LevelOne

FCS-3021

PoE IP Dome Camera

User Manual

Ver 1.2.0 – 0809

Before You Use This Product

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 list in the "Package Contents" chapter. Take notice of the warnings 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. The “Troubleshooting” chapter in the Appendix provides remedies to the most common errors in set up and configuration. You should consult this chapter first if you run into a system error.

The Network Camera is designed for various applications including video sharing, general security/surveillance, etc. The “How to Use” 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" chapter serves to be a helpful reference to customize existing homepages or integrating with the current web server.

> For paragraphs preceded by ⚠ the reader should use caution to understand completely the warnings. Ignoring the warnings may result in serious hazards or injuries.

Table of Contents

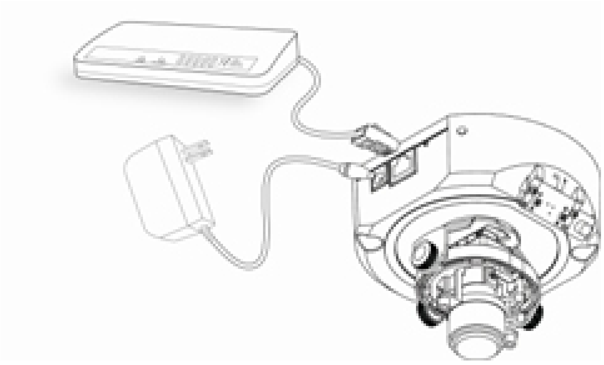
Package Content

1. FCS-3021
2. Alignment Sticker
3. Screw Kit and I/O Connector
4. CD Manual/Utility
5. Quick Installation Guide

Installation

In this manual, "User" refers to whoever has access to the Network Camera, and "Administrator" refers to the person who can configure the Network Camera and grant user access to the camera.

Hardware installation



Please verify that your product package contains all the accessories listed in the foregoing Package Contents. Depending on the user's application, an Ethernet cable may be needed. The Ethernet cable should meet the specs of UTP Category 5 and not exceed 100 meters in length.

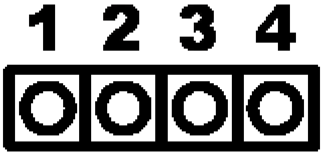
⚠ Since FCS-3021 is a PoE IP camera, it could work without attaching to power outlet as long as it connects to PoE switch.
Connect the power adapter jack to the Network Camera before plugging in to the power socket. This will reduce the risk of accidental electric shock.

Upon powering up, the status LED will become lighted first and then the device will go through booting process. The status LED will be steady orange for getting IP address. After getting IP Address, the LED will blink orange and red as heartbeat to indicate alive.

To install in Ethernet

Make sure the Ethernet is firmly connected to a switch hub. After attaching the Ethernet cable plug in the power adapter. If the LED turns out to blink orange-color, go to next paragraph "Software installation".

This Network Camera provides a general I/O terminal block with one digital input and one digital output device control. The pin definition is as below.



1: Power
2: Digital output
3: Digital input

4: Ground

Ext./Int.

Switch **"Internal"** or **"External"** to set up the source of audio input

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 serial number. **The serial number is printed on the labels which is on the bottom of the Network Camera body.** Please refer to the Quick installation guide of Installation Wizard for details.

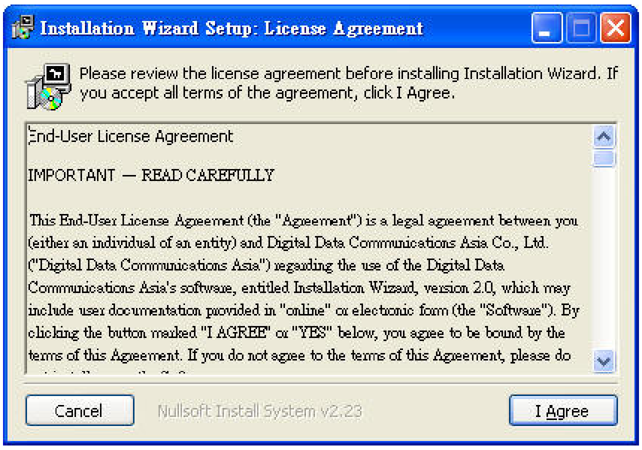
Once installation is complete, the Administrator should proceed to the next section "Initial Access to the Network Camera" for necessary checks and configurations.

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 Setup: License Agreement

Please review the license agreement before installing Installation Wizard. If you accept all terms of the agreement, click I Agree.

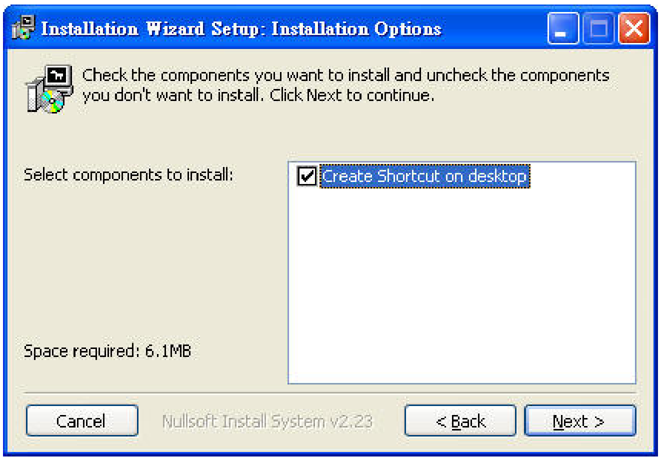
End-User License Agreement

IMPORTANT — READ CAREFULLY

This End-User License Agreement (the "Agreement") is a legal agreement between you (either an individual of an entity) and Digital Data Communications Asia Co., Ltd. ("Digital Data Communications Asia") regarding the use of the Digital Data Communications Asia's software, entitled Installation Wizard, version 2.0, which may include user documentation provided in "online" or electronic form (the "Software"). By clicking the button marked "I AGREE" or "YES" below, you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, please do

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.



Installation Wizard Setup: Installation Options

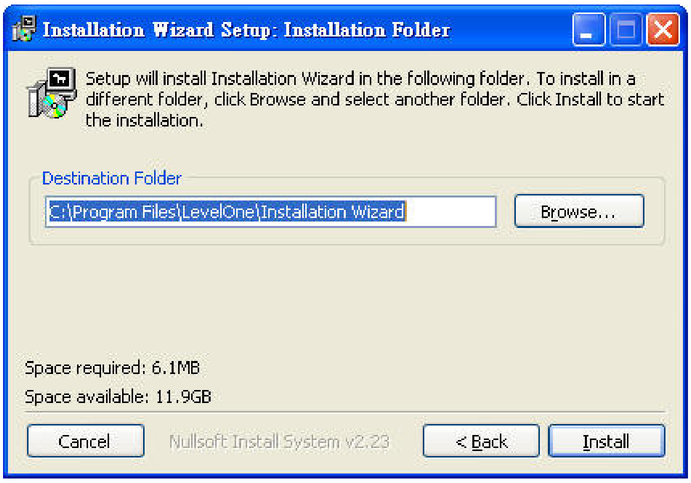
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install: ☑ Create Shortcut on desktop

Space required: 6.1MB

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.



Installation Wizard Setup: Installation Folder

Setup will install Installation Wizard in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

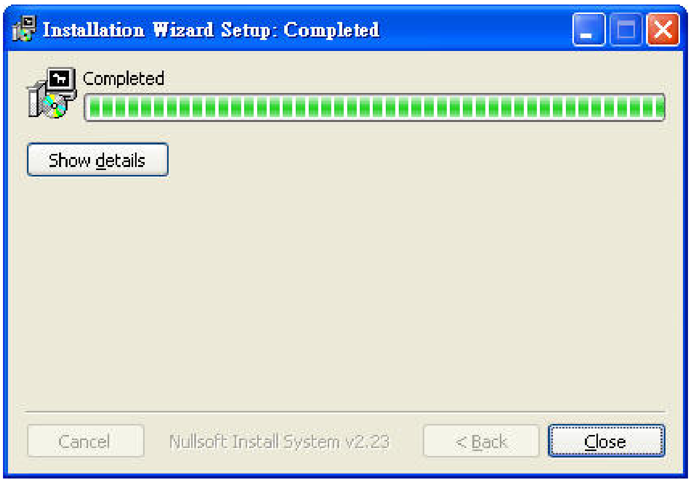
Destination Folder: C:\Program Files\LevelOne\Installation Wizard

Space required: 6.1MB

Space available: 11.9GB

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.



Installation Wizard Setup: Completed

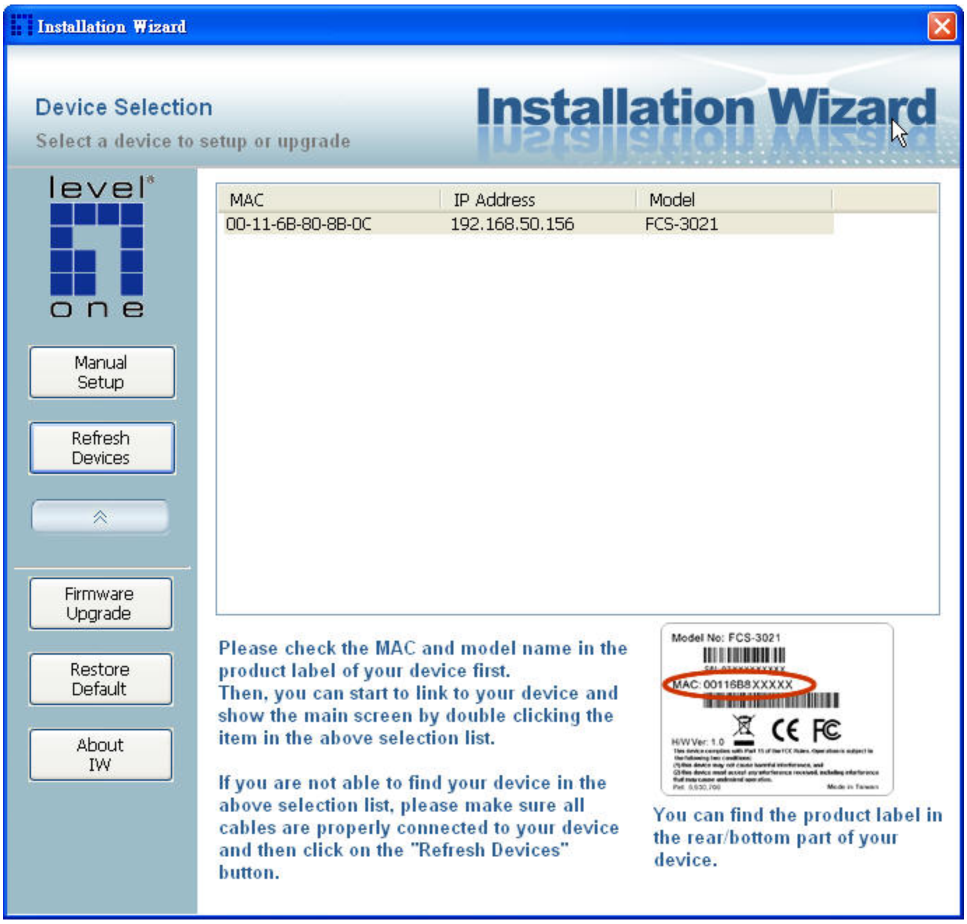
Completed

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.



Device Selection

Select a device to setup or upgrade

MAC	IP Address	Model
00-11-6B-80-8B-0C	192.168.50.156	FCS-3021

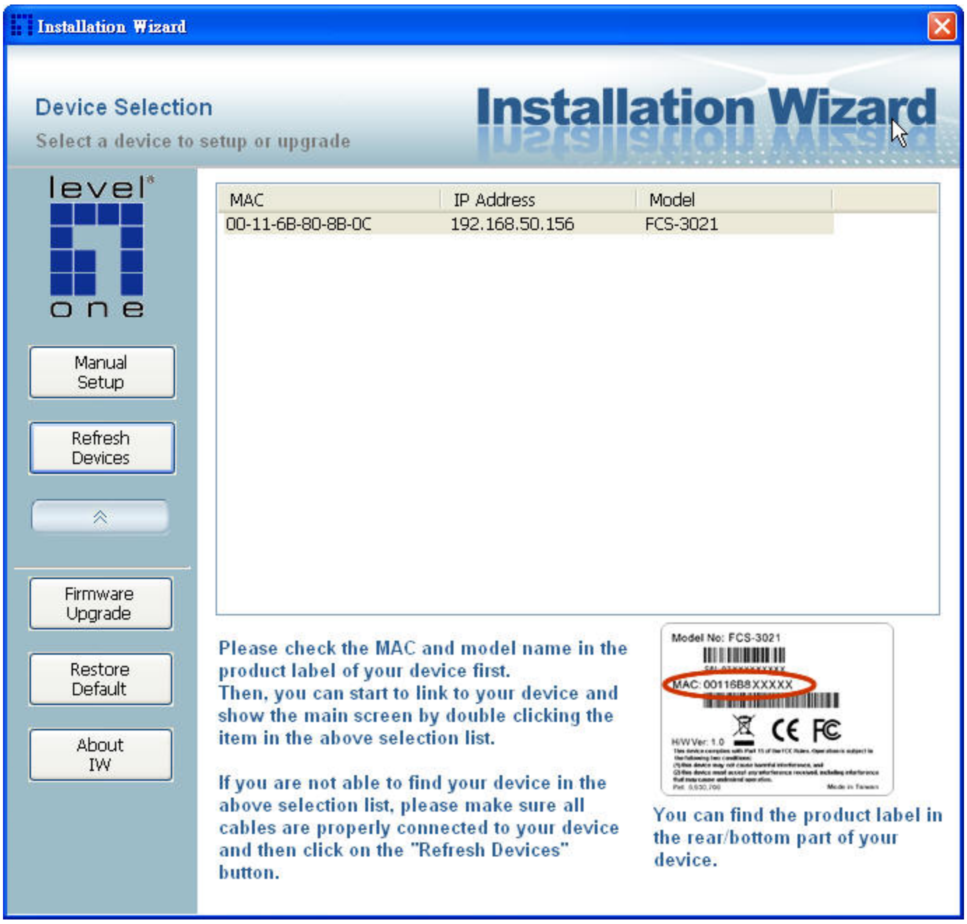
Please check the MAC and model name in the product label of your device first. Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your 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.



Device Selection

Select a device to setup or upgrade

MAC	IP Address	Model
00-11-6B-80-8B-0C	192.168.50.156	FCS-3021

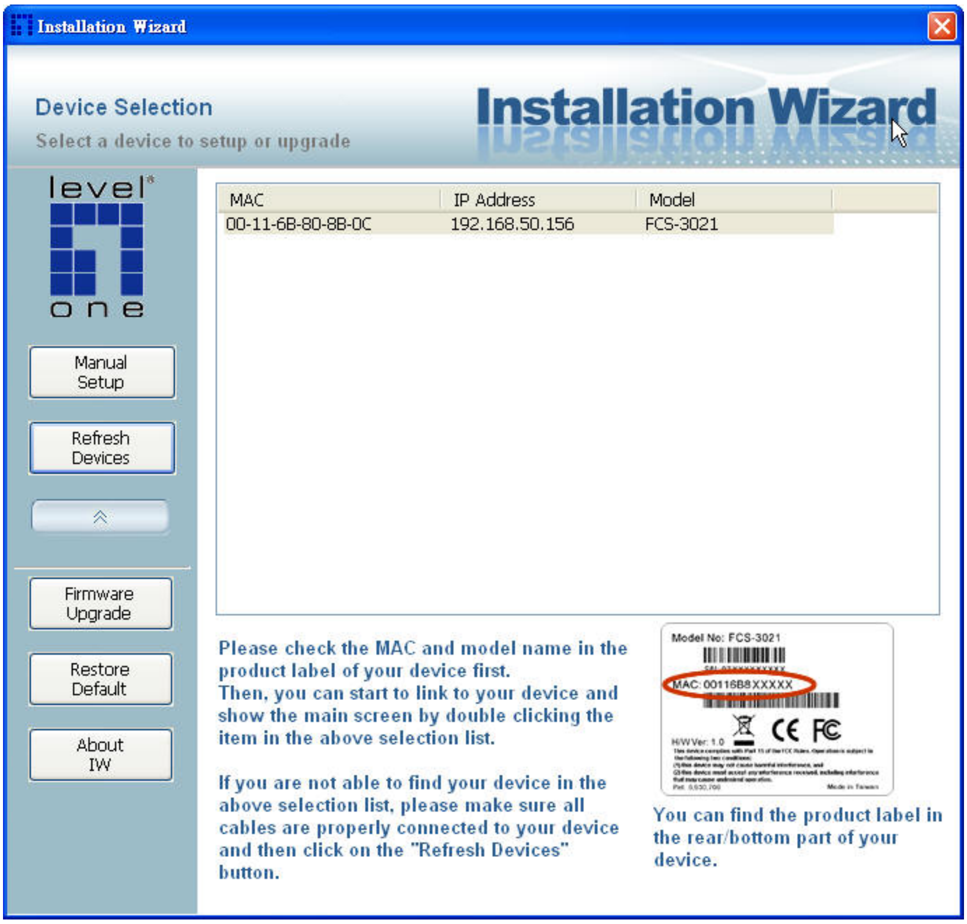
Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your device.

User interface of Installation Wizard after clicking on the arrow button

Action buttons



MAC	IP Address	Model
00-11-6B-80-8B-0C	192.168.50.156	FCS-3021

Please check the MAC and model name in the product label of your device first. Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

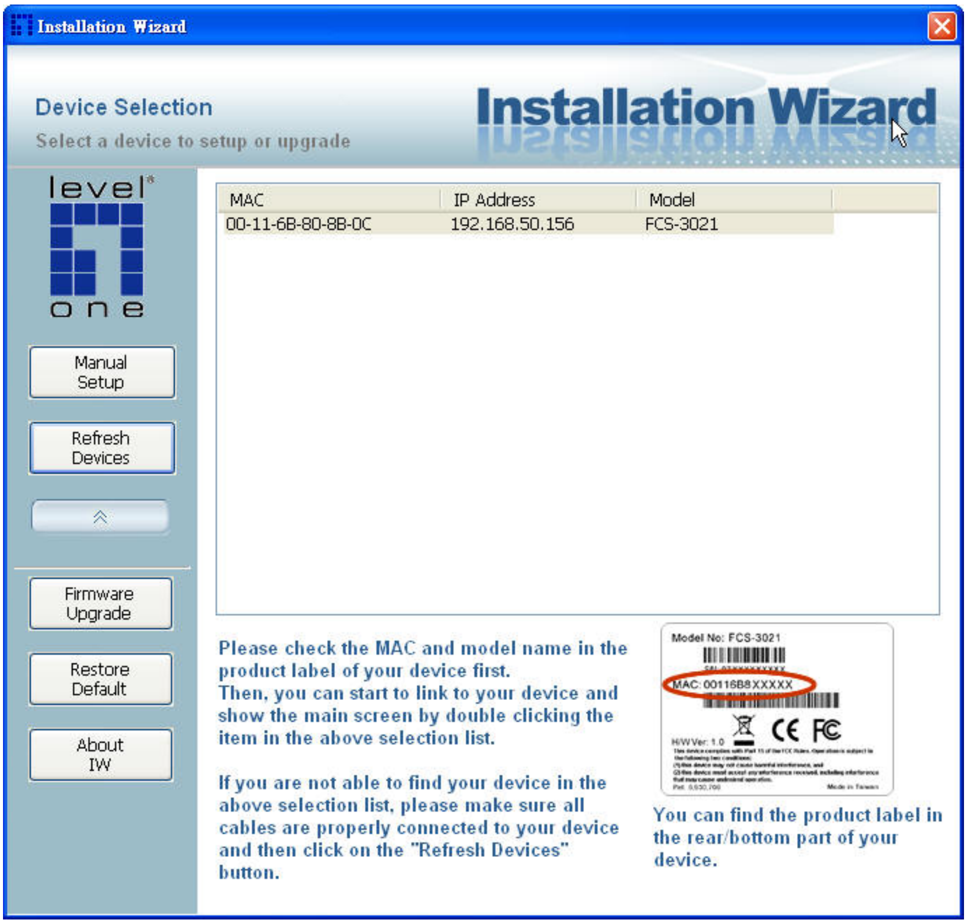
You can find the product label in the rear/bottom part of your device.

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



Device Selection

Select a device to setup or upgrade

MAC	IP Address	Model
00-11-6B-80-8B-0C	192.168.50.156	FCS-3021

Please check the MAC and model name in the product label of your device first. Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your device.

Function buttons

Manual Setup

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

Firmware Upgrade

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

Restore Default

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

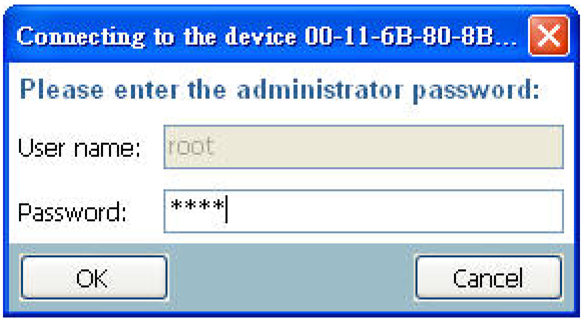
About IW

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.

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.



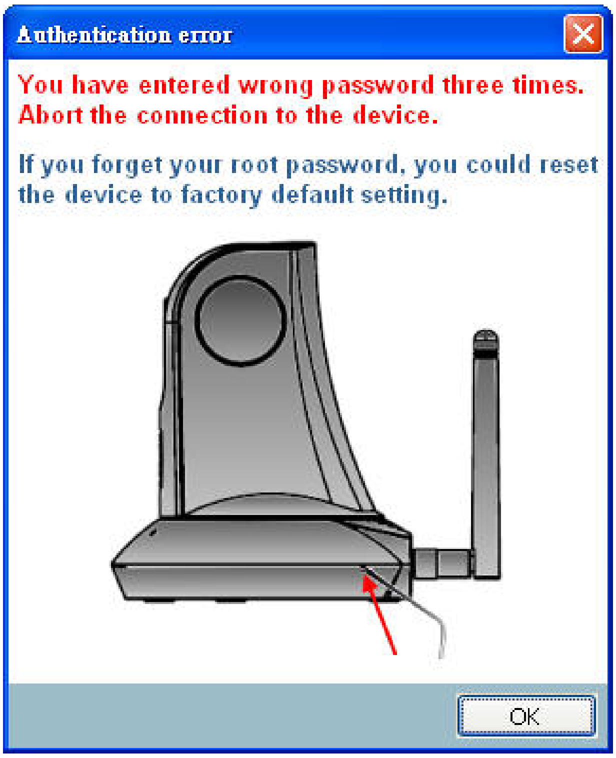
Connecting to the device 00-11-6B-80-8B...

