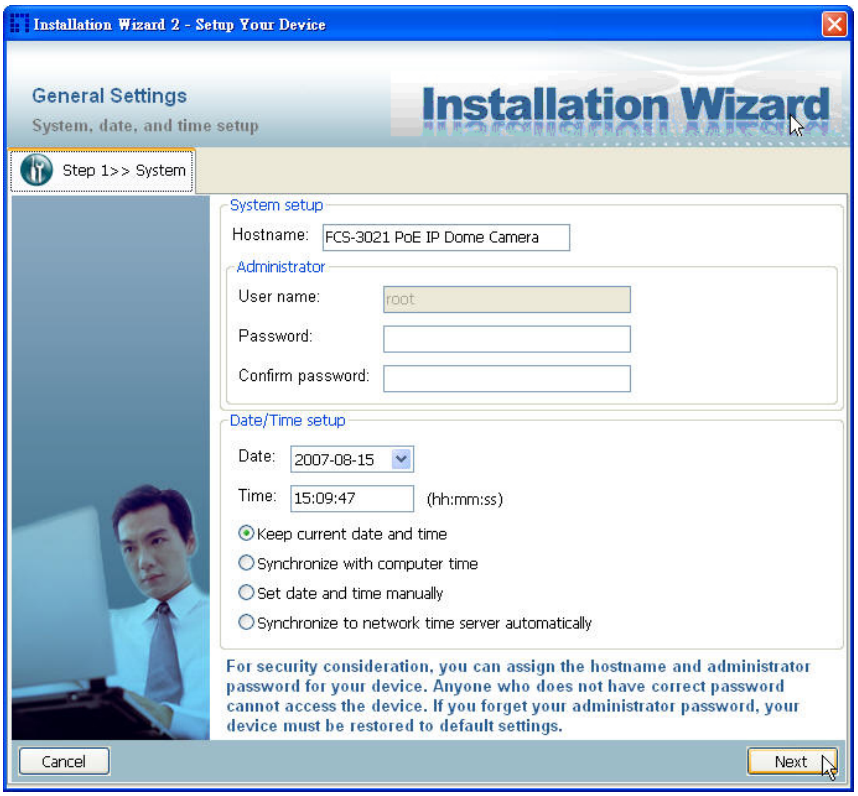
Authentication Dialog Window



Authentication error

System Setting

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



System setting page

Cancel

Click on this button to cancel the setup progress.

Next

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

Change Host Name

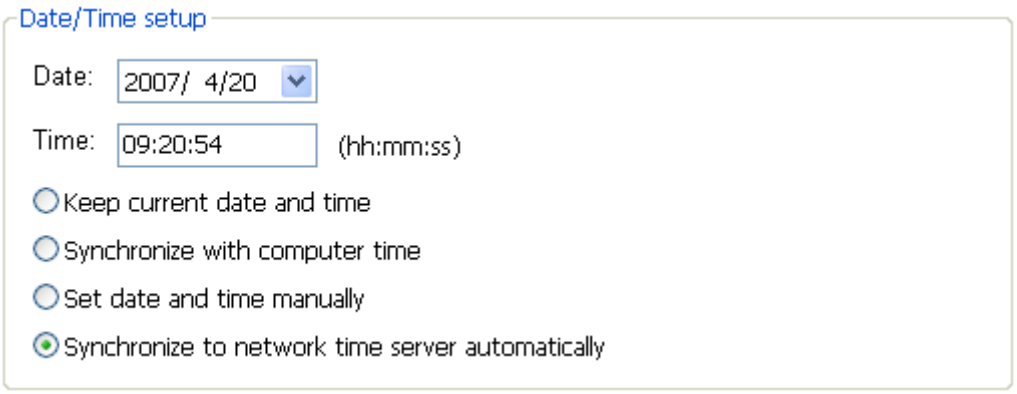
The "**Hostname**" is used for the homepage title of main page and is displayed as the title in the video window of the main page. The maximum string length is 40 characters or 20 characters in double-byte-character-systems like Chinese or Japanese. But for some models supported Unicode, the maximum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

Change root password

To change the administrator's password, type the new password in both

“Password” and **“Confirm Password”** text boxes identically. What is typed will be displayed as asterisks for security purposes. The maximum password depends on the server you connected.

Adjust date and time



Date/Time setup

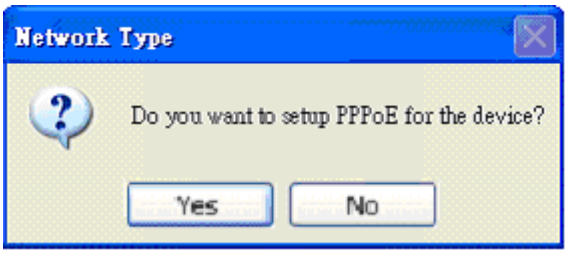
There are three ways to adjust system date and time:

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

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

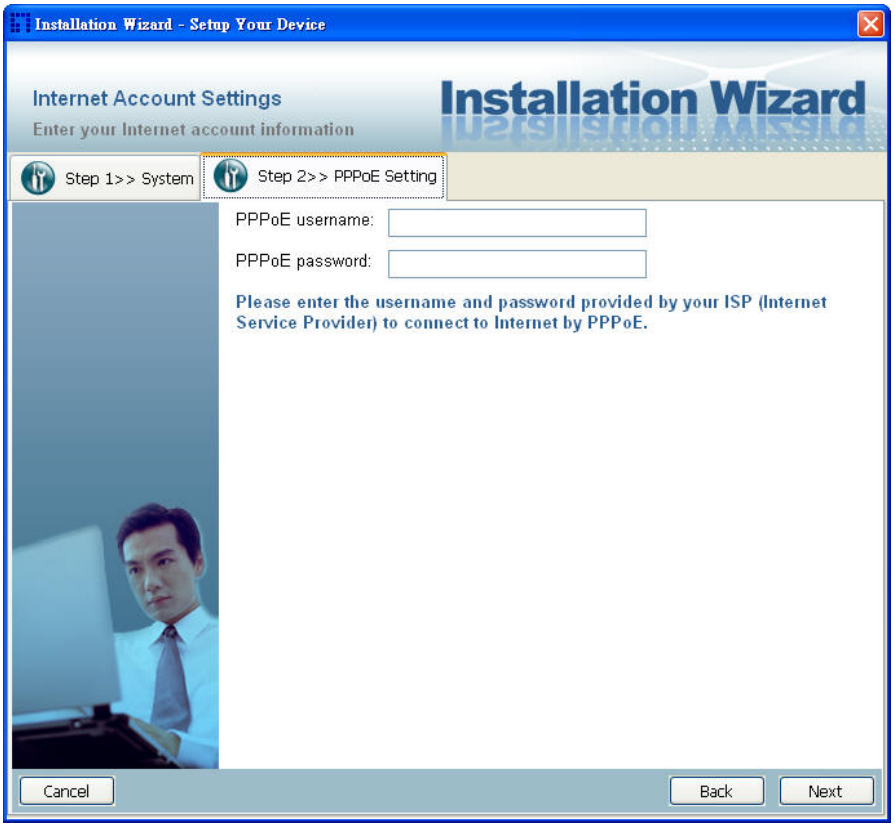
Network Setting

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



Choosing the network type

PPPoE Setting



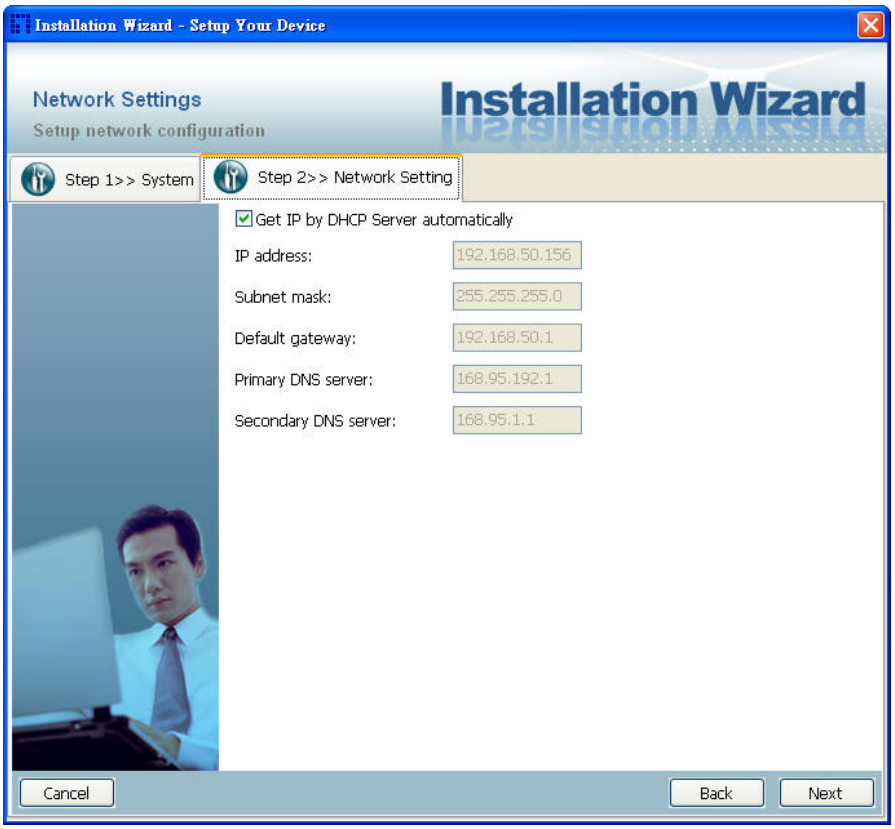
Network setting for PPPoE

If you click on **"Yes"** in the "Network Type" dialog window, you will be led to the PPPoE setting page. In this page, you can input the **"PPPoE**

username” and **“PPPoE password”** provided by your ISP, and then the server will be set to PPPoE mode rather than LAN mode when the setup is completed. If you don’t know the account information, please contact your ISP. After inputting the account information, please click on the **“Next”** button to continue your next step.

LAN Setting

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



Network Setting for LAN

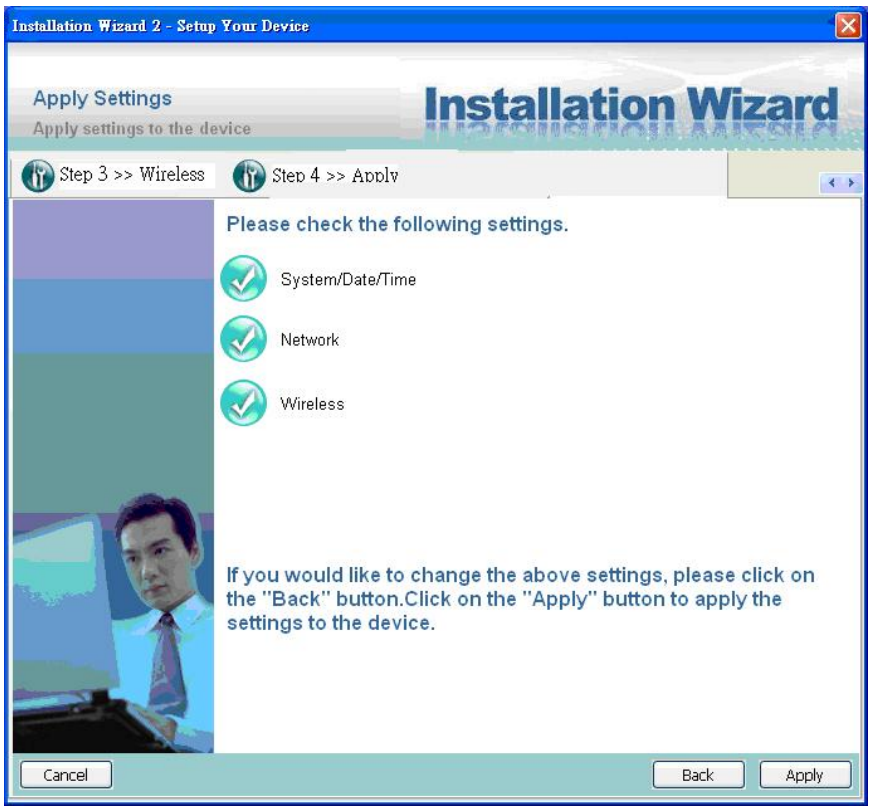
You could set up the network with DHCP or fixed IP:

1. DHCP: Check the **"Get IP by DHCP Server automatically"** will force the device to renew its IP address whenever it reboots, and the related network configuration is provided by the DHCP server.
2. Fixed IP: If you want the device to use a fixed IP, please uncheck the **"Get IP by DHCP Server automatically"** checkbox and assign a valid IP

address, subnet mask, default gateway and DNS server for the device.

Apply to selected device

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



Apply page

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

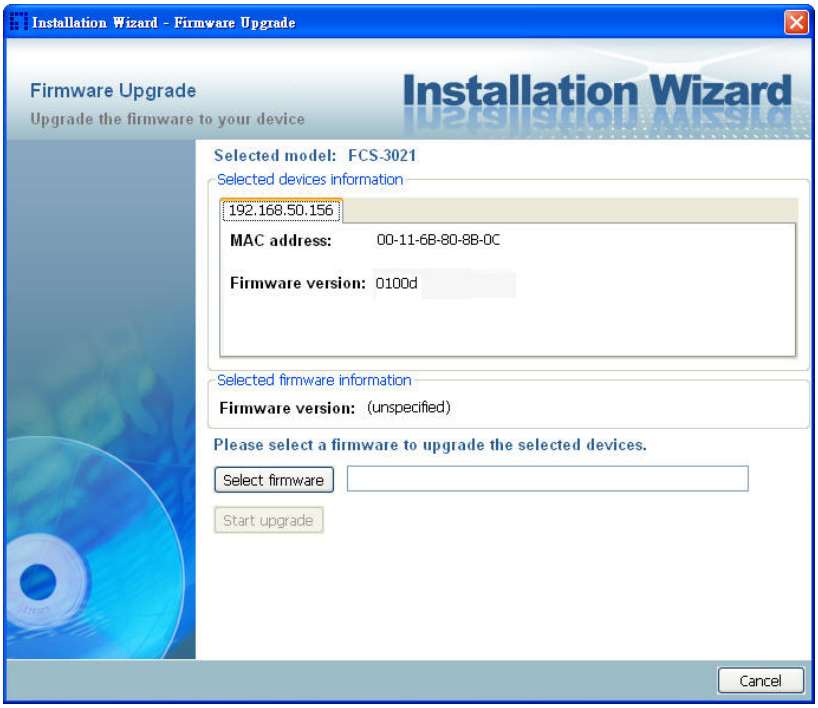
Upgrade

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

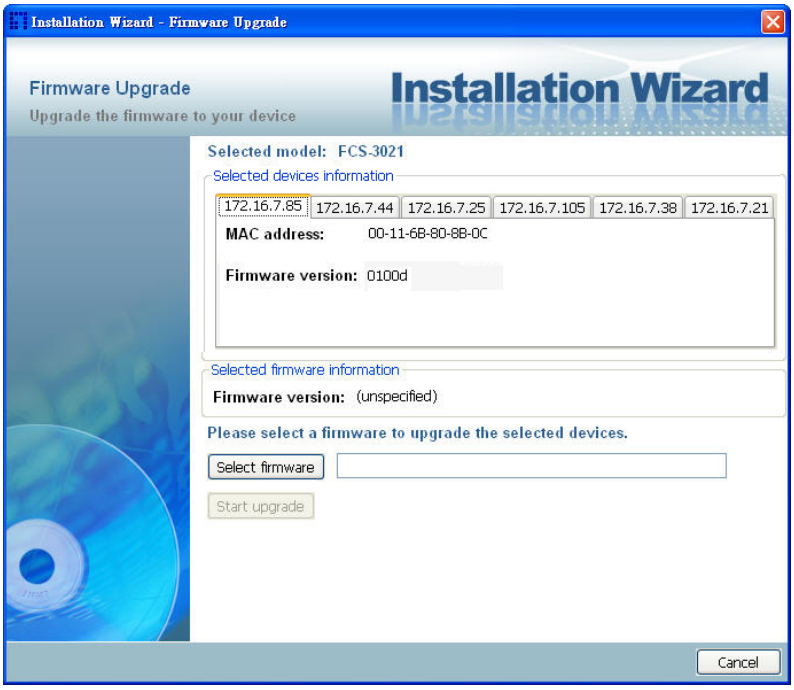
Click on the "Firmware Upgrade"

Device Information

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



Device information



Multiple devices information

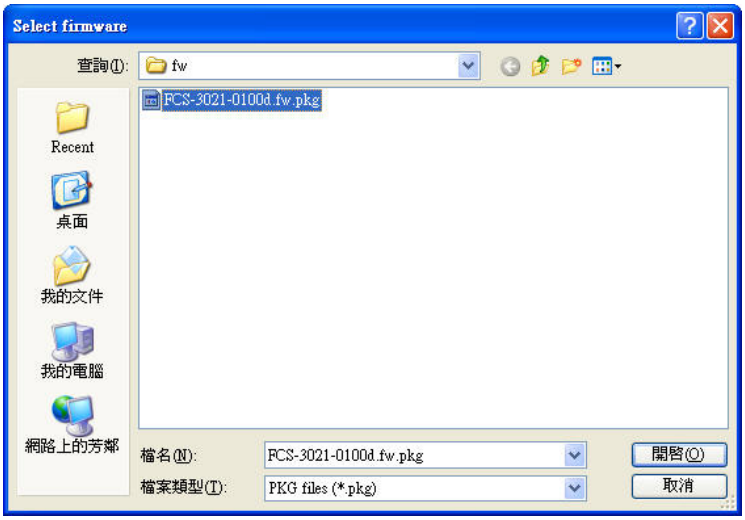
Firmware Information

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

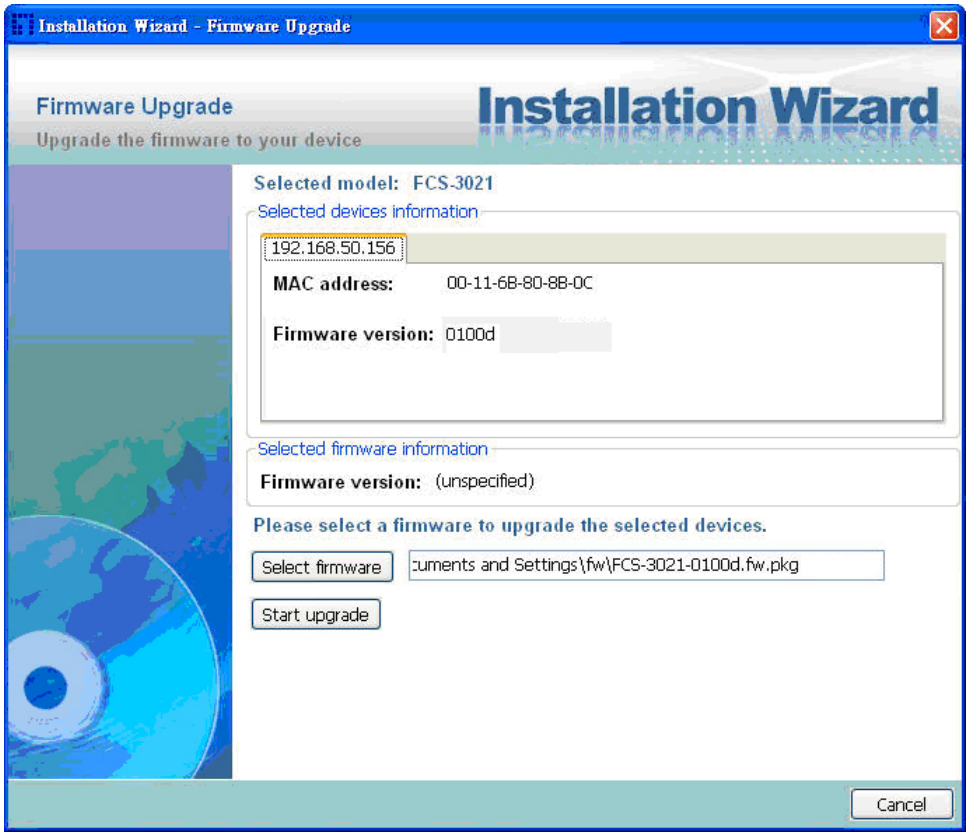
- **Firmware version:** The version number of the selected firmware.

