2 Megapixel IP Camera
User Manual

iDC-95CD

WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE.

DO NOT INSERT ANY METALLIC OBJECT THROUGH VENTILATION GRILLS.

CAUTION

CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK.

DO NOT REMOVE COVER (OR BACK). NO USER-SERVICEABLE PARTS INSIDE.

REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

COPYRIGHT

THE TRADEMARKS MENTIONED IN THE MANUAL ARE LEGALLY REGISTERED TO THEIR RESPECTIVE COMPANIES.

Contents

version_1.1_130808

I. Preface

This IP Camera is a 2 Megapixel Real Time IP camera with the web server built in. User can view real-time video via IE browser. IP Camera supports simultaneously H.264, Motion JPEG & MPEG4 video compression and dual streaming which provides smooth and high video quality. The video can be stored in the SD card and played back remotely. With user friendly interface, it is an easy-to-use IP camera which is designed for security application.

II. Product Specifications

Main Features:

- Full HD 1080P Real time
- 3D+2D Digital Noise Reduction
- Digital Wide Dynamic Range
- Day&Night Switch time control manually
- IR-Cut filter
- Power over Ethernet available (Option)
- Video output
- Wireless Network (Option)
- H.264/ M-JPEG / MPEG4 compression
- SD card backup
- Support iPhone/Android/Mac
- Triple Streaming
- SDK for Software Integration
- Free Bundle 36 ch recording software

Hardware	
CPU	ARM 9 ,32 bit RISC
RAM	256MB
Flash	16MB
Image sensor	1/2.7” 2Megapixel CMOS sensor
Lens Changeable	Yes, CS Mount
Sensitivity	Color : 0.1 Lux (AGC ON) B / W: 0.05 Lux (AGC ON)
Support DC IRIS	Yes
ICR	Mechanism IR cut Filter
I/O	1 Alarm in / 1 Relay out
Video output	Yes
RS-485	Yes
Audio	G.711(64K) and G.726(32K,24K) audio compression Input : audio in or Mic built-in(auto switch) Output: 3.5mm phone jack, Support 2-way.
Power over Ethernet	Yes (Optional)
Power	12V DC Power consumption Max：3.84W 24V AC Power consumption Max：4.32W PoE Power consumption Max：4.8W
Operating Temperature	-10°C ~ 45°C
Dimensions	65mm (W) x 58mm (H) x 132mm (L)
Weight	450 g
Network	
Ethernet	10/ 100 Base-T
Network Protocol	HTTP, HTTPS, SNMP, QoS/DSCP, Access list, IEEE 802.1X, RTSP, TCP/ IP, UDP, SMTP, FTP, PPPoE, DHCP, DDNS, NTP, UPnP, 3GPP, SAMBA, Bonjour
Wireless	802.11b/g/n WEP,WPA-PSK,WPA2-PSK.
System	
Video Resolution	1920x1080@30fps, 1280x720@30fps, ,640x480@30fps, 320x240@30fps, 176x144@30fps
Video Adjust	Brightness, Contrast, Hue, Saturation, Sharpness, AGC, Night Mode, D-WDR, Flip, Mirror, Noise reduction, Day & Night adjustable

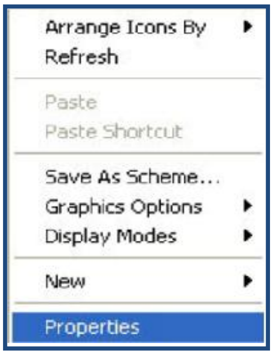
Triple Streaming	Yes
Image snapshot	Yes
Full screen monitoring	Yes
Privacy Mask	Yes, 3 different areas
Compression format	H.264/ M-JPEG/ MPEG4
Video bitrates adjust	CBR, VBR
Motion Detection	Yes, 3 different areas
Triggered action	Mail, FTP, Save to SD card, Relay output, SAMBA
Pre/ Post alarm	Yes, configurable
Security	Password protection, IP address filtering, HTTPS encrypted data transmission, 802.1X port-based authentication for network protection, QoS/DSCP
Firmware upgrade	HTTP mode, can be upgraded remotely
Simultaneous connection	Up to 10
SD Card Management	
Recording trigger	Motion Detection, IP check, Network break down (wire only), Schedule, Alarm in
Video format	AVI, JPEG
Video playback	Yes
Delete files	Yes
Client System	
OS	Windows 7, 2000, XP, 2003, Microsoft IE 6.0 or above, Chrome, Safari, Firefox
Mobile Support	iOS 4.3 or above, Android 1.6 or above.
Hardware Suggested	Intel Dual Core 2.53G,RAM: 1024MB, Graphic card: 128MB

*SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTICE

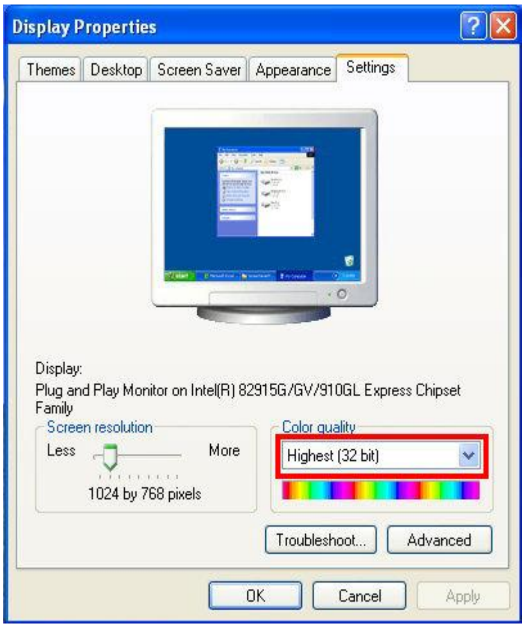
III. Product Installation

A. Monitor Settings

1. Right-Click on the desktop. Select “Properties”



2. Change color quality to highest (32bit).



Display:
Plug and Play Monitor on Intel(R) 82915G/GV/910GL Express Chipset Family

Screen resolution: 1024 by 768 pixels

Color quality: Highest (32 bit)

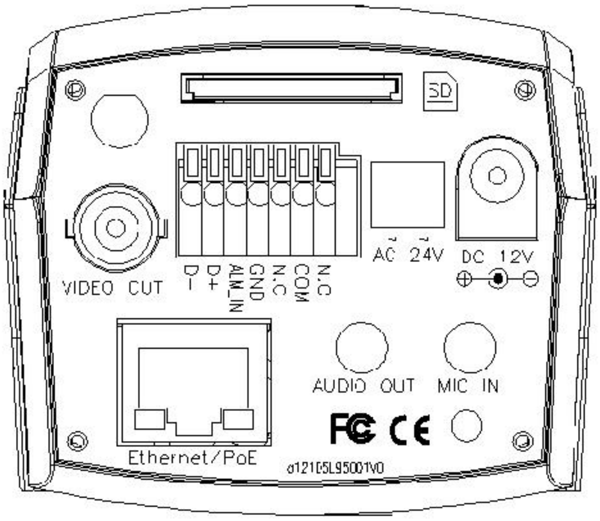
B. Hardware Installation

1. Connector Instruction

The connectors are as below. Plug in the DC adapter power, or use the 2P terminal block to connect with AC power, or use POE.

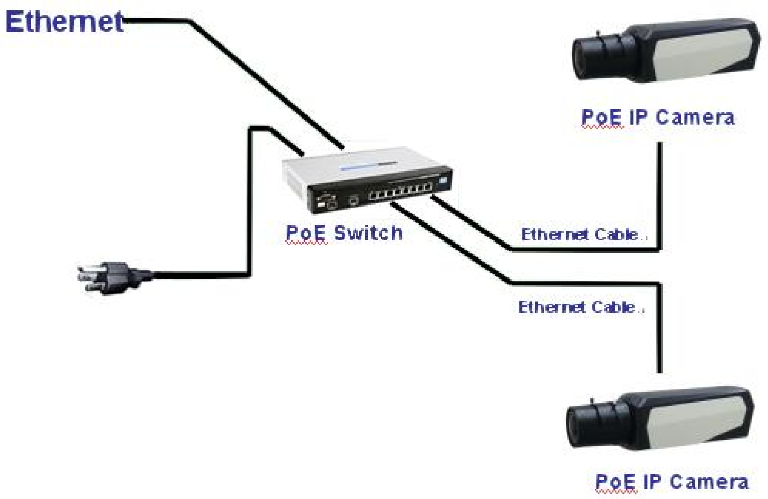
Connect the IP Camera to your PC or network, and set up the network configurations according to the network environment.