Please enter the administrator password:

User name: root

Password: ****

Authentication Dialog Window



Authentication error

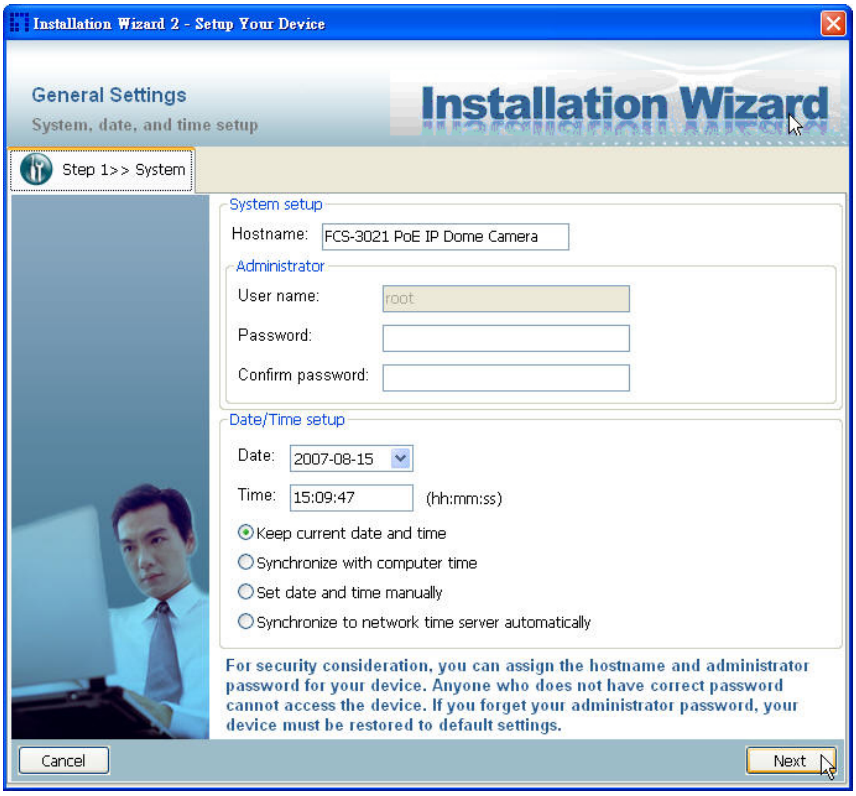
You have entered wrong password three times.
Abort the connection to the device.

If you forget your root password, you could reset the device to factory default setting.

Authentication error

System Setting

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



General Settings

System, date, and time setup

System setup

Hostname: FCS-3021 PoE IP Dome Camera

Administrator

User name: root

Password:

Confirm password:

Date/Time setup

Date: 2007-08-15

Time: 15:09:47 (hh:mm:ss)

● Keep current date and time

○ Synchronize with computer time

○ Set date and time manually

○ Synchronize to network time server automatically

For security consideration, you can assign the hostname and administrator password for your device. Anyone who does not have correct password cannot access the device. If you forget your administrator password, your device must be restored to default settings.

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.

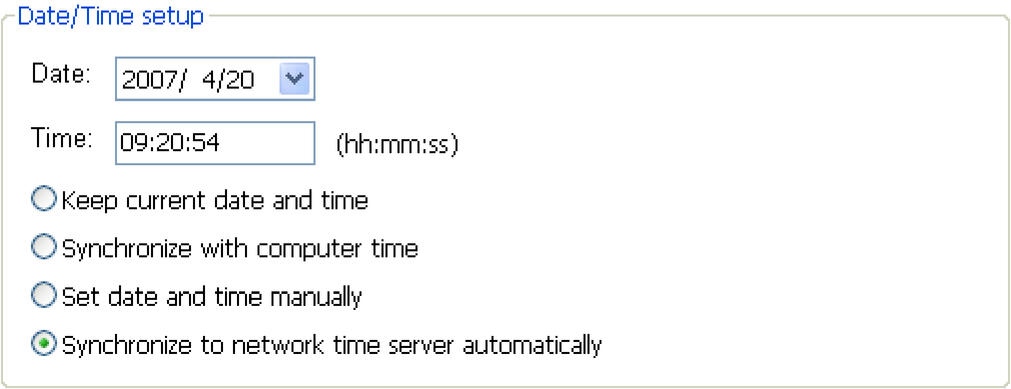
Change Host Name

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

Date: 2007/ 4/20

Time: 09:20:54 (hh:mm:ss)

○ Keep current date and time

○ Synchronize with computer time

○ Set date and time manually

● Synchronize to network time server automatically

Date/Time setup

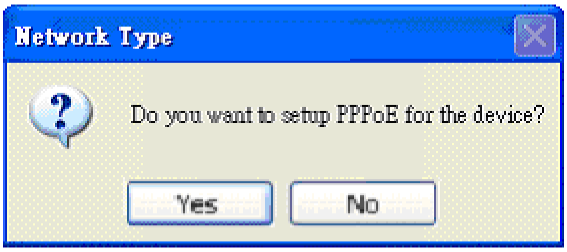
There are three ways to adjust system date and time:

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

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

Network Setting

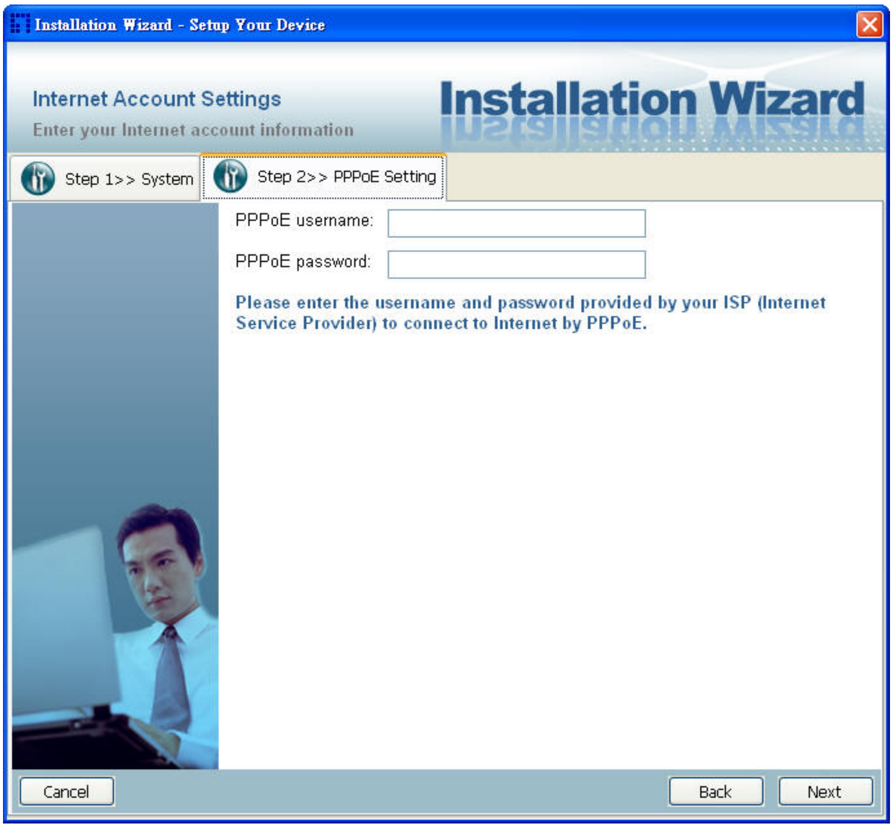
The Installation Wizard can help you to setup the network connection with LAN or PPPoE. After you clicked on the **"Next"** button on the System page, the Installation Wizard would lead you to the PPPoE setting page. If you want to connect your server to Internet via PPPoE, please click on **"Yes"**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



Do you want to setup PPPoE for the device?

Choosing the network type

PPPoE Setting



Internet Account Settings

Enter your Internet account information

PPPoE username:

PPPoE password:

Please enter the username and password provided by your ISP (Internet Service Provider) to connect to Internet by PPPoE.

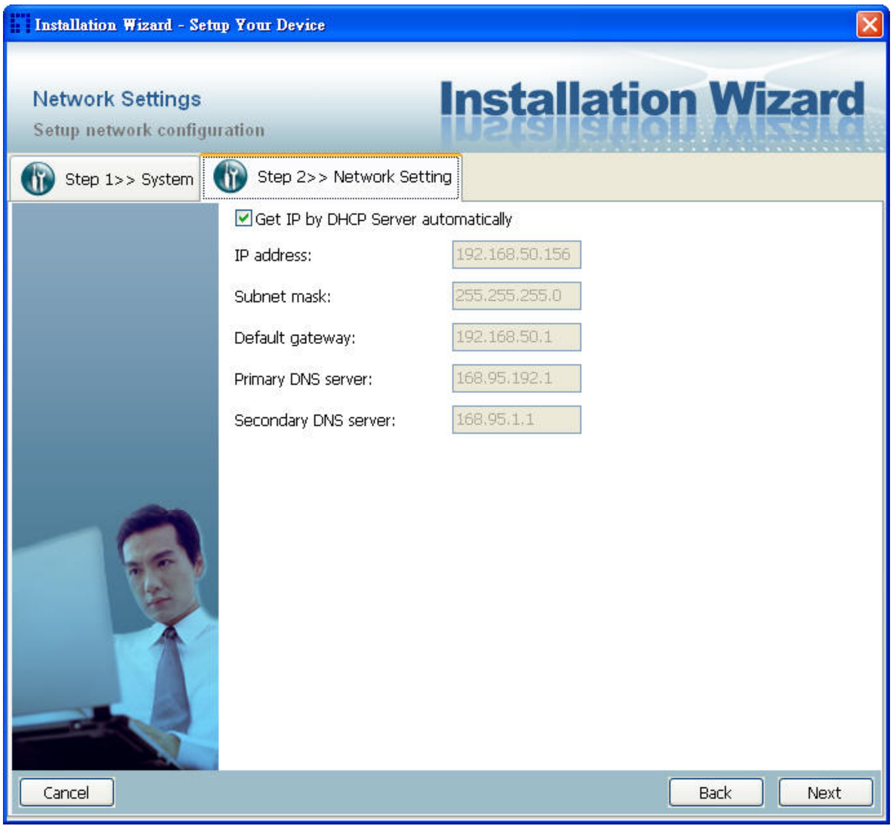
Network setting for PPPoE

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 Settings

Setup network configuration

Step 1>> System

Step 2>> Network Setting

☑ Get IP by DHCP Server automatically

IP address: 192.168.50.156

Subnet mask: 255.255.255.0

Default gateway: 192.168.50.1

Primary DNS server: 168.95.192.1

Secondary DNS server: 168.95.1.1

Network Setting for LAN

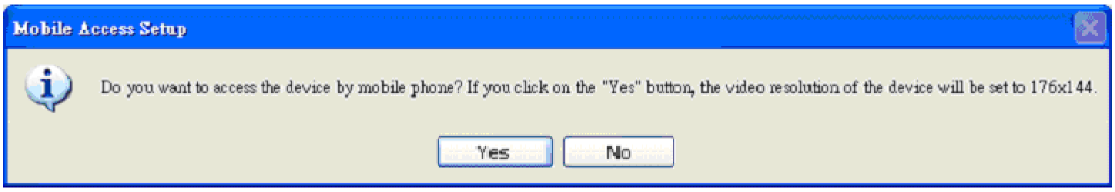
You could set up the network with DHCP or fixed IP:

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

Mobile Access

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

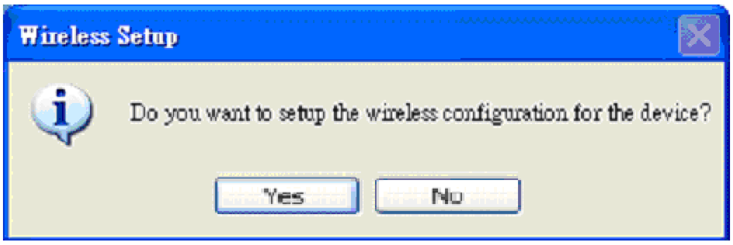
1. Video: The video codec will be set to MPEG-4, and the resolution will be set to 176x144 pixels.
2. Audio: The audio codec will be set to AAC.



Do you want to access the device by mobile phone? If you click on the "Yes" button, the video resolution of the device will be set to 176x144.

Mobile Access

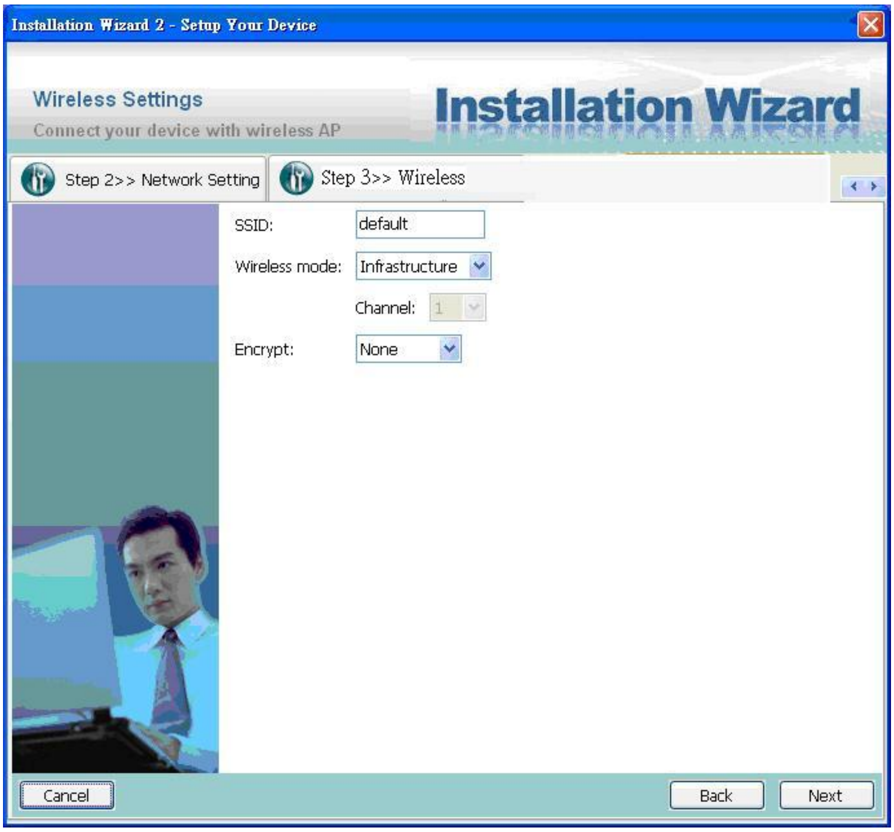
Wireless Setting



Do you want to setup the wireless configuration for the device?

Ask if you want to setup the wireless configuration

This above page will show up only when you select the model with wireless support. It allows you to configure the wireless setting. Please refer to the below page.



SSID: default

Wireless mode: Infrastructure

Channel: 1

Encrypt: None

Wireless Setting

Basic Settings

"SSID" (Service Set Identifier), it is a name which identified a wireless network. Access Points and wireless clients attempting to connect to a specific WLAN (Wireless Local Area Network) must use the same SSID. The default setting is ***default***. *Note: The maximum length of SSID is 32 single-byte characters.*

"Wireless mode" Click on the pull-down menu, and you can see the following options:

1. **"Infrastructure"** Make the device connect to the WLAN via an Access Point (The default setting). **"Ad-Hoc"** Make the device connect directly to a host equipped with a wireless adapter in peer-to-peer mode.
2. **"Channel"** While in infrastructure mode, the channel will be set automatically to the same channel setting of the selected Access Point. While in Ad-Hoc mode, the channel must be set to the same channel for each wireless adapter. The default channel setting depends on the installed region.

Data Encryption

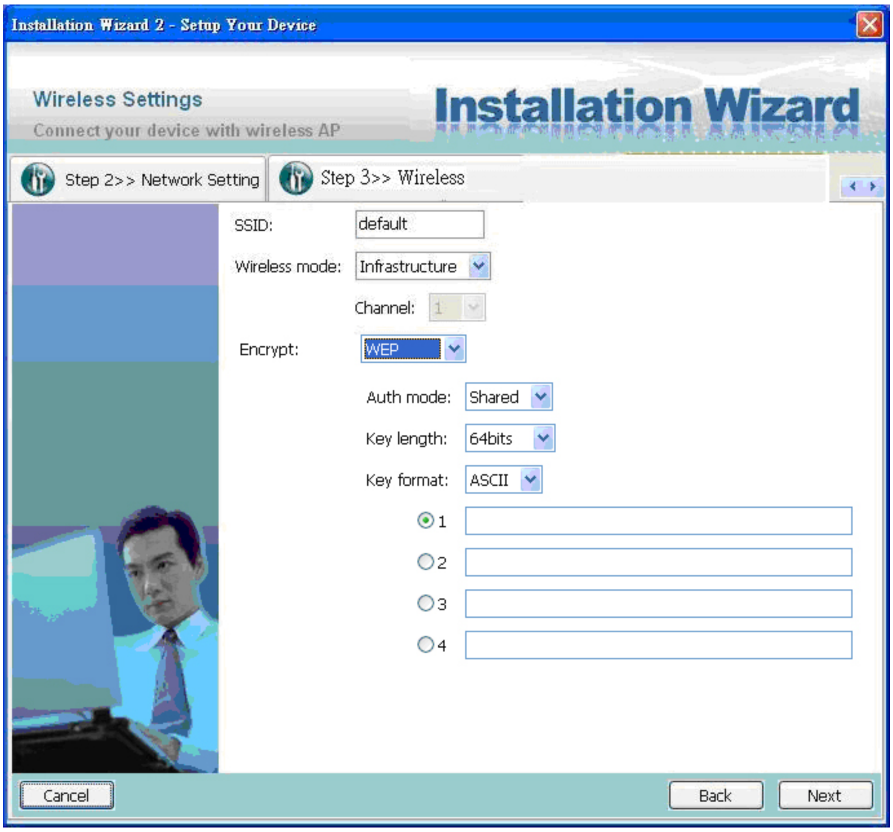
"Encrypt" You can choose the encryption type you want in the pull-down menu, there are three items: None, WEP and WPA-PSK.

None

If your wireless environment doesn't need encryption, please choose "None".

WEP

If your encryption is WEP, please choose the **"WEP"** in the Encrypt pull-down menu, and you have to enter the following information.



SSID: default

Wireless mode: Infrastructure

Channel: 1

Encrypt: WEP

Auth mode: Shared

Key length: 64bits

Key format: ASCII

● 1

○ 2

○ 3

○ 4

WEP Setting page

"Auth. Mode" Choose one of the following modes,

"Shared" – allows communication only with other devices on identical WEP settings.

"Open" – communicates the key across the network.

"Key length": The administrator can select the key length among 64 or128 bits. The selection will depend on the selected device.

"Key format": Hexadecimal or ASCII.

"**HEX"** digits consist of the numbers 0~9 and the letters A-F.

"ASCII" is a code for representing English letters as numbers from 0-127 except ", <, > and space characters that are reserved.

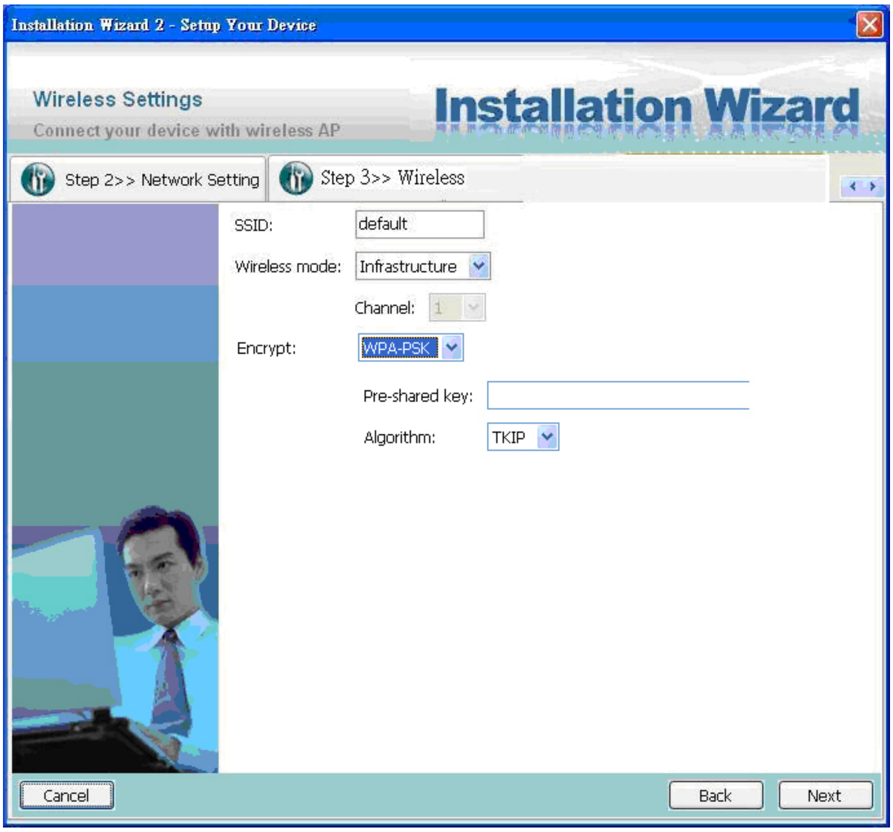
"Key": Enter a key in either hexadecimal or ASCII format. When selecting different key length, acceptable input length is listed as following:

64 bits key length: 10 Hex digits or 5 characters.

128 bites key length: 26 Hex digits or 13 characters.

WPA-PSK

If your encryption type is WPA, please choose the **"WPA-PSK"**. And you have to enter the pre-shared key and choose a proper encryption algorithm (TKIP, AES)



SSID: default

Wireless mode: Infrastructure

Channel: 1

Encrypt: WPA-PSK

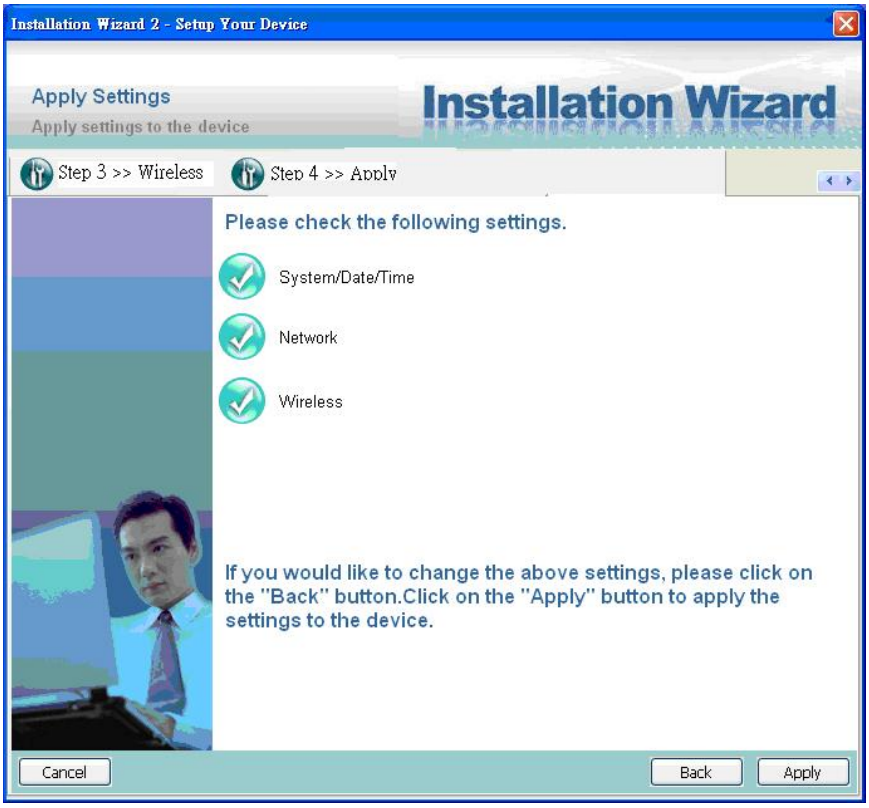
Pre-shared key:

Algorithm: TKIP

WPA-PSK Setting page

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.