Select Firmware

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



Select firmware

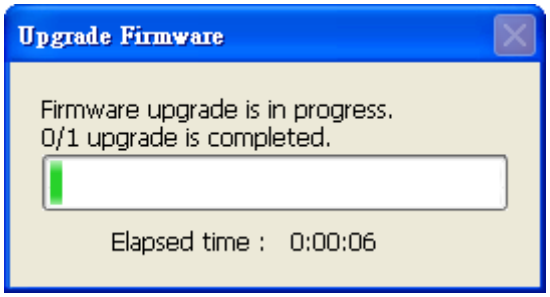


Firmware Information

Warning message for unmatched firmware

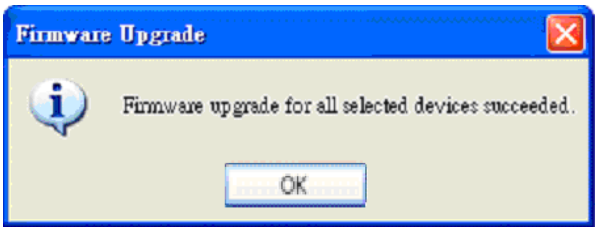
Start Upgrade

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



Update progress

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



Upgrade Done

Accessing the Network Camera

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

Using web browsers

1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press Enter.
3. The live video will be displayed in your web browser.

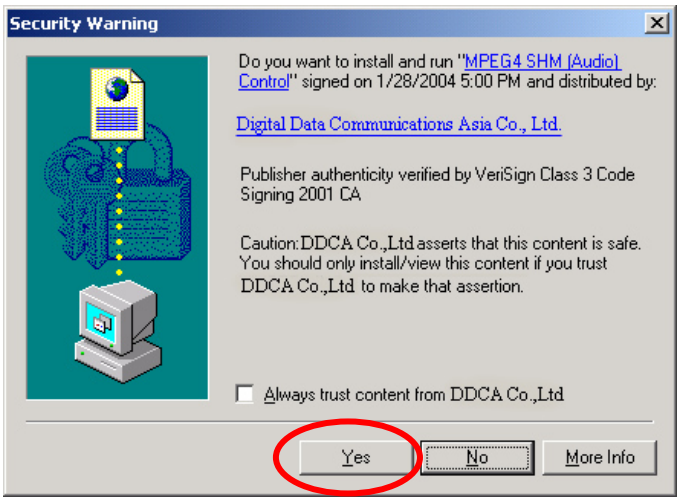
NOTE

► For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video.

► By default, the Network Camera is not password-protected. To prevent unauthorized accesses, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on latter pages.

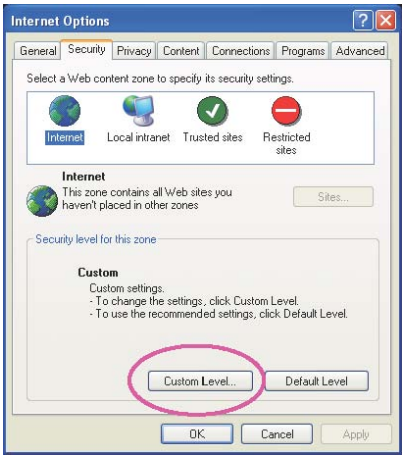
► If you see a warning message at initial access, click Yes to install an ActiveX® control on

your computer.

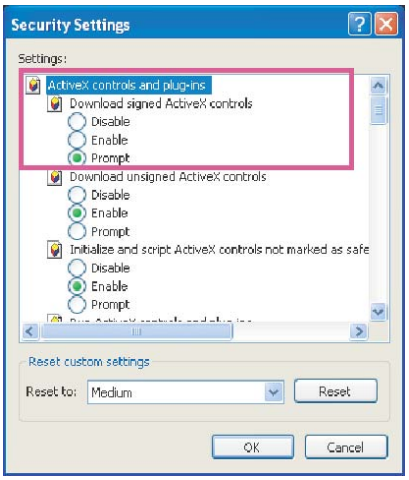


► If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable your ActiveX® Controls for your browser.

1. Choose Tools > Internet Options > Security > Custom Level.



2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click OK.



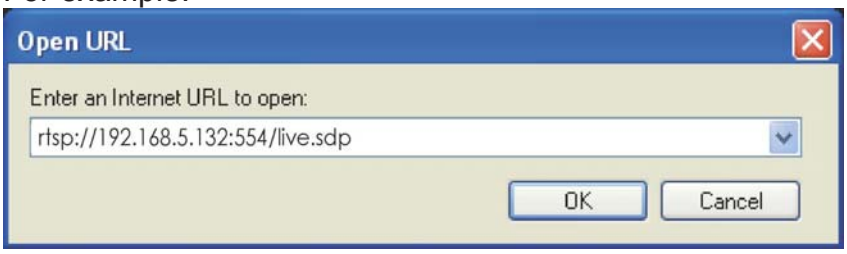
Using RTSP players

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 a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box. The format is rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example:



4. The live video will be displayed in your player.
   For more information on how to configure RTSP access name, please refer to RTSP Streaming on latter pages for details.

Using 3GPP-compatible mobile devices

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

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

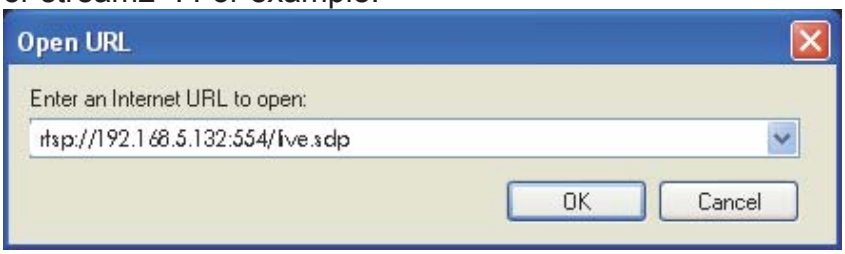
1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable. For more information, please refer to RTSP Streaming on latter pages.

2. As the 3G network bandwidth is limited, you can't use large video size. Please set the video and audio streaming parameters as listed below. For more information, please refer to Audio and video on latter pages.

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 ISP and players only support port number 554 to allow RTSP streaming to go through, please set the RTSP port to 554.For more information, please refer to RTSP Streaming on latter pages.

4. Launch the players on 3GPP-compatible mobile devices, (ex. Real Player).Type the URL commands in the player.
The format is rtsp://<public ip address of your camera>:<rtsp port>/<access name for stream1 or stream2>. For example:



Using recording software

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

Main Page

This chapter explains the layout of the main page. It is composed of the following four sections: Logo of LEVELONE, Menu, Host Name, and Live Video Window.

Logo of LEVELONE

Click this logo to visit LEVELONE website.

Menu

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.

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

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

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

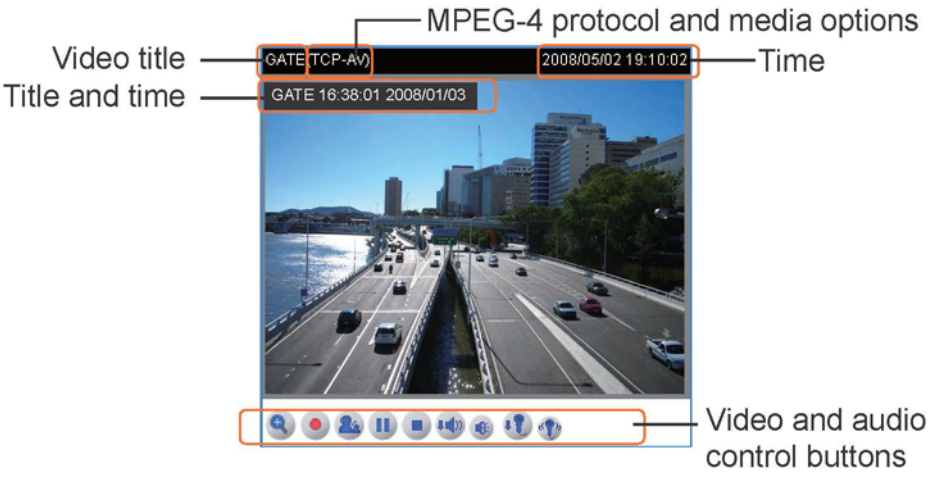
Digital Output: Click this button to turn on or off the digital output device.

Host Name

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

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 latter pages.

Time: Display the current time. For more information, please refer to Video settings on latter pages.
Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on latter pages.

MPEG-4 protocol and media options: The transmission protocol and media options for MPEG-4 video streaming. For more information, please refer to Client Settings on latter pages.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Digital zoom edit: Deselect Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is 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 quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on latter pages for details.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera.

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

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

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

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

Mute: Turn off the volume at local computer.

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

Mute: Turn off the microphone volume at local computer.

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 latter pages.

Time: Display the current time. For more information, please refer to Video settings on latter pages.

Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on latter pages.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Digital zoom edit: Deselect Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is 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 quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on latter pages for details.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera.

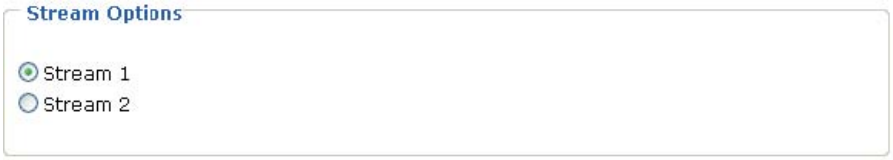
Mic Volume: When the mute function is not activated, move the slider bar to adjust the microphone volume at local computer.

Mute: Turn off the microphone volume at local computer.

Client Settings

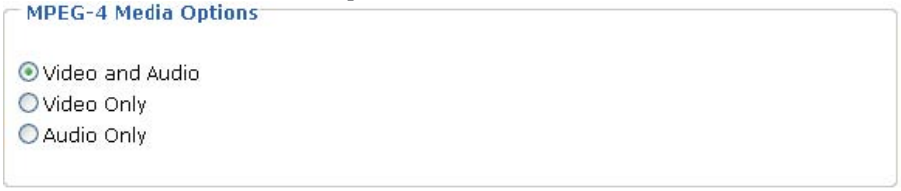
This chapter explains how to select the streaming source, transmission mode and saving options at local computer. It is composed of the following four sections: Stream Options, MPEG-4 Media Options, MPEG-4 Protocol Options and MP4 Saving Options. When completed with the settings on this page, click Save on the page bottom to take effect.

Stream Options



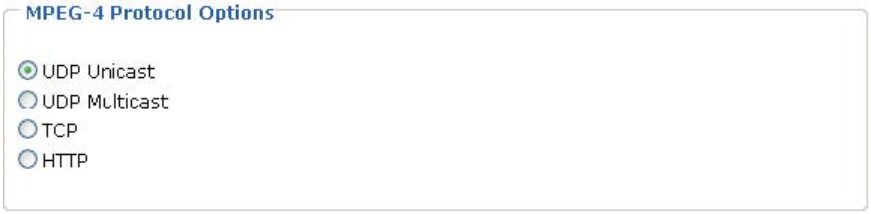
The Network Camera supports MPEG-4 and MJPEG dual streams. For more information, please refer to Video settings on latter pages.

MPEG-4 Media Options



Select to stream video or audio data. This works only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options



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

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

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

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. Nevertheless, the downside with 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 and you don't need to open specific port for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data to come through.

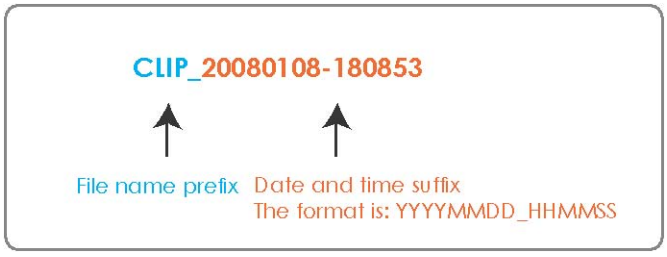
MP4 Saving Options

Users can record the 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 put in front of the video file name.

Add date and time suffix to the file name: Select this option to add date and time to the file name suffix.



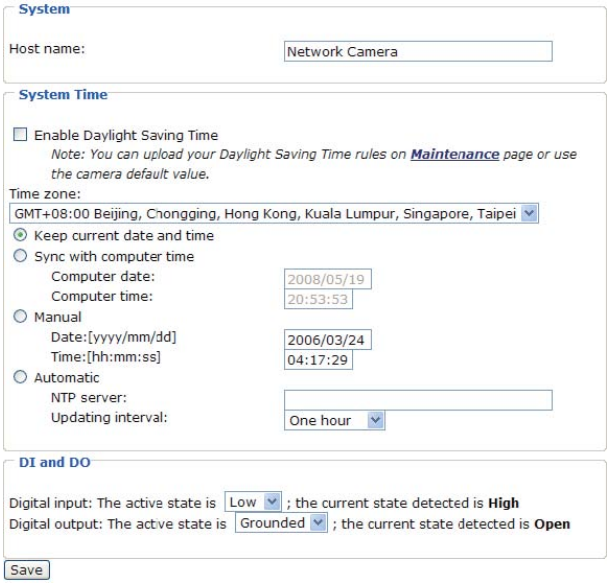
Configuration

Only Administrators can access the system configuration page. Each category in the left menu will be explained in the following sections.

System

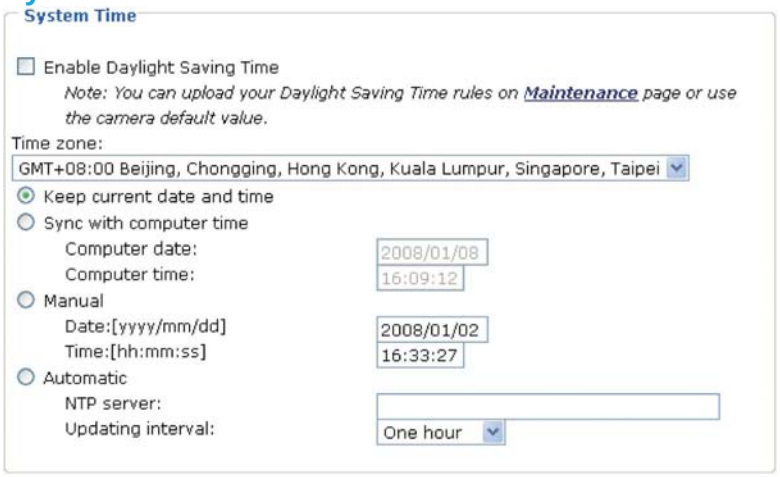
This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When completed with the settings on this page, click Save on the page bottom to take effect.

System



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

System Time



Enable Daylight Saving Time: Select this option to enable daylight saving time (DST). During DST, the system clock moves one hour ahead. Note that to utilize this feature, please set the time zone for your Network Camera first. Then, the starting time and ending time of the DST is displayed upon selecting this option. To manually configure the daylight saving time rules, please refer to Upload / Export Daylight Saving Time Configuration File for details.

Time zone: According to your local time zone, select one from the drop-down list.