About I/O settings, please refer to chapter VII in User Manual: "I/O Configuration" for detail.



2. PoE (Power Over Ethernet) 802.3af PoE Switch is recommended

Power over Ethernet (PoE) is a technology that integrates power into a standard LAN infrastructure. It enables power to be provided to the network device, such as an IP phone or a network camera, using the same cable as that used for network connection. It eliminates the need for power outlets at the camera locations and enables easier application of uninterruptible power supplies (UPS) to ensure 24 hours a day, 7 days a week operation.



C. IP Settings

1. You can use the software “IP Scanner” to assign the IP address of IP Camera. The software is in the attached CD.

2. There are two language versions of IP Scanner. Choose one as your need:

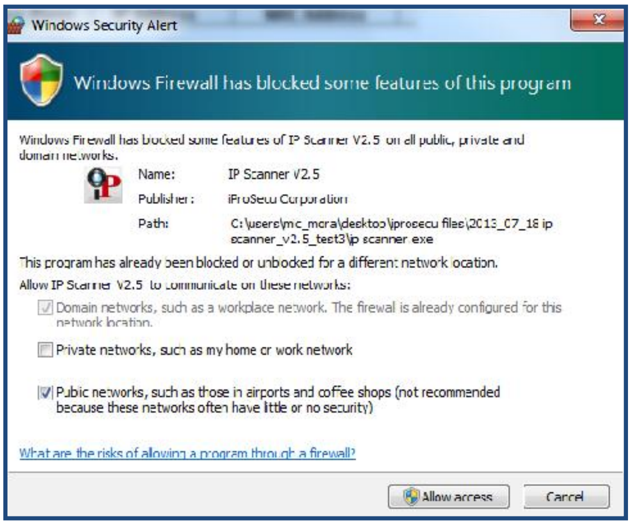
IP Scanner.exe: English version

3. There are 3 kinds of IP configuration.

a. Fixed IP (Public IP or Virtual IP)
b. DHCP (Dynamic IP)
c. Dial-up (PPPoE)

4. Execute IP Scanner

5. On Windows, the following message box may pop up. Please click “Allow Access” or “Unblock”.



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of IP Scanner V2.5 on all public, private and domain networks.

Name: IP Scanner V2.5
Publisher: iProSecu Corporation
Path: C:\users\mc_mora\desktop\iprosecu files\2013_07_18 ip scanner_v2.5_test3\ip scanner.exe

This program has already been blocked or unblocked for a different network location.

Allow IP Scanner V2.5 to communicate on these networks:

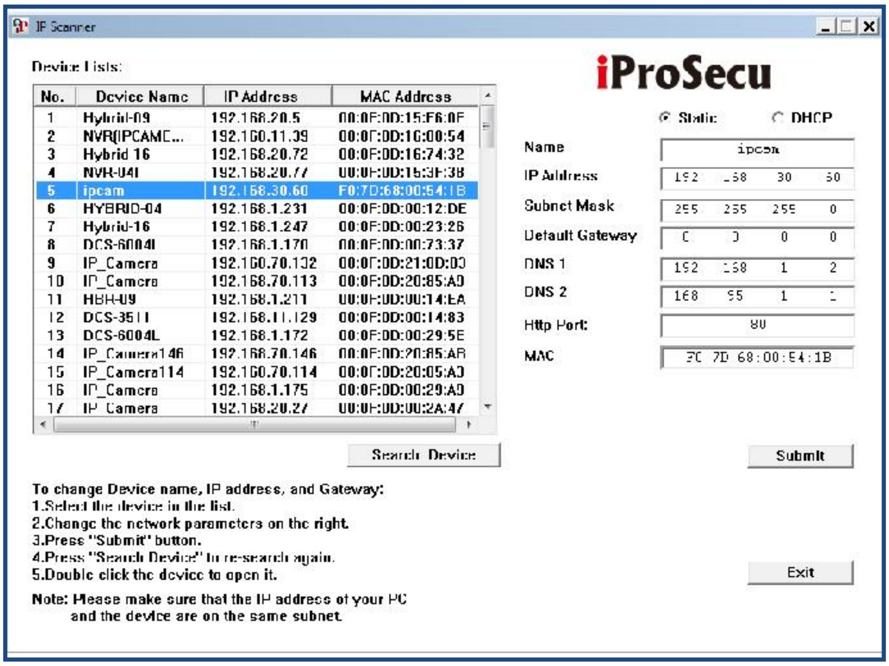
☑ Domain networks, such as a workplace network. The firewal is already configured for this network location.

☐ Private networks, such as my home or work network

☑ Pubic networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

6. IP Scanner configuration:



IP Scanner

Device Lists:

No.	Device Name	IP Address	MAC Address
1	Hybrid-09	192.168.20.5	00:0F:0D:15:F6:0F
2	NVR(IPCAME...	192.168.11.39	00:0F:0D:10:00:54
3	Hybrid 16	192.168.20.72	00:0F:0D:16:74:32
4	NVR-04I	192.168.20.77	00:0F:0D:15:3F:38
5	ipcam	192.168.30.60	F0:7D:68:00:54:1B
6	HYBRID-04	192.168.1.231	00:0F:0D:00:12:DE
7	Hybrid-16	192.168.1.247	00:0F:0D:00:23:26
8	DCS-6004I	192.168.1.170	00:0F:0D:00:73:37
9	IP_Camera	192.168.70.132	00:0F:0D:21:0D:03
10	IP_Camera	192.168.70.113	00:0F:0D:20:85:A0
11	HBH-09	192.168.1.211	00:0F:0D:00:14:EA
12	DCS-3511	192.168.11.129	00:0F:0D:00:14:83
13	DCS-6004L	192.168.1.172	00:0F:0D:00:29:5E
14	IP_Camera146	192.168.70.146	00:0F:0D:20:85:AB
15	IP_Camera114	192.168.70.114	00:0F:0D:20:05:A0
16	IP_Camera	192.168.1.175	00:0F:0D:00:29:A0
17	IP_Camera	192.168.20.27	00:0F:0D:00:2A:47

● Static ○ DHCP

Name	ipcam
IP Address	192 168 30 60
Subnet Mask	255 255 255 0
Default Gateway	0 0 0 0
DNS 1	192 168 1 2
DNS 2	168 95 1 1
Http Port:	80
MAC	F0 7D 68:00:54:1B

To change Device name, IP address, and Gateway:
1.Select the device in the list.
2.Change the network parameters on the right.
3.Press "Submit" button.
4.Press "Search Device" to re-search again.
5.Double click the device to open it.

Note: Please make sure that the IP address of your PC and the device are on the same subnet.

7. IP Scanner will search for all IP Cameras connected on LAN. Click “Search Device” to refresh the result list.

8. Click one of the IP Camera listed on the left side. The network configuration of this IP camera shows on the right side. You may change the “name” of the IP Camera as your preference (e.g.: Office, warehouse). Change the parameter and click “Submit”. It will apply the change and reboot the Device.

9. Please make sure that the IP address of your PC and IP Camera are on the same subnet.

The same Subnet:

IP CAM IP address: 192.168.1.200

PC IP address: 192.168.1.100

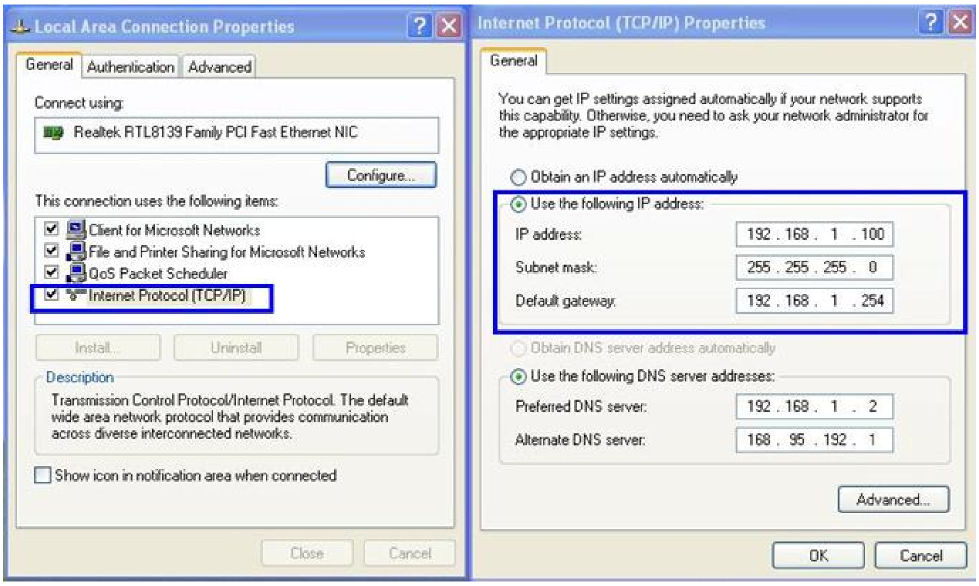
Different Subnets:

IP CAM IP address: 192.168.2.200

PC IP address: 192.168.1.100

To Change PC IP address:

Control Panel→Network Connections→ Local Area Connection Properties→ Internet Protocol (TCP/IP) → Properties



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Realtek RTL8139 Family PCI Fast Ethernet NIC

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

Close | Cancel

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

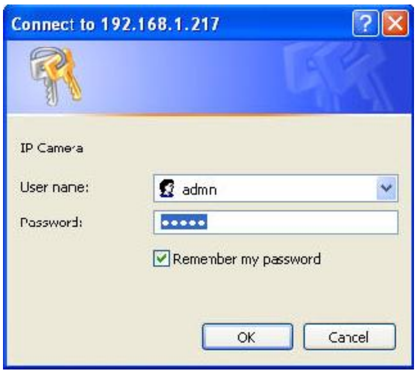
Preferred DNS server: 192 . 168 . 1 . 2
Alternate DNS server: 168 . 95 . 192 . 1

Advanced...

OK | Cancel

10. A quick way to access remote monitoring is to double-click the selected IP Camera listed on “Device list” of IP Scanner. An IE browser will be opened.

11. If you link to the IP Camera successfully, there pops a box asking you to log in. Please key-in the default user name "admin" and password "admin" when you link to the IP Camera for the first time. You can revise the user name and password later.



IP Camera

User name: admin

Password: •••••

☑ Remember my password

D. Install ActiveX Controls

1. To users of IE 6.0 above

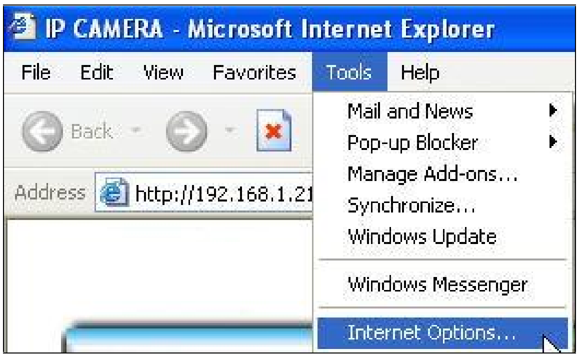
At the first time you access the camera via IE, it will ask you to install the ActiveX component. If the installation failed, please check the security setting for the IE browser.

a. Follow the steps: IE→Tools → Internet Options… → Security Tab → Custom Level… → Security Settings.

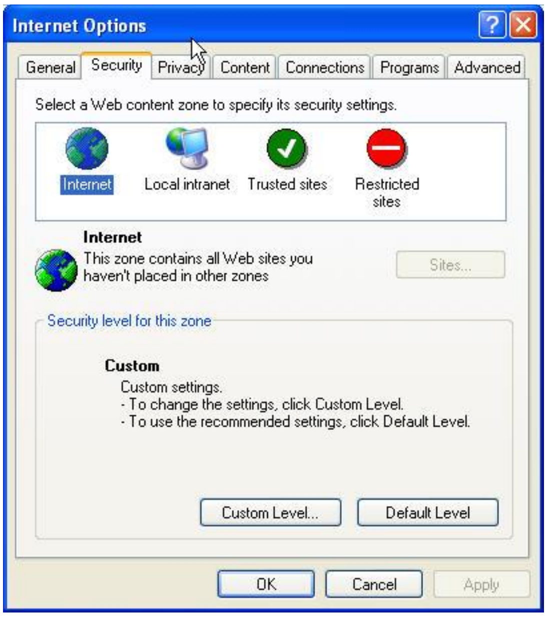
Find the option "Download unsigned ActiveX control"→ Select “Enable” or Prompt.

Find the option "Initialize and script ActiveX controls not marked as safe" → Select “Enable” or Prompt.

1



2



Select a Web content zone to specify its security settings.

Internet

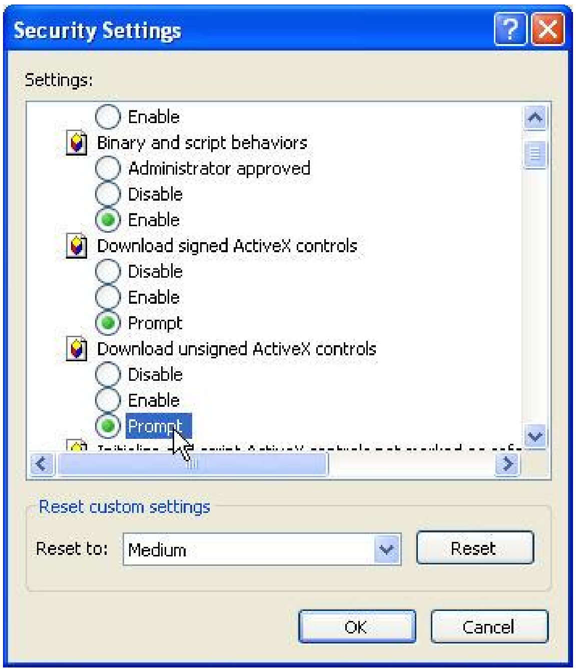
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

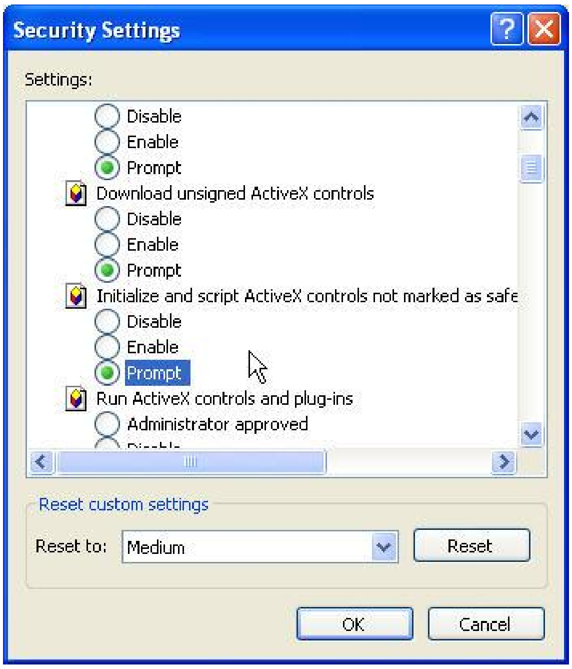
3



Settings:

- ○ Enable
- Binary and script behaviors
  - ○ Administrator approved
  - ○ Disable
  - ● Enable
- Download signed ActiveX controls
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Download unsigned ActiveX controls
  - ○ Disable
  - ○ Enable
  - ● Prompt

4

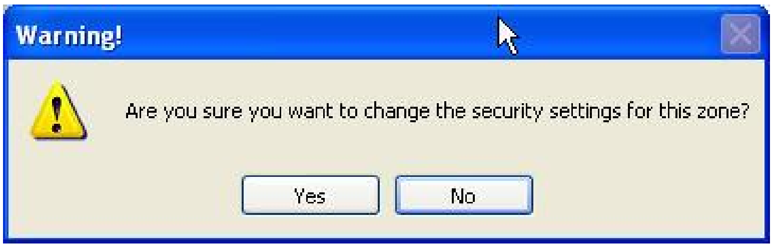


Settings:

- ○ Disable
- ○ Enable
- ● Prompt
- Download unsigned ActiveX controls
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Initialize and script ActiveX controls not marked as safe
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Run ActiveX controls and plug-ins
  - ○ Administrator approved

5

When popup the following dialogue box, click “Yes”.