Please check the following settings.

✓ System/Date/Time

✓ Network

✓ Wireless

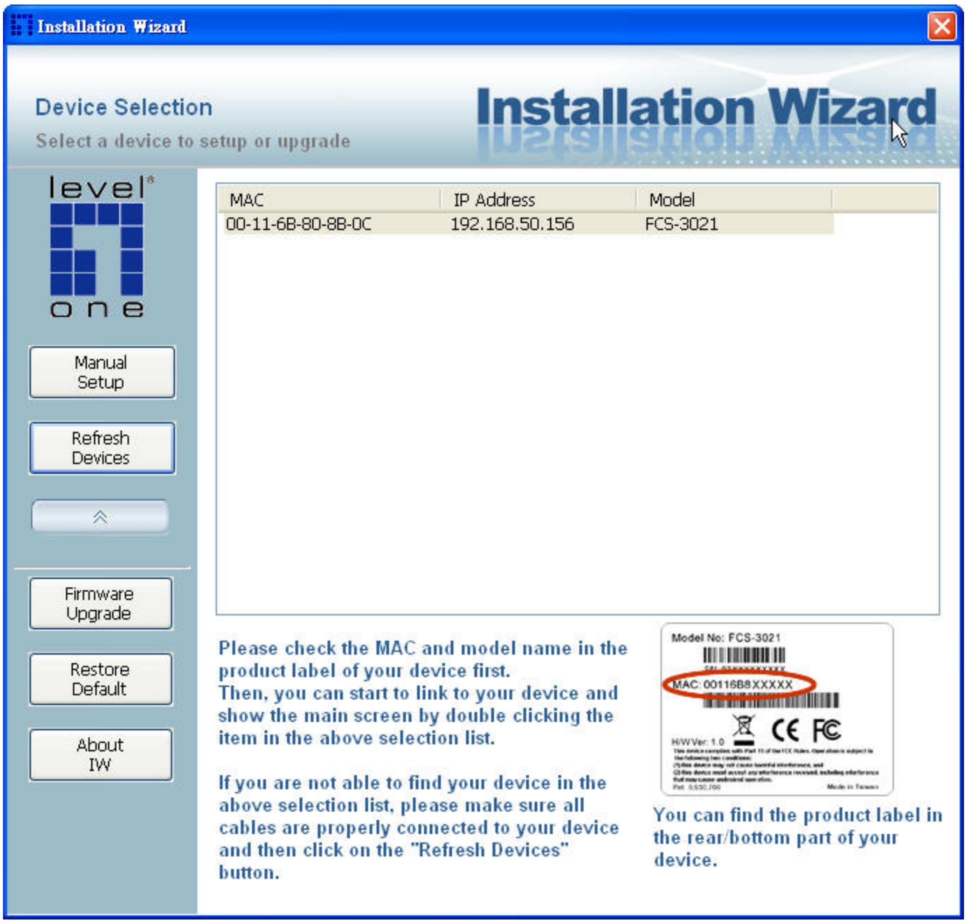
If you would like to change the above settings, please click on the "Back" button.Click on the "Apply" button to apply the settings to the device.

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.



Device Selection

Select a device to setup or upgrade

MAC	IP Address	Model
00-11-6B-80-8B-0C	192.168.50.156	FCS-3021

Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

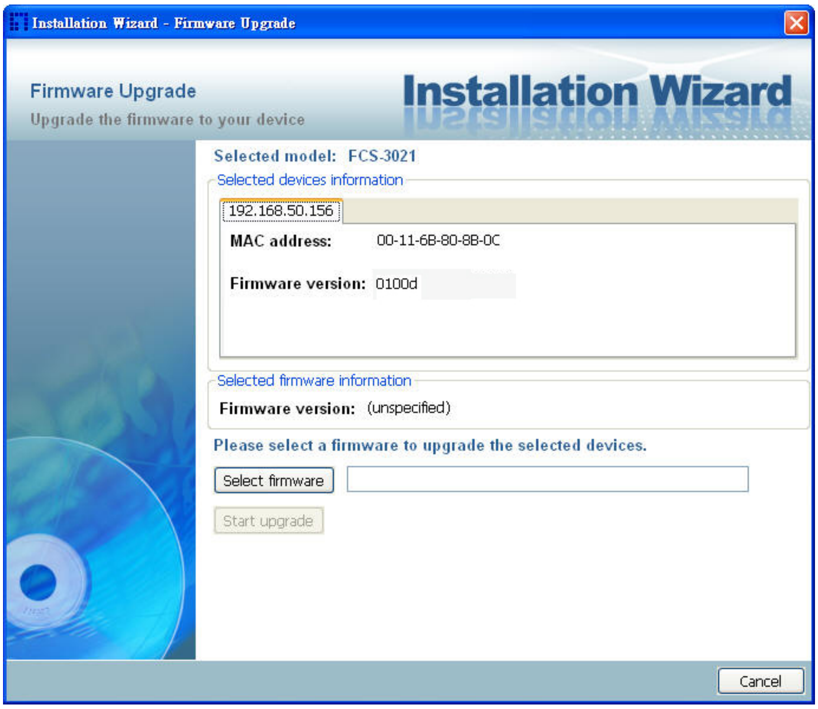
If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your device.

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.


Installation Wizard - Firmware Upgrade
Installation Wizard
Firmware Upgrade
Upgrade the firmware to your device

Selected model: FCS-3021

Selected devices information

192.168.50.156

MAC address: 00-11-6B-80-8B-0C

Firmware version: 0100d

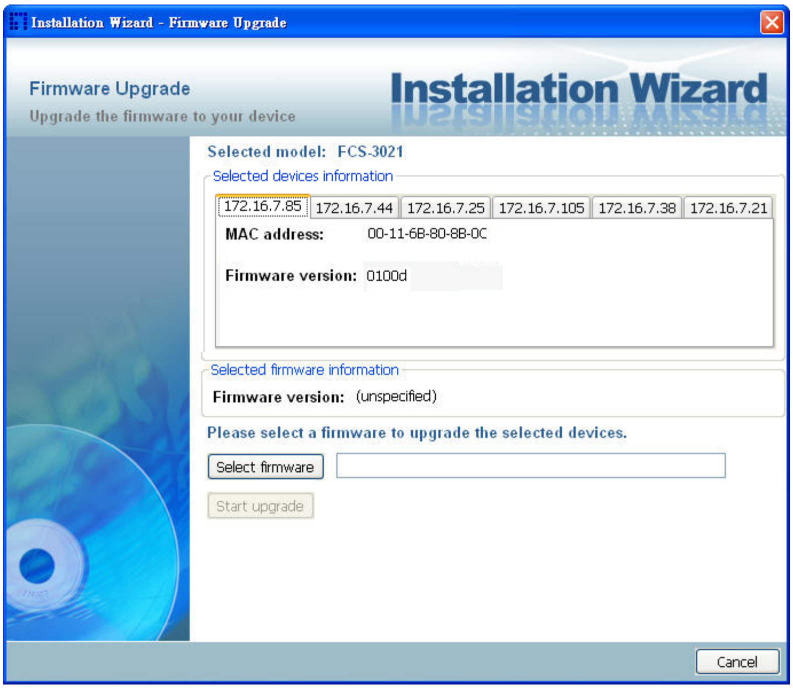
Selected firmware information

Firmware version: (unspecified)

Please select a firmware to upgrade the selected devices.

Select firmware
Start upgrade
Cancel

Device information


Installation Wizard - Firmware Upgrade
Installation Wizard
Firmware Upgrade
Upgrade the firmware to your device

Selected model: FCS-3021

Selected devices information

172.16.7.85 | 172.16.7.44 | 172.16.7.25 | 172.16.7.105 | 172.16.7.38 | 172.16.7.21

MAC address: 00-11-6B-80-8B-0C

Firmware version: 0100d

Selected firmware information

Firmware version: (unspecified)

Please select a firmware to upgrade the selected devices.

Select firmware
Start upgrade
Cancel

Multiple devices information

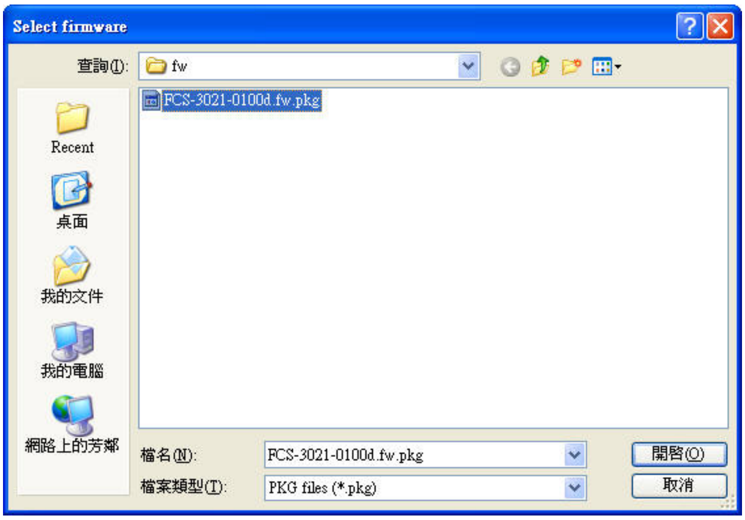
Firmware Information

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

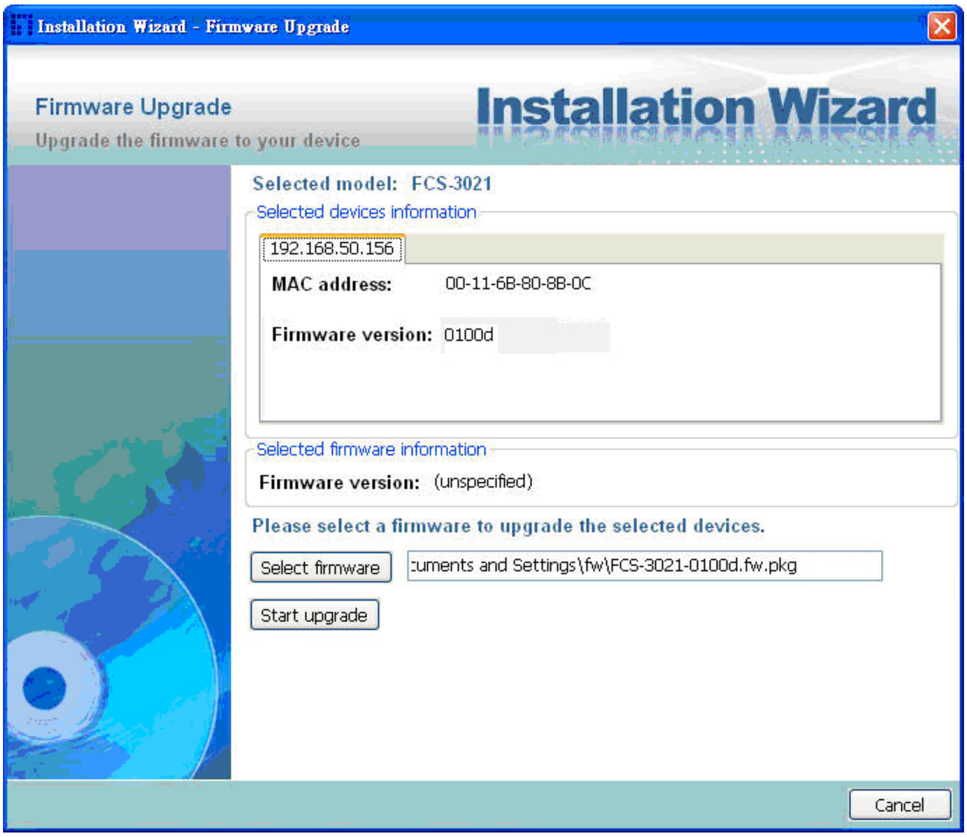
查詢(I): fw

FCS-3021-0100d.fw.pkg

檔名(N): FCS-3021-0100d.fw.pkg

檔案類型(T): PKG files (*.pkg)

Select firmware



Installation Wizard - Firmware Upgrade

Firmware Upgrade

Upgrade the firmware to your device

Selected model: FCS-3021

Selected devices information

192.168.50.156

MAC address: 00-11-6B-80-8B-0C

Firmware version: 0100d

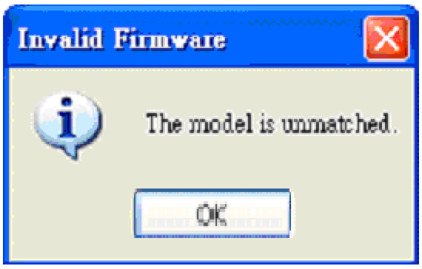
Selected firmware information

Firmware version: (unspecified)

Please select a firmware to upgrade the selected devices.

:uments and Settings\fw\FCS-3021-0100d.fw.pkg

Firmware Information



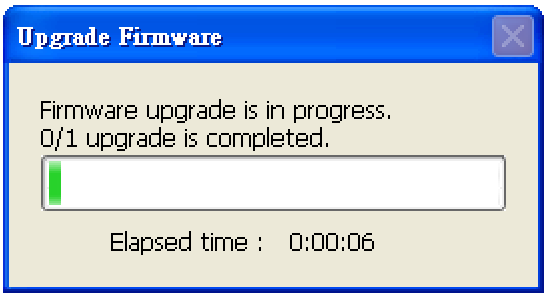
Invalid Firmware

The model is unmatched.

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.



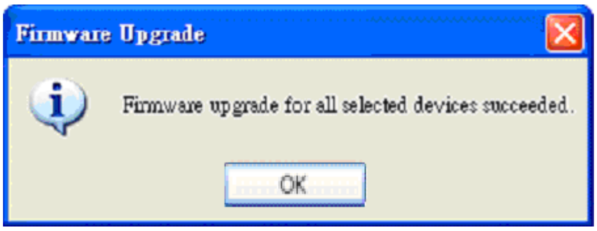
Upgrade Firmware

Firmware upgrade is in progress.
0/1 upgrade is completed.

Elapsed time : 0:00:06

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.



Firmware Upgrade

Firmware upgrade for all selected devices succeeded.

Upgrade Done

Initial Access to the Network Camera

Check Network Settings

The Network Camera can be connected either before or immediately after software installation onto the Local Area Network. The Administrator should complete the network settings on the configuration page, including the correct subnet mask and IP address of gateway and DNS. Ask your network administrator or Internet service provider for the detail information. By default the Network Camera requires the Administrator to run installation every time it reboots. If the network settings are to remain unchanged, disable the Install option. Refer to "Network settings" on the System Configuration page for details. If any setting is entered incorrectly and cannot proceed to setting up the Network Camera, restore the factory settings following the steps in the "Troubleshooting" chapter of the Appendix.

Add Password to prevent Unauthorized Access

The default Administrator's password is blank and the Network Camera initially will not ask for any password. **The Administrator should immediately implement a new password as a matter of prudent security practice.** Once the Administrator's password is saved, the Network Camera will ask for the user's name and password before each access. The Administrator can set up a maximum of twenty (20) user accounts. Each user can access the Network Camera except to perform system configuration. Some critical functions are exclusive for the Administrator, such as system configuration, user administration, and software upgrades. The user name for the Administrator is permanently assigned as "root". Once the password is changed, the browser will display an authentication window to ask for the new password. **Once the password is set, there is no provision to recover the Administrator's password. The only option is to restore to the original factory default settings.**

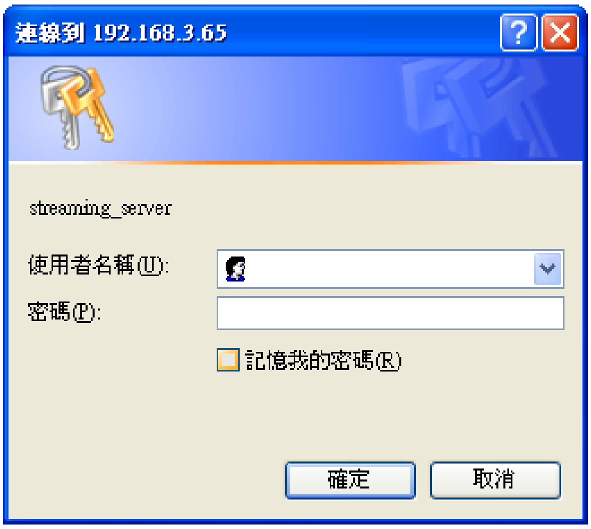
How to Use

A PC with Windows operating system can use the Internet Explorer to connect to the Network Camera. A plug-in will be installed into the IE when it is connected for the first time. A PC with Linux operating system can connect to the camera using a browser like Firefox. It needs to install QuickTime first to view streaming.

Authentication

After opening the Web browser and typing in the URL of the Network Camera, a dialogue window pops up to request a username and password. Upon successful authentication, the following figure is displayed.

The foreground is the login window and the background shows the message if authentication fails. The user may check the option box to save the password for future convenience. This option is not available to the Administrator for obvious reason.



連線到 192.168.3.65

streaming_server

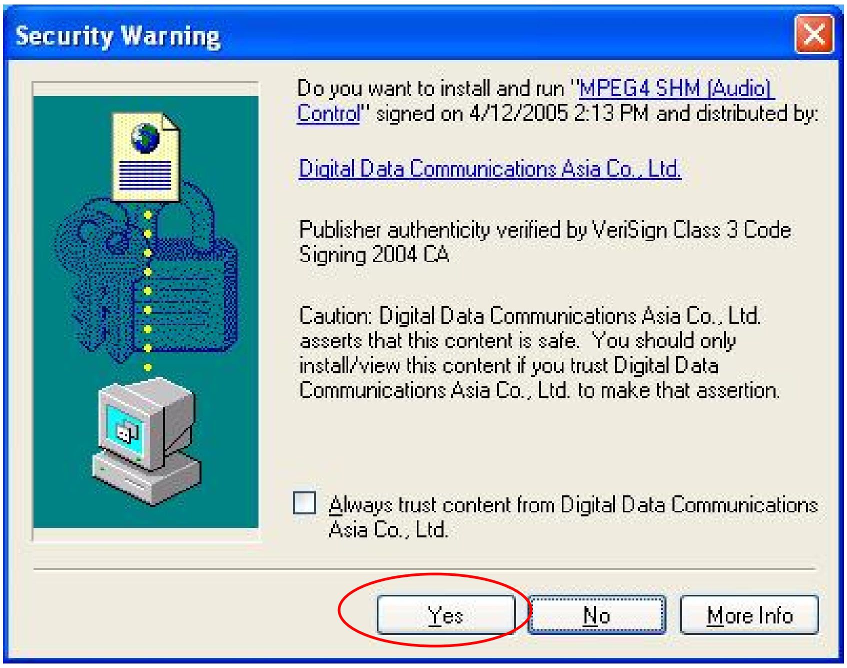
使用者名稱(U):

密碼(P):

□ 記憶我的密碼(R)

Installing plug-in

For the initial access to the Network Camera in Windows, the web browser may prompt for permission to install a new plug-in for the Network Camera on the Internet Explorer. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt. This plug-in has been registered for certificate and is used to display the video in the browser. Users may click on Yes to proceed. If the web browser does not allow the user to continue to install, check the Internet security option and lower the security levels or contact your IT or networking supervisor for help.



Security Warning

Do you want to install and run "MPEG4 SHM (Audio) Control" signed on 4/12/2005 2:13 PM and distributed by:

Digital Data Communications Asia Co., Ltd.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2004 CA

Caution: Digital Data Communications Asia Co., Ltd. asserts that this content is safe. You should only install/view this content if you trust Digital Data Communications Asia Co., Ltd. to make that assertion.

□ Always trust content from Digital Data Communications Asia Co., Ltd.

Primary user's capability

Main Screen with Camera View

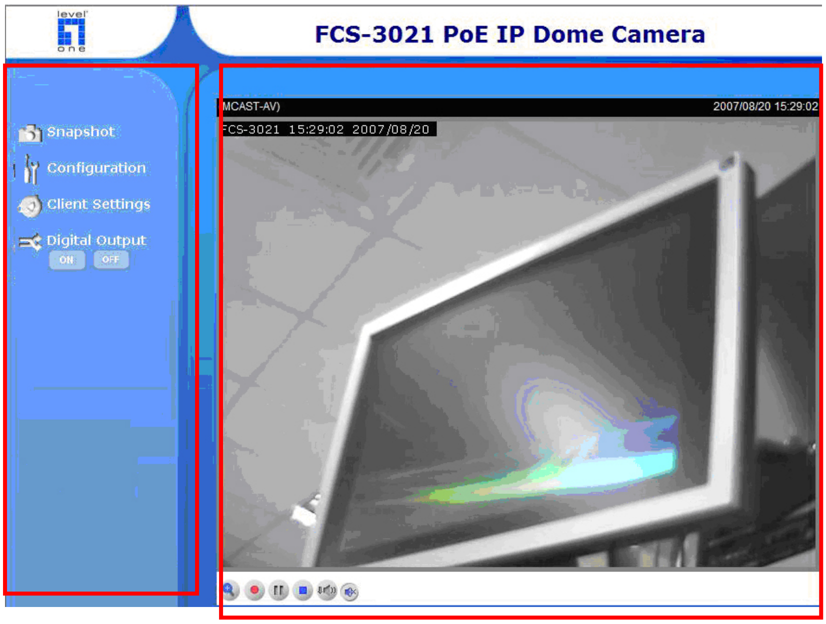
The main page layout has two parts:

Configuration functions: The camera can be configured using these user interfaces.

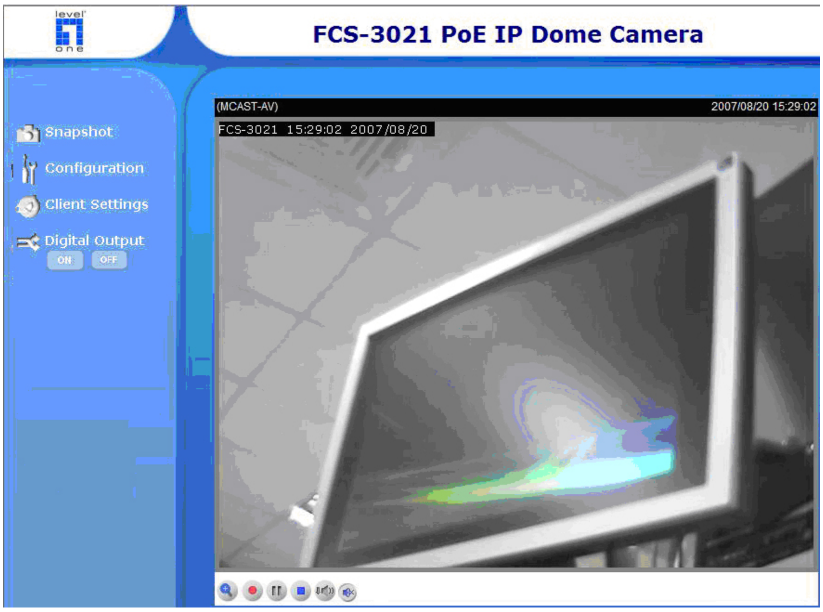
Camera View: What the camera sees.