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

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

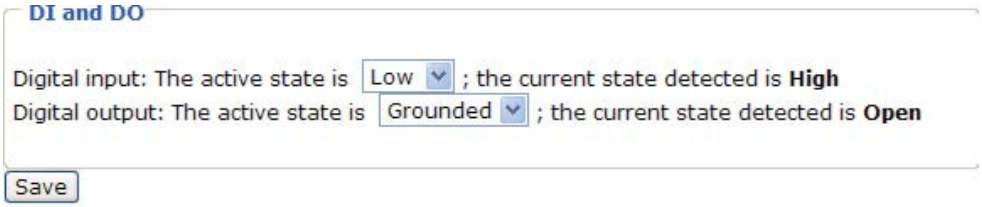
Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

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

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

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

DI and DO



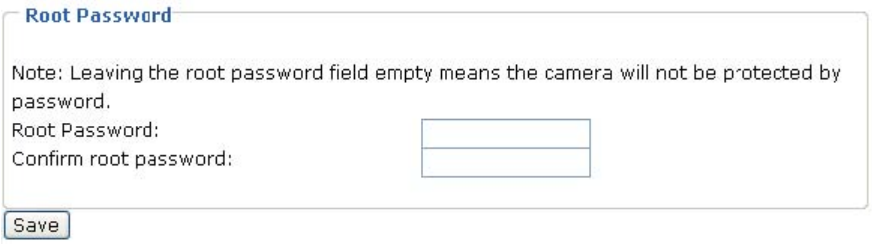
Digital input: Select High or Low to define normal status of the digital input. The Network Camera will report the current status.

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

Security

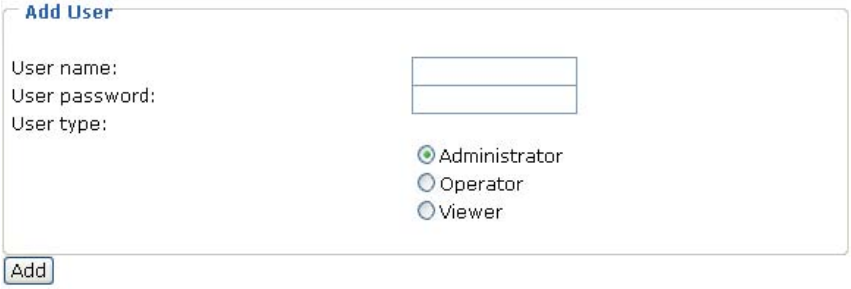
This section explains how to enable password protection and create multiple accounts. It is composed of the following three columns: Root Password, Add User and Manage User.

Root Password



The administrator account “root” is permanent and can not be deleted. Please note that if you want to add more accounts, you must apply a password for the “root” account first.
1. Type the password identically in both text boxes.
2. Click Save to enable password protection.
3. A window will be prompted for authentication; type the correct user’s name and password in related
fields to access the Network Camera.

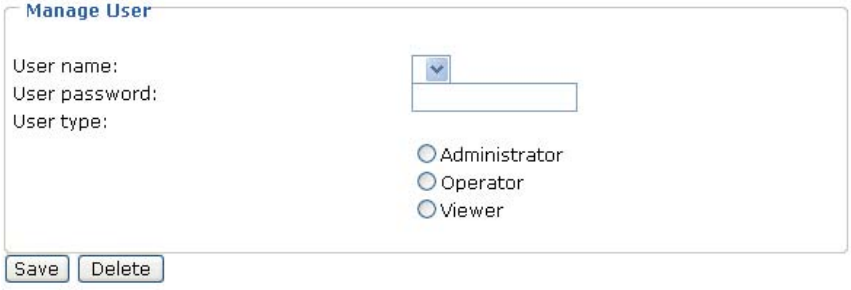
Add User



Administrators can add up to twenty user accounts.
1. Input the new user’s name and password.
2. Select the desired security level. Click Add to take effect.

Access rights are sorted by user types. There are three kinds of user types. Only administrators can access the Configuration page. Operators and viewers can not access the configuration page. Though operators can not access the page, they are capable of using the url commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera. Viewers can only access the main page.

Manage User



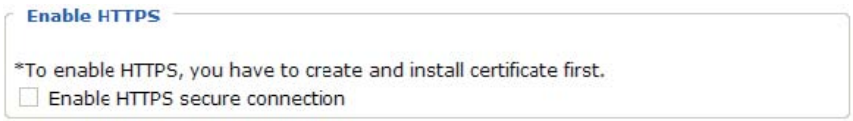
Here you can change user’s access rights or delete user accounts.
1. Pull down the user list to find an account.
2. Make necessary changes and then click Save or Delete to take effect.

HTTPS

This section explains how to enable authentication and encrypted communication over SSL.

Enable HTTPS

Select this option to turn on the HTTPS communication.



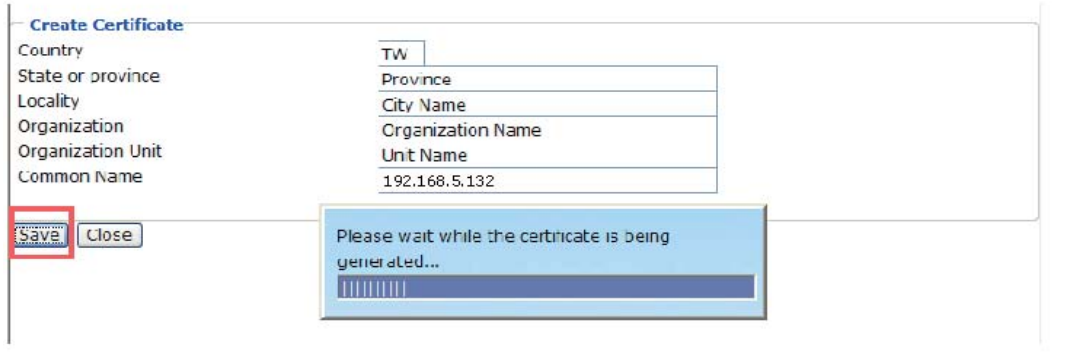
Create and Install Certificate

Select either to create a self-signed certificate or a signed certificate.

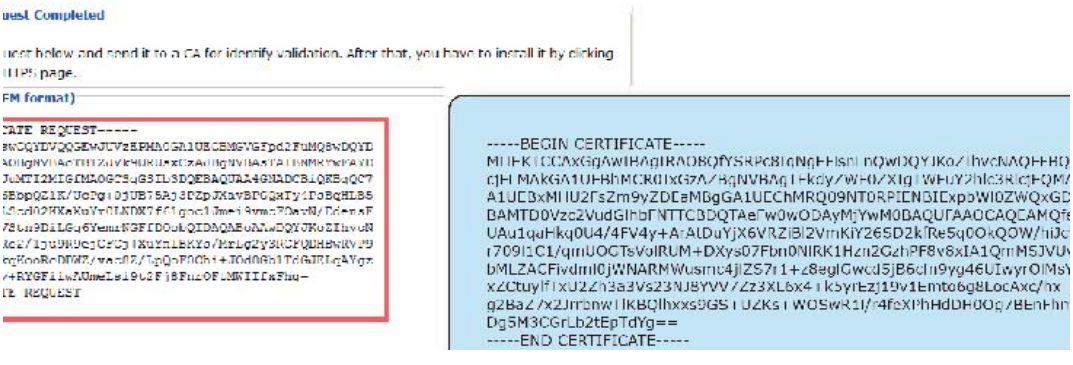
To create a certificate from a certificate authority

1. Click Create for Certificate request. The Create Certificate window will pop up.

2. Fill in the information required for generating a Certificate Signing Request (CSR) and click Save.



example of a CSR:



3. Here is an example of a CSR:

4. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera.

Wait for the certificate authority to issue a SSL certificate; then upload the issued certificate to the

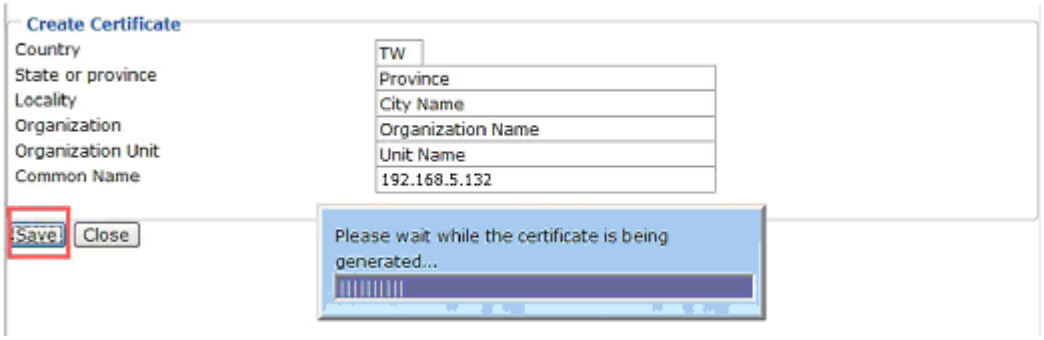
Network Camera.

5. Browsing the Network Camera using HTTPS helps to protect streaming data over the Internet.

To create a self-signed certificate

1. Click Create for Create and Install Certificate. This pops up the Create Certificate window.

2. Fill in the information required for generating a Certificate Signing Request (CSR) and click Save.



3. Browsing the Network Camera using HTTPS helps to protect streaming data over the Internet.

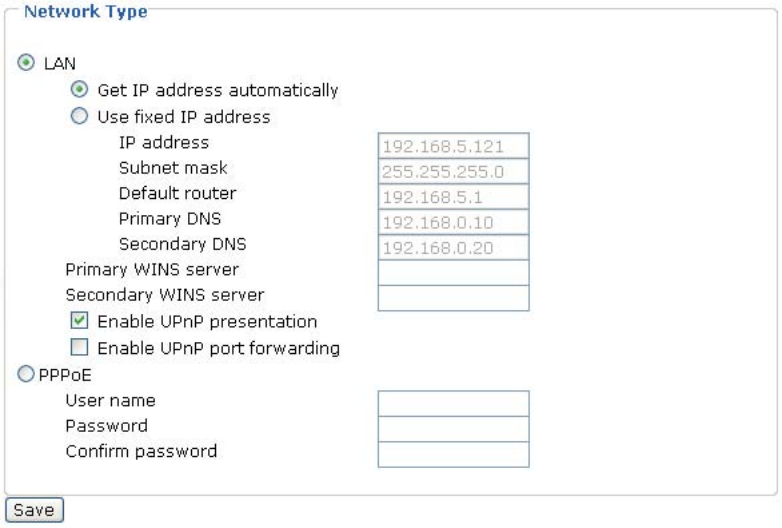
Certificate Information

Here display the certification information. Users may click Property for details. To remove the signed certificated, uncheck the Enable HTTPS secure connection and click Remove.

Network

This section explains how to configure wired network connection for the Network Camera. It is composed of the following five columns: Network Type, HTTP, Two way audio, FTP and RTSP Streaming. When completed with the settings on this page, click Save to take effect.

Network Type



LAN

Select this option when the Network Camera is deployed in a local area network (LAN) and is intended to be accessed by local computers.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by a DHCP server each time the camera is connected to the LAN. If there is no DHCP server in the LAN, the default IP address will be 169.254.xxx.xxx.You may execute Installation Wizard to find the IP address of your Network camera.

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

Enable UPnP presentation: Select this option to enable UPnPTM presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. Currently, UPnPTM is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnPTM component is installed on your computer.

Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnPTM and it is activated.

PPPoE (Point-to-point over Ethernet)

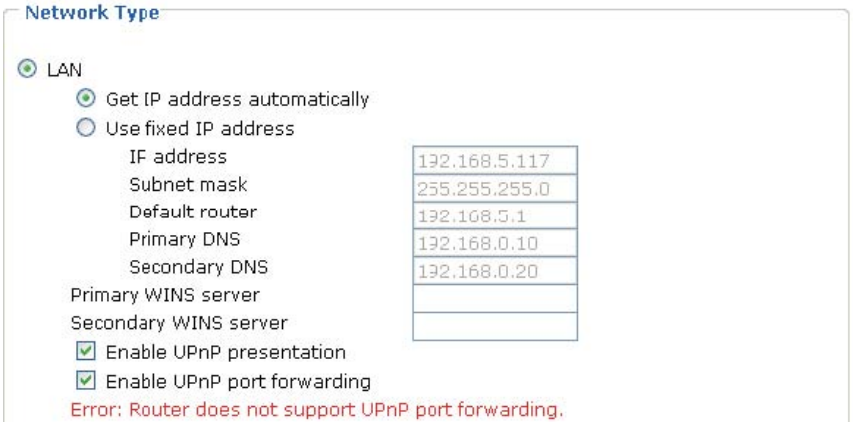
Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.
1. Set up the Network Camera in a LAN.
2. Go to Configuration > Application > Server Settings (please refer to Server Settings) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings). Select System log so that you will receive a list of 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 take effect.
5. The Network Camera starts to reboot.
6. Disconnect the power source of the Network Camera; remove it from the LAN environment to the Internet.

NOTE

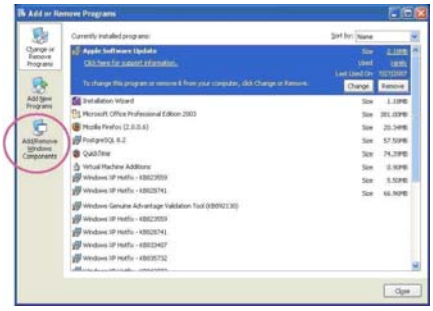
► If the default ports are already used by other device connecting to the same router, the Network Camera will select other ports for the Network Camera.

► If UPnPTM is not supported by your router, you will see the following message.

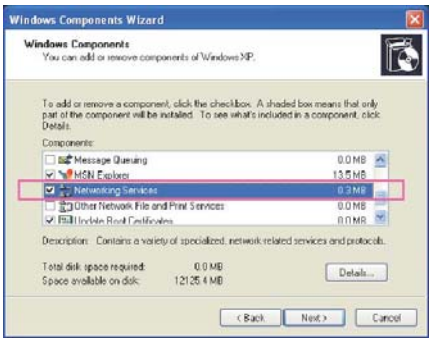


► Steps to enable UPnPTM user interface on your computer:
Note that you must log on to the computer as a system administrator to install the UPnPTM components.

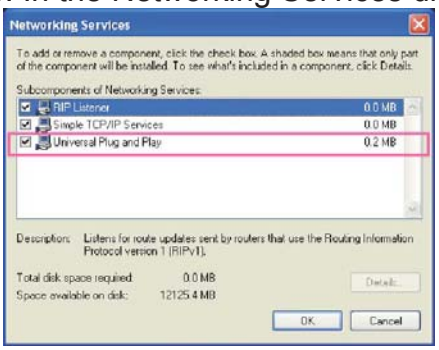
1. Go to Start, click Control Panel, and then click Add or Remove Programs.
2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.



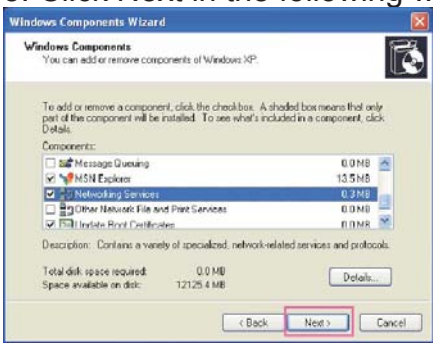
3. In the Windows Components Wizard dialog box, select Networking Services and then click Details.



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



5. Click Next in the following window.



6. Click Finish. UPnPTM is enabled.

► How does UPnPTM work?

UPnPTM 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 bothersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts at My Network Places.

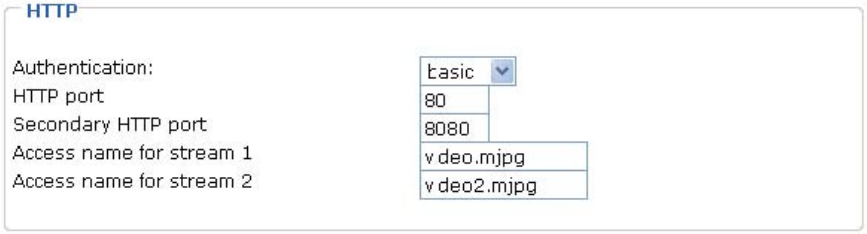
Below for the Network Camera's IP address.

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

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

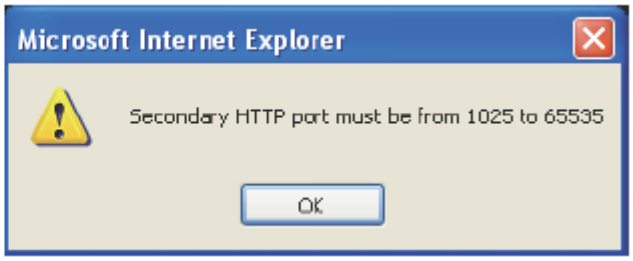
► If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on latter pages for details. After the Network Camera is reset to factory default, it is accessible in a LAN.

HTTP



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for a HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in 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. Also, they can be assigned with another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages are displayed:



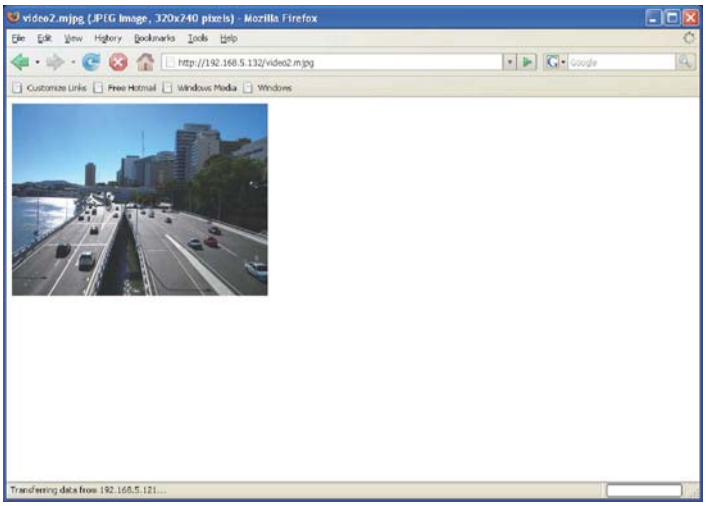
To access the Network Camera within a LAN, both HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

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

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source. When using Mozilla Firefox or Netscape to access the Network Camera, and the video mode is set to JPEG, users will receive continuous JPEG pictures. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.
Use http://<ip address>:<http port>/<access name for stream1 or stream2> to make

connection.