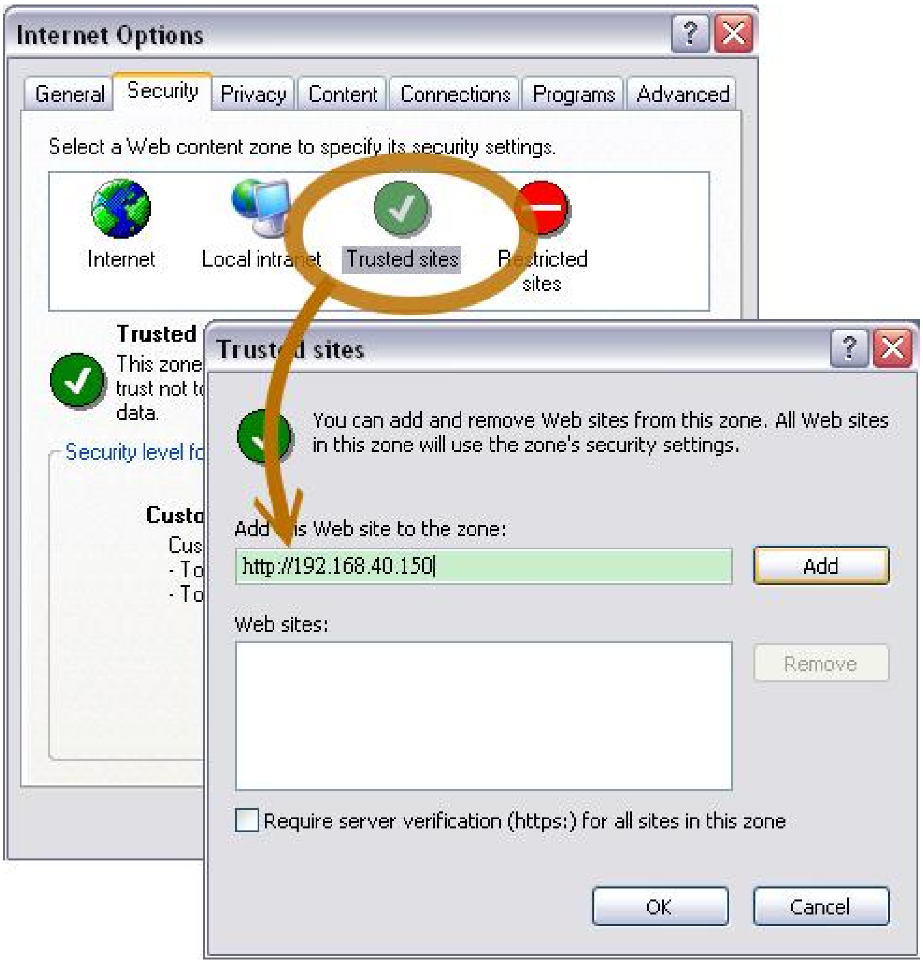


Warning!

Are you sure you want to change the security settings for this zone?

b. You can choose another way. Go to: IE→Tools → Internet Options… → Security Tab → Trusted sites → Add the IP address and click "OK".

In the site list you can key one single IP address or a LAN address. For example, if you add "192.168.21.*", all the IP address under .21 LAN will be regarded as trusted sites.



You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone: http://192.168.40.150

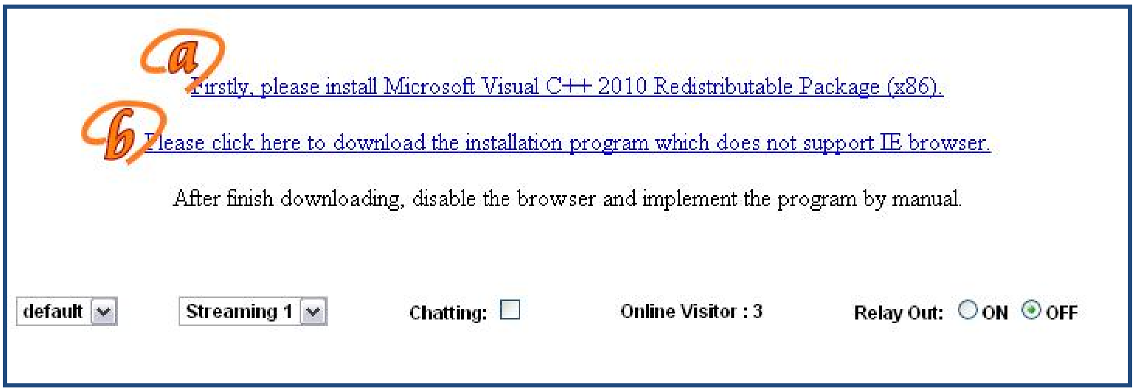
Web sites:

□ Require server verification (https:) for all sites in this zone

2. Use Non-IE Web Browser

If you use Firefox or Google chrome to access the IP camera but fail to watch the live video, please follow the steps to install necessary tools:
(the following pictures are based on chrome.)

a. You may see the prompt message as the picture below. First, Click the link: "Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86)."



Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86).

Please click here to download the installation program which does not support IE browser.

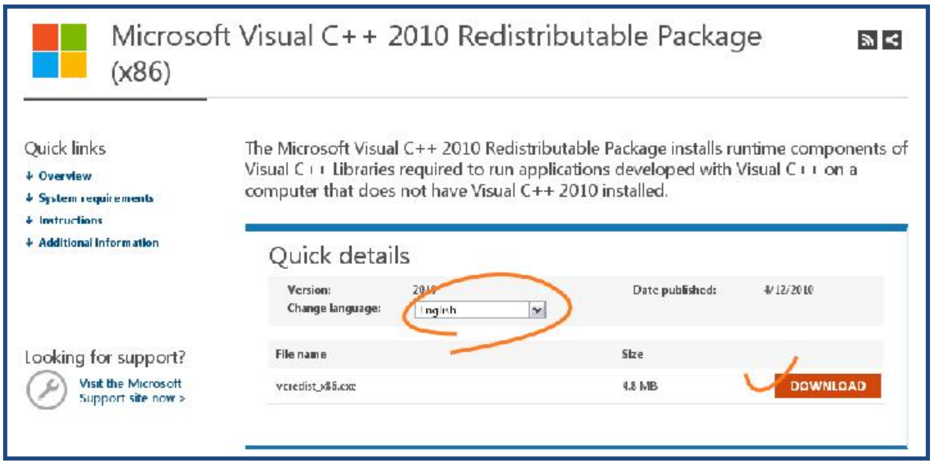
After finish downloading, disable the browser and implement the program by manual.

Chatting: □

Online Visitor : 3

Relay Out: ○ON ●OFF

(i) The link conducts you to the Microsoft official site that you can download the tools. Please select the language and click "download".



Microsoft Visual C++ 2010 Redistributable Package (x86)

The Microsoft Visual C++ 2010 Redistributable Package installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ on a computer that does not have Visual C++ 2010 installed.

Quick details

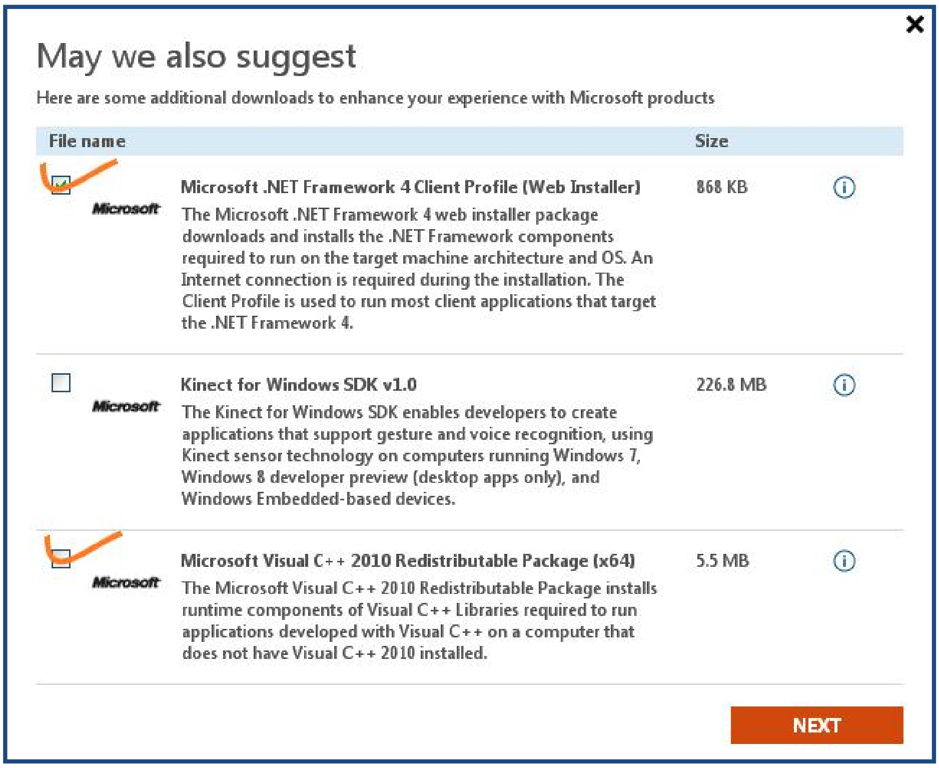
Version: 2010

Change language: English

Date published: 4/12/2010

File name	Size	
vcredist_x86.exe	4.8 MB	DOWNLOAD

(ii) In the pop-up window, please tick the first and the third file as the picture below. Click "Next" to download both "Microsoft .NET Framework 4 Client Profile (Web Installer)" and "Microsoft Visual C++ 2010 Redistributable Package (x64)".