Click on the configuration link to the left of the image window to enter the configuration page.

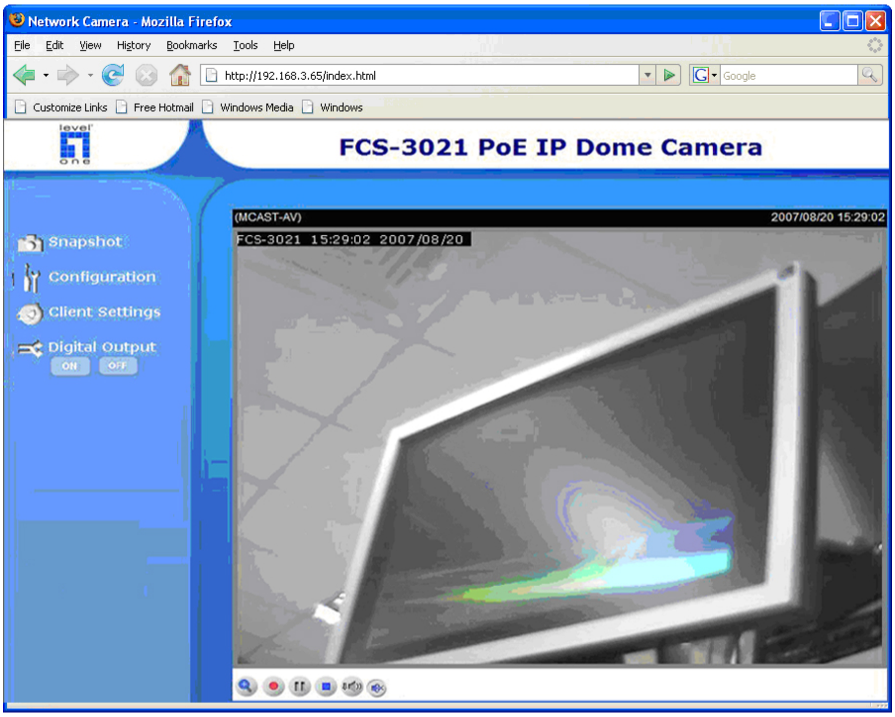
Here is the layout in IE when it is MPEG-4 streaming.



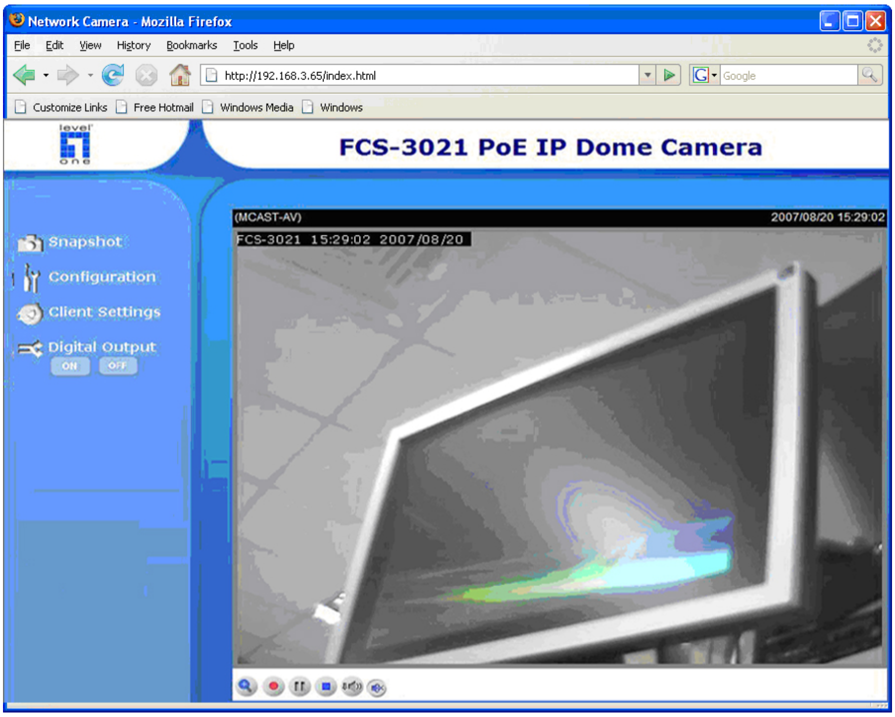
The function in JPEG will be a little different when it is JPEG streaming. Only digital zoom and record button are supported.



Here is the layout in Firefox when it is MPEG-4 streaming. It uses QuickTime to streaming.

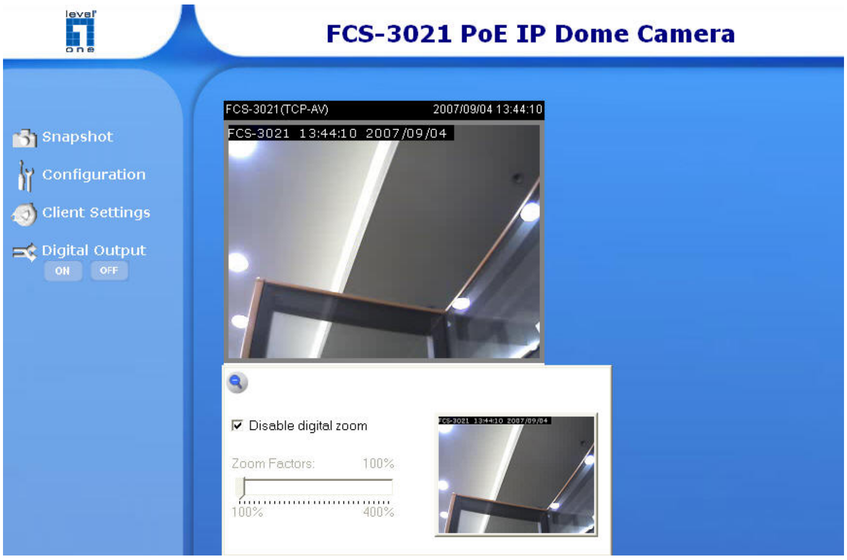


Here is the layout in Firefox when it is JPEG streaming.


Network Camera - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.3.65/index.html
Customize Links
Free Hotmail
Windows Media
Windows
FCS-3021 PoE IP Dome Camera
Snapshot
Configuration
Client Settings
Digital Output
ON
OFF
(MCAST-AV)
2007/08/20 15:29:02
FCS-3021 15:29:02 2007/08/20

Digital Zoom

Click on the magnifier icon under the camera view then the digital zoom control panel will be shown. Uncheck “Disable digital zoom” and use the slider control to change the zoom factors.

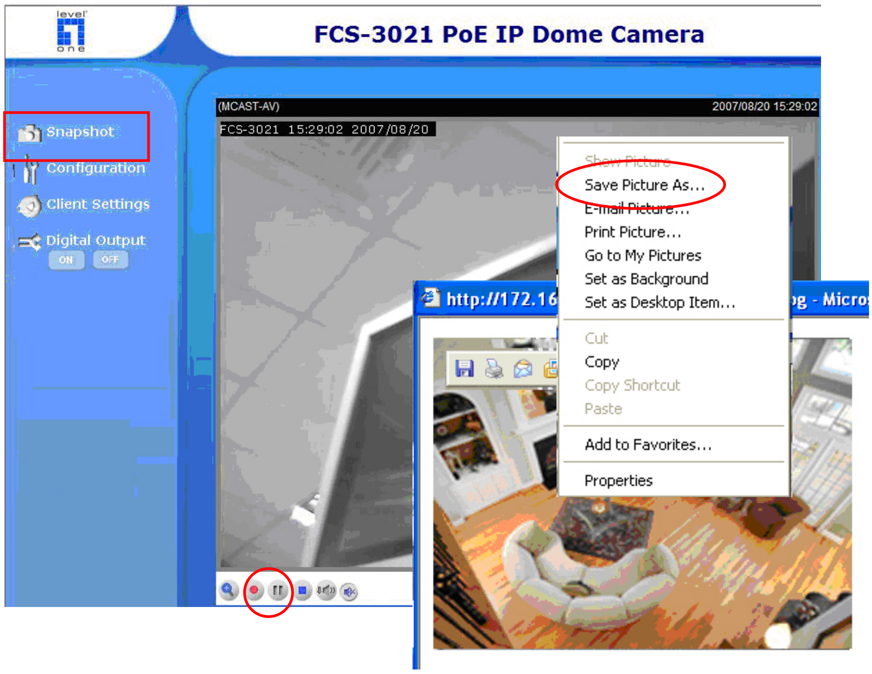


MP4 Recording

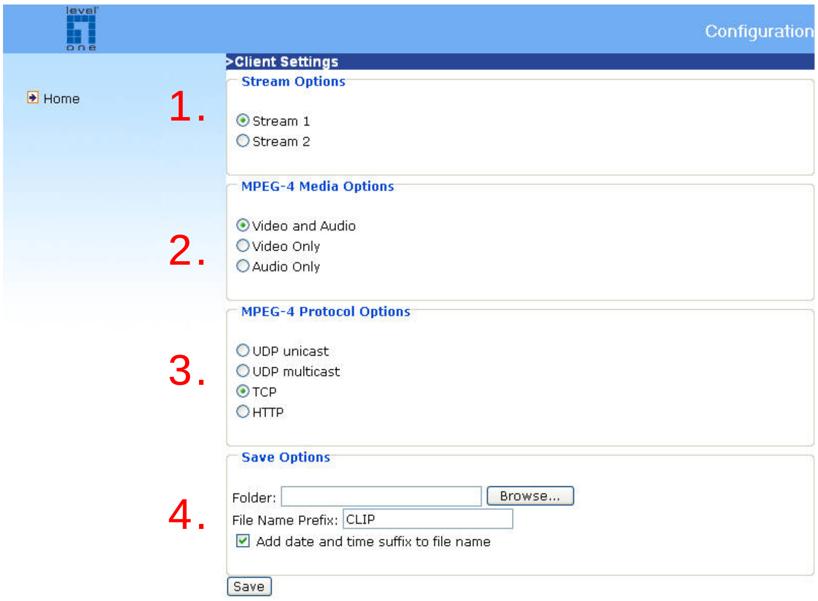
Click on the red circle button ● on the plugin to start MP4 recording. You can set the related options in client setting page.

Snapshot

Click on "**Snapshot**", web browser will pop up a new window to show the snapshot. Users can point at the snapshot and click the right button of mouse to save it.



Client settings



>Client Settings

Stream Options

● Stream 1
○ Stream 2

MPEG-4 Media Options

● Video and Audio
○ Video Only
○ Audio Only

MPEG-4 Protocol Options

○ UDP unicast
○ UDP multicast
● TCP
○ HTTP

Save Options

Folder: [ ] Browse...
File Name Prefix: CLIP
☑ Add date and time suffix to file name

Save

There are four settings for the client side in IE.

1. The first one is "**Stream Options**" for users to determine which stream to be streaming. This product supports dual-stream. Therefore, there are two streams to choose.

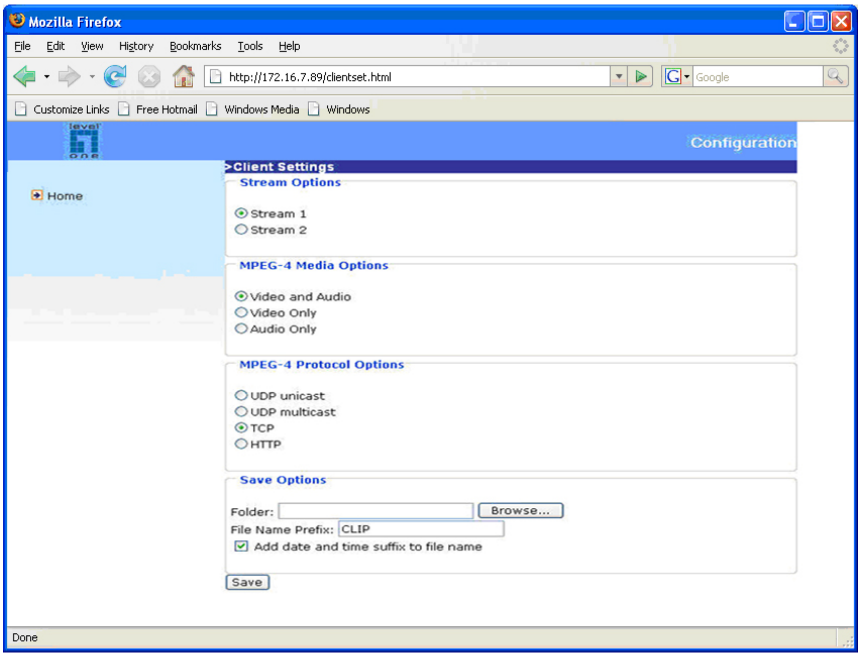
2. The second one is "**MPEG-4 Media Options**" for users to determine which media to be streaming under MPEG-4 mode.

3. The third one is "**MPEG-4 Protocol Options**" which allows choices on connection protocol between client and server. There are four protocols choices to optimize your usage – UDP unicast, UDP multicast, TCP and HTTP.
   - The **UDP unicast** protocol allows for more real-time audio and video streams. However, some packets may be lost due to network burst traffic and images may be obscured.
   - The **UDP multicast** protocol allows to save the bandwidth of server while serving multiple clients at the same time.
   - The **TCP** protocol allows for less packet loss and produces a more accurate video display. The downside with this protocol is that the real-time effect is worse than that with the UDP protocol.
   - The **HTTP** protocol allows the same quality as TCP protocol and the user don't need to open specific port to streaming under some network environment.

If no special need is required, UDP unicast protocol is recommended. Generally speaking, the client's choice will be in the order of UDP multicast → UDP unicast → TCP → HTTP. After the Network Camera is connected successfully, "Protocol Option" will indicate the selected protocol. The selected protocol will be recorded in the user's PC and will be used for the next connection. If the network environment is changed, or the user wants to let the web browser to detect again, manually select the UDP protocol, save, and return HOME to re-connect.

4. The fourth one is “**Save Options**”. User can specify the recording folder, file name prefix and suffix here.

There is only one setting “**Stream Options**” for the client side in Firefox. User can choose to view stream1 and stream2.



>Client Settings

Stream Options

● Stream 1
○ Stream 2

MPEG-4 Media Options

● Video and Audio
○ Video Only
○ Audio Only

MPEG-4 Protocol Options

○ UDP unicast
○ UDP multicast
● TCP
○ HTTP

Save Options

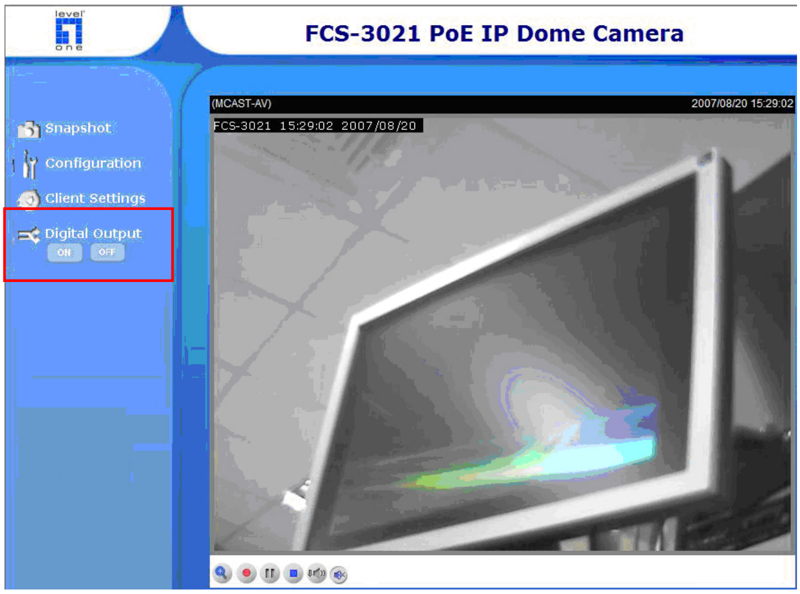
Folder: Browse...
File Name Prefix: CLIP
☑ Add date and time suffix to file name

Save

<url> *http://<Network Camera>/clientset.html* <Network Camera> is the domain name or the original IP address of the Network Camera.

Digital output

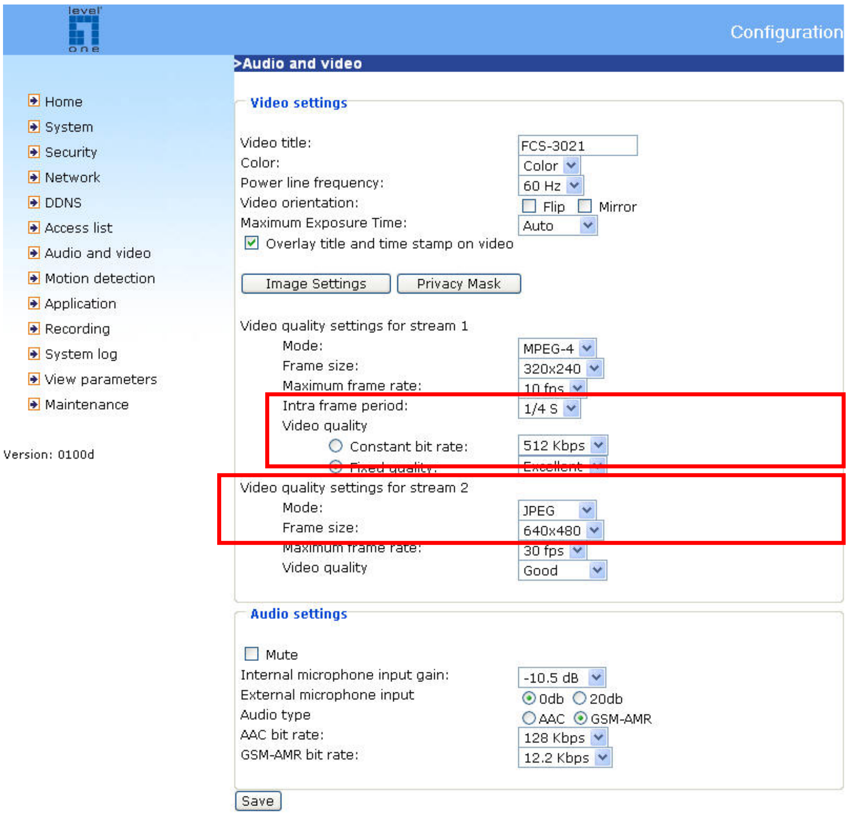
Click on “ON”, the digital output of the Network Camera will be triggered. Or, clicking on “OFF” can let the digital output turn into normal state.



Administrator’s capability

Fine-tuning for Best Performance

Best performance generally equates to the fastest image refresh rate with the best video quality, and at the lowest network bandwidth as possible. The three factors, “Maximum frame rate”, “Constant bit rate”, and “Fixed quality” for MPEG-4 mode and “Maximum frame rate” and “Fixed quality” for JPEG mode on the Audio and Video Configuration page, are correlative to allow for achieving the best performance possible.



>Audio and video

Video settings

Video title: FCS-3021
Color: Color
Power line frequency: 60 Hz
Video orientation: □ Flip □ Mirror
Maximum Exposure Time: Auto
☑ Overlay title and time stamp on video

Video quality settings for stream 1
Mode: MPEG-4
Frame size: 320x240
Maximum frame rate: 10 fps
Intra frame period: 1/4 S
Video quality
○ Constant bit rate: 512 Kbps
○ Fixed quality: Excellent

Video quality settings for stream 2
Mode: JPEG
Frame size: 640x480
Maximum frame rate: 30 fps
Video quality Good

Audio settings

□ Mute
Internal microphone input gain: -10.5 dB
External microphone input ● 0db ○ 20db
Audio type ○ AAC ● GSM-AMR
AAC bit rate: 128 Kbps
GSM-AMR bit rate: 12.2 Kbps

For Viewing by Mobile Phone

Most 3GPP cell phone supports media streaming with MPEG4 video and GSM-AMR audio. Due to the limitation of the bandwidth for 3GPP, only 176x144 video solution will be supported for cell phone viewing. Please set related video settings first as mentioned when viewing by mobile phone.

For Best Real-time Video Images

To achieve good real-time visual effect, the network bandwidth should be large enough to allow a transmission rate of greater than 20 image frames per second. If the broadband network is over 1 Mbps, set the “Constant bit rate” to 1000Kbps or 1200Kbps, or set “Fixed quality” at the highest quality. The maximum frame rate is 30. If your network bandwidth is more than 512Kbps, you can adjust the bit rate according to your bandwidth and set the maximum frame rate to 30 fps. If the images vary dramatically in your environment, you may want to slow the maximum frame rate down to 20 fps in order to lower the rate of data transmission. This allows for better video quality and the human eyes cannot readily detect the differences between those of 20, 25, or 30 frames per second. If your network bandwidth is below 512 Kbps, set the “Constant bit rate” according to your bandwidth and try to get the best performance by fine-tuning with the “Maximum frame rate”. In a slow network, greater frame rate results in blur images. Video quality performance will vary somewhat due to the number of users viewing on the network; even when the parameters have initially been finely tuned. Performance will also suffer due to poor connectivity because of the network’s burst constraint.