For example, when the access name for stream 1 is set to video.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address field. Press Enter.
3. The JPEG images will be displayed in your web browser.



NOTE

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

► Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.

HTTPS

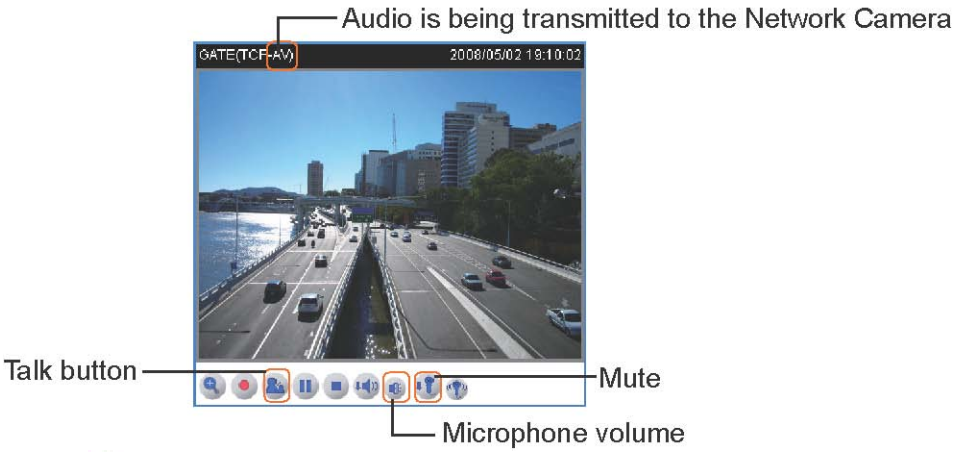
By default, the HTTPS port is set to 443. Also, it can be assigned with another port number between 1025 and 65535.

Two way audio

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

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

Note that as JPEG only transmits a series of JPEG images to the client, to utilize this feature, make sure the video mode is set to "MPEG-4" and the media option is set to "Video and Audio".

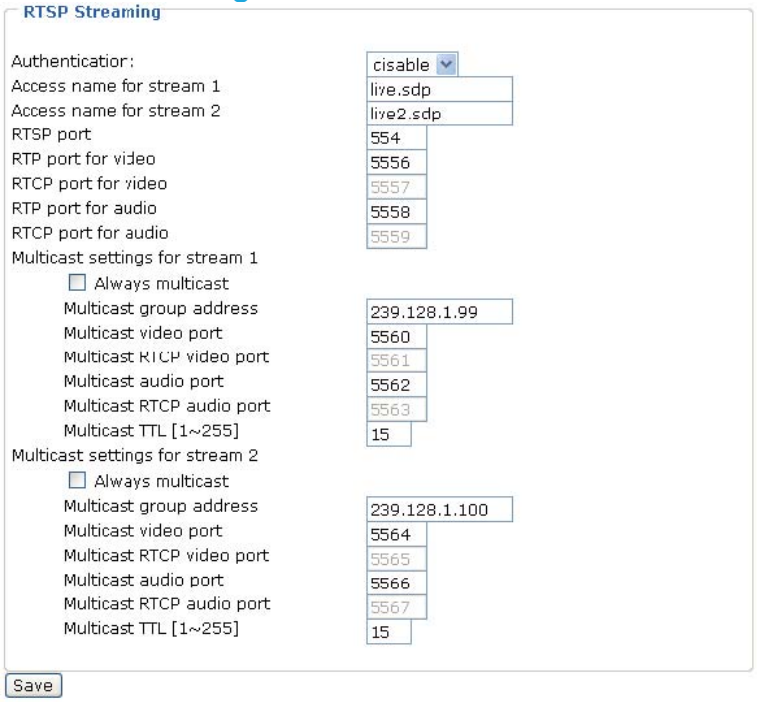


Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP

The FTP server allows the Network Camera to utilize LEVELONE Installation Wizard 2 to upgrade firmware. By default, the FTP port is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

RTSP Streaming



Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

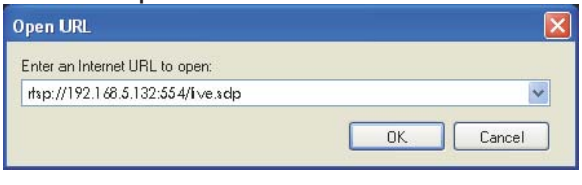
The accessibility of the RTSP streaming for the three authentication modes are listed in the following table:

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

O indicates that the authentication mode is supported by the RTSP player.
X indicates that the authentication mode is NOT supported by the RTSP player.

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source. When using a RTSP player to access the Network Camera, and the video mode is set to MPEG-4, use the following RTSP URL command to request a transmission of streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box.
For example:



4. The live video will be displayed in your player.

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

The RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

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

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

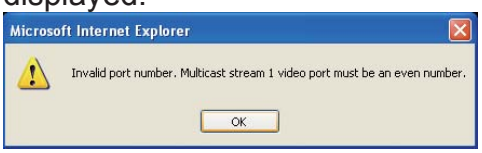
The five ports can be changed between 1025 and 65535. The RTP port must be an even number and the RTCP port is RTP port number plus one, and thus always be odd. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message is displayed:

Multicast settings for stream 1 / Multicast settings for stream 2: Select the Always multicast to enable multicast for stream 1 or stream 2. 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 by requesting a copy from the Multicast group address.

The five ports can be changed 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 it is always be 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 is 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.

The path of multicast stream1 is http://camera's IP address/live1.sdp while the one of multicast stream2 is http://camera's IP address/live2.sdp.

NOTE

► To utilize the RTSP streaming authentication, make sure that your have set a password for the Network Camera first; please refer to Security section for details.

DDNS

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

DDNS: Dynamic domain name service

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

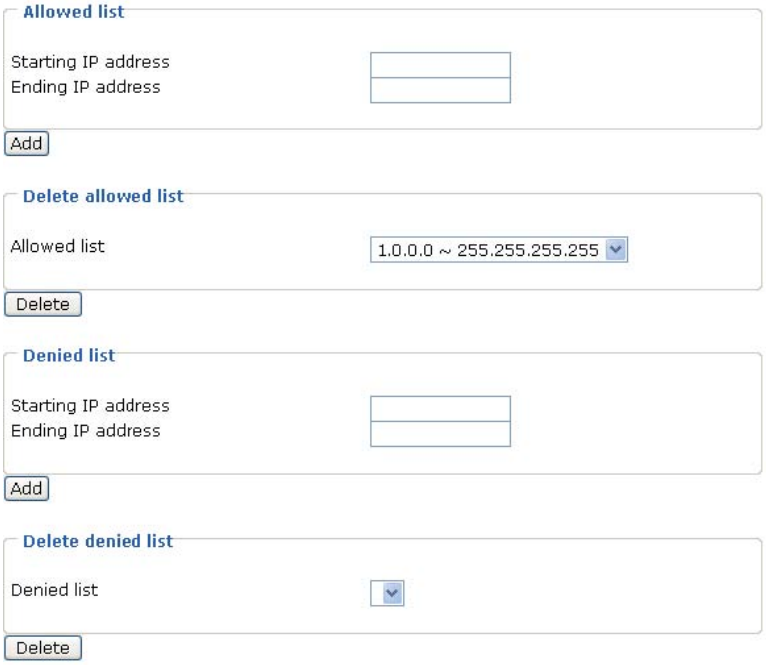
Provider: Select a DDNS provider of your choice from the Provider drop-down list.
We offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, dyn-interfree.it. Note that to utilize this feature, please apply a dynamic domain account first.

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

Access list

This section explains how to control the access permission by checking the client PC's IP addresses. It is composed of the following four columns: Allowed list, Denied list, Delete allowed list, and Delete denied list.

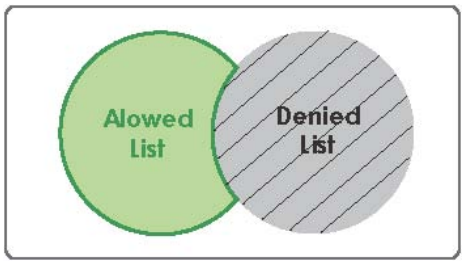
Allowed list / Denied list



There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are in the Allowed list and not in the Denied list can access the Network Camera.
1. In the Allowed list or Denied list column, type the starting IP address and ending IP address in the text boxes. A total of ten lists can be configured for both columns.
2. Click Add to take effect.

NOTE

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



Delete allowed list / Delete denied list

1. In the Delete allowed list or Delete denied list, select a list from the drop-down list.
2. Click Delete to take effect.

Audio and video

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

Video settings

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

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

Power line frequency: Set the power line frequency in consistent with local utility settings to eliminate uncomfortable image flickering associated with fluorescent lights. Note that after the power line frequency is changed, it is required to disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.
Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation.

White balance: Adjust the value for best color temperature.
■ Auto
The Network Camera automatically adjusts the color temperature of light in response to different light sources. The white balance setting defaults to Auto and works well in most situations.

■ Keep current value
Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions.
1. Set the White balance to Auto.
2. Place a sheet of white paper in front of the lens; then allow the Network Camera to adjust the color temperature automatically.

Maximum Exposure Time: 1/30 S, 1/15 S, 1/5 S, and Auto.

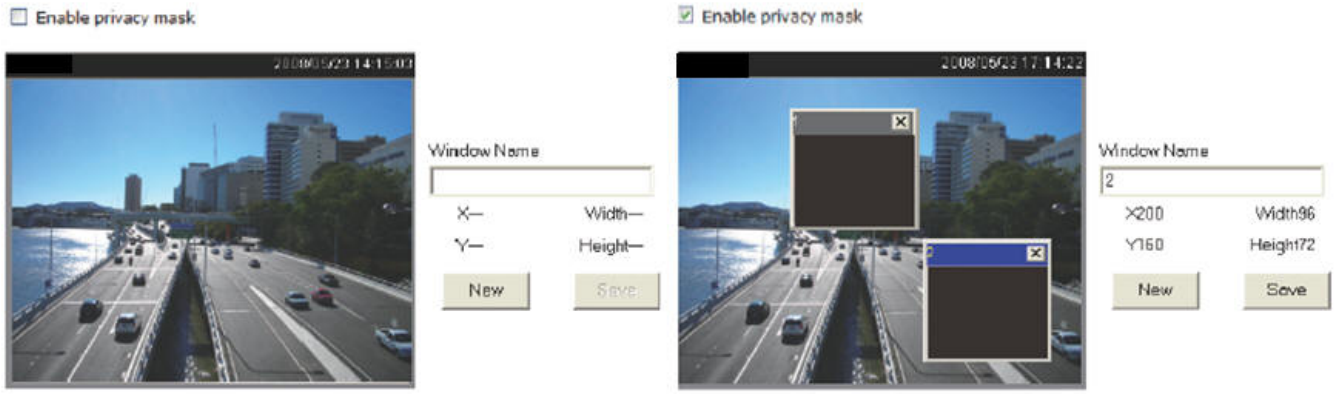
Overlay title and time stamp on video: Select this option to place the video title and time on video streams.
Note that when the frame size is set to 176 x 144 as the right picture below, only time will be stamped on video streams.

Image Settings

Click Image settings to open the Image Settings page. In this page, you can tune Brightness, Saturation, Contrast, and Hue for video compensation. Each field has eleven levels ranged from -5 to +5. The value 0 indicates default auto tuning. 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 take effect and click Close to quit the page.

Privacy mask

Click Privacy Mask to open the Privacy Mask page. In this page, you can block out some sensitive zones for privacy concerns.



■ To set the privacy mask windows, follow the steps below:
1. Click New to add a new window.
2. To resize 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 descriptive Window Name and click Save to take effect.
4. Select Enable privacy mask to enable this function.

NOTE

► Up to 5 privacy mask windows can be set in the same screen.

► If you want to delete the window, please click on the ‘x’ at the upper right-hand corner of the window to close the window.

Sensor Settings

Click Sensor Settings to open the Sensor Settings page. In this page, you can set the exposure level, AGC, WDR (Wide Dynamic Range), night mode, and IR cut filter.

Exposure level 4
Enable AGC 8X
Enable WDR
Switch to B/W in night mode
IR cut filter Auto

Preview Restore Save Close

Exposure level:

You can manually set up the Exposure level, which ranges from 1 to 8. The default value is 4.

Exposure level 4
Enable AGC 8X
Enable WDR
Switch to B/W in night mode
IR cut filter Auto

Preview Restore Save Close

AGC (Auto Gain Control):

You can manually set up the AGC level (2X, 4X, or 8X). The default value is 4X.

Enable WDR (Wide Dynamic Range):

Select it to enable the WDR function. This Network Camera with WDR feature can cope with very challenging lighting conditions. It is capable of capturing both of the dark part and bright part of a target and combining the differences into a scene to generate a highly realistic image as the human eyes can see. Note that if you select this function, Exposure level and AGC function will be disabled.

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

IR cut filter:
With a removable IR-cut filter and built-in IR illuminators, up to 15m, this Network Camera can automatically remove the filter and turn on the IR illuminators during the nighttime to accept IR illumination for low light sensitivity.

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

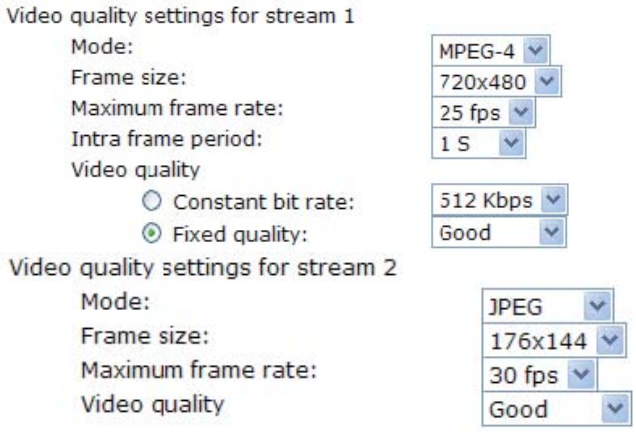
■ Schedule mode
The Network Camera switches between day mode and night mode based on specified schedule. Enter the starting time and ending time for the day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the starting time and ending time of day mode are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

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

■ Night mode
In night mode, the Network Camera switches off (remove) the IR cut filter to allow the infrared light to pass through. This improves the sensitivity of the Network Camera in low-light conditions.

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 take effect and click Close to quit the page.

Video quality settings for stream 1 / stream 2: You can set up two seperate streams for the Network Camera for different viewing devices. For example, set the Network Camera to a smaller frame size and a lower bit rate for remote viewing on mobile phones. Or, set the Network Camera to a larger video size and a higher bit rate for live viewing on web browsers.



■ Mode
The Network Camera offers two choices of video compression standards for real-time viewing: MPEG-4 and MJPEG.
If MPEG-4 is selected, it is streamed in RTSP protocol. There are four dependent parameters provided in MPEG-4 mode for video performance adjustment.

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 352 x 240 and 720 x 480.

■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 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 the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps and 30fps.

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

■ Video quality
A complex scene generally produces 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 performances. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps and 4Mbps.

On the other hand, if Fixed quality is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and Excellent.

If JPEG mode is selected, the Network Camera continuously sends JPEG images to the clients, producing dynamic effects similar to movies. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. And because the media contents are a combination of JPEG images, no audio data is transmitted to the clients.

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are
selectable in the following resolutions: 176 x 144, 352 x 240 and 720 x 480.

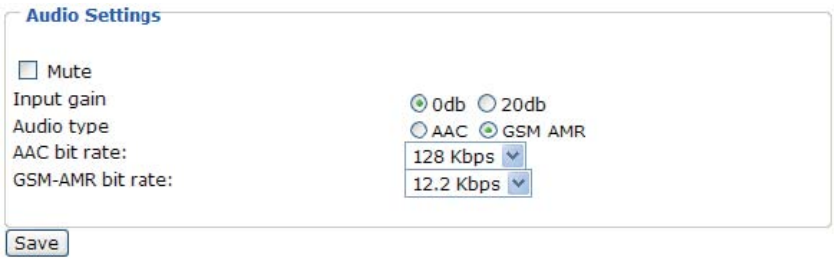
■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video
quality.

If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 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 the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps and 30fps.

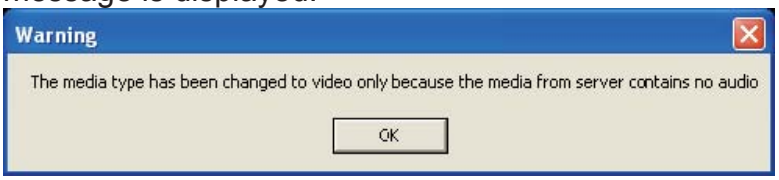
■ Video quality
```The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and ```Excellent.

Disable IR LED:
If you don't want to let others know that the network camera is on, you can select this option to turn off the LED illuminators. This will prevent the Network Camera's operation from being noticed.
```

Audio settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted to all clients even though the audio transmission is enabled in the Client Settings page. In that case, the following message is displayed.



Input gain: There are two options for external microphone input gain, 0db and 20db.

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.
■ AAC targets at performing good sound quality at the cost of higher bandwidth consumption. The bit
rates are selectable at the following rates: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps and128Kbps.

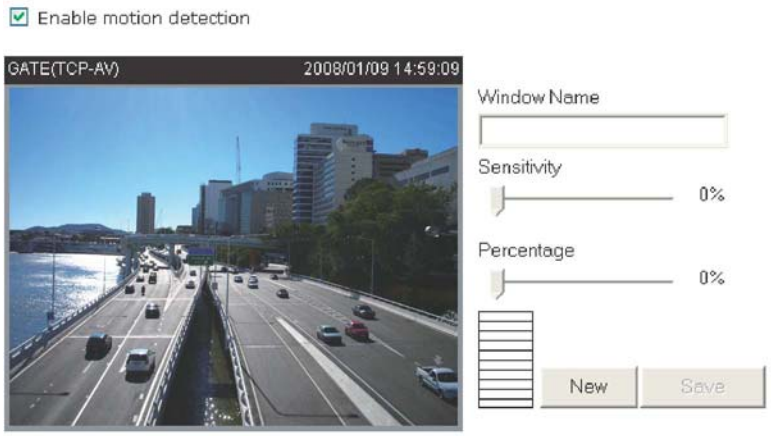
■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable at the following rates: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps and 12.2Kbps.