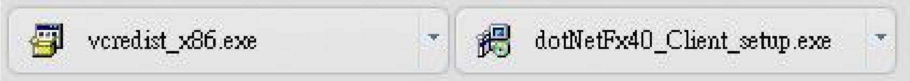


May we also suggest

Here are some additional downloads to enhance your experience with Microsoft products

	File name	Size	
☑	**Microsoft .NET Framework 4 Client Profile (Web Installer)** The Microsoft .NET Framework 4 web installer package downloads and installs the .NET Framework components required to run on the target machine architecture and OS. An Internet connection is required during the installation. The Client Profile is used to run most client applications that target the .NET Framework 4.	868 KB	ⓘ
□	**Kinect for Windows SDK v1.0** The Kinect for Windows SDK enables developers to create applications that support gesture and voice recognition, using Kinect sensor technology on computers running Windows 7, Windows 8 developer preview (desktop apps only), and Windows Embedded-based devices.	226.8 MB	ⓘ
☑	**Microsoft Visual C++ 2010 Redistributable Package (x64)** The Microsoft Visual C++ 2010 Redistributable Package installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ on a computer that does not have Visual C++ 2010 installed.	5.5 MB	ⓘ

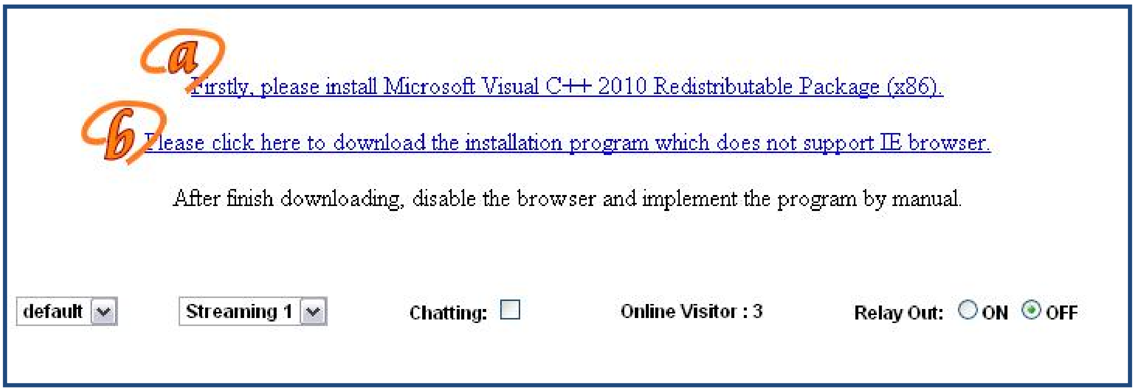
(iii) After finishing downloading, execute the two files respectively to install them. The windows may ask you to reboot the PC when the installation finished.



vcredist_x86.exe

dotNetFx40_Client_setup.exe

b. Then, Click the second link "Please click here to download the installation program which does not support IE browser." to download Setup ActiveX.



Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86).

Please click here to download the installation program which does not support IE browser.

After finish downloading, disable the browser and implement the program by manual.

Chatting: □

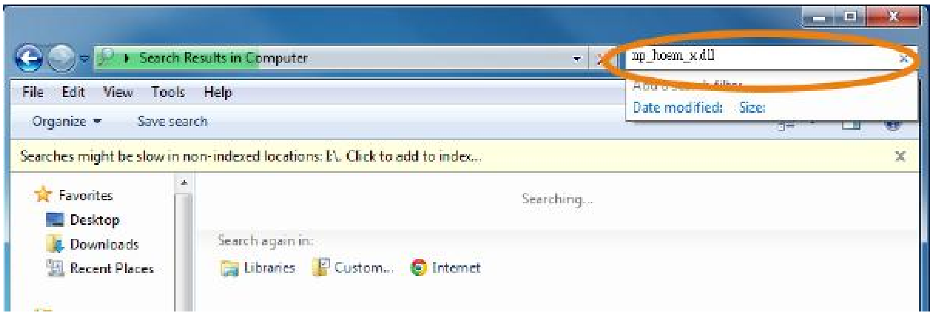
Online Visitor : 3

Relay Out: ○ ON ● OFF

After finishing downloading, execute the files to install ActiveX. Then restart the browser.

c. If you execute the steps above but still cannot see the live video normally, please try the solution:

(i) Search for the file "np_hoem_x.dll" in your system disk. For Windows XP users, please go to "Start" → "Search" → Search for "All files and folders" and key-in "np_hoem_x.dll". For Windows 7 users, please use the search bar on the top-right of the Windows Explorer.



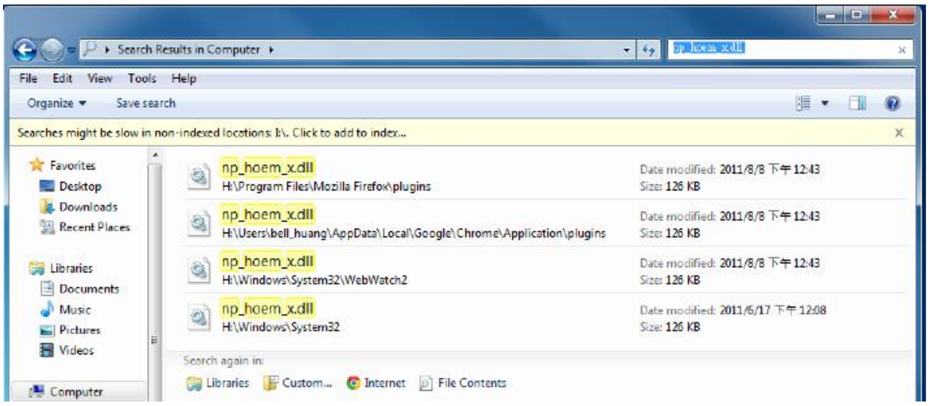
np_hoem_x.dll

Searches might be slow in non-indexed locations: E:\. Click to add to index...

Searching...

Search again in:

(ii) Delete all the files named "np_hoem_x.dll". They're the ActiveX control tools having been installed in your computer, but the old version of ActiveX might not compatible with the new version of browser. Therefore, we delete them in order to install the latest ActiveX control.



Searches might be slow in non-indexed locations: I:\. Click to add to index...

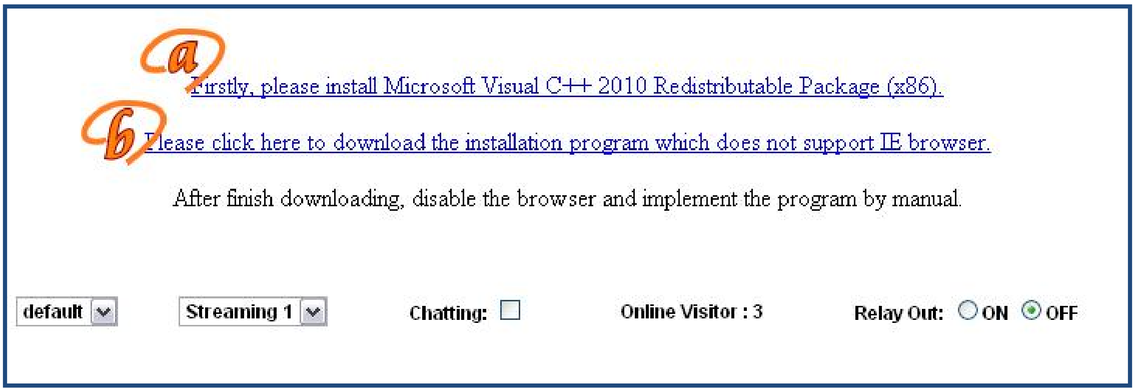
np_hoem_x.dll
H:\Program Files\Mozilla Firefox\plugins
Date modified: 2011/8/8 下午 12:43
Size: 126 KB

np_hoem_x.dll
H:\Users\bell_huang\AppData\Local\Google\Chrome\Application\plugins
Date modified: 2011/8/8 下午 12:43
Size: 126 KB

np_hoem_x.dll
H:\Windows\System32\WebWatch2
Date modified: 2011/8/8 下午 12:43
Size: 126 KB

np_hoem_x.dll
H:\Windows\System32
Date modified: 2011/6/17 下午 12:08
Size: 126 KB

(iii) Start your web browser, and repeat the step 2-b: "Download the installation program which does not support IE browser" to download and install ActiveX.



Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86).

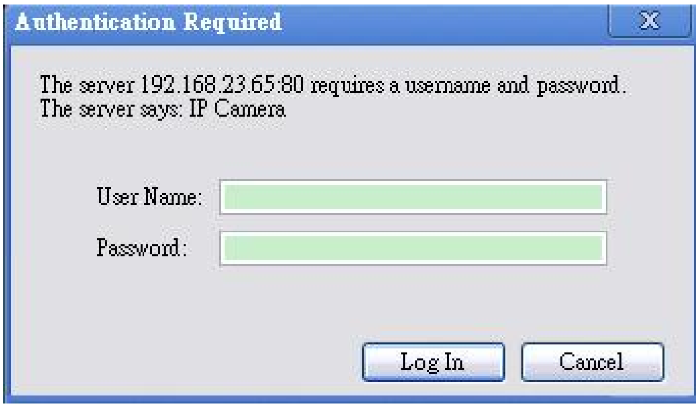
Please click here to download the installation program which does not support IE browser.

After finish downloading, disable the browser and implement the program by manual.

default
Streaming 1
Chatting: □
Online Visitor : 3
Relay Out: ○ ON ● OFF

IV. Live Video

Start an IE browser, type the IP address of the IP camera in the address field. It will show the following dialogue box. Key-in the user name and password. The default user name and password are “admin” and “admin”.



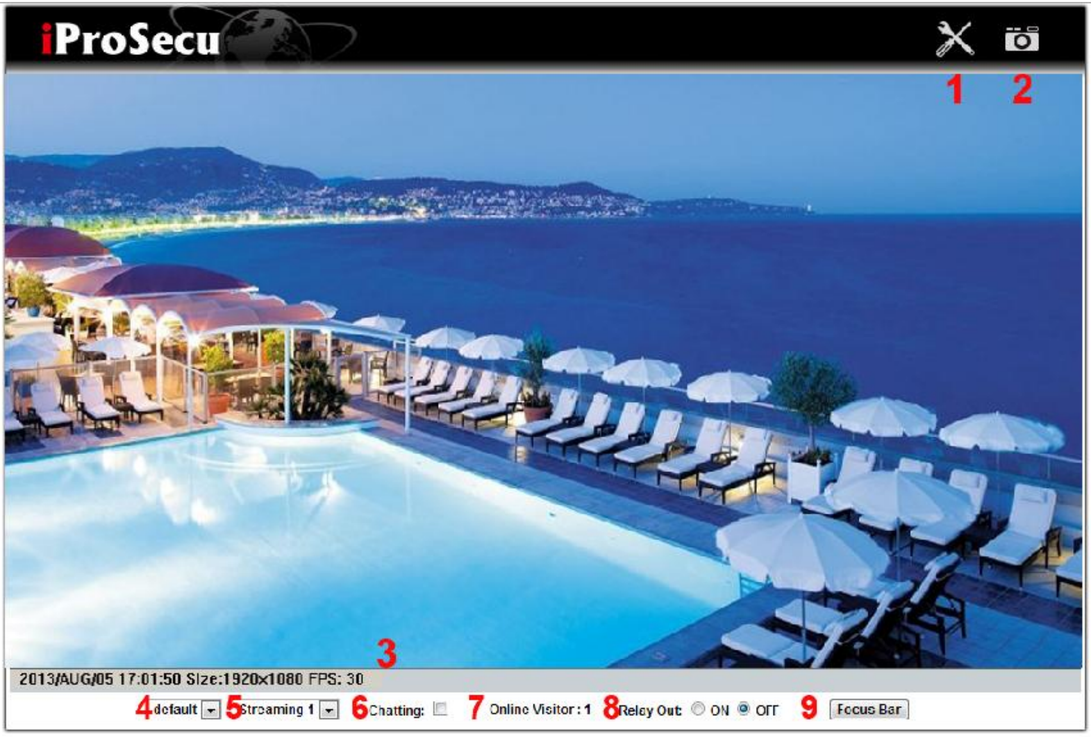
Authentication Required

The server 192.168.23.65:80 requires a username and password.
The server says: IP Camera

User Name:

Password:

When the IP Camera is connected successfully, it shows the following program interface:



2013/AUG/05 17:01:50 Size:1920×1080 FPS: 30

Online Visitor : 1

Relay Out: ○ ON ● OFF

Chatting: □

1. Shows the administration page

2. Video Snapshot

3. Show the system time, video resolution, and video refreshing rate

4. Adjust image, 1/2x, 1x, 2x

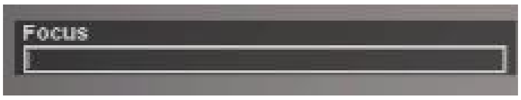
5. Select video streaming source (If in”Video Setting” the streaming 2 setting is closed, this option will not appear here.)

6. The IP Camera supports 2-way audio. Click the “Chatting” check box, then you can use microphone connected to the PC to talk to the Camera side.

7. Show how many people are connected to this IP camera.

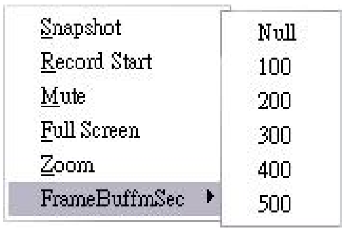
8. Tick the Relay out "ON" box to trigger the relay output for testing. Tick "Off" to stop triggering.

9. Focus Bar: Display the focus bar in the top left corner.



The focus bar represents the degree of focus of the IP camera. If the IP Cam is totally focus the bar will be totally full.

Right-Click the mouse on the video, it will show a pop-up menu.



1. Snapshot: Save a JPEG picture

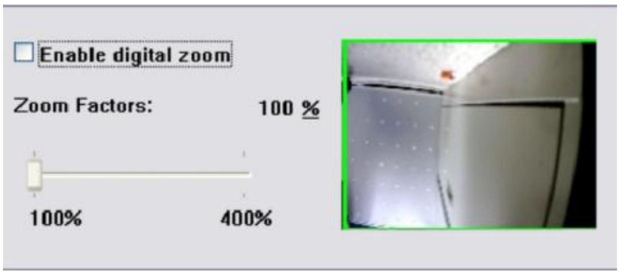
2. Record Start: Record the video in the local PC. It will ask you where to save the video. To stop recording, right-click the mouse again. Select “Record Stop”. The video format is AVI. Use Microsoft Media Player to play the recorded file.

3. Mute: Turn off the audio. Click again to turn on it.

The "mute" button does not affect the playback recording video. As long as the "IP Camera to PC" option in the audio setting is enabled, all the audio will be recorded into the playback video even you click "mute" in the live page.

4. Full Screen: Full-screen mode.

5. ZOOM: Enable zoom-in and zoom-out functions. Select “Enable digital zoom” option first within the pop-up dialogue box and then drag and drop the bar to adjust the zoom factors.