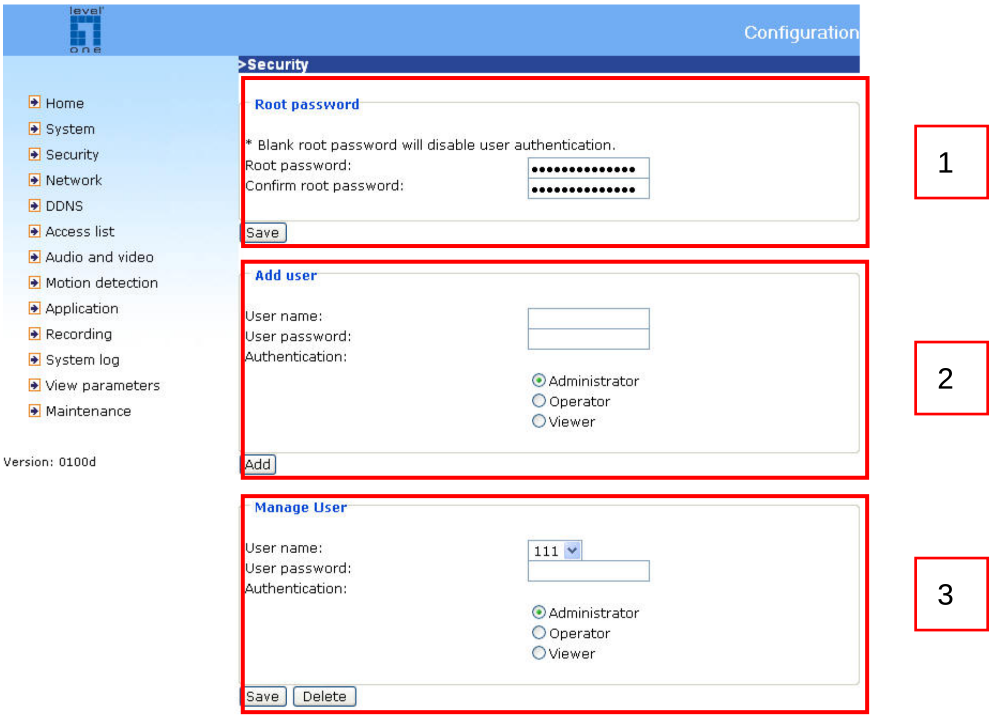
Only Quality Images Will Do

To have the best video quality, you should set “Fixed quality” at “Detailed” or “Excellent” and adjust the “Maximum frame rate” to match your network’s bandwidth. If your network is slow and you receive “broken” pictures, go to the TCP or HTTP protocol in “MPEG-4 Protocol Options” and choose a more appropriate mode of transmission. The images may suffer a time delay due to a slower connection. The delay will also increase with added number of users.

Somewhere Between Real-time and Clear Images

If you have a broadband network, set “Fixed quality” at “Good” or better, rather than setting “Constant bit rate”. You can also fix the bandwidth according to your actual network speed and adjust the frame rate. Start from 30 fps down for best results but not below 15 fps. If the image qualities are not improved, select a lower bandwidth setting.

Opening accounts for new use



Root password

* Blank root password will disable user authentication.

Root password: ••••••••••••••

Confirm root password: ••••••••••••••

Add user

User name:

User password:

Authentication: ● Administrator ○ Operator ○ Viewer

Manage User

User name: 111

User password:

Authentication: ● Administrator ○ Operator ○ Viewer

Protect Network Camera by passwords

The Network Camera is shipped without any password by default. That means everyone can access the Network Camera including the configuration as long as the IP address is known. It is necessary to assign a password if the Network Camera is intended not to be accessed by others. Type a new word twice in ① to enable protection. This password is used to identify the administrator. Then add an account with user name, password and authentication for your friends in ②. You can edit or delete users from ③.

Build a security application

The Administrator can use the built-in motion detection to monitor any movement to perform many useful security applications. To upload the snapshots, users can choose either email, FTP, HTTP or Network storage according to user's needs. All servers setting are in Server section on Application page. Refer to the definition section for detail configuration.

1. Click on "**Configuration**" on homepage,
2. Click on "**Motion detection**" at the left column,
3. Check "Enable motion detection",
4. Click on new to have a new window to monitor video,
5. Type in a name to identify the new window,
6. Use the mouse to click, hold, and drag the window corner to resize or the title bar to move
7. Fine-tune using the "Sensitivity" and "Percentage" fields to best suit the camera's environment. Higher "Sensitivity" detects the slighter motion. Higher "Percentage" discriminates smaller objects,
8. Clicking on "Save" enables the activity display. Green means the motion in the window is under the watermark set by Administrator and red means it is over the watermark,
9. Click on "**Application**" at the left column,
10. Add a server in server section,
11. Add a media with snapshot type in media section. And Set the number of pre-event and post-event images to be uploaded
12. Add a event in event section
    - Enter one event name and enable this event.
    - Check the weekdays as you need and give the time interval to monitor the motion detection every day,
    - Select the Trigger on Motion detection and Check the window name set in step 5
    - Set the appropriate delay time to avoid continuous false alarms following the original event
    - Check the server name set in Step 10 and select the media name set in Step 11.
13. Click on save to validate.

Software revision upgrade

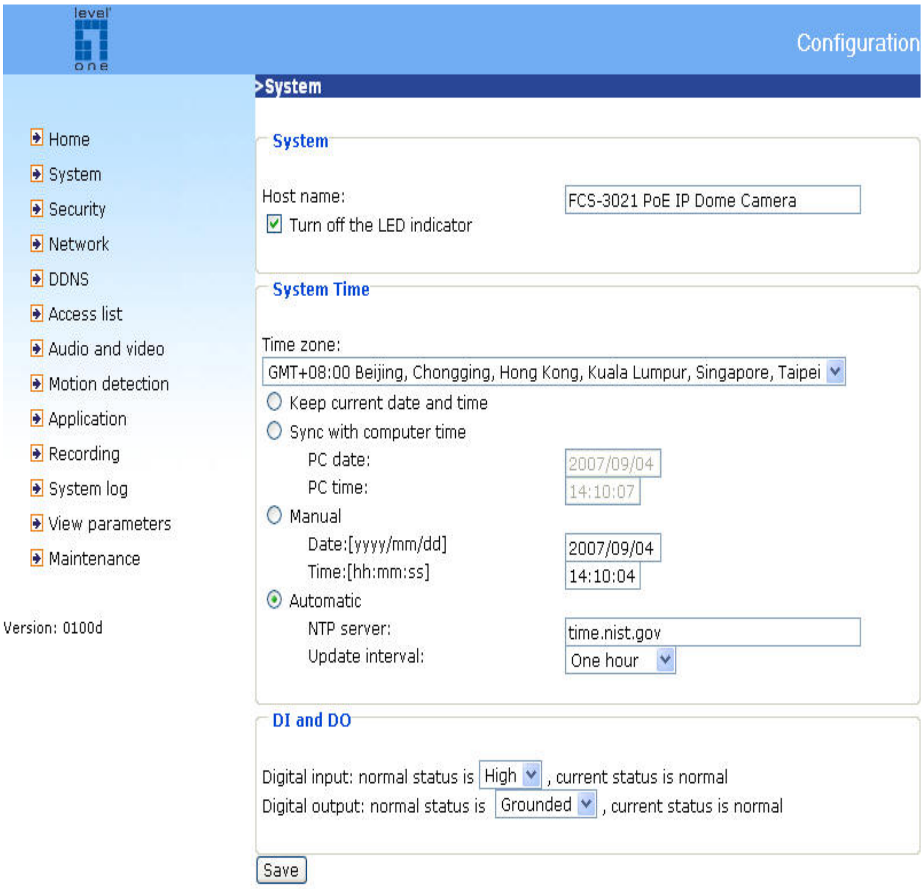
Customers can obtain the up-to-date software from the web site of LevelOne. An easy-to-use Upgrade Wizard is provided to upgrade the Network Camera with just a few clicks. The upgrade function is opened to the Administrator only. To upgrade the system, follow the procedures below.

1. Download the firmware file named “xxx.pkg” from the appropriate product folder.
2. Run the Installation Wizard and proceed following the prompts. Refer to the instructions of the Installation Wizard on CD-ROM for details.
3. Or upgrade firmware from HTTP web page directly.
4. The whole process will finish in a few minutes and it will automatically restart the system.

⚠ If power fails during the writing process of Flash memory, the program in the memory of the Network Camera may be destroyed permanently. If the Network Camera cannot restart properly, ask your dealer for technical service.

Definitions in Configuration

Only the Administrator can access system configuration. Each category in the left column will be explained in the following pages. The bold texts are the specific phrases on the Option pages. The Administrator may type the URL below the figure to directly enter the frame page of configuration. If the Administrator also wants to set certain options through the URL, read the reference appendix for details.



System

Host name: FCS-3021 PoE IP Dome Camera

☑ Turn off the LED indicator

System Time

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

○ Keep current date and time

○ Sync with computer time

PC date: 2007/09/04

PC time: 14:10:07

○ Manual

Date:[yyyy/mm/dd] 2007/09/04

Time:[hh:mm:ss] 14:10:04

● Automatic

NTP server: time.nist.gov

Update interval: One hour

DI and DO

Digital input: normal status is High , current status is normal

Digital output: normal status is Grounded , current status is normal

<url> http://<Network Camera>/setup/system.html

<Network Camera> is the domain name or original IP address of the Network Camera.

System parameters

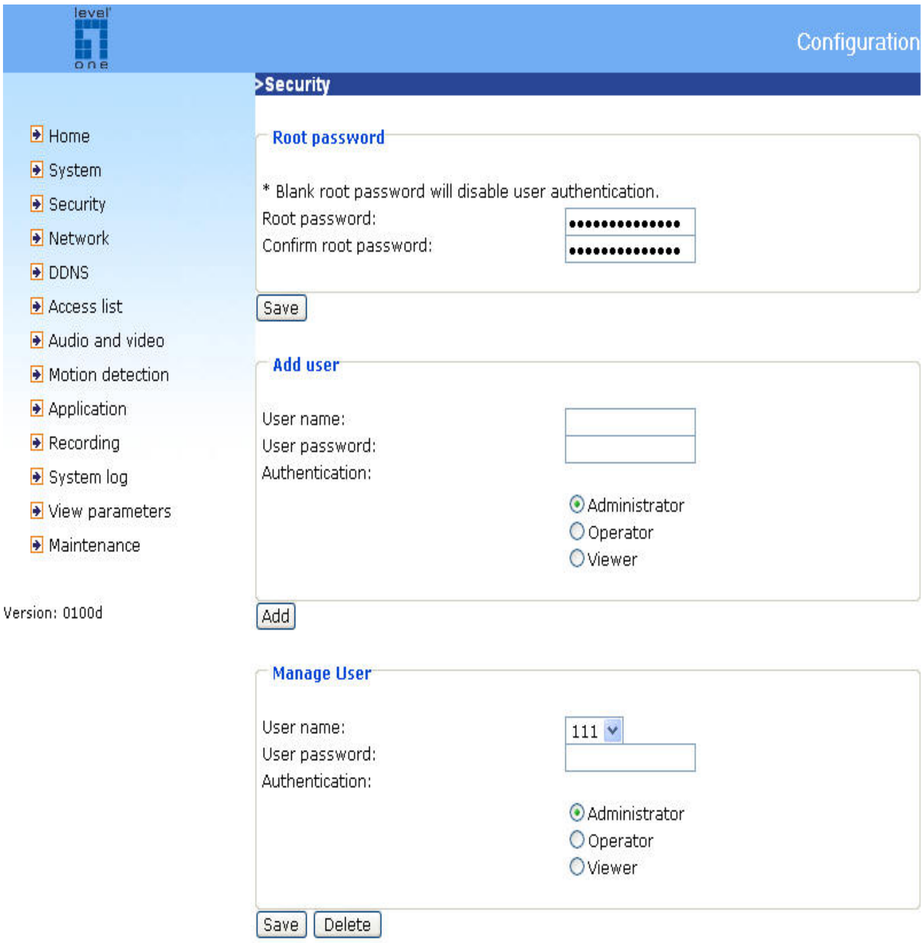
"Host name" The text displays the title at the top of the main page.
“Turn off the LED indicator” Check this option to shut off the LED on the rear. It can prevent the camera’s operation being noticed.
"Time zone" Adjust the time with that of the time-servers for local settings.
"Keep current date and time" Click on this to reserve the current date and time of the Network Camera. An internal real-time clock maintains the date and time even when the power of the system is turned off.
"Sync with computer time" 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” Adjust the date and time according to what is entered by the Administrator. Notice the format in the related fields while doing the entry.
Network Camera starts up. It will fail if the assigned time-server cannot be reached.
“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 hourly, daily, weekly, or monthly update with the time on the NTP server.
“**Digital input**” Select High or Low to define normal status of the digital input. The current status is shown, too.
“**Digital output**” Select Grounded or Open to define normal status of the digital output. The current status is shown, too.

Security settings

"Root password" Change the Administrator's password by typing in the new password identically in both text boxes. The typed entries will be displayed as asterisks for security purposes. After pressing Save, the web browser will ask the Administrator for the new password for access.

"Add user" Type the new user's name and password and press Add to insert the new entry. The new user will be displayed in the user name list. There is a maximum of twenty user accounts. There are three kinds of authentication: Administrator, Operator and Viewer. Administrator can fully control the camera operation. Operator's access right can modify most of camera's parameters except some privilege and network options. Viewer can view, listen to camera; control DIDO of camera. Network Camera can provide twenty accounts for your valuable customers or friends.

"Manage user" Pull down the user list to find the user's name and press Delete to delete the selected user. Or edit the password or authentication of the selected user and press Save to take effect.



Root password

* Blank root password will disable user authentication.

Root password: ••••••••••••••

Confirm root password: ••••••••••••••

Add user

User name:

User password:

Authentication:

● Administrator
○ Operator
○ Viewer

Manage User

User name: 111

User password:

Authentication:

● Administrator
○ Operator
○ Viewer

<url> http://<Network Camera>/setup/security.html

<Network Camera> is the domain name or original IP address of the Network Camera.

Network settings

Any changes made on the Network type section will restart the system in order to validate the changes. Make sure every field is entered correctly before clicking on Save.

Network type

“LAN” & **“PPPoE”**
The default type is LAN. Select PPPoE if using ADSL
"Get IP address automatically" & “Use fixed IP address”
The default status is “**Get IP address automatically**”. This can be tedious having to perform software installation whenever the Network Camera starts. Therefore, once the network settings, especially the IP address, have been entered correctly, select “**Use fixed IP address**” then the Network Camera will skip installation at the next boot. The Network Camera can automatically restart and operate normally after a power outage. Users can run IP installer to check the IP address assigned to the Network Camera if the IP address is forgotten or using the UPnP function provided by the Network Camera (MS Windows XP provides UPnP function at **My Network Place**). **“IP address”** This is necessary for network identification.
“Subnet mask” This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.
“Default router” This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.
“Primary DNS” The primary domain name server that translates hostnames into IP addresses.
“Secondary DNS” Secondary domain name server that backups the Primary DNS.
“Primary WINS server” The primary WINS server that maintains the database of computer name and IP address.
“Secondary WINS server” The secondary WINS server that maintains the database of computer name and IP address.
“Enable UPnP presentation” Enable the UPnP camera short cut.
“**Enable UPnP port forwarding**” Enable UPnP port forwarding
“PPPoE” If using the PPPoE interface, fill the following settings from ISP
“User name” The login name of PPPoE account
“Password” The password of PPPoE account
“Confirm password” Input password again for confirmation

HTTP

“Authentication” It supports basic and digest modes.

“HTTP port” This can be other than the default Port 80. Once the port is changed, the users must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Network Camera whose IP address is 192.168.0.100 from 80 to 8888, the users must type in the web browser “http://192.168.0.100:8888” instead of “http://192.168.0.100”.

“Secondary HTTP port” It support alternate port to access HTTP server.

“Access name for stream 1” This is the access URL of stream 1 for making connection from client software when its codec type is JPEG.

“Access name for stream 2” This is the access URL of stream 2 for making connection from client software when its codec type is JPEG.

Using http://<ip address>:<http port>/<access name> to make connection.

FTP

“FTP port” This can be other than the default port 21. The user can change this value from 1025 to 65535. After the changed, the external FTP client program must change the server port of connection accordingly.

RTSP Streaming

“Authentication” It supports disable, basic and digest modes.

“Access name for stream 1” This is the access URL of stream 1 for making connection from client software when the codec type is MPEG-4.

“Access name for stream 2” This is the access URL of stream 2 for making connection from client software when the codec type is MPEG-4.

Using rtsp://<ip address>/<access name> to make connection

“RTSP port” This can be other than the default Port 554

“RTP port for video” The video channel port for RTP. It must be an even number.

“RTCP port for video” The video channel port for RTCP. It must be the port number of video RTP plus 1.

“RTP port for audio” The audio channel port for RTP. It must be an even number.

“RTCP port for audio” The audio channel port for RTCP. It must be the port number of audio RTP plus 1.

User can modify Multicast setting for stream1 and stream2.

“Always multicast” Select it to enable multicast always.

“Multicast group address” It is used by sources and the receivers to send and receive content.

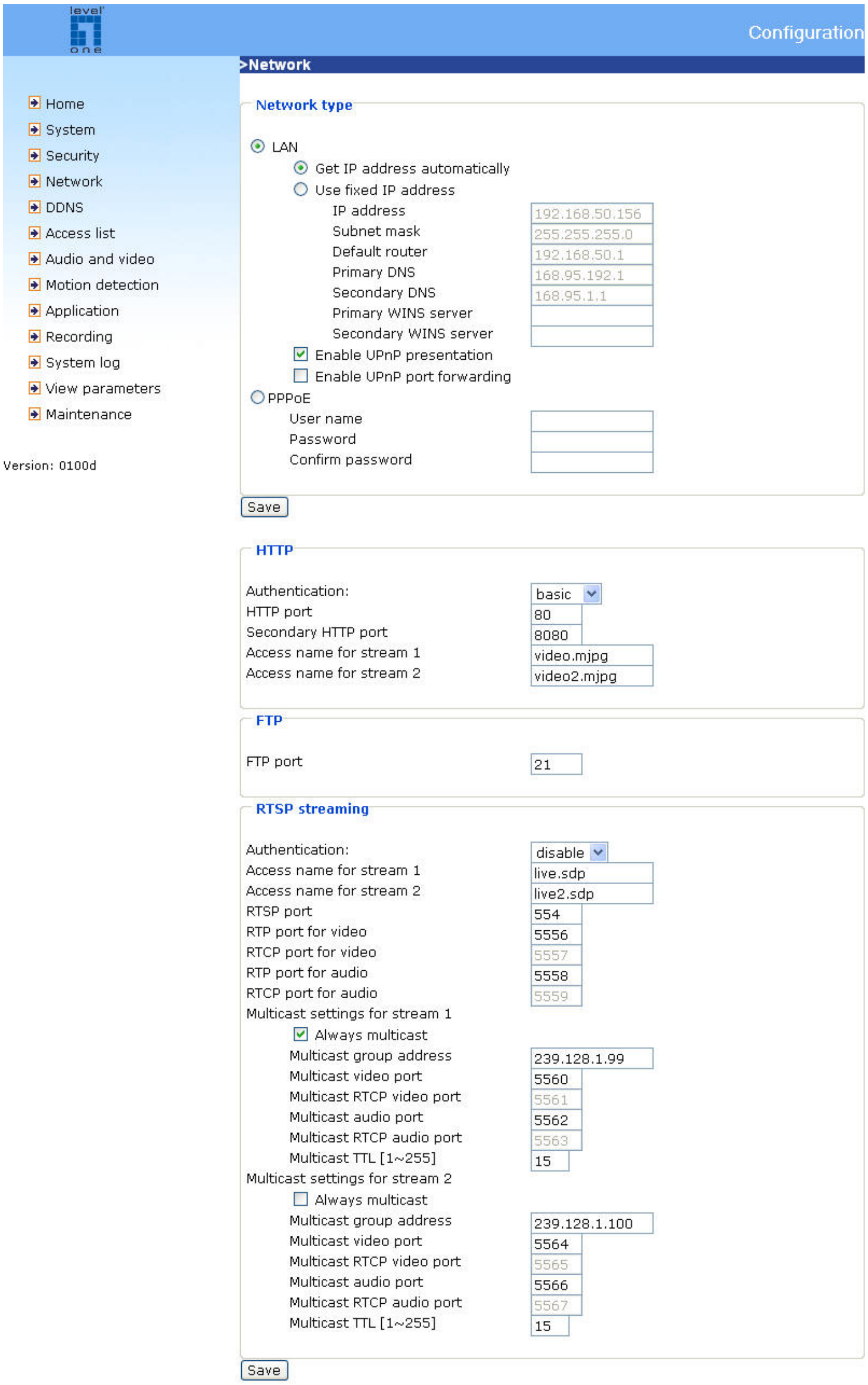
“Multicast video port” The video channel port for multicast. It must be an even number.

“Multicast RTCP video port” The video channel port for multicast RTCP. It must be the port number of multicast video port plus 1.

“Multicast audio port” The audio channel port for multicast. It must be an even number.

“Multicast RTCP audio port” The audio channel port for multicast RTCP. It must be the port number of multicast audio port plus 1.

“Multicast TTL” It specifies the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.



>Network

Network type

● LAN

● Get IP address automatically
○ Use fixed IP address

IP address	192.168.50.156
Subnet mask	255.255.255.0
Default router	192.168.50.1
Primary DNS	168.95.192.1
Secondary DNS	168.95.1.1
Primary WINS server	
Secondary WINS server	

☑ Enable UPnP presentation
□ Enable UPnP port forwarding

○ PPPoE

User name	
Password	
Confirm password	

HTTP

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

FTP

FTP port	21

RTSP streaming

Authentication:	disable
Access name for stream 1	live.sdp
Access name for stream 2	live2.sdp
RTSP port	554
RTP port for video	5556
RTCP port for video	5557
RTP port for audio	5558
RTCP port for audio	5559
Multicast settings for stream 1	
☑ Always multicast	
Multicast group address	239.128.1.99
Multicast video port	5560
Multicast RTCP video port	5561
Multicast audio port	5562
Multicast RTCP audio port	5563
Multicast TTL [1~255]	15
Multicast settings for stream 2	
□ Always multicast	
Multicast group address	239.128.1.100
Multicast video port	5564
Multicast RTCP video port	5565
Multicast audio port	5566
Multicast RTCP audio port	5567
Multicast TTL [1~255]	15

<url> *http://<Network Camera>/setup/network.html*

<Network Camera> is the domain name or original IP address of the Network Camera.

DDNS

“Enable DDNS” This option turns on the DDNS function.

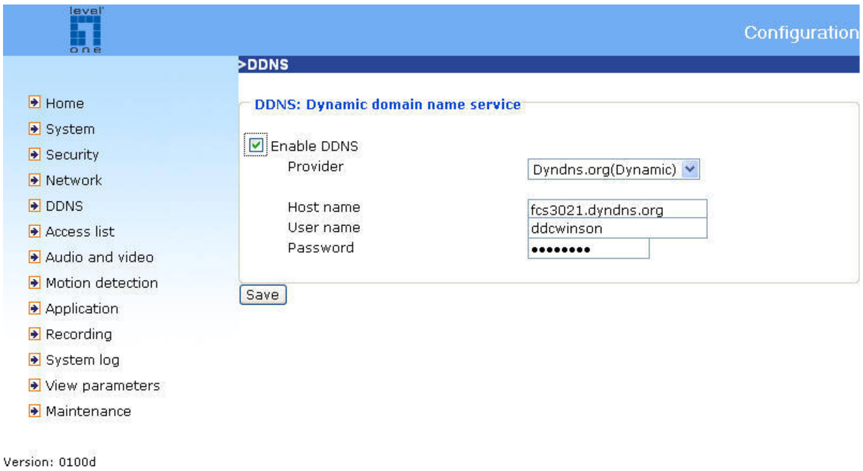
“Provider” The provider list contains seven hosts that provide DDNS services. Please connect to the service provider’s website to make sure the service charges.

“Host Name” If the User wants to use DDNS service, this field must be filled. Please input the hostname that is registered in the DDNS server.