When completed with the settings on this page, click Save to take effect.

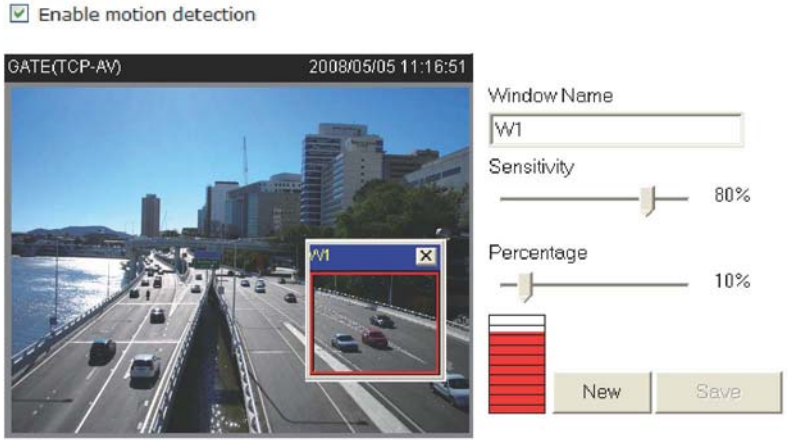
Motion detection

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

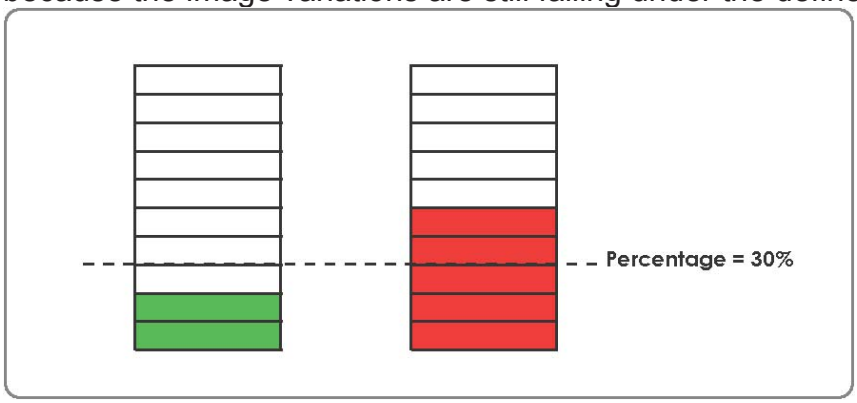
To enable motion detection, follow the steps below:
1. Click New to add a new motion detection window.
2. In the Window Name text box, enter a descriptive name for the motion detection window.
   ■ To move and resize the window, drag-drop the window.
   ■ To delete window, click X at top right of the 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 take effect.
5. Select Enable motion detection to enable this function.



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

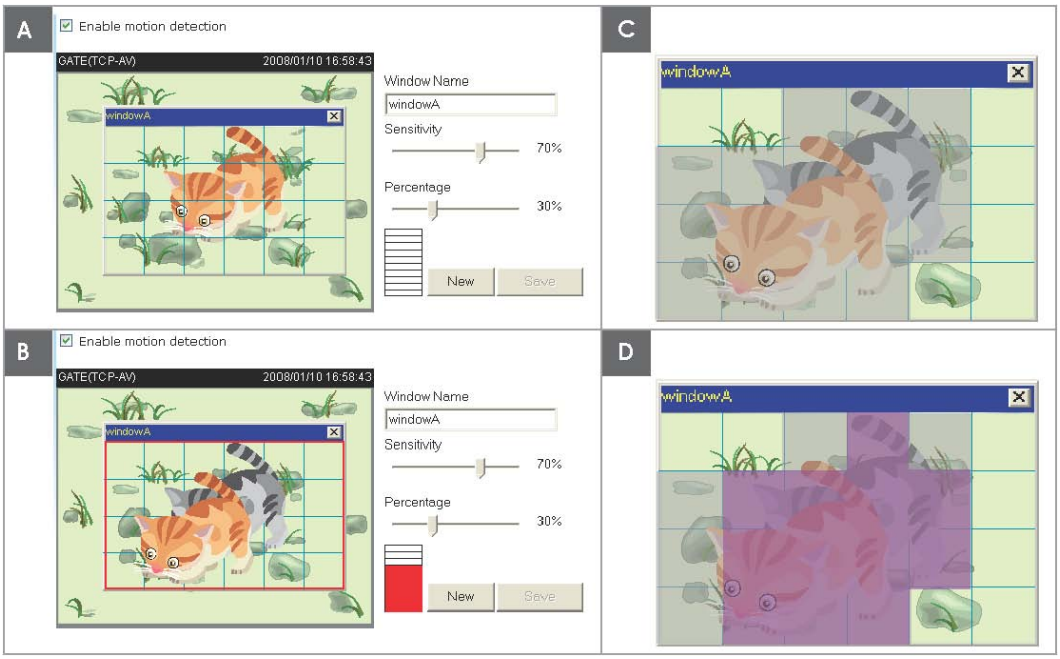


A green bar indicates that even though motions are detected, the event will not be triggered because the image variations are still falling under the defined threshold.



NOTE

► How does motion detection work?



There are two parameters for setting the motion detection: 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 sense a slight movement while smaller sensitivity settings tend to neglect it. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as “alerted pixels” (frame D).

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

For applications that require higher security management, it is suggested to set higher sensitivity settings and smaller percentage values.

Camera control

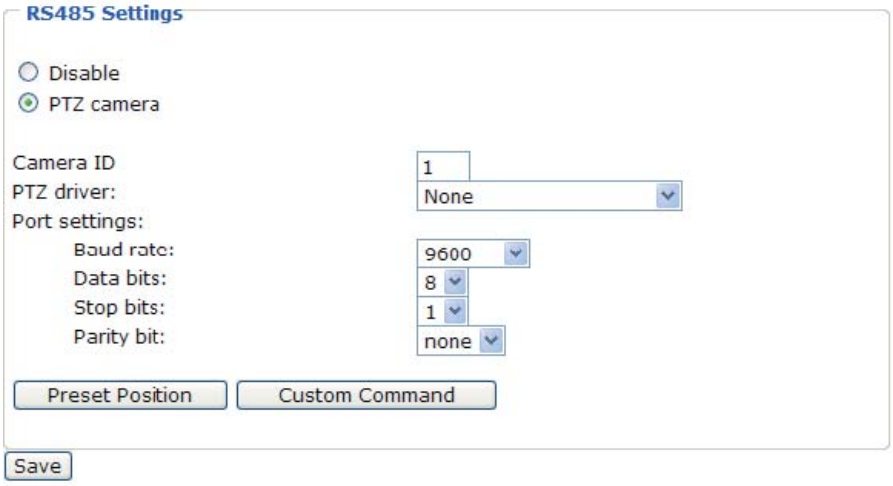
This section explains how to control the Network Camera’s Pan/Tilt/Zoom operation by connecting with a PTZ driver or scanner via RS485 interface.

RS485 Settings

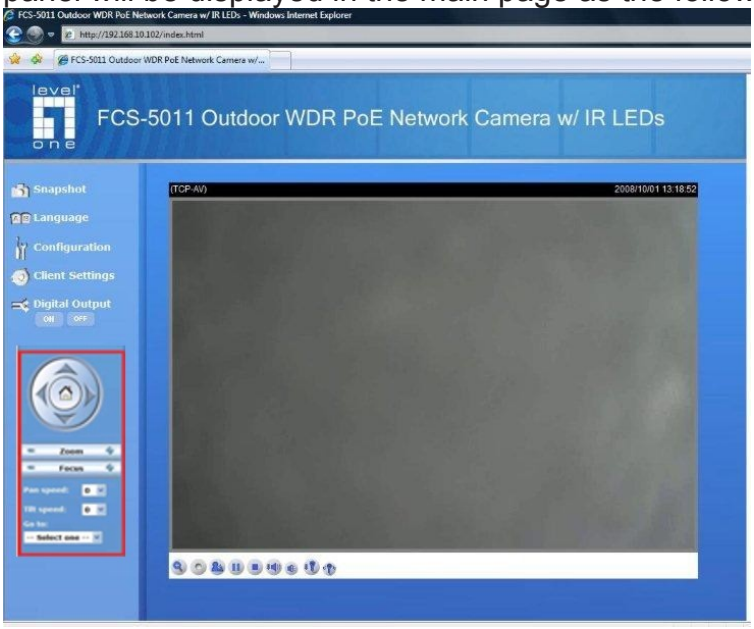
Disable: Select this option to disable this function.

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

the following diagram.



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 set the Camera ID, PTZ driver, and Port settings. The Camera ID is necessary for multiple cameras control. If you select PTZ camera and click Save to enable this function, the camera control panel will be displayed in the main page as the following diagram:



Preset Position

Click Preset Position to open the Preset Position page. In this page, you can set the preset position for the Network Camera. A total of 20 preset positions can be configured.

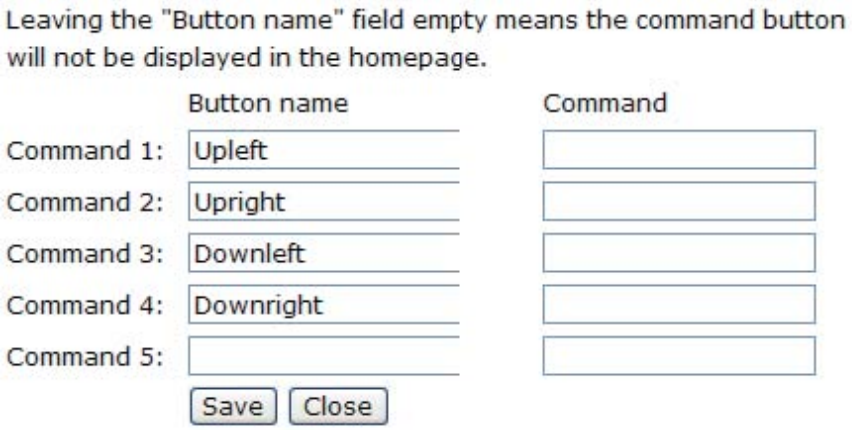
Follow the steps below to set preset positions:

1. Adjust the Network Camera to a desired position with the buttons on the right side of the window.
2. In the Preset position name text box, enter a descriptive name for the preset position. The preset position name allows up to forty characters. Click Add to take effect. The preset position name will appear in the Preset Positions drop-down list. To remove a preset position from the list, select a preset position name from the Preset Positions drop-down list and then click Delete.
3. You can click "Go to" to aim at preset positions, which will also displayed in the main page.
4. Click Save to take effect.

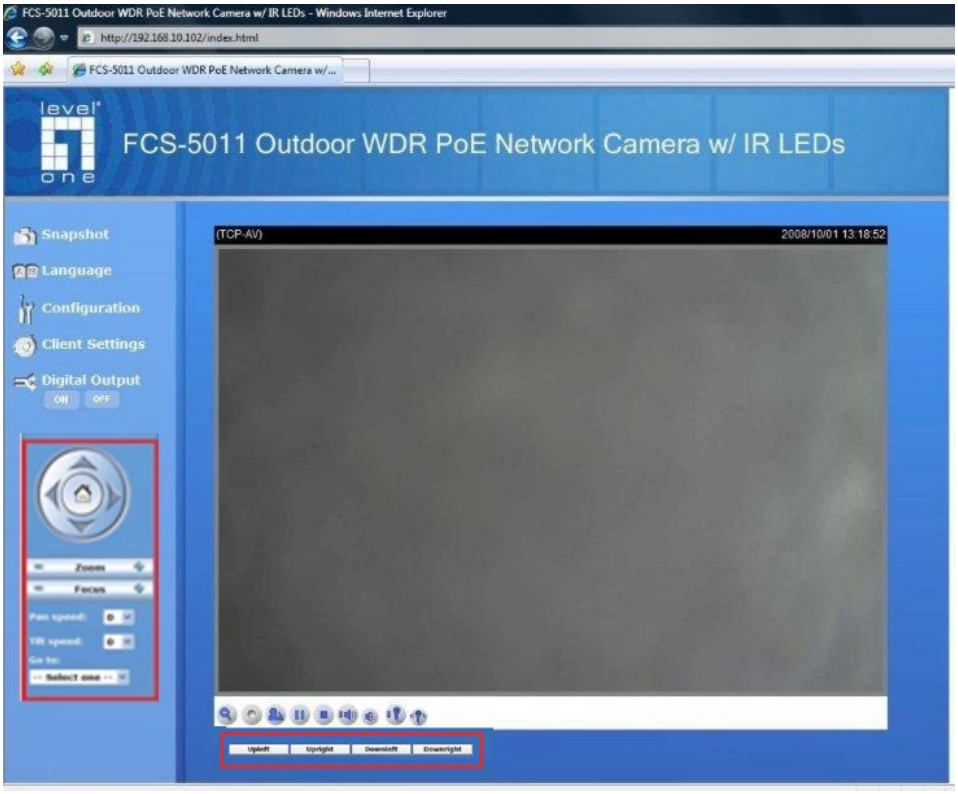
Custom Command

If the Custom camera (scanner) is selected as the PTZ driver, the PTZ control panel on the main page will not take effect. You need to **configure command buttons to control the PTZ scanner. Click Custom Command to open the Custom Command page. A total of five command buttons can be configured. Please refer to the user's manual of your PTZ scanner to enter the command in the following blanks.**

Click Save to enable the settings and click Close to quit the page.



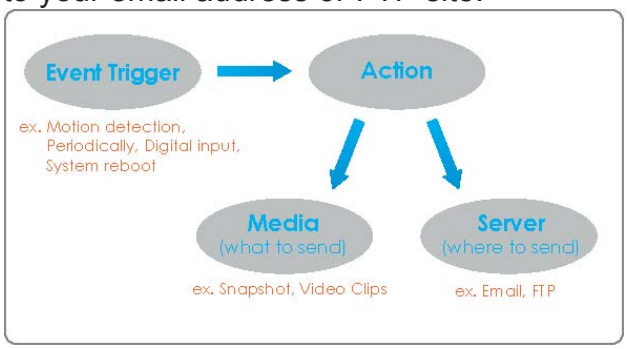
The command button will appear in the main page as the following diagram.



Application

This section explains how to configure the Network Camera to react in response to particular situations. A typical application is that when a motion is detected, the Network Camera sends buffered images to a FTP server or via e-mail as notifications.

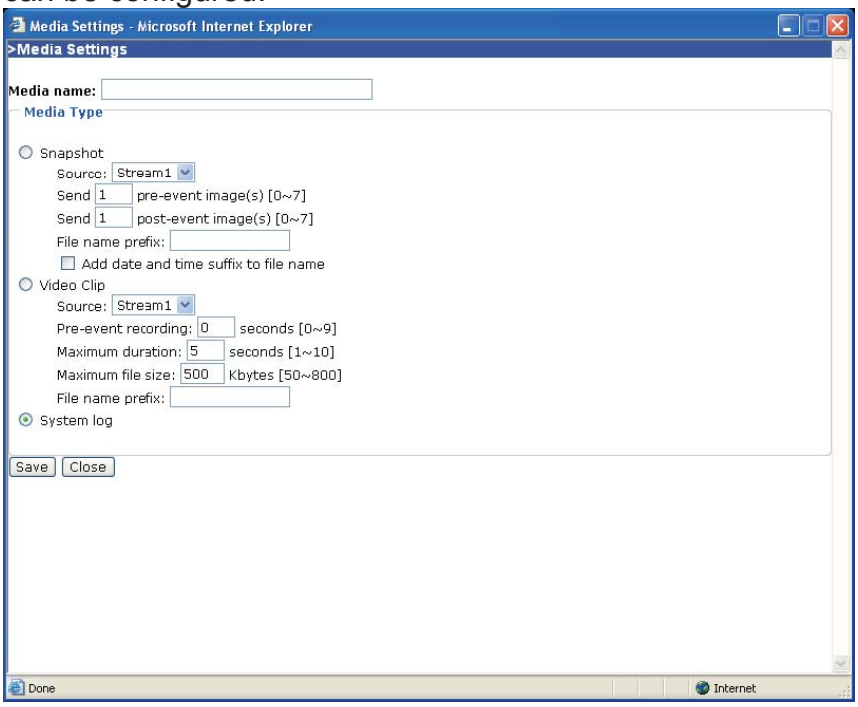
In the illustration below, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what kind of action will be performed. You can configure the Network Camera to send snapshots or videos to your email address or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



To start plotting an event, it is suggested to configure server and media columns first so that the Network Camera will know what action shall be performed when a trigger is activated.

Media Settings

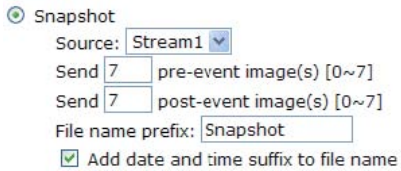
In Media Settings column, click Add to open the media setting page. In this page, you can specify what kind of media to send when a trigger is activated. A total of five media settings can be configured.



Media name: Enter a descriptive name for the media setting.

Media Type: There are three choices of media types available: Snapshot, Video Clip, and System log.

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

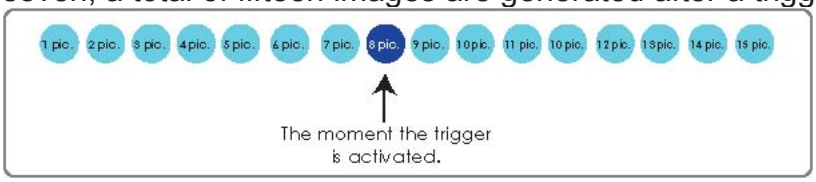


■ Source: Select to take snapshots from stream 1 or stream 2.