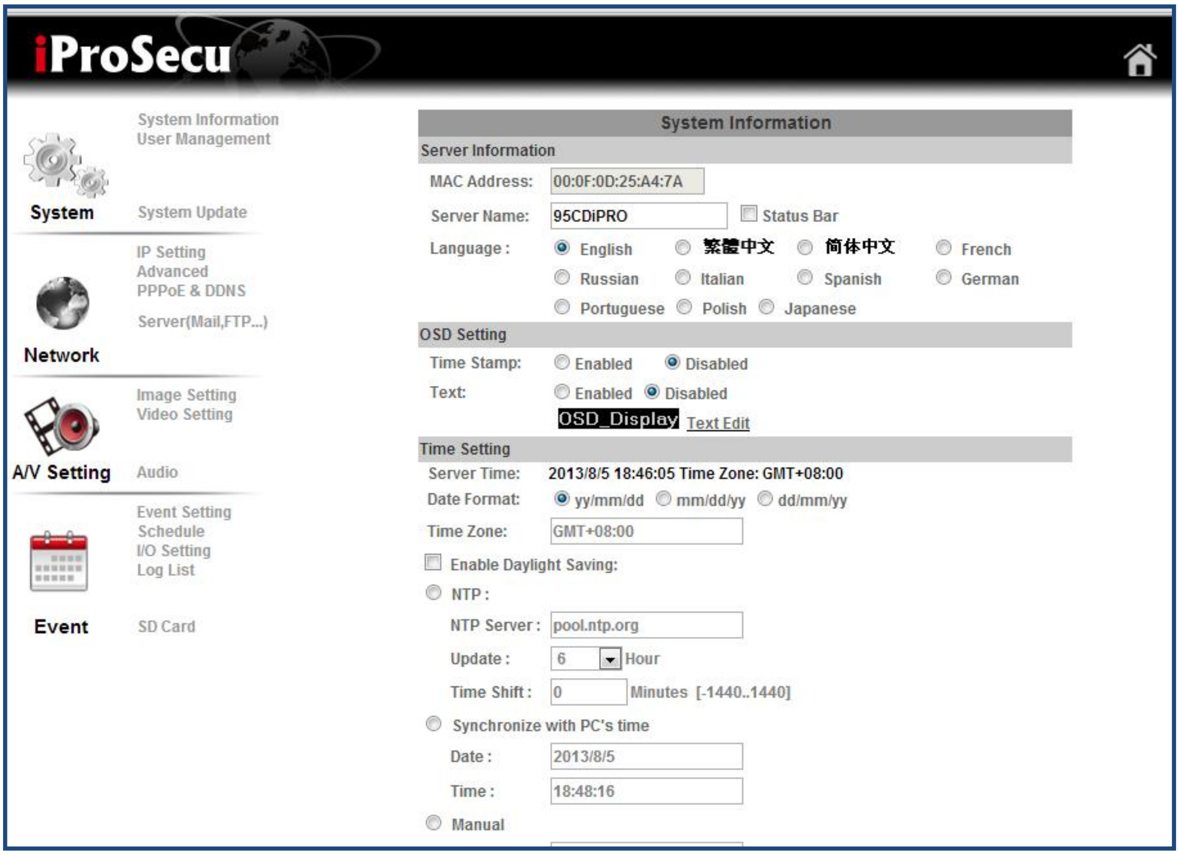


6. Frame Buffm Sec: This function is to build a temporary buffm to accumulate several video frames. This function can make video smooth-going when the Network speed is slow and lag. If you select “100”, then it plays video after 100 mSec when starting receiving images from camera. The slower the Network is, the bigger value should be selected. The default value is null.

V. IP Camera Configuration

Click on 🛠 to get into the administration page as below

Click on 🏠 to back to the live video page.



System Information

Server Information

MAC Address: 00:0F:0D:25:A4:7A

Server Name: 95CDiPRO ☐ Status Bar

Language : ● English ○ 繁體中文 ○ 简体中文 ○ French ○ Russian ○ Italian ○ Spanish ○ German ○ Portuguese ○ Polish ○ Japanese

OSD Setting

Time Stamp: ○ Enabled ● Disabled

Text: ○ Enabled ● Disabled

OSD_Display Text Edit

Time Setting

Server Time: 2013/8/5 18:46:05 Time Zone: GMT+08:00

Date Format: ● yy/mm/dd ○ mm/dd/yy ○ dd/mm/yy

Time Zone: GMT+08:00

☐ Enable Daylight Saving:

○ NTP :

NTP Server : pool.ntp.org

Update : 6 Hour

Time Shift : 0 Minutes [-1440..1440]

○ Synchronize with PC's time

Date : 2013/8/5

Time : 18:48:16

○ Manual

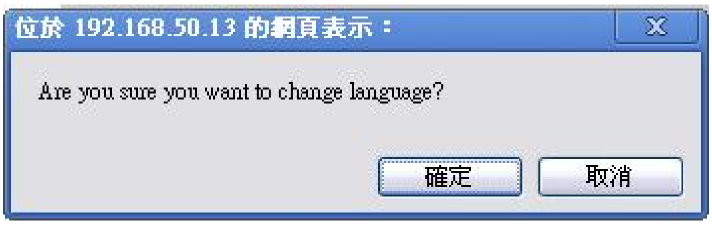
A. System

1. System Information

a. Server Information: Set up the camera name, select language, and set up the camera time.

(i) Server Name: This is the Camera name. This name will show on the IP Scanner.

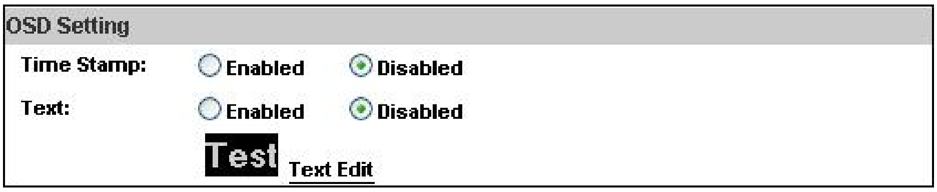
(ii) Select language: There are 11 languages to choose from. When you change the language, it will show the following dialogue box for confirmation.



位於 192.168.50.13 的網頁表示：

Are you sure you want to change language?

b. OSD Setting: Select a position where date & time stamp / text showing on screen.



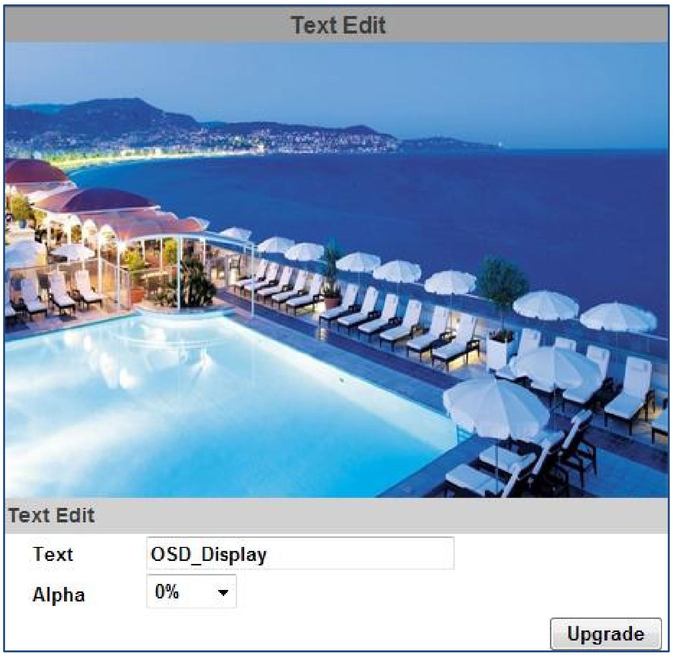
OSD Setting

Time Stamp: ○ Enabled ● Disabled

Text: ○ Enabled ● Disabled

Test Text Edit

Click Text Edit to adjust the OSD text contents. Alpha means background transparency of the text. If you select 100%, the text stamp will be directly displayed on the live screen. If you select 0%, the text stamp will be displayed with a black background.

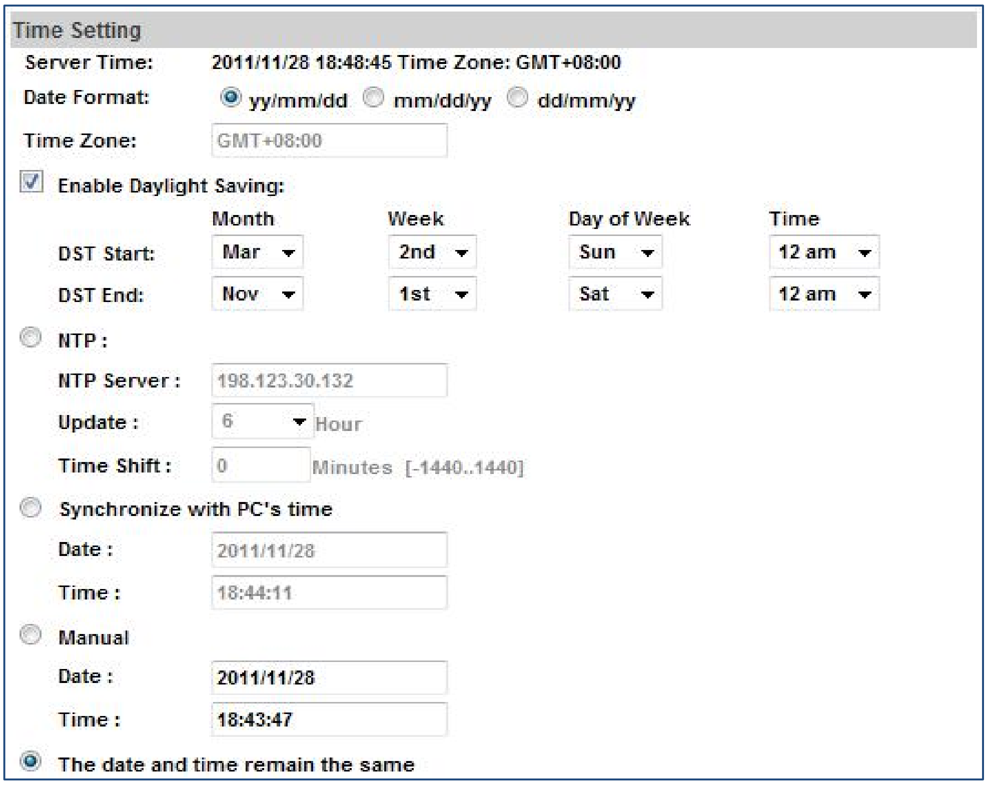


Text Edit

Text Edit

Text	OSD_Display
Alpha	0%

c. Server time setting: Select options to set up time - “NTP”, “Synchronize with PC’s time”, “Manual”, “The date and time remain the same”.