“Username/E-mail” The Username or E-mail field is necessary for logging in the DDNS server or notify the User of the new IP address. Note: when this field is input as “Username” the following field must be input as “Password”.

“Password/Key” Please input the password or key to get the DDNS service.

“**Save**” Click on this button to save current settings for the DDNS service and UPnP function.



>DDNS

DDNS: Dynamic domain name service

☑ Enable DDNS

Provider: Dyndns.org(Dynamic)

Host name: fcs3021.dyndns.org

User name: ddcwinson

Password: ••••••••

Version: 0100d

<url> http://<Network Camera>/setup/ddns.html

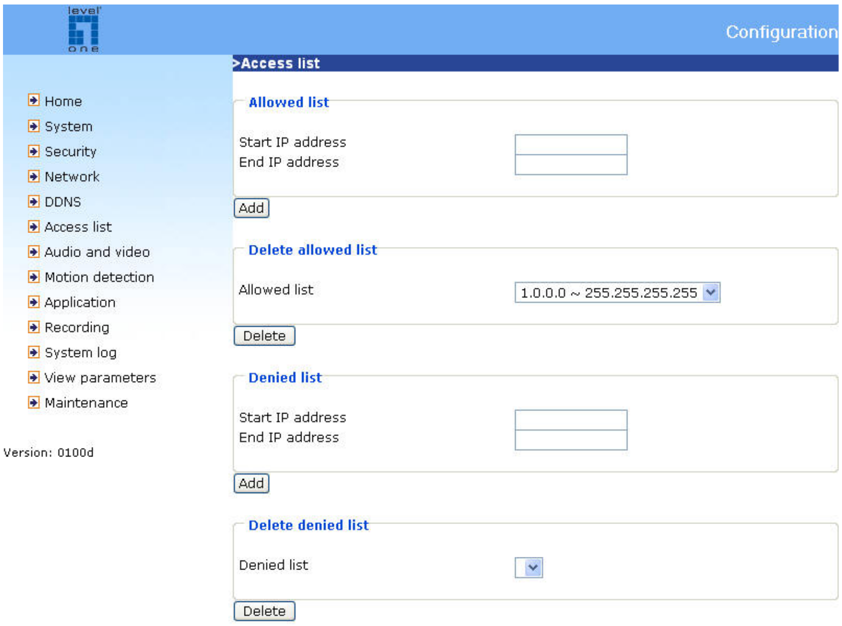
<Network Camera> is the domain name or original IP address of the Network Camera.

Access List

The access list is to control the access permission of clients by checking the client IP address. There are two lists for permission control: **Allow List** and **Deny List**. Only those clients whose IP address is in the **Allow List** and not in the **Deny List** can connect to the Video Server or Network Camera for receiving the audio/video streaming.

Both **Allow List** and **Deny List** consist of a list of IP ranges. If you want to add a new IP address range, type the **Start IP Address** and **End IP Address** in the text boxes and click on the **Add** button. If you want to remove an existing IP address range, just select from the pull-down menu and click on the **Delete** button.

Both the Allow List and Deny List can have 10 entries.



<url> http://<Network Camera>/setup/accesslist.html

<Network Camera> is the domain name or original IP address of the Network Camera.

Audio and Video

This product supports dual-stream. It provides two setting for video streams, but only one setting for audio.

Video Settings

“Video title” The text string can be displayed on video

“Color” Select either for color or monochrome video display.

“Power line frequency” The fluorescent light will flash according to the power line frequency that depends on local utility. Change the frequency setting to eliminate uncomfortable flash image when the light source is only fluorescent light.

“Video orientation”

- **Flip:** Vertically rotate the video.
- **Mirror:** Horizontally rotate the video. Check options both if the Network Camera is installed upside down.

“White balance” Adjust the value for best color temperature.

“Maximum Exposure Time” Adjust the maximum exposure time in different environment.

- **Overlay title and time stamp on video:** Check it the title is shown on video.

There are different video quality settings for stream1 and stream2.

- **Mode:** It can be MPEG-4 or JPEG. If MPEG-4 is selected, it is streamed in RTSP protocol. If JPEG is selected, it is streamed in server push mode.
- **Frame size:** If the mode is MPEG-4, there are three options, **“176x144”, “320x240”** and **“640x480”**. If the mode is JPEG, there are three options, **“176x144”, “320x240”** and **“640x480”.**

There are three dependent parameters provided in MPEG-4 mode for video performance adjustment.

“Intra frame period” The interval of intra frame.

“Maximum frame rate” This limits the maximal refresh frame rate, which can be combined with the **“Video quality”** to optimize bandwidth utilization and video quality. Choose “**Constant bit rate**” If the user wants to fix the bandwidth utilization regardless of the video quality, choose **“Fixed quality”** and select the desired bandwidth. The video quality may be poor due to the sending of maximal frame rate within the limited bandwidth when images are moving rapidly. Consequently, to ensure detailed video quality (quantization rate) regardless of the network, it will utilize more bandwidth to send the maximal frames when images change drastically.

In JPEG mode, user can set **"Maximum frame rate"** and **"Video quality"** to adjust the video performance.

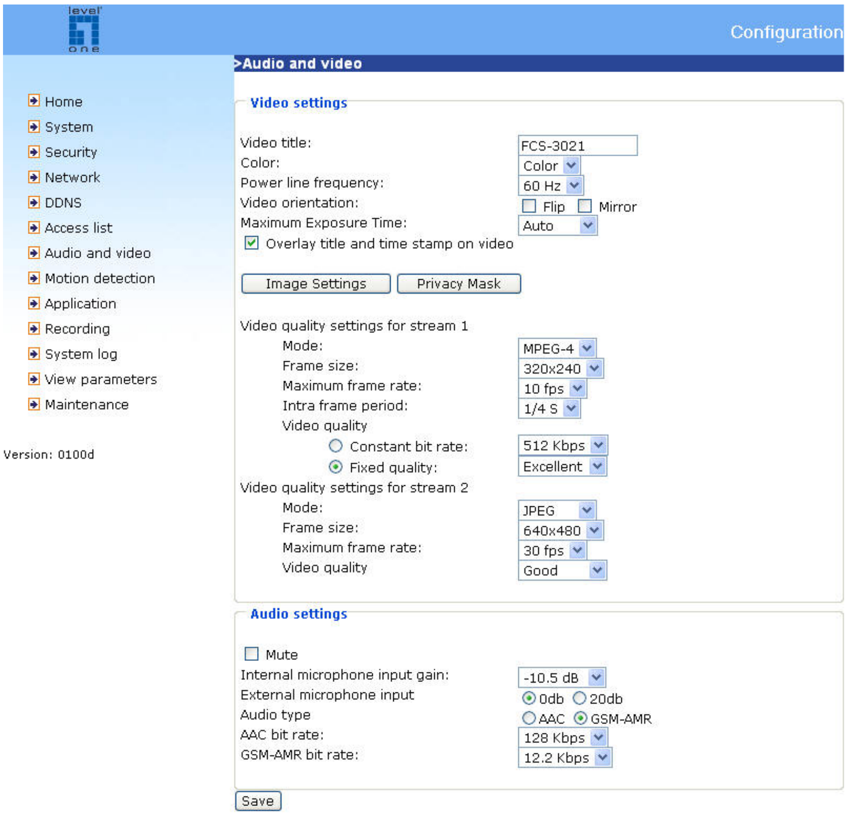
Audio settings

"Mute" Turn off audio.

"Internal microphone input gain" Modify the gain of the internal audio input.

"External microphone input" There are two gain options, 0db and 20db.

"Audio type" Select audio codec **"AAC"** or **"GSM-AMR"** and the bit rate.



Video settings

Video title: FCS-3021
Color: Color
Power line frequency: 60 Hz
Video orientation: □ Flip □ Mirror
Maximum Exposure Time: Auto
☑ Overlay title and time stamp on video

Video quality settings for stream 1
Mode: MPEG-4
Frame size: 320x240
Maximum frame rate: 10 fps
Intra frame period: 1/4 S
Video quality
○ Constant bit rate: 512 Kbps
● Fixed quality: Excellent

Video quality settings for stream 2
Mode: JPEG
Frame size: 640x480
Maximum frame rate: 30 fps
Video quality: Good

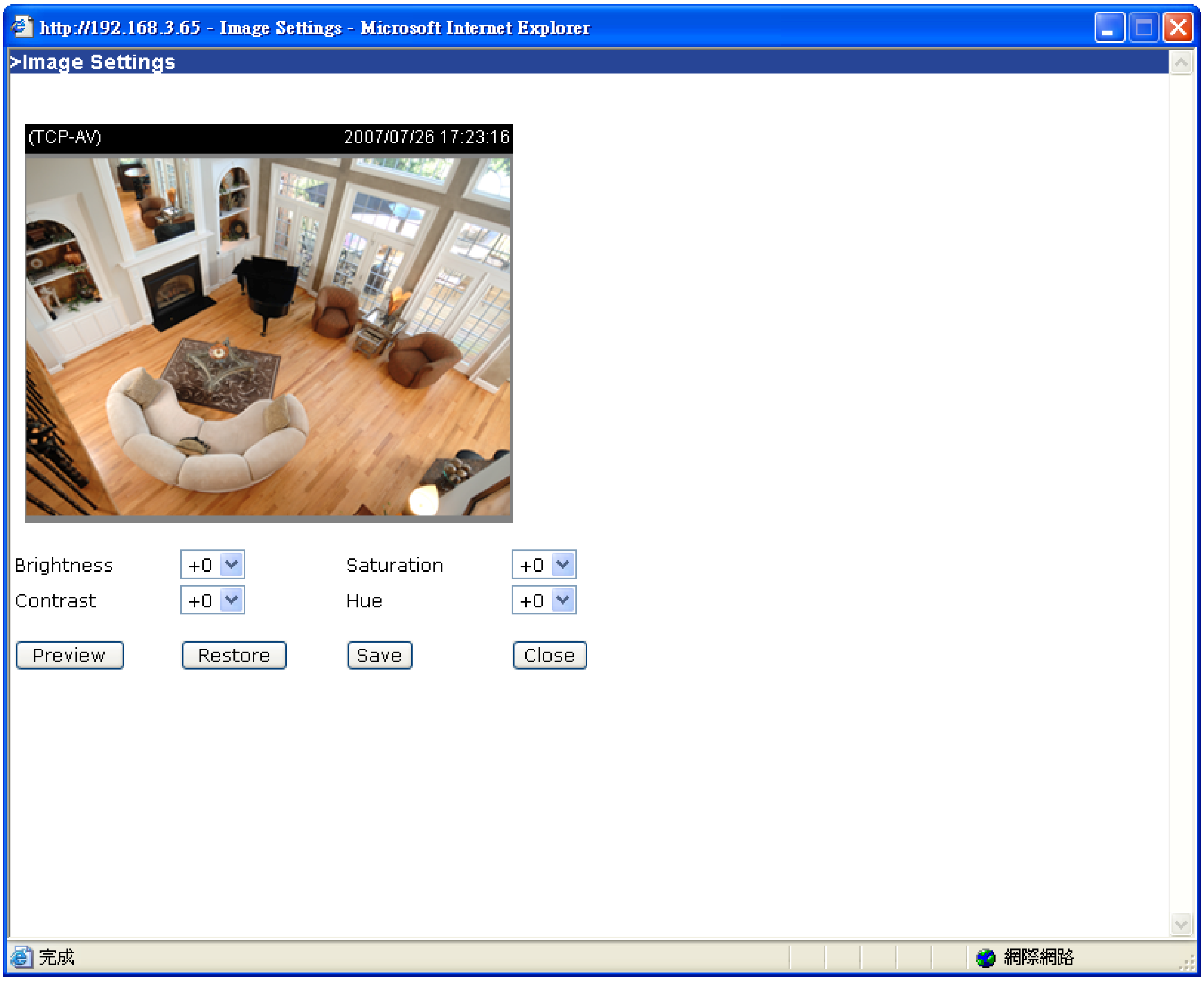
Audio settings

□ Mute
Internal microphone input gain: -10.5 dB
External microphone input: ● 0db ○ 20db
Audio type: ○ AAC ● GSM-AMR
AAC bit rate: 128 Kbps
GSM-AMR bit rate: 12.2 Kbps

<url> *http://<Network Camera>/setup/audiovideo.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

Image Settings



http://192.168.3.65 - Image Settings - Microsoft Internet Explorer

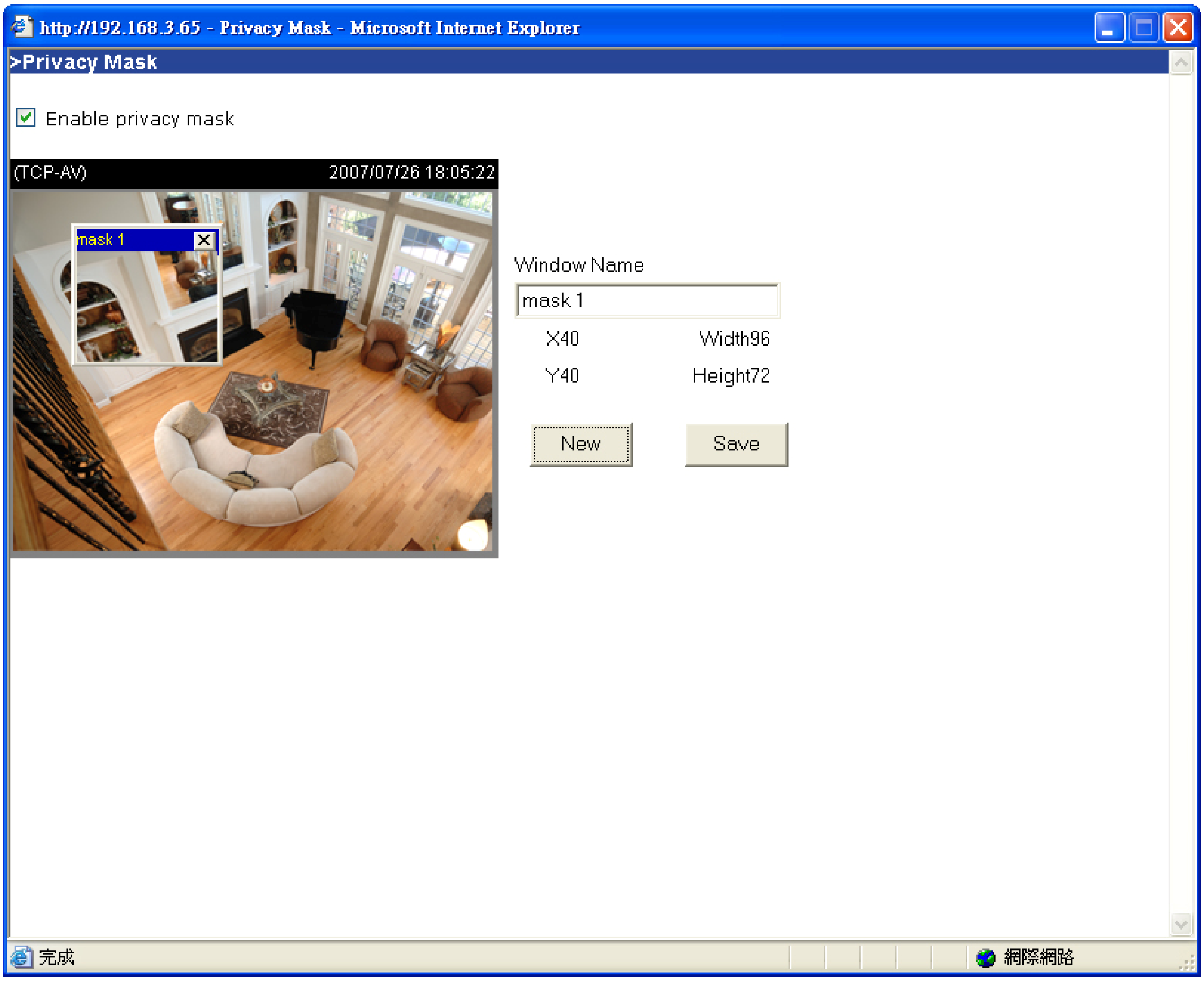
>Image Settings

(TCP-AV) 2007/07/26 17:23:16

Brightness	+0	Saturation	+0
Contrast	+0	Hue	+0

Image Settings Click on this button to pop up another window to tune **"Brightness"**, **"Contrast"**, **"Hue"** and **"Saturation"** for video compensation. Each field has eleven levels ranging from -5 to +5. In **"Brightness"** and **"Contrast"** fields the value 0 indicates auto tuning. The user may press Preview to fine-tune the image. When the image is O.K., press Save to set the image settings. Click on Restore to recall the original settings without incorporating the changes.

Privacy Mask



http://192.168.3.65 - Privacy Mask - Microsoft Internet Explorer

>Privacy Mask

☑ Enable privacy mask

Window Name: mask 1

X40 Width96

Y40 Height72

Click on the button to pop up another window to set privacy mask window. All users can not view the block under privacy mask window.

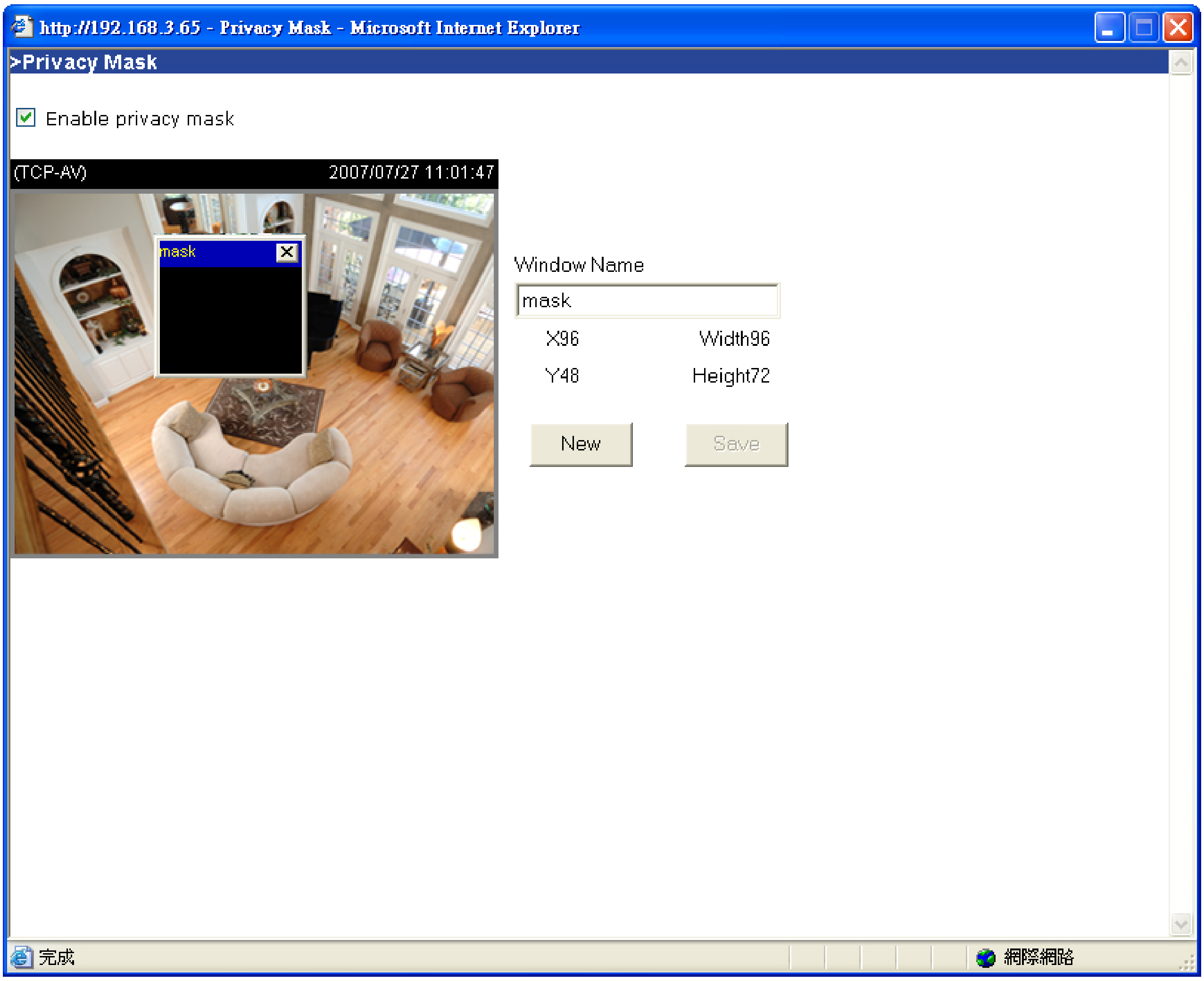
“Enable privacy mask” Check this option to turn on privacy mask.

New Click on this button to add a new window. At most five windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the ‘x’ at the upper right-hand corner of the window deletes the window. Remember to click save in order to validate the changes. The base of window axis is eight. You can see the X, Y, width and height of the window.

Save Click on this button to save the related window settings.

"Window Name" The text will show at the top of the window.

The following figure shows the screen when Save is clicked and the privacy mask is enabled.



http://192.168.3.65 - Privacy Mask - Microsoft Internet Explorer

>Privacy Mask

☑ Enable privacy mask

(TCP-AV) 2007/07/27 11:01:47

mask

Window Name: mask

X96 Width96

Y48 Height72

Motion detection

"Enable motion detection" Check this option to turn on motion detection.

New Click on this button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right-hand corner of the window deletes the window. Remember to save in order to validate the changes.

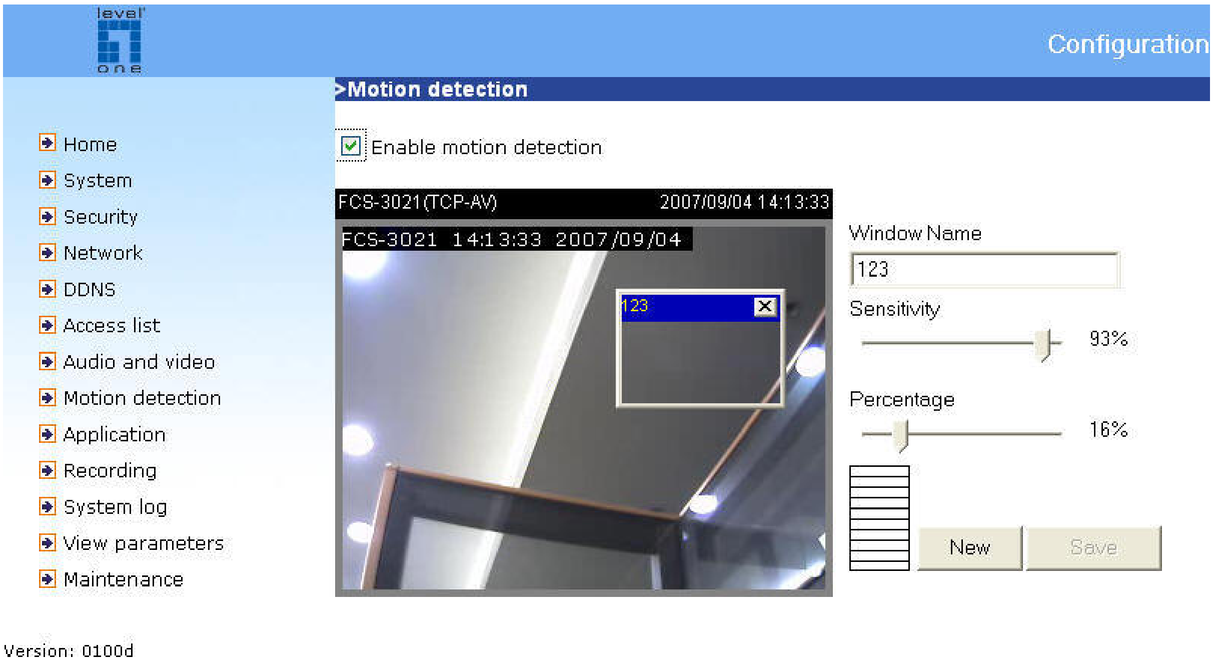
Save Click on this button to save the related window settings. A graphic bar will rise or fall depending on the image variation. A green bar means the image variation is under monitoring level and a red bar means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

"Window Name" The text will show at the top of the window.