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

■ Send ☐ post-event images
Specify to capture how many images after a trigger is activated. Up to seven images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to seven, a total of fifteen images are generated after a trigger is activated.

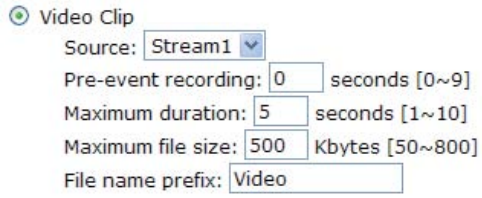


■ File Name Prefix
Enter the text that will be put in front of the file name.

■ Add date and time suffix to the file name
Select this option to add date and time to the file name suffix.

For example:

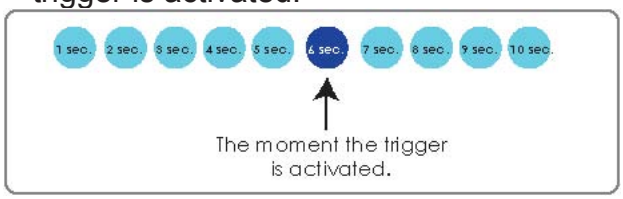
Video Clip: Select to send video clips when a trigger is activated.



■ Source: Select to record video clips from stream 1 or stream 2.

■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to record video clips for how many seconds before a trigger is activated. Up to nine seconds can be set.

■ Maximum duration
Specify the maximal recording duration in seconds. Up to ten seconds can be set.
For example, if the Pre-event recording is set to five seconds and the Maximum duration is set to ten seconds, the Network Camera continues to record for another four seconds after a trigger is activated.



■ Maximum file size
Specify the maximal file size allowed.

■ File Name Prefix
Enter the text that will be put in front of the file name.

For example:

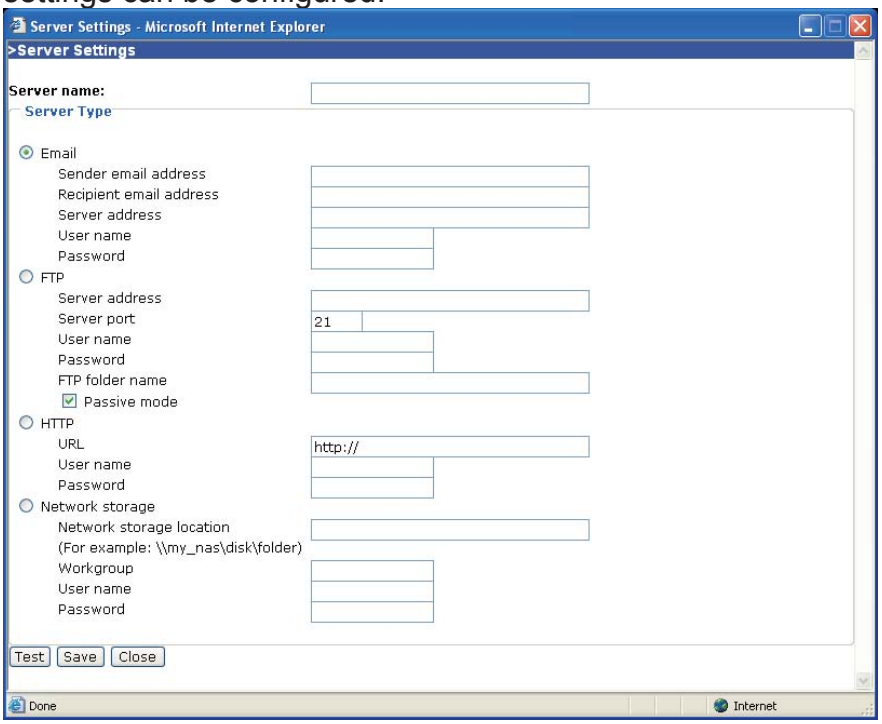
System log: Select to send a system log when a trigger is activated.

When completed, click Save to take effect and then click Close to quit this page. The new

media name will appear in the media drop-down list on the Application page as below. To remove a media setting from the list, select a media name from the drop-down list and then click Delete. Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

In the Server column, click Add to open the server setting page. In this page, you can specify where the notification messages will be send when a trigger is activated. A total of five server settings can be configured.



Server name: Enter a descriptive name for the server setting.

Server Type: There are four choices of server types available: Email, FTP, HTTP, and Network storage.

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

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

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

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

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

■ Password: Enter the password of the email account.

To verify if the email settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive an email indicating the result.

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

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

■ Server port
By default, the FTP port server is set to 21. Also, it can be assigned with 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.

■ Remote folder name
Enter a folder to place the media file. If the folder name does not exist, the Network Camera will create one on the FTP server.

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

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

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

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name.

■ Password: Enter the password.

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

Network storage: Select to send the media to a Network storage when a trigger is activated.

■ Network storage location: Enter the path of the network storage.

■ Workgroup: Enter the workgroup for network storage.

■ User name: Enter the user name.

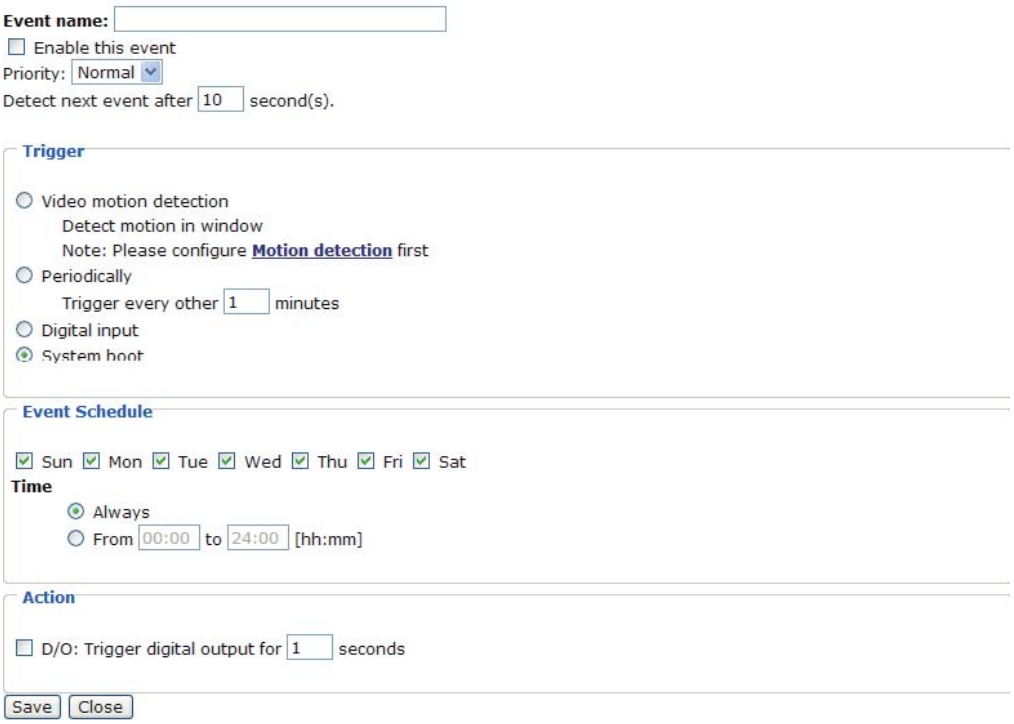
■ Password: Enter the password.

To verify if the network storage settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the network storage server.

When completed, click Save to take effect and then click Close to quit this page. The new server name will appear in the server drop-down list on the application page as below. To remove a server setting from the list, select a server name from the drop-down list and then click Delete. Note that only when the server setting is not being applied to an event setting can it be deleted.

Event Settings

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



Event name: Enter a descriptive name for the event setting.

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

Priority: Select the relative importance of this event (High, Normal, and Low). Events with 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 user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger: Also referred as the cause or stimulus, defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.There are four choices of trigger sources:

■ Video motion detection
Select this option to allow the Network Camera to use the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure Motion detection first. For more information, please refer to Motion detection section for details.

■ Periodically
Select this option to allow the Network Camera to trigger periodically for every other defined minute. At most 999 minutes can be set.

■ Digital input
Select one of the Digital inputs to allow the Network Camera to use external digital input device as a trigger source. Depending on your applications, there are choices of digital input

devices on the market which helps to sense any changes in temperature, vibration, sound and light, etc.

■ System boot
Select this option to allow the Network Camera to trigger when the power of Network Camera is disconnected.

Event Schedule: The effective period in which the event stays active. Specify the effective period for the event.

■ Select the days on weekly basis.

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

Action: Also referred as the effect, defines the action to be performed by the Network Camera when the trigger is activated. Select the action to perfom when a trigger is activated.

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

■ Server name / Media name
Select the server and media name to allow the Network Camera to send the media files to the server when a trigger is activated.

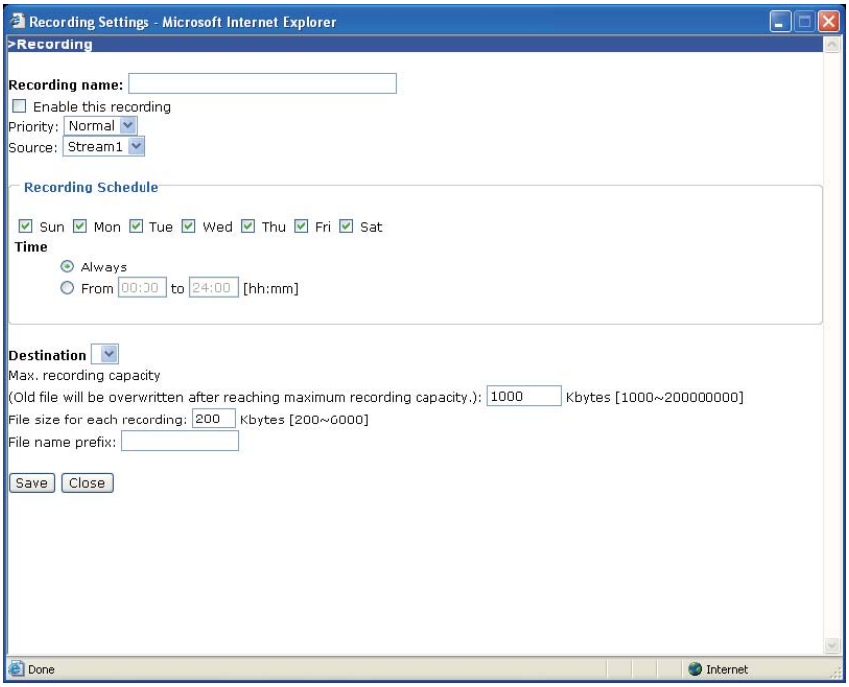
When completed, select Enable this event. Click Save to take effect and then click Close to quit this page. The new event name will appear in the event drop-down list on the application page. To remove an event setting from the list, select an event name from the drop-down list and then click Delete.

Recording

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

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 two recording settings can be configured.



Recording name: Enter a descriptive name for the recording setting.

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

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

Source: Select the recording source (stream 1 or stream 2).

Recording Schedule: Specify the recording duration.

■ Select the days on weekly basis.

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

Destination: Specify a storage destination for the recorded video files. Note that the destination field is empty by default. Please go to Configuration > Application > Server Settings to set a Network storage server; please refer to Server Settings section.

Max. recording capacity: Please note that when the maximum capacity is reached, the oldest

file will be overwritten by the latest one.

File size for each recording: Specify the file size for each recording media.

File name prefix: Enter the text that will be put in front of the file name.

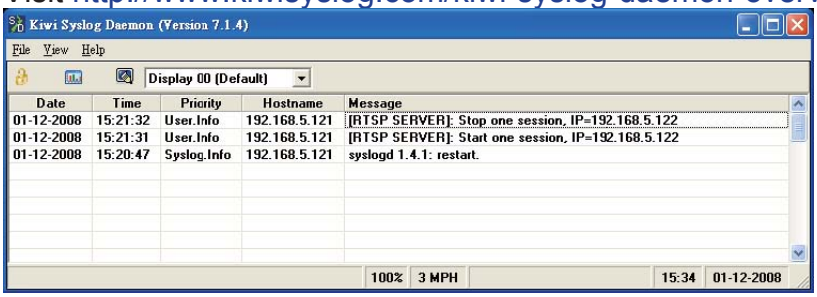
When completed, select Enable this recording. Click Save to take effect and then click Close to quit this page. The new recording name will appear in the recording drop-down list on the recording page. To remove a recording setting from the list, select a recording name from the drop-down list then and click Delete.

System log

This section explains how to configure the Network Camera to send system log to remote server as a backup. It is composed of the following two columns: Remote Log and Current Log.

Remote Log

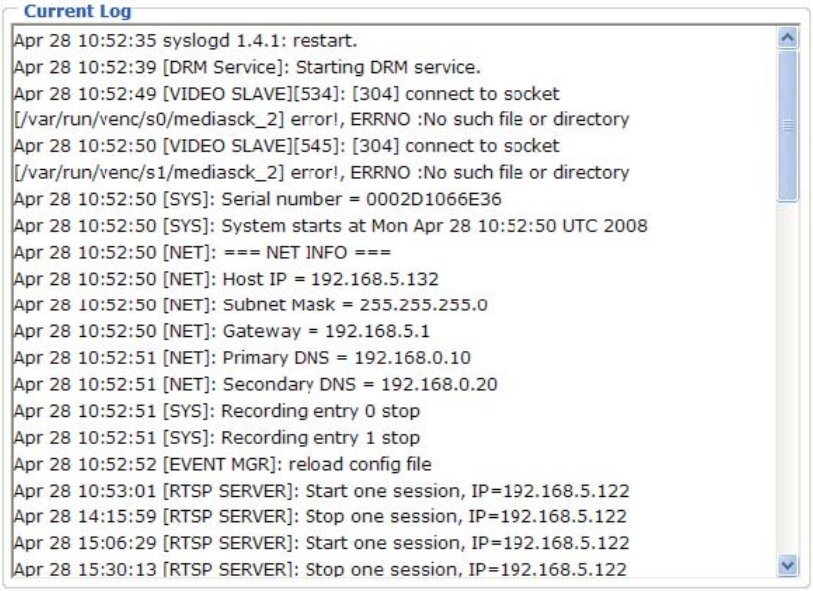
You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested to install a log-recording tool to receive system log messages from the Network Camera. For example, a tool -- Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



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 take effect.

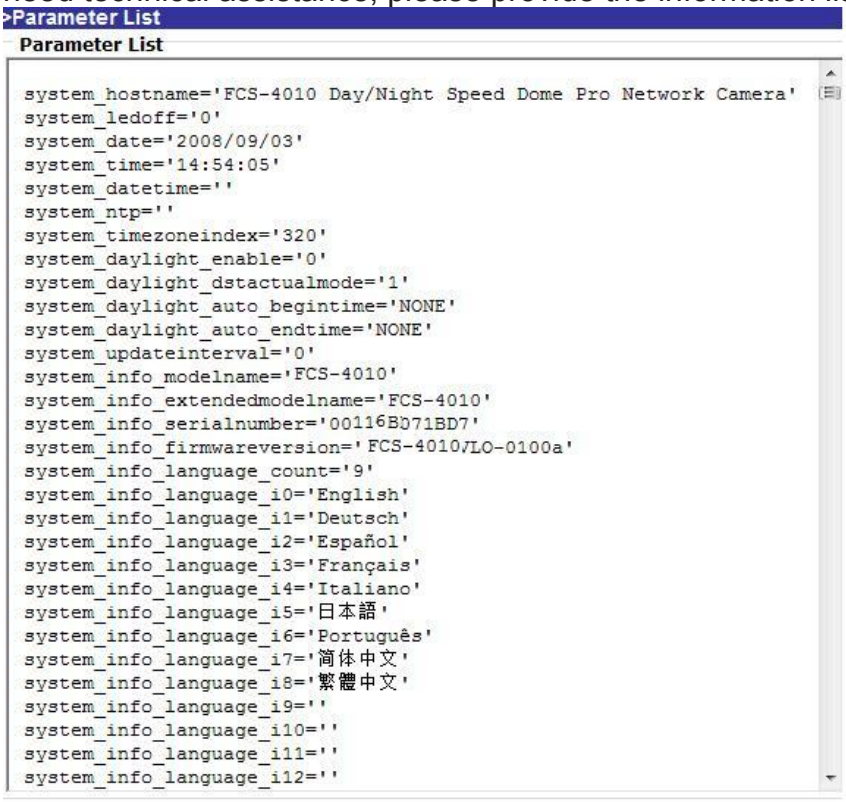
Current Log

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



View parameters

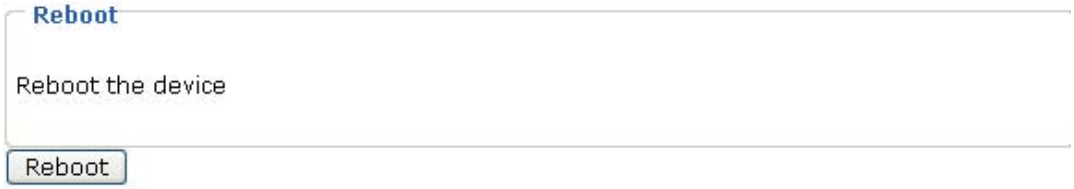
The View parameters page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed in this page.



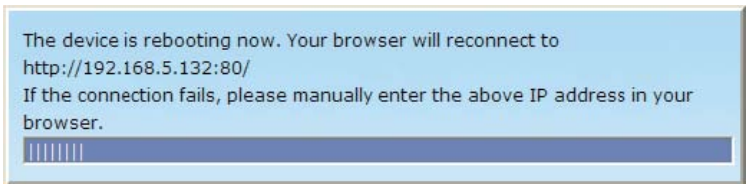
Maintenance

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

Reboot



This feature allows you to turn off and then turn on the Network Camera. It takes about one ~ two minutes to complete the process. When completed, the live video will be displayed in your browser. The following message is displayed during the rebooting process.