Time Setting

Server Time: 2011/11/28 18:48:45 Time Zone: GMT+08:00

Date Format: ● yy/mm/dd ○ mm/dd/yy ○ dd/mm/yy

Time Zone: GMT+08:00

☑ Enable Daylight Saving:

	Month	Week	Day of Week	Time
DST Start:	Mar	2nd	Sun	12 am
DST End:	Nov	1st	Sat	12 am

○ NTP :

NTP Server : 198.123.30.132

Update : 6 Hour

Time Shift : 0 Minutes [-1440..1440]

○ Synchronize with PC's time

Date : 2011/11/28

Time : 18:44:11

○ Manual

Date : 2011/11/28

Time : 18:43:47

● The date and time remain the same

- Server Time: It shows current IPCam server time.

- Date Format: Select the date display format.

- Time Zone: Select your time zone. It affects server time when you use
“NTP” time.

- Enable Daylight Saving: Give the start and end daylight saving time.

During daylight saving, the time will be 1 hour faster.

- NTP: Key-in the NTP server IP address and update interval. The camera time will be synchronized with NTP server time. To use this option, if the NTP Server is under WAN, the camera must be set to access WAN.

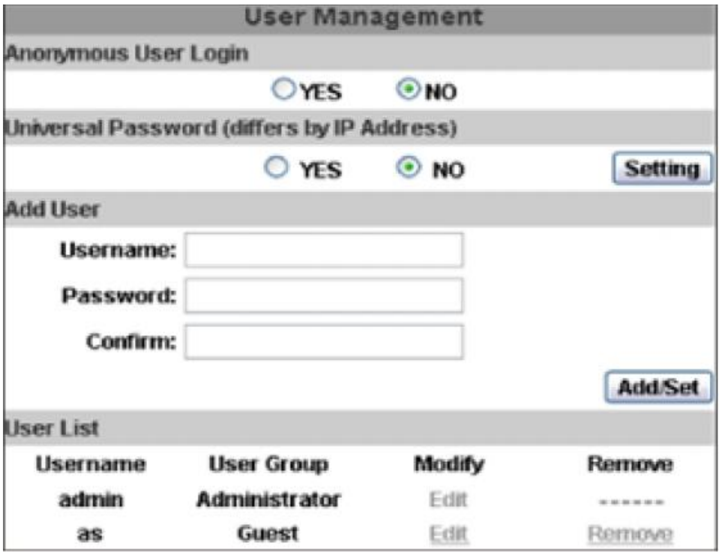
- Synchronize with PC’s time: In “Date” and “Time” column it shows your current PC time. Click “Apply” to make the camera time the same with PC time.

- Manual: Key-in the date and time, and click “Apply”.

- The date and time remain the same: After you select “Synchronize with PC’s time” or “Manual”, and click “Apply”, the selected mark will jump to this option.

2. User Management

IP CAMERA supports three different users, administrator, general user, and anonymous user.



User Management

Anonymous User Login

○ YES ● NO

Universal Password (differs by IP Address)

○ YES ● NO

Add User

Username:

Password:

Confirm:

User List

Username	User Group	Modify	Remove
admin	Administrator	Edit	------
as	Guest	Edit	Remove

a. Anonymous User Login:

Select “Yes”, then anyone access the camera can watch the live video without username and password. However, If you try to enter the configuration page, the camera will ask you to key-in the username and password to log in.
Select "No", and then username and password are required to access the camera.

b. Universal Password:

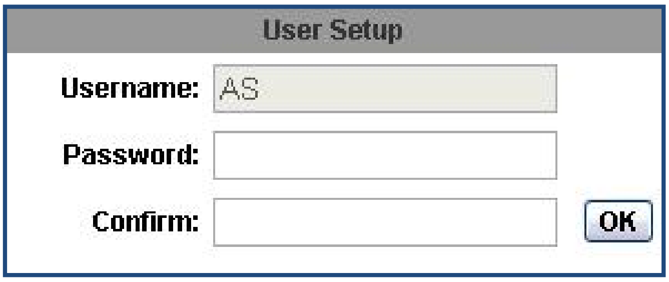
Select “Yes”, then user is allowed to login this IP Cam by universal password. Please refer to “Universal Password” chapter for more explanations.

Select “No” for universal password disabled.

c. Add user:

Type the user name and password, then click “Add/Set”. The guest user can only browse the live video page and is not allowed to enter the configuration page.

d. Click “edit” or “delete” in the user list to modify them. The system will ask you to key-in the password in the pop-up window before you edit the user information.



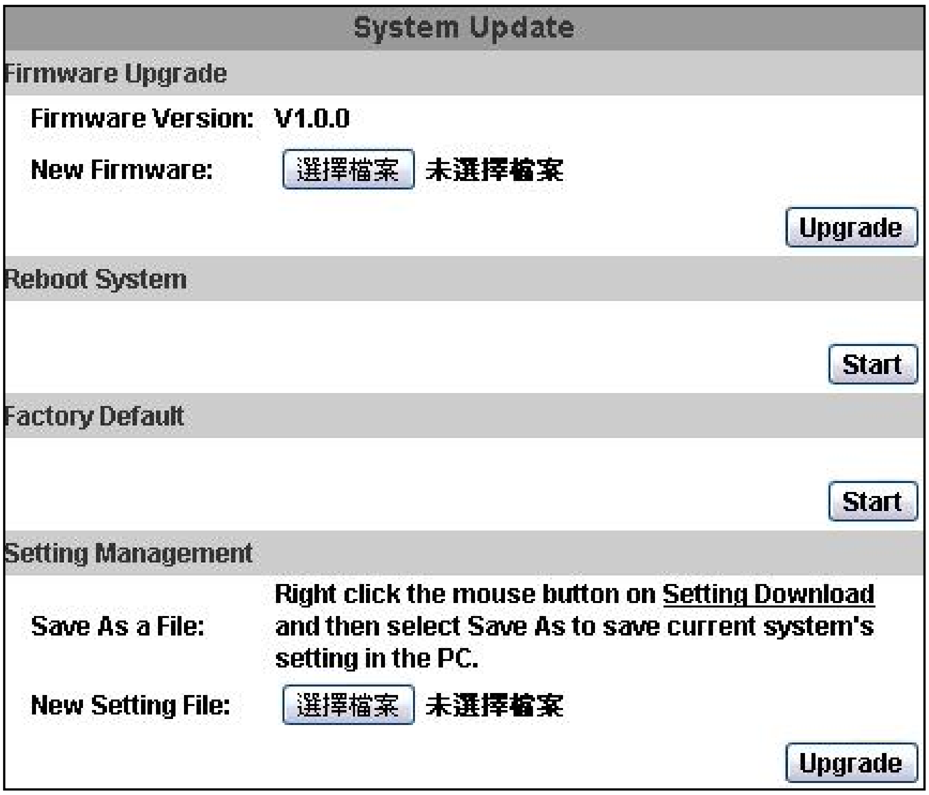
User Setup

Username: AS

Password:

Confirm:

3. System update:



System Update

Firmware Upgrade

Firmware Version: V1.0.0

New Firmware: 選擇檔案 未選擇檔案

Reboot System

Factory Default

Setting Management

Save As a File: Right click the mouse button on Setting Download and then select Save As to save current system's setting in the PC.

New Setting File: 選擇檔案 未選擇檔案

a. To update the firmware online, click “Browse…” to select the firmware. Then click “Upgrade” to proceed.

Note: The firmware upgrade might be accompanied by the changing of some setting and function, and the setting options might become different to the user manual that you're reading now.

b. Reboot system: re-start the IP camera

c. Factory default: delete all the settings in this IP camera.

d. Setting Management: User may download the current setting to PC, or upgrade from previous saved setting.

(i) Setting download:

Right-click the mouse button on Setting Download → Select "Save
AS…" to save current IP CAM setting in PC → Select saving directory
→ Save