"Sensitivity" This sets the endurable difference between two sequential images.

"Percentage" This sets the space ratio of moving objects in the monitoring window. Higher sensitivity and small percentage will allow easier motion detection.

The following figure shows the screen when Save is clicked.



>Motion detection

☑ Enable motion detection

Window Name: 123

Sensitivity: 93%

Percentage: 16%

<url> *http://<Network Camera>/setup/motion.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

Application

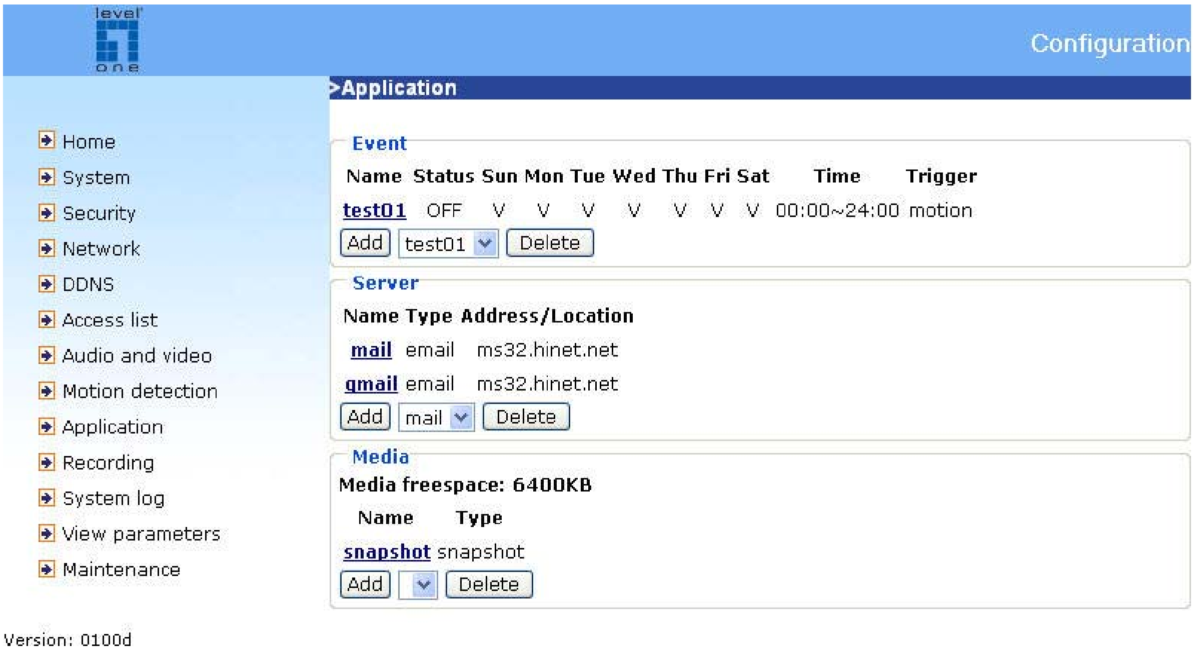
There are three sections in application page. They are event, server and media. Click [Add] to pop a window to add a new item of event, server or media. Click [Delete] to delete the selected item from event, server or media. Click on the item name to pop a window to edit it.

There can be at most three events. There can be at most five server and five media configurations.

User can know the event name, status, weekly and time schedule and trigger type in event section. The server name, type and address/location are shown in server section.

The current media free space, media name and type are shown in media section. After adding a new media, the value of free space will be updated. User cannot add media which size is larger than media free space.

It is suggested to set server and media first before setting event. The servers and medias selected in event list are not modified or deleted. Please remove them first from the event if you want to delete or modify them. Recommend that using different media in different event to make use all media be produced and received correctly. If using the same media in different events and the events trigger almost simultaneously, the servers in the second triggered event will not receive any media; there would be only notifications.



>Application

Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
test01	OFF	V	V	V	V	V	V	V	00:00~24:00	motion

Server

Name	Type	Address/Location
mail	email	ms32.hinet.net
gmail	email	ms32.hinet.net

Media

Media freespace: 6400KB

Name	Type
snapshot	snapshot

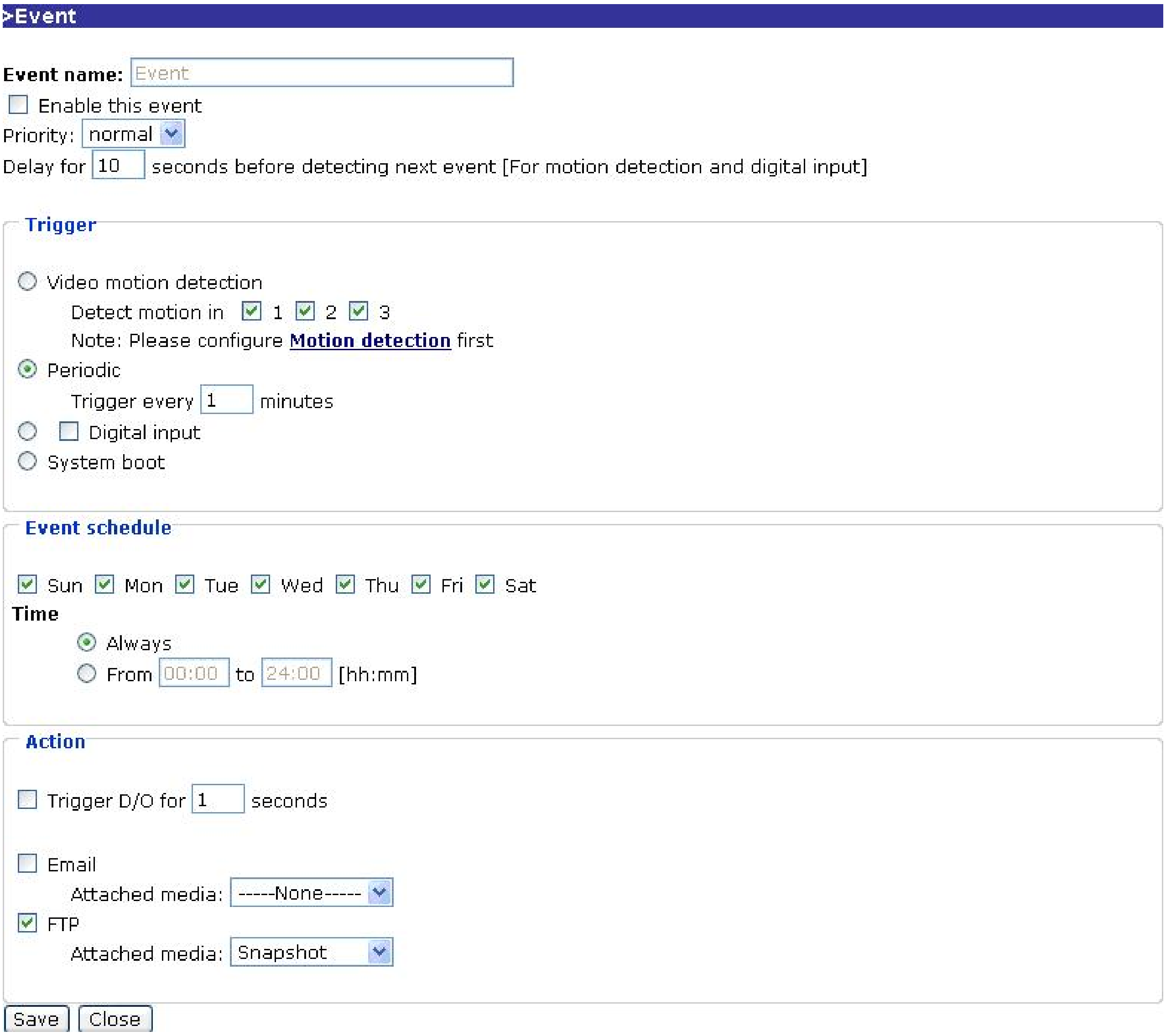
Version: 0100d

<url> *http://<Network Camera>/setup/application.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

Event

“Event name” The unique name for event
“Enable this event” Check it to enable this event.
“Priority” The event with higher priority will be executed first.
“Delay second(s) before detecting next event” The delay to check next event. It is used in motion detection and digital input trigger type.
There are four kinds of trigger supported.
“Video motion detection” Select the windows which need to be monitored.
“Periodic” The event is triggered in specified intervals. The unit of trigger interval is minute.
“Digital input” To monitor digital input
“System boot” The event is triggered when the system boots up.
The weekly and time schedules are provided.
“Sun” ~ “Sat” Select the days of the week to perform the event.
“Time” show **“Always”** or input the time interval.
The default action is triggering DO. If there are servers configured, the user can select them from **“Server name”**, too.
“Trigger DO” Check it to trigger digital output for specific seconds when event is triggered.
“Server name” Check it to sending the selected media when event is triggered.



>Event

Event name: Event

□ Enable this event

Priority: normal

Delay for 10 seconds before detecting next event [For motion detection and digital input]

Trigger

○ Video motion detection

Detect motion in ☑ 1 ☑ 2 ☑ 3

Note: Please configure **Motion detection** first

● Periodic

Trigger every 1 minutes

○ □ Digital input

○ System boot

Event schedule

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

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Action

□ Trigger D/O for 1 seconds

□ Email

Attached media: -----None-----

☑ FTP

Attached media: Snapshot

Server

"Server name" The unique name for server

There are four kinds of servers supported. They are email server, FTP server, HTTP server and network storage.

Here is setting for email server.

"Sender email address" The email address of the sender

"Recipient email address" The email address of the recipient

"Server address" The domain name or IP address of the external email server.

"User name" This granted user name on the external email server.

"Password" This granted password on the external email server.

Here is setting for FTP server.

"Server address" The domain name or IP address of the external FTP server.

"Server port" This can be other than the default port 21. The user can change this value from 1025 to 65535.

"User name" This granted user name on the external FTP server.

"Password" This granted password on the external FTP server.

"Remote folder name" Granted folder on the external FTP server. The string must conform to that of the external FTP server. Some FTP servers cannot accept preceding slash symbol before the path without virtual path mapping. Refer to the instructions for the external FTP server for details. The folder privilege must be open for upload.

"Passive Mode" Check it to enable passive mode in transmission.

Here is setting for HTTP server.

"URL" The URL to upload the media.

"User name" This granted user name on the external HTTP server.

"Password" This granted password on the external HTTP server.

Here is setting for network storage. Only one network storage is supported.

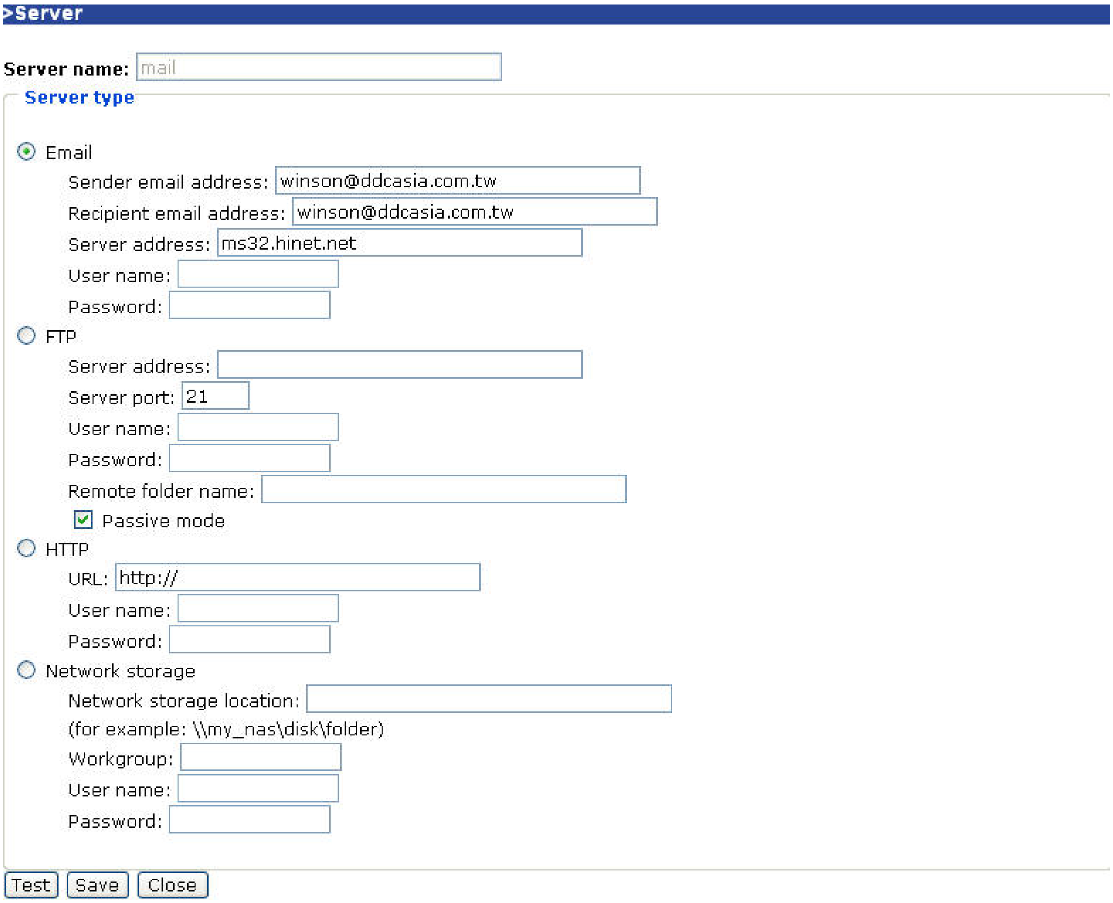
"Network storage location" The path to upload the media

"Workgroup" The workgroup for network storage.

"User name" This granted user name on the network storage.

"Password" This granted password on the network storage.

After input the setting of server, user can click on Test to test whether the setting is correct. The testing result will be shown in a pop-up window.



>Server

Server name: mail

Server type

● Email

Sender email address: winson@ddcasia.com.tw

Recipient email address: winson@ddcasia.com.tw

Server address: ms32.hinet.net

User name:

Password:

○ FTP

Server address:

Server port: 21

User name:

Password:

Remote folder name:

☑ Passive mode

○ HTTP

URL: http://

User name:

Password:

○ Network storage

Network storage location:

(for example: \\my_nas\disk\folder)

Workgroup:

User name:

Password:

Media

"Media name" The unique name for media

There are three kinds of media. They are snapshot, video clip and system log.

Here is setting for snapshot.

"Source" The source of stream, stream1 or stream2.

"Send pre-event images" The number of pre-event images

"Send post-event images" The number of post-event images

"File Name Prefix" The prefix name will be added on the file name of the snapshot images.

"Add date and time suffix to file name" Check it to add timing information as file name suffix.

Here is setting for video clip

"Source" The source of stream, stream1 or stream2.

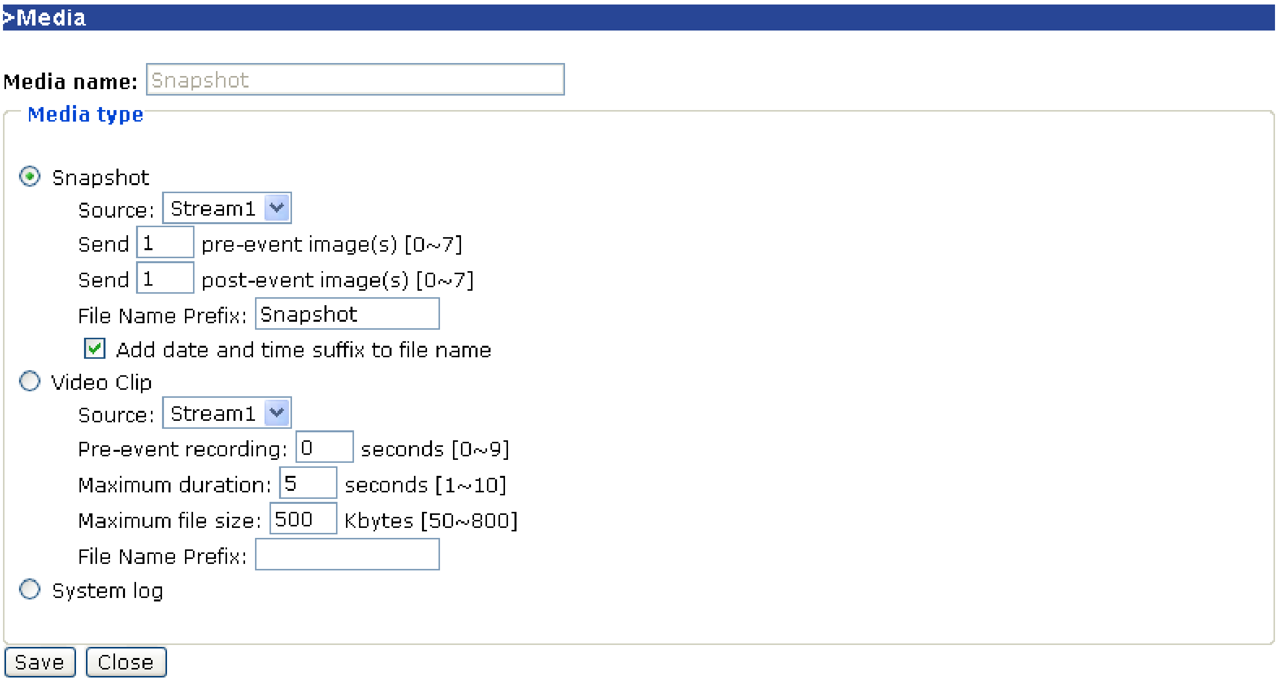
"Pre-event recording" The interval of pre-event recording in seconds

There are two limitations for video clip file.

"Maximum duration" The maximal recording file duration in seconds

"Maximum file size" The maximal file size would be generated.

“File name prefix” The prefix name will be added on the file name of the video clip.



>Media

Media name: Snapshot

Media type

● Snapshot

Source: Stream1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File Name Prefix: Snapshot

☑ Add date and time suffix to file name

○ Video Clip

Source: Stream1

Pre-event recording: 0 seconds [0~9]

Maximum duration: 5 seconds [1~10]

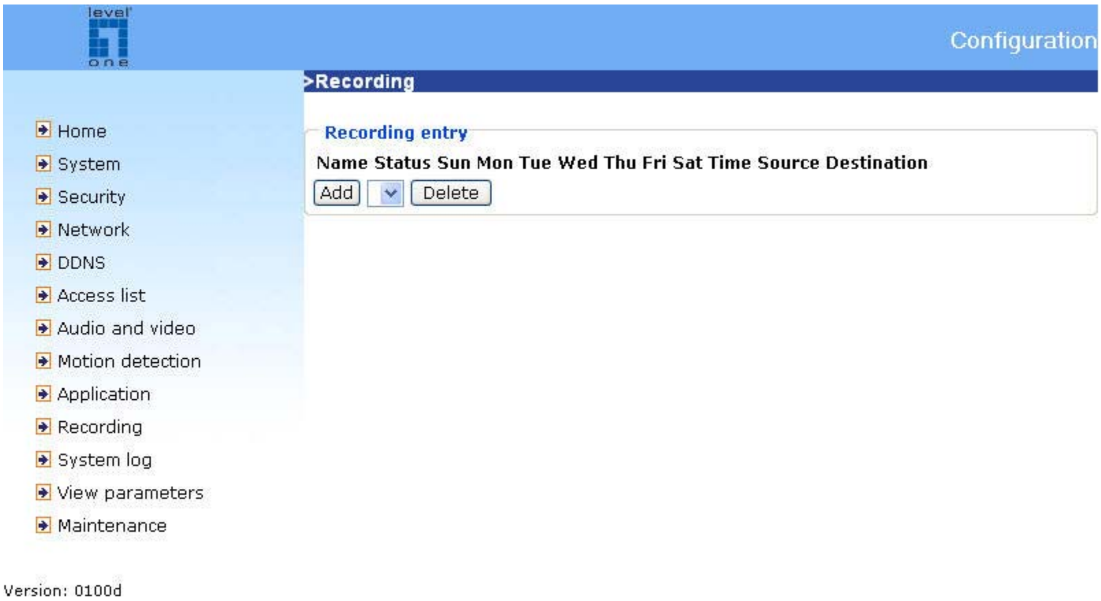
Maximum file size: 500 Kbytes [50~800]

File Name Prefix:

○ System log

Recording

The Network camera supports recording on network storage. The operation of editing recording item is the same as the one in application page. User can know the recording name, status, weekly and time schedule, stream source and destination of recording. There can be at most two recording entries. To do recording on network storage, please add network storage server in application page first.



<url> *http://<Network Camera>/setup/recording.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

“Recording entry name” The unique name for recording entry

“Enable this recording” Check it to enable this event.

“Priority” The recording with higher priority will be executed first.

“Source” The source of stream, stream1 or stream2.

The weekly and time schedules are provided.

“Sun” ~ “Sat” Select the days of the week to perform the event.