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

Restore

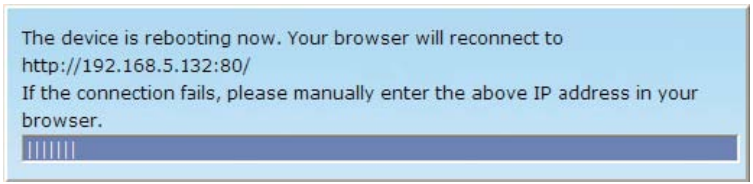
This feature allows you to restore the Network Camera to factory default. Two settings can be excluded:

Network Type: Select this option to retain the Network Type settings (please refer to Network Type section).

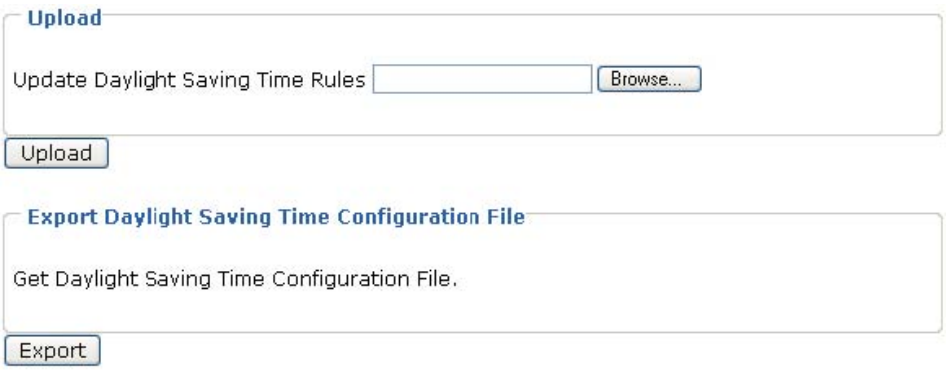
Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to System section)

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

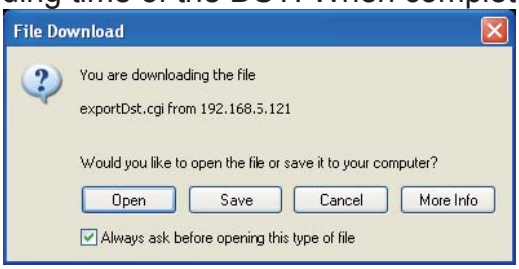
The following message is displayed during the restoring process.



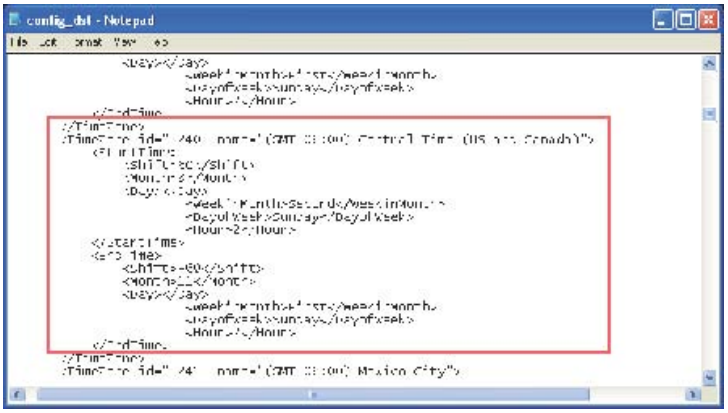
Upload / Export Daylight Saving Time Configuration File



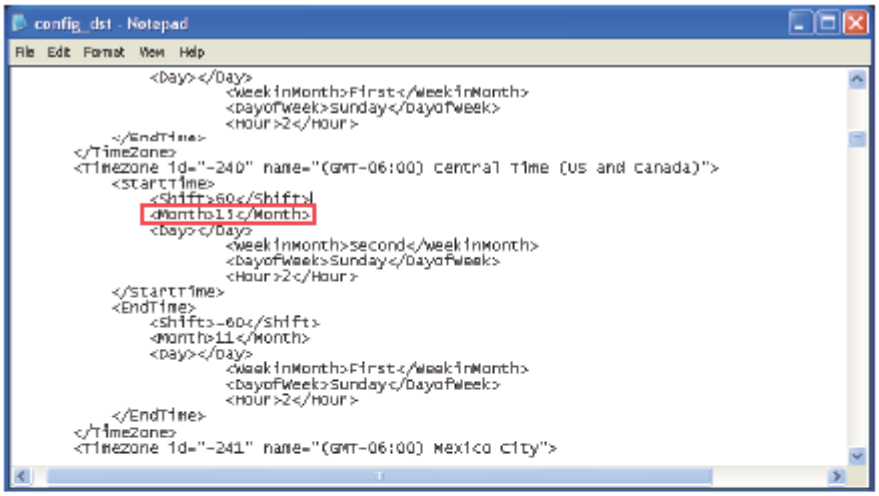
This feature allows you to set the starting time and ending time of DST.
Follow the steps below to set up:
1. In the Export Daylight Saving Time Configuration File Column, click Export to export an Extensible Markup Language (*.xml) file from the Network Camera.
2. Open the XML file using Microsoft® Notepad and locate your time zone; set the starting time and
ending time of the DST. When completed, save the file.



In the example below, the 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.



3. In the Upload Column, click Browse… and specify the XML file.
If the incorrect date and time is assigned, you will see the following warning message when uploading the file to the Network Camera.



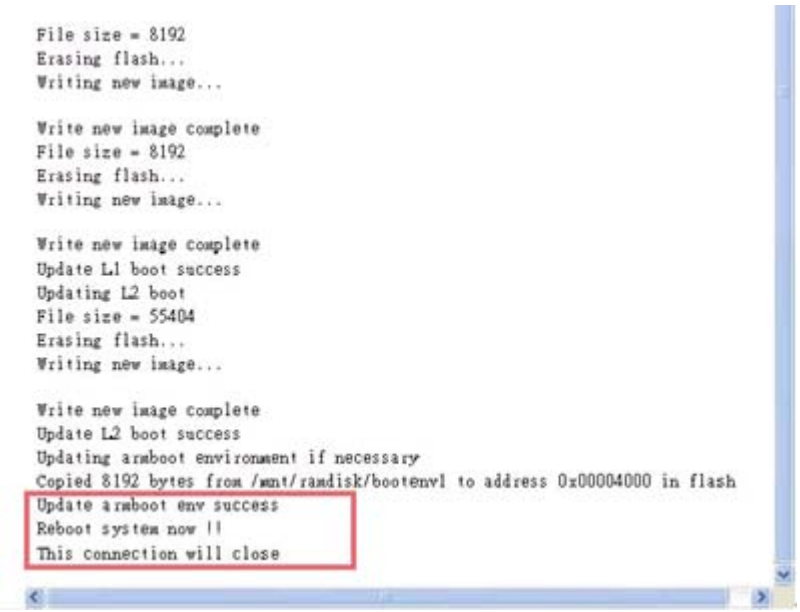
4. Click Upload. To enable the DST, see System Time section.
   The following message is displayed when attempting to upload an incorrect file format.

Upgrade Firmware

This feature allows you to upgrade the firmware on your Network Camera. It takes about five minutes to complete the process.
Note that do not power off the Network Camera during the upgrade.

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

The upgrade is successful as you see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.
The following message is displayed when the upgrade is succeeded.



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.
It will takes about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

Appendix

URL Commands of the Network Camera

Overview

For some customers who already have their own web site or web control application, Network Camera/Video server can be easily integrated through convenient URLs. This section specifies the external HTTP based application programming interface. The HTTP based camera interface provides the functionality to request a single image, to control camera functions (PTZ, output relay etc.) and to 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, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall 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, also below.

URL syntax' are written with the "**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This 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 returned as HTTP formatted, i.e., starting with the string HTTP is line 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, the internal parameters must be written exactly as they are

named in the camera or video server. The CGIs are organized in function related directories under the cgi-bin directory. The file extension of the CGI is required.

Syntax:

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

Example: Setting 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 dido, ptz of camera
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator's access right can modify most of camera's parameters except some privilege and network options
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator's access right can fully control the camera's operation.
7	N/A	Internal parameters. Unable to be changed by any external interface.

Get server parameter values

Note: 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 the any parameters, all the parameters on the server will be returned. If you specify only <group>, the parameters of related group will be returned.

When query parameter values, the current parameter value are returned.

Successful control request returns parameter pairs as follows.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-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 it's 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
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

Set server parameter values

Note: 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 actually update all fields (no need to use 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 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 LEVELONE server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-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 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

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-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 string shorter than ‘n’ characters. The characters “,’, <,>,& are invalid.
password[<n>]	The same as string but display ‘*’ instead
integer	Any number between (-2_{31} – 1) and (2_{31} – 1)
positive integer	Any number between 0 and (2_{32} – 1)
<m> ~ <n>	Any number between ‘m’ and ‘n’
domain name[<n>]	A string limited to contain a domain name shorter than ‘n’ characters (eg. www.ibm.com)
email address [<n>]	A string limited to contain a email address shorter than ‘n’ characters (eg. joe@www.ibm.com)
ip address	A string limited to contain an ip address (eg. 192.168.1.1)
mac address	A string limited to contain mac address without hyphen or colon connected
boolean	A boolean value 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 <>	As description

Note: The Network Camera should prevent to restart when parameter changed.

Group: **system**

Name	Value	Security (get/set)	Description
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to ‘keep’ keeping date unchanged. Set to ‘auto’ to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current date of system. Set to ‘keep’ keeping date unchanged. Set to ‘auto’ to use NTP to synchronize time.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server *Do not use “skip to invoke default server” for default

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 -160: GMT-04:00 Atlantic Time, Canada, Caracas, 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 Time:Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa

daylight_enable	<boolean>	6/6	Enable automatic daylight saving to time zone
daylight_dstactualmode	<boolean>	6/7	Check if current time is under daylight saving time.
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving begin time.
daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end time.
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.

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

Name	Value	Security (get/set)	Description
modelname	string[40]	0/7	Model name of server
serialnumber	<mac address>	0/7	12 characters mac address without hyphen connected
firmwareversion	string[40]	0/7	The version of firmware, including model, company, and version number in the format.
language_count	<integer>	0/7	Number of webpage language available on the server
language_i <0~(count-1)>	string[16]	0/7	Available language lists

Group: **status**

Name	Value	Security (get/set)	Description
videoinactualcolor	<boolean>	1/4	0 => actual color 1 => not actual color
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	Current RTSP connection numbers
onlinenum_ httppush	integer	6/7	Current HTTP push server connection numbers

Group: **di_i<0~(ndi-1)>**

Name	Value	Security (get/set)	Description
normalstate	high, low	1/1	Indicate whether open circuit or closed circuit represents inactive status

Group: **do_i<0~(ndo-1)>**

Name	Value	Security (get/set)	Description
normalstate	open, grounded	1/1	Indicate whether open circuit or closed circuit represents inactive status

Group: **security**

Name	Value	Security (get/set)	Description
user_i0_name	string[64]	6/7	User’s name of root

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

Group: **network**

Name	Value	Security (get/set)	Description
type	lan, pppoe	6/6	Network connection type
resetip	<boolean>	6/6	1 => get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot 0 => use preset ipaddress, subnet, rounter, 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: 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	Alternative HTTP port
authmode	basic, digest	1/6	HTTP authentication mode
s0_accessname	string[32]	1/6	Http server push access name for stream 1
s1_accessname	string[32]	1/6	Http server push access name for stream 2

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	6/6	RTSP port
authmode	disable, basic, digest	1/6	RTSP authentication mode
s0_accessname	string[32]	1/6	RTSP access name for stream 1
s1_accessname	string[32]	1/6	RTSP access name for stream 2
s0_audiotrack	<integer>	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of **rtsp_s<0~(n-1)>: multicast**, n is stream count

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
ttl	1 ~ 255	4/4	Mutlicast time to live value

Subgroup of **network: sip**

Name	Value	Security (get/set)	Description
port	5060, 1025 ~ 65535	6/6	SIP port

Subgroup of **network: rtp**

Name	Value	Security (get/set)	Description
videoport	1025 ~ 65535	6/6	Video channel port for RTP
audioport	1025 ~ 65535	6/6	Audio channel port for RTP

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
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IP address for RTSP connection
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IP address for RTSP connection
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IP address for RTSP connection
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IP address for RTSP connection

Group: **videoin**

Name	Value	Security (get/set)	Description
cmosfreq	50, 60	4/4	CMOS frequency
whitebalance	auto, keep current value	4/4	auto => auto white balance keep current value => keep current value fluorescent => 5500K outdoor => > 5500K
atwbvalue1	0 ~ 9999999999	4/4	The auto white balance value 1.
atwbvalue2	0 ~ 9999999999	4/4	The auto white balance value 2.
exposurelevel	1~8	4/4	exposure level
enablewdr	<boolean>	4/4	Enable wide dynamic range
agc	0~2	4/4	Set auto gain control
daynight	auto, schedule, on, off	4/4	set IR cut filter mode
bwlowluxmode	<boolean>	4/4	Turn on or off black/white video in low lux mode

Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number

Name	Value	Security (get/set)	Description
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	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support Network Camera control function. 0(not support), 1(support) Bit 1 => **Build-in** or **external** Network Camera. 0(external), 1(build-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]	4/4	Enclosed caption
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video
maxexposure	1~120	4/4	Maximum exposure time
s<0~(m-1)>_codectype	mpeg4, mjpeg	4/4	Video codec type mpeg4 => MPEG-4 mjpeg => JPEG
s<0~(m-1)>_ resolution	176x144, 352x240, 720x480	4/4	Video resolution in pixel 176x144 => 176x144 352x240 => 352x240 720x480 => 720x480
s<0~(m-1)>_ mpeg4_ intraperiod	250, 500, 1000, 2000, 3000, 4000,	4/4	The period of intra frame in milliseconds 250 => 1/4 S 500 => 1/2 S 1000 =>1 S 2000 => 2 S 3000 => 3 S 4000 => 4 S
s<0~(m-1)>_mpeg4_ ratecontrolmode	cbr, vbr	4/4	cbr => constant bitrate vbr => fix quality
s<0~(m-1)>_ mpeg4_quant	1, 2, 3, 4, 5	4/4	Quality of video when choosing vbr in “ratecontrolmode”. 1 is worst quality and 5 is the best quality. 1 => medium 2 => standard 3 => good 4 => detailed 5 => excellent
s<0~(m-1)>_ mpeg4_bitrate	20000, 30000, 40000, 50000, 64000, 128000, 256000, 384000, 512000, 768000, 1000000, 1200000, 1500000, 2000000, 3000000, 4000000	4/4	Set bit rate in bps when choose cbr in “ratecontrolmode”. 20000 => 20 Kbps 30000 => 30 Kbps 40000 => 40 Kbps 50000 => 50 Kbps 64000 => 64 Kbps 128000 => 128 Kbps 256000 => 256 Kbps 512000 => 512 Kbps 768000 => 768 Kbps 1000000 => 1 Mbps 1500000 => 1.5 Mbps 2000000 => 2 Mbps 3000000 => 3 Mbps 4000000 => 4 Mbps

s<0~(m-1)>_ mpeg4_ maxframe	1, 2, 3, 5, 10, 15, 20, 25, 30 (only for 60Hz)	4/4	Set maximum frame rate in fps (for MPEG-4). 1 => 1 fps 2 => 2 fps 3 => 3 fps 5 => 5 fps 8 => 8 fps 10 => 10 fps 15 => 15 fps 20 => 20 fps 25 => 25 fps 30 => 30 fps (only for 60Hz)
s<0~(m-1)>_ mjpeg_quant	1, 2, 3, 4, 5	4/4	Quality of jpeg video. 1 is worst quality and 5 is the best quality. 1 => medium 2 => standard 3 => good 4 => detailed 5 => excellent
s<0~(m-1)>_ mjpeg_ maxframe	1, 2, 3, 5, 10, 15, 20, 25, 30 (only for 60Hz)	4/4	Set maximum frame rate in fps (for JPEG). 1 => 1 fps 2 => 2 fps 3 => 3 fps 5 => 5 fps 8 => 8 fps 10 => 10 fps 15 => 15 fps 20 => 20 fps 25 => 25 fps 30 => 30 fps (only for 60Hz)

Group: **audioin_c<0~ (n-1)>** for n channel products

Name	Value	Security (get/set)	Description
source	micin, linein	4/4	micin => use external microphone input linein => use line input, i.e. internal microphone
mute	0, 1	4/4	Enable audio mute 0 => Disable 1 => Enable

gain	0~31	4/4	Gain of input 31 => +12 dB 30 => +10.5 dB 29 => +9 dB 28 => +7.5 dB 27 => +6 dB 26 => +4.5 dB 25 => +3 dB 24 => +1.5 dB 23 => 0 dB 22 => -1.5 dB 21 => -3 dB 20 => -4.5 dB 19 => -6 dB 18 => -7.5 dB 17 => -9 dB 16 => -10.5 dB 15 => -12 dB 14 => -13.5 dB 13 => -15 dB 12 => -16.5 dB 11 => -18 dB 10 => -19.5 dB 9 => -21 dB 8 => -22.5 dB 7 => -24 dB 6 => -25.5 dB 5 => -27 dB 4 => -28.5 dB 3 => -30 dB 2 => -31.5 dB 1 => >-33 dB 0 => -34.5 dB
s<0~(m-1)>_ codectype	aac4, gamr	4/4	Set audio codec type for input aac4 => AAC gamr => GSM-AMR
s<0~(m-1)>_ aac4_bitrate	16000, 32000, 48000, 64000, 96000 128000	4/4	Set AAC4 bitrate in bps 16000 => 16 Kbps 32000 => 32 Kbps 48000 => 48 Kbps 64000 => 64 Kbps 96000 => 96 Kbps 128000 => 128 Kbps
s<0~(m-1)>_ gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	Set AMR bitrate in bps 4750 => 4.75 Kbps 5150 => 5.15 Kbps 5900 => 5.90 Kbps 6700 => 6.7 Kbps 7400 => 7.4 Kbps 7950 => 7.95 Kbps 10200 => 10.2 Kbps 12200 => 12.2 Kbps

Group: **image_c<0~(n-1)>** for n channel products

Name	Value	Security (get/set)	Description
brightness	-5 ~ 5	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.
hue	-5 ~ 5	4/4	Adjust hue of image according to mode settings.