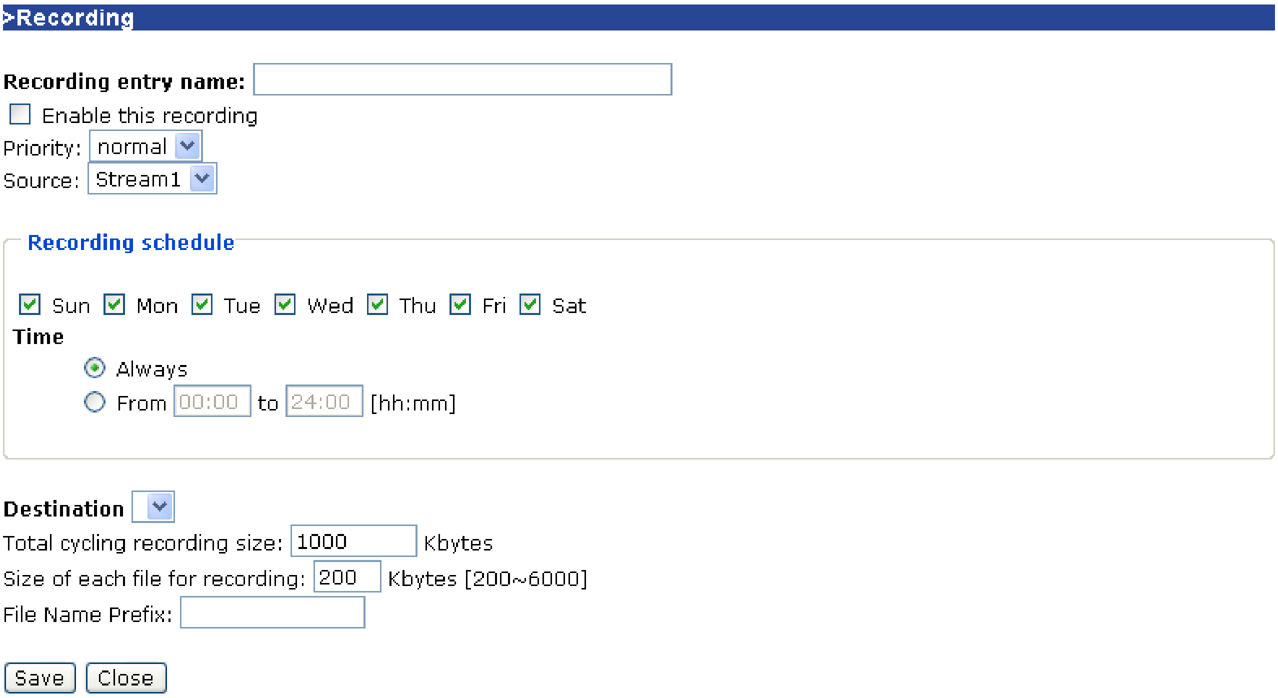
“Time” shows **“Always”** or input the time interval.

“Destination” Network storage server user added.

“Total cycle recording size” The total size for cycle recording in Kbytes

“Size of each file for recording” The single file size in Kbytes

"File Name Prefix" The prefix name will be added on the file name of the recording.



>Recording

Recording entry name:

□ Enable this recording

Priority: normal

Source: Stream1

Recording schedule

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

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Destination

Total cycling recording size: 1000 Kbytes

Size of each file for recording: 200 Kbytes [200~6000]

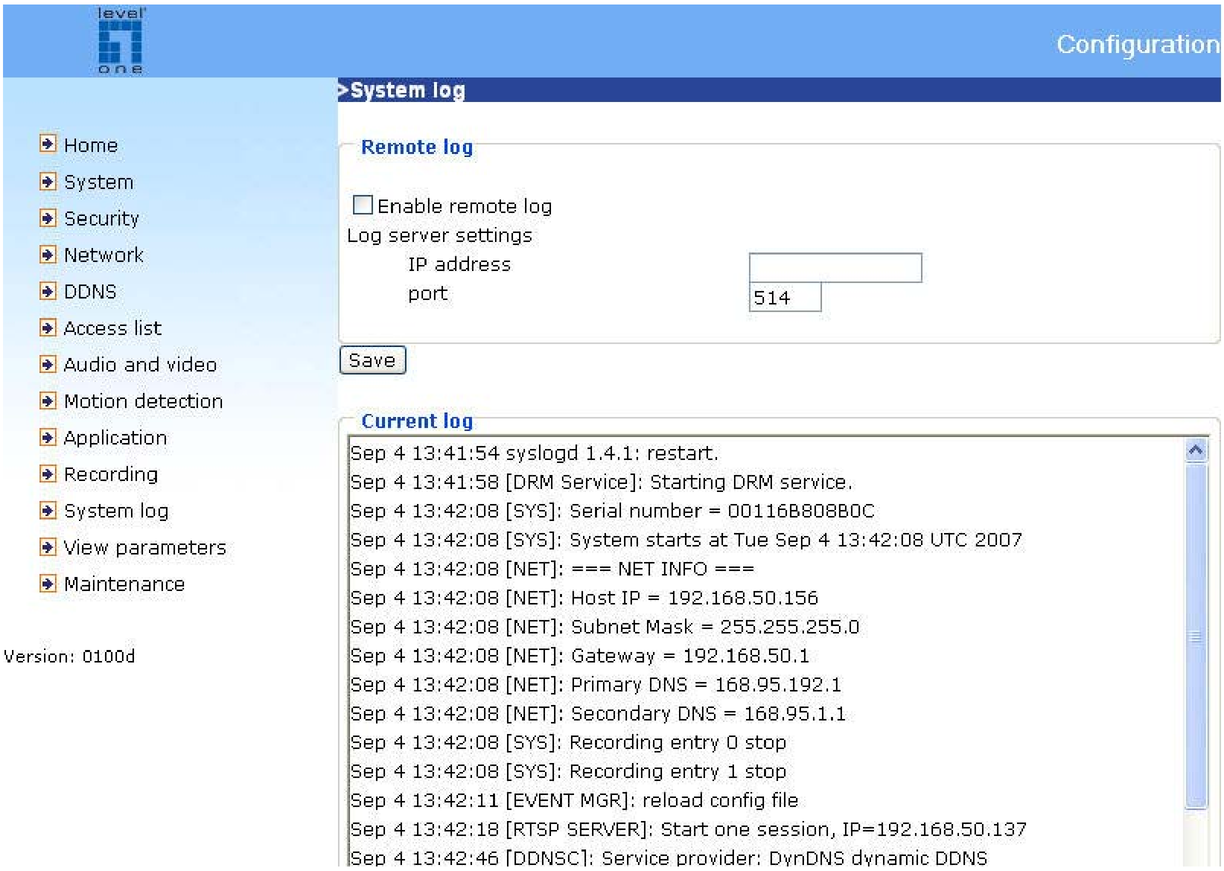
File Name Prefix:

System log

The Network camera support log the system messages on remote server. The protocol is compliant to RFC 3164. If you have external Linux server with syslogd service, use “-r” option to turn on the facility for receiving log from remote machine. Or you can use some software on Windows which is compliant to RFC 3164.

Check **“Enable remote log**” and input the **“IP address**” and **“port”** number of the log server to enable the remote log facility.

In the **“Current log”**, it displays the current system log file. The content of the log provides useful information about configuration and connection after system boot- up.



Remote log

□ Enable remote log

Log server settings

IP address

port 514

Current log

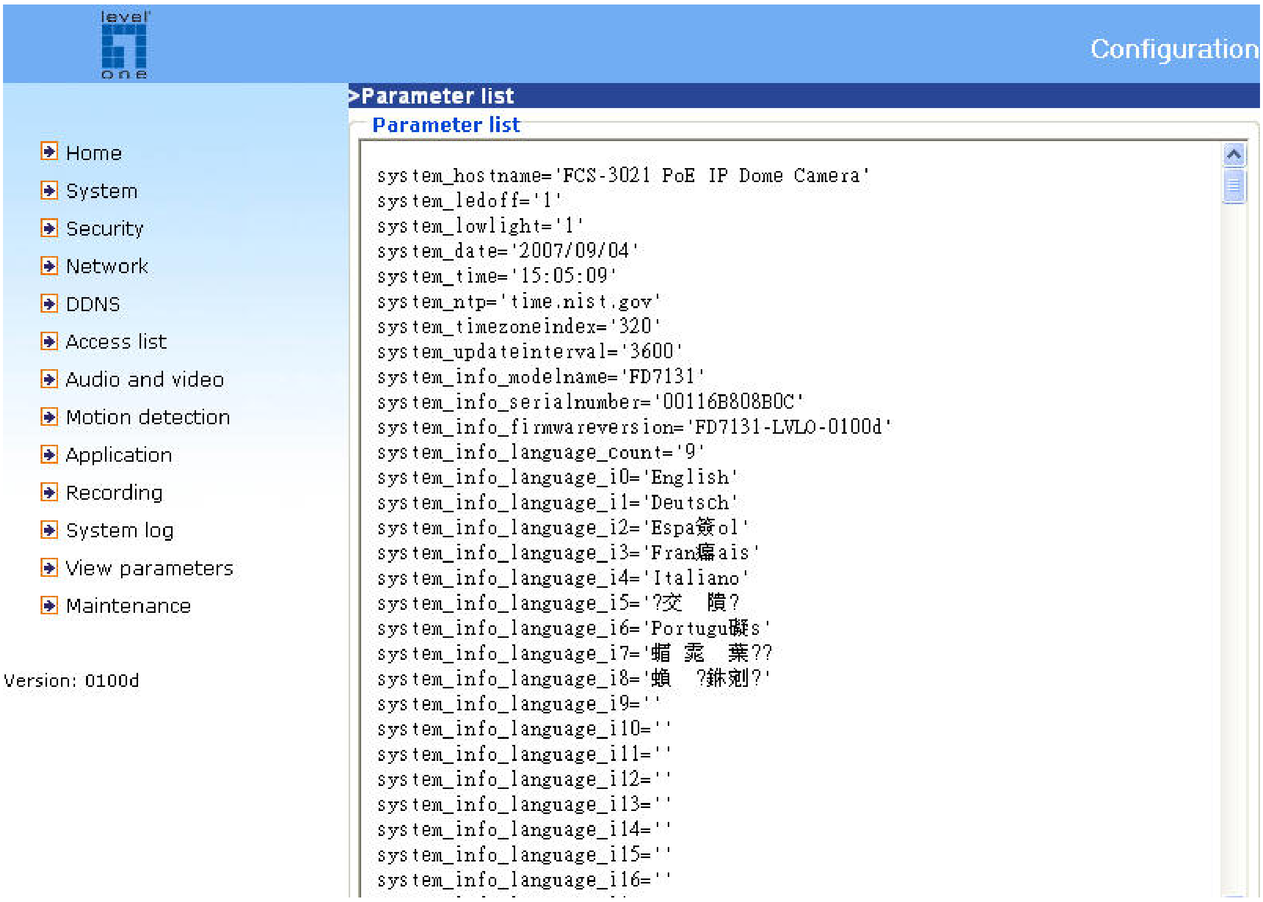
```
Sep 4 13:41:54 syslogd 1.4.1: restart.
Sep 4 13:41:58 [DRM Service]: Starting DRM service.
Sep 4 13:42:08 [SYS]: Serial number = 00116B808B0C
Sep 4 13:42:08 [SYS]: System starts at Tue Sep 4 13:42:08 UTC 2007
Sep 4 13:42:08 [NET]: === NET INFO ===
Sep 4 13:42:08 [NET]: Host IP = 192.168.50.156
Sep 4 13:42:08 [NET]: Subnet Mask = 255.255.255.0
Sep 4 13:42:08 [NET]: Gateway = 192.168.50.1
Sep 4 13:42:08 [NET]: Primary DNS = 168.95.192.1
Sep 4 13:42:08 [NET]: Secondary DNS = 168.95.1.1
Sep 4 13:42:08 [SYS]: Recording entry 0 stop
Sep 4 13:42:08 [SYS]: Recording entry 1 stop
Sep 4 13:42:11 [EVENT MGR]: reload config file
Sep 4 13:42:18 [RTSP SERVER]: Start one session, IP=192.168.50.137
Sep 4 13:42:46 [DDNSC]: Service provider: DynDNS dynamic DDNS
```

<url> *http://<Network Camera>/setup/syslog.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

Viewing system parameters

Click on this link on the configuration page to view the entire system's parameter set.



>Parameter list

Parameter list

```
system_hostname='FCS-3021 PoE IP Dome Camera'
system_ledoff='1'
system_lowlight='1'
system_date='2007/09/04'
system_time='15:05:09'
system_ntp='time.nist.gov'
system_timezoneindex='320'
system_updateinterval='3600'
system_info_modelname='FD7131'
system_info_serialnumber='00116B808B0C'
system_info_firmwareversion='FD7131-LVLO-0100d'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Espa簽ol'
system_info_language_i3='Fran癟ais'
system_info_language_i4='Italiano'
system_info_language_i5='?交  隫?
system_info_language_i6='Portugu礙s'
system_info_language_i7='蝖 霐  葉??
system_info_language_i8='蝢  ?鉥剜?'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''
system_info_language_i15=''
system_info_language_i16=''
```

<url> *http://<Network Camera>/setup/parafile.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

Maintenance

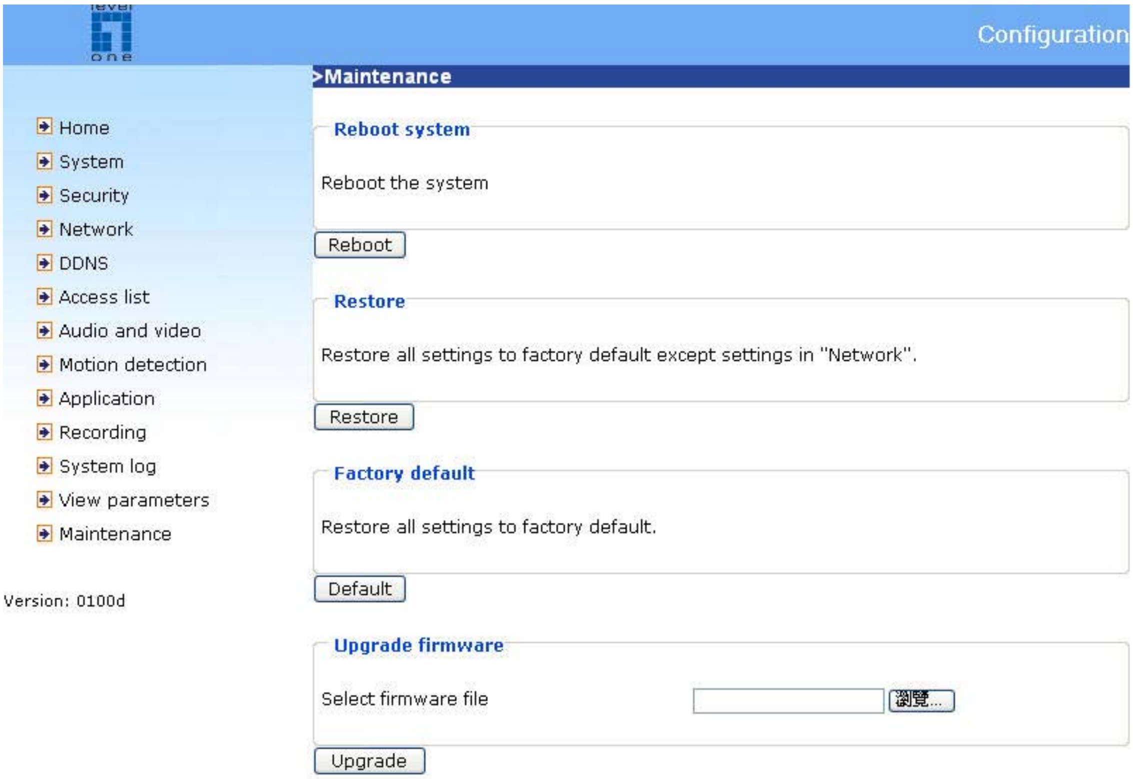
Five actions can be selected.

“Reboot system” Click the reboot button to restart system.

“Restore” Click it to restore all setting to factory default except setting in “Network type” in network page.

“Factory default” Click on Factory default button on the configuration page to restore the factory default settings. Any changes made so far will be lost and the system will be reset to the initial factory settings. The system will restart and require the installer program to set up the network again.

“Upgrade firmware” Select the firmware file and click upgrade button.



Configuration

>Maintenance

Reboot system

Reboot the system

Reboot

Restore

Restore all settings to factory default except settings in "Network".

Restore

Factory default

Restore all settings to factory default.

Default

Upgrade firmware

Select firmware file

瀏覽...

Upgrade

<url> *http://<Network Camera>/setup/maintain.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

Appendix

A. Troubleshooting

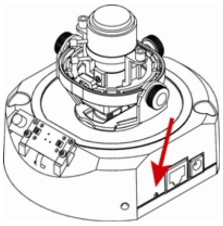
Status LED

The following table lists the LED patterns in general.

Condition	LED color
Loading system after power on	Blink green and orange (twice)
During booting procedure	Non light
Detecting and setting network	Steady orange till IP address is confirmed
After network is setup (system up)	Blink orange and red
During the upgrade firmware process	Rapidly blink orange till firmware is upgraded

Reset and restore

There is a button in the back of the Network Camera. It is used to reset the system or restore the factory default settings. Sometimes resetting the system sets the system back to normal state. If the system problems remain after reset, restore the factory settings and install again.



RESET: Click on the button.

RESTORE:

1. Press on the reset button continuously until the status LED rapidly blinks orange. It takes about 30 seconds.
2. Upon successful restore, the status LED will blink orange and red.

> ⚠ Restoring the factory defaults will erase any previous settings. Reset or restore the system after power on.

B. 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 paramter 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 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
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 camera should prevent to restart when parameter changed.

Group: **system**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	host name of server
ledoff	<boolean>	6/6	turn on(0) or turn off(1) all led indicators
lowlight	<boolean>	6/6	(0) Turn on white light LED in all condition (1) Only turn on white light LED in low light condition
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 time of system. Set to ‘keep’ keeping time unchanged. Set to ‘auto’ to use NTP to synchronize time.

ntp	<domain name>, <ip address>, <blank>	6/6	**NTP server**
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
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.
restore	0, <positive integer>	7/6	Restore the system parameters to default value. Restart the server after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds.
restoreexceptnet	0, <positive integer>	7/6	Restore the system parameters to default value except (ipaddress, subnet, router, dns1, dns2, ddns settings). Restart the server after <value> seconds.

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 <MODEL-BRAND-VERSION>
language_default	string[16]	0/7	Default webpage language.

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
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~ndi-1)>	<boolean>	1/1	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	string [64]	6/6	Root's password
user_i<1~20>_pass	string [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**: **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 stream1
s1_accessname	string[32]	1/6	RTSP access name for stream2

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**: **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, indoor, fluorescent, outdoor	4/4	auto, auto white balance indoor, 3200K fluorescent, 5500K outdoor, > 5500K

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 camera control function 0(not support), 1(support) Bit 1 => **Build-in** or **external**

			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]	1/4	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
s<0~(m-1)>_keyinterval	1, 3, 5, 10, 30, 60, 90, 120	4/4	Key frame interval
s<0~(m-1)>_resolution	176x144, 320x240, 640x480, 800x600, 1280x1024	4/4	Video resolution in pixel
s<0~(m-1)>_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_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.
s<0~(m-1)>_bitrate	20000, 30000, 40000, 50000, 64000, 128000, 256000, 384000, 512000, 768000, 1000000,	4/4	set bit rate in bps when choose cbr in “ratecontrolmode”

	1200000, 1500000, 2000000, 3000000, 4000000		
s<0~(m-1)>_maxframe	1, 2, 3, 5, 10, 15, 20, 25, 30 (only for NTSC or 60Hz CMOS)	4/4	set maximum frame rate in fps
s<0~(m-1)>_forcei	1	7/6	Force I frame

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
mute	0, 1	4/4	Enable audio mute
gain	0~31	4/4	Gain of input
boostmic	0, 1	4/4	Enable microphone boost
s<0~(m-1)>_codectype	aac4, gamr	4/4	set audio codec type for input
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	set AAC4 bitrate in bps
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	set AMR bitrate in bps

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION

brightness	-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: **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,
	PeanutHull,
	CustomSafe100
		6/6	Safe100 => safe100.net
			DyndnsDynamic => dyndns.org (dynamic)
			DyndnsCustom => dyndns.org (custom)
			TZO => tzo.com
			DHS => dhs.org
			DynInterfree =>dyn-interfree.it
			PeanutHull => peanut hull

			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 is OK, 1 is FAIL, 2 is no IGD router, 3 is 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: **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	0/7	number of digital output

	integer>		
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	< boolean >	0/7	indicate whether to support PTZ control
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_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

camctrl_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for camera control
uart_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for uart transfer
transmission_mode	Tx, Rx, Both	0/7	Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box, Both: DVR?.
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>

PARAMETER	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.
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" indicates system boot. "di" indicates digital input. "motion" indicates video motion detection. "seq" indicates periodic condition.
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. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates 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.

action_do_i<0~(ndo-1)>_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>

PARAMETER	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" is email server. "ftp" is ftp server. "http" is http server. "ns" is 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_location	string[128]	6/6	The location to upload or store the media.
ftp_passive	0, 1	6/6	To enable or disable the passive mode. 0 is to disable the passive mode. 1 is to enable the passive mode.
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>

PARAMETER	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 means the first stream. 1 means 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 means to add date and time suffix. 0 means 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 means the first stream. 1 means 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: record_i<0~1>

PARAMETER	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.

priority	0, 1, 2	6/6	Indicate the priority of this recoding. “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates 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	200~6000	6/6	The max size for one file in Kbytes
dest	0~4	6/6	The destination to store the recording data. “0~4” means the index of network storage.

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 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=<*value*>]
[&privilege=<value>][…][&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 the 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.

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*>]
[&return=<return 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 then 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 then 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 the the current path. If you omit this parameter, it will redirect to an empty page.

RTSP SDP

Note: This request requires viewer access privilege

Method: GET/POST

Syntax:

```
http://<servername>/viewer/<0~(n-1)>/<network_accessname_<0~(m-1)>>
rtsp://<servername>/<0~(n-1)>/<network_accessname_<0~(m-1)>>
```

“n” is the channel number and “m” is the stream number.
You can get the SDP by HTTP or just describe by RTSP protocol directly. For detailed streaming protocol, please refer to “control signaling” and “data format” documents.

D. Specifications

- System

RAM: 64MB SDRAM
ROM: 8MB FLASH ROM

- Networking

Protocol
TCP/IP, HTTP, SMTP, FTP, DDNS, UPnP, Telnet, NTP, DNS, DHCP and RTSP
Physical
10 baseT or 100 baseT Fast Ethernet auto negotiation

- Video

Algorithm supported
MPEG4(simple profile) for streaming video
JPEG for still image
Features
Adjustable image size, quality and bit rate
Time stamp and text overlay
3 motion detection windows
Resolution
640x480 up to 30/25 fps

- Camera Specification

1/4 inch VGA CMOS
176x144: 30/25fps
320x240: 30/25fps
640x480: 30/25fps
1.5Lux/F2.0

- Lens

3~6mm, F1.2~1.5

- Audio (will be supported by f.w update)

AAC, GSM-AMR

- Microphone

Internal microphone:
Omni-directional
Frequency: 50 – 16000Hz
S/N ratio: more than 60dB
External microphone

- LED indicator

Dual color status indicator

- Dimension

FCS-3021: 147mm(L) x 96mm(W) x 47mm(H)

- Weight

NET. 276g

- Power

Power adapter is not included with FCS-3021.
POW-1201,12V/1.25A power adapter, is optional for the power supply.

- Operating Environment

Temperature: 0-50°C/32-122°F
Humidity: 95%RH

- EMI & Safety

CE, FCC

- Viewing system requirement

Operating system
Microsoft Windows 2000/XP/VISTA
Browser
Internet Explorer 6.x or above
Firefox 1.5.0.x or above

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. SEE 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 seperation 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

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

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

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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.