Group: **imagepreview_c<0~(n-1)>** for n channel products

Name	Value	Security (get/set)	Description
brightness	-5 ~ 5	4/4	Preview of adjusting brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Preview of adjusting saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Preview of adjusting contrast of image according to mode settings.
hue	-5 ~ 5	4/4	Preview of adjusting hue of image according to mode settings.
videoin_whitebalance	auto, manual	4/4	Preview of adjusting white balance of image according to mode settings.
videoin_restoreatwb	Positive integer	4/4	Restore auto white balance.

Group: **motion_c<0~(n-1)>** for 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: **ddns**

Name	Value	Security (get/set)	Description
enable	<boolean>	6/6	Enable or disable the dynamic dns.

provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree, CustomSafe100	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree =>dyn-interfree.it CustomSafe100 =>Custom server using safe100 method
<provider>_ hostname	string[128]	6/6	Your dynamic hostname.
<provider>_ usernameemail	string[64]	6/6	Your user or email to login ddns service provider
<provider>_ passwordkey	string[64]	6/6	Your password or key to login ddns service provider
<provider>_ servername	string[128]	6/6	The server name for safe100. (This field only exists for provider is customsafe100)

Group: **upnppresentation**

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 IGD router 3 => no need to do 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	The levels to distinguish the importance of 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

Name	Value	Security (get/set)	Description
panspeed	-5 ~ 5	1/4	Pan speed -5 ~ 5
tiltspeed	-5 ~ 5	1/4	Tilt speed -5 ~ 5
zoomspeed	-5 ~ 5	1/4	Zoom speed -3 ~ +3
autospeed	1 ~ 5	1/4	Auto pan/patrol speed 1 ~ 5
focusspeed	-5 ~ 5	1/4	Auto focus speed
dwelling	0 ~ 9999	1/4	Time to dwelling when patrol
axisx	-8250~ 8250	1/4	Axis X coordinate, used internally
axisy	-560 ~ 1664	1/4	Axis Y coordinate, used internally
pantilt_port	<integer>	1/4	The pan and tilt channel.
pantilt_camid	0 ~ 255	1/4	ID of camera on pan/tilt channel.
zoom_port	<integer>	1/4	The zoom channel.
zoom_camid	0 ~ 255	1/4	ID of camera on zoom channel.
preset_i<0~19>_name	string[40]	1/4	The name of preset location.
preset_i<0~19>_dwelling	0 ~ 255	1/4	The dwelling time of each preset location
uart	0 ~ (m-1), m is uart count	1/4	Select correspond uart
cameraid	0~255	1/4	Camera ID to control external PTZ cameral
isptz	<boolean>	1/7	To distinguish the video channel if mapping to a PTZ camera
disablemdonptz	<boolean>	1/4	Disable motion detection on PTZ operation

Group: **uart**

Name	Value	Security (get/set)	Description
ptzdrivers_i<0~19, 127>_name	string[40]	1/4	The name of the PTZ driver.
ptzdrivers_i<0~19, 127>_location	string[128]	1/4	The full path of the PTZ driver.
enablehttptunnel	<boolean>	4/4	Enable HTTP tunnel channel to control UART.

Group: **uart_i<0~(n-1)> n is uart port count**

Name	Value	Security (get/set)	Description
baudrate	110 300 600 1200 2400 3600 4800 7200 9600 19200 38400 57600 115200	4/4	Set baud rate of COM port 110 => 110 300 => 300 600 => 600 1200 => 1200 2400 => 2400 3600 => 3600 4800 => 4800 7200 => 7200 9600 => 9600 19200 => 19200 38400 => 38400 57600 => 57600 115200 => 115200
databit	5 6 7 8	4/4	Data bits in a character frame 5 => 5 6 => 6 7 => 7 8 => 8
paritybit	none odd even	4/4	For error checking none => none odd => odd even => eve
stopbit	1 2	4/4	1 => 1 2 => 2
uartmode	rs485 rs232	4/4	rs485 or rs232
uartreset	<boolean>	4/4	Set this flag to true to apply change of UART configuration.
customdrvcmd_i<0~9>	string[128]	1/4	PTZ command for custom camera.
speedlink_i<0~4>_name	string[40]	1/4	Additional PTZ command name
speedlink_i<0~4>_cmd	string[128]	1/4	Additional PTZ command list
ptzdriver	0~19 127 (custom) 128 (no driver)	4/4	Which PTZ driver is used by this COM port

Group: **privacymask_c<0~(n-1)**> for n channel product

Name	Value	Security (get/set)	Description
enable	<boolean>	4/4	Enable the privacy mask
win_i<0~4>_enable	<boolean>	4/4	Enable the privacy mask window
win_i<0~4>_name	string[14]	4/4	The name of 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_http_version	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	The server bootup time
nir	0, <positive integer>	0/7	Number of IR interface
ndi	0, <positive integer>	0/7	Number of digital input
ndo	0, <positive integer>	0/7	Number of digital output
naudioin	0, <positive integer>	0/7	Number of audio input
naudioout	0, <positive integer>	0/7	Number of audio output
nvideoin	<positive integer>	0/7	Number of video input
nmediastream	<positive integer>	0/7	Number of media stream per channel
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 interface
ptzenabled	<positive integer>	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support Network Camera control function 0(not support), 1(support) Bit 1 => Build-in or external Network Camera. 0(external), 1(build-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)
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_ maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections
protocol_ rtp_multicast_ scalable	<boolean>	0/7	Indicate whether to support scalable multicast
protocol_ rtp_multicast_ scalable	<boolean>	0/7	Indicate whether to support scalable multicast
protocol_rtp_multicast_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_ mjpeg	<boolean>	0/7	Indicate whether to support server push motion jpeg
protocol_snmp	<boolean>	0/7	Indicate whether to support snmp
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_ resolution	<a list of the available resolution separates by comma>	0/7	Available resolutions list
videoin_codec	<a list of the available codec types separaters by comma>	0/7	Available codec list
videoout_codec	<a list of the available codec types separaters by comma>	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_ headphoneout	<boolean>	0/7	Indicate whether to support headphone output

audioin_codec	<a list of the available codec types separaters by comma>	0/7	Available codec list
audioout_codec	<a list of the available codec types separaters by comma>	0/7	Available codec list
uart_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for uart transfer
transmission_ mode	Tx, Rx	0/7	Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box
network_wire	<boolean>	0/7	Indicate whether to support the Ethernet
network_wireless	<boolean>	0/7	Indicate whether to support the wireless
wireless_ 802dot11b	<boolean>	0/7	Indicate whether to support the wireless 802.11b+
wireless_ 802dot11g	<boolean>	0/7	Indicate whether to support the wireless 802.11g
wireless_ encrypt_wep	<boolean>	0/7	Indicate whether to support the wireless WEP
wireless_ encrypt_wpa	<boolean>	0/7	Indicate whether to support the wireless WPA
wireless_encrypt _wpa2	<boolean>	0/7	Indicate whether to support the wireless WPA2

Group: **event_i<0~2>**

Name	Value	Security (get/set)	Description
name	string[40]	6/6	The identification of this entry
enable	0, 1	6/6	To enable or disable this event. 0 => Disable 1 => Enable
priority	0, 1, 2	6/6	Indicate the priority of this event. 0 => indicates low priority. 1 => indicates normal priority. 2 => indicates high priority.
delay	1~999	6/6	Delay seconds before detect next event.
trigger	boot, di, motion, seq	6/6	Indicate the trigger condition. boot => system boot. di => digital input. motion => video motion detection. seq => periodic condition. visignal => indicates video input signal loss.

di	<integer>	6/6	Indicate which di detected. 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 detected. This field is required when trigger condition is “md”. One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
inter	1~999	6/6	Interval of period snapshot in minute. This field is used when trigger condition is “seq”.
weekday	<interger>	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 weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00 ~ 24:00 means always.)
action_do_i<0~(ndo-1)>_enable	0, 1	6/6	To enable or disable trigger digital output. 0 => Disable 1 => Enable
action_do_i<0~(ndo1)>_duration	1~999	6/6	The duration of digital output is triggered in seconds.
action_server_i<0~4>_enable	0, 1	6/6	To enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	The index of attached media.

Group: **server_i<0~4>**

Name	Value	Security (get/set)	Description
name	string[40]	6/6	The 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	The url of http server to upload.
http_username	string[64]	6/6	The username to login in the server.
http_passwd	string[64]	6/6	The password of the user.
ftp_address	string[128]	6/6	The ftp server address
ftp_username	string[64]	6/6	The username to login in the server.

ftp_passwd	string[64]	6/6	The password of the user.
ftp_port	0~65535	6/6	The port to connect the server.
ftp_passive	0, 1	6/6	To enable or disable the passive mode. 0 => disable the passive mode. 1 => enable the passive mode.
ftp_location	string[128]	6/6	The location to upload or store the media.
email_address	string[128]	6/6	The email server address
email_username	string[64]	6/6	The username to login in the server.
email_passwd	string[64]	6/6	The password of the user.
email_ senderemail	string[128]	6/6	The email address of sender.
email_ recipientemail	string[128]	6/6	The email address of recipient.
ns_location	string[128]	6/6	The location to upload or store the media.
ns_username	string[64]	6/6	The username to login in the server.
ns_passwd	string[64]	6/6	The password of the user.
ns_workgroup	string[64]	6/6	The workgroup for network storage.

Group: **media_i<0~4>**

Name	Value	Security (get/set)	Description
name	string[40]	6/6	The identification of this entry
type	snapshot, systemlog, videoclip	6/6	The media type to send to the server or store by the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 => the first stream. 1 => the second stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_ datesuffix	0, 1	6/6	To add date and time suffix to filename or not. 1 => to add date and time suffix. 0 => not to add it.
snapshot_ preevent	0~7	6/6	It 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 => the first stream. 1 => the second stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_ preevent	0 ~ 9	6/6	It indicates the time of pre-event recording in seconds.
videoclip_ maxduration	1 ~ 10	6/6	The time of maximum duration of one video clip in seconds.
videoclip_ maxsize	50 ~ 1500	6/6	The maximum size of one video clip file in Kbytes.

Group: **recording_i<0~1>**

Name	Value	Security (get/set)	Description
name	string[40]	6/6	The identification of this entry

enable	0, 1	6/6	To enable or disable this recoding. 0 => Disable 1 => Enable
priority	0, 1, 2	6/6	Indicate the priority of this recoding. 0 => low priority. 1 => normal priority. 2 => high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 => the first stream. 1 => the second stream and etc.
weekday	<interger>	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 weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00~24:00 means always.)
prefix	string[16]	6/6	Indicate the prefix of the filename.
cyclesize	<integer>	6/6	The maximum size for cycle recording in Kbytes.
maxfilesize	50~6000	6/6	The max size for one file in Kbytes
dest	0~4	6/6	The destination to store the recording data. 0~4 => the index of network storage.

Group: **path**

Name	Value	Security (get/set)	Description
encoder1_start	<boolean>	7/7	Specify the http push server is active for stream 1
encoder2_start	<boolean>	7/7	Specify the http push server is active for stream 2

Group: **https**

Name	Value	Security (get/set)	Description
connect	1025 ~ 65535	7/7	Specify the stunnel connect port
enable	<boolean>	6/6	To enable or disable this secure http
status	-2 ~ 1	6/6	Specify the https status. -2 => invalid public key -1 => waiting for certificated 0 => not installed 1 => active
countryname	string[2]	6/6	Country name in certificate information
stateorprovincename	string[128]	6/6	State or province name in in certificate information
localityname	string[128]	6/6	The locality name in certificate information
organizationname	string[64]	6/6	Organization name in certificate information

unit	string[32]	6/6	Unit name in certificate information.
commonname	string[64]	6/6	Common name in certificate information
validdays	0 ~ 9999	6/6	Certificatation valid period

Drive the digital output

Note: This request requires the privilege of viewer.

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, 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 the current path. If you omit this parameter, it will redirect to an empty page.

Example: 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

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

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

If no parameter is specified, all the status of digital input 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
[di3=<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 the privilege of viewer.

Method: GET/POST

Syntax:

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

If no parameter is specified, all the status of digital output 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 require normal user privilege

Method: GET/POST

Syntax:

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

If the user requests the size larger than all stream setting on the server, this request will failed!

Parameter	Value	Default	Description
channel	0~(n-1)	0	The channel number of video source
resolution	<available resolution>	0	The resolution of image
quality	1~5	3	The quality of image

Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and quality of 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 privilege

Method: GET/POST

Syntax:

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

Parameter	Value	Description
method	add	Add an account to server. When using this method, “username” field is necessary. It will use default value of other fields if not specified.
	delete	Remove an account from server. When using this method, “username” field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, “username” field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify.
	viewer	Viewer’s privilege
	operator	Operator’s privilege
	admin	Administrator’s 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 require administrator privilege

Method: GET/POST

Syntax:

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

Server will return the 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
\r\n
<system log information>\r\n

Upgrade firmware

Note: This request requires administrator privilege

Method: POST

Syntax:

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

Post data:

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

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

System Information

Note: This request requires normal user privilege

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 the fields in the previous version (0100) is obsolete. Please use “getparam.cgi?capability” instead.

Return:

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

Parameter	Value	Description
Model	system.firmwareversion	Model name of server. Ex:IP3133-VVTK-0100a
CapVersion	MMmm, MM is major version from 00 ~ 99 mm is minor version from 00 ~ 99 ex: 0100	The capability field version

IP filtering

Note: This request requires administrator access privilege

Method: GET/POST

Syntax:

http://<servername>/cgi-bin/admin/ipfilter.cgi?method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>][&re
page>]

Parameter	Value	Description
Method	addallow	Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	adddeny	Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	deleteallow	Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority than the [index] parameter.

	deletedeny	Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority than the [index] parameter.
start	<ip address>	The start IP address to add or to delete.
end	<ip address>	The end IP address to add or to delete.
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 Streamings

Note: This request requires viewer access privilege

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 method.

Open the network streamings

Note: This request requires viewer access privilege

Syntax:

For http push server (mjpeg):

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

For rtsp (mp4), user needs to input the url below for a rtsp compatible player.

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

“m” is the stream number.

For detailed streaming protocol, please refer to “control signaling” and “data format” documents.

Senddata

Note: This request requires privilege of viewer

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 s series of digit within 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes => receive data buffer of 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 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 is hex decimal data is a series of digit within 0 ~ 9, A ~ F.

Technical Specifications

System
- Flash: 8MB
- RAM: 64MB
- Embedded OS: Linux 2.4

Image Sensor
- 1/3.3” Wide Dynamic Range CMOS Sensor

Lens
- Board lens,vari-focal, f=3.3 mm ~ 12 mm, F1.4
- Focus range: 50 cm to infinity

Infrared Facility
- IR Illuminators up to 15 meters
- Removable IR-cut filter: Auto/Schedule

Angle of view
- 23° ~ 85.2° (horizontal)
- 14.8° ~ 51.6° (vertical)

Shutter Time
- 1/30 sec. to 1/15000 sec.

Minimum Illumination
- 0 Lux with IR Illuminators

Video
- Compression: MJPEG & MPEG-4
- Streaming: Simultaneous dual-streaming

MPEG-4 streaming over UDP, TCP, or HTTP
MPEG-4 multicast streaming
MJPEG streaming over HTTP

- Supports 3GPP mobile surveillance
- Resolution:

720x480 up to 30/25fps
352x240 up to 30/25fps
176x144 up to 30/25fps

Image settings
- Adjustable image size, quality, and bit rate
- Time stamp and text caption overlay
- Flip & mirror
- Configurable brightness, contrast, and saturation
- AGC, AWB, AEC
- Automatic or manual day/night mode
- Supports privacy masks

Audio
- Compression:

GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps
MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps

- Interface:

External microphone input
Audio output

- Supports two-way audio by SIP protocol
- Supports audio mute

Networking
- 10/100 Mbps Ethernet, RJ-45
- Protocols: IPv4, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, and PPPoE

Alarm and Event Management
- Triple-window video motion detection
- One D/I and one D/O for external sensor and alarm
- Event notification using HTTP, SMTP, or FTP
- Local recording of MP4 file

Security
- Multi-level user access with password protection
- IP address filtering

Users
- Camera live viewing for up to 10 clients

Dimension
- 180 mm (D) x 70 mm (W) x 70 mm (H)

Weight
- Net: 969 g

LED Indicator
- System power and status indicator
- System activity and network link indicator

Power
- 12V DC/1.5A
- 802.3af compliant Power over Ethernet

Viewing System Requirements
- OS: Microsoft Windows 2000/XP/Vista
- Browser: Internet Explorer 6.x or above, Firefox, Mozilla, Netscape
- Cell phone: 3GPP player
- Real Player: 10.5 or above
- Quick Time: 6.5 or above

Installation, Management, and Maintenance
- Installation Wizard to search the IP address of IP cameras
- Industry-leading 32-channel IP CamSecure Lite™ software included
- Supports firmware upgrade

Applications
- SDK available for application development and system integration

Operating Environments
- Temperature: -20° ~ 60°C
- Humidity: 20 % ~ 80 % RH
- IP66-rated housing for weatherproof

Approvals
- CE, FCC

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

■ Reorient or relocate the receiving antenna.

■ Increase the separation between the equipment and receiver.

■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

■ Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Europe CE -- This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

Liability

LEVELONE Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. LEVELONE Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the soft-ware or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

Terms And Conditions For Copying, Distribution And Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and condi-tions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consis-tent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and condi-tions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES

PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at http://global.level1.com.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US$9.99 plus the cost of shipping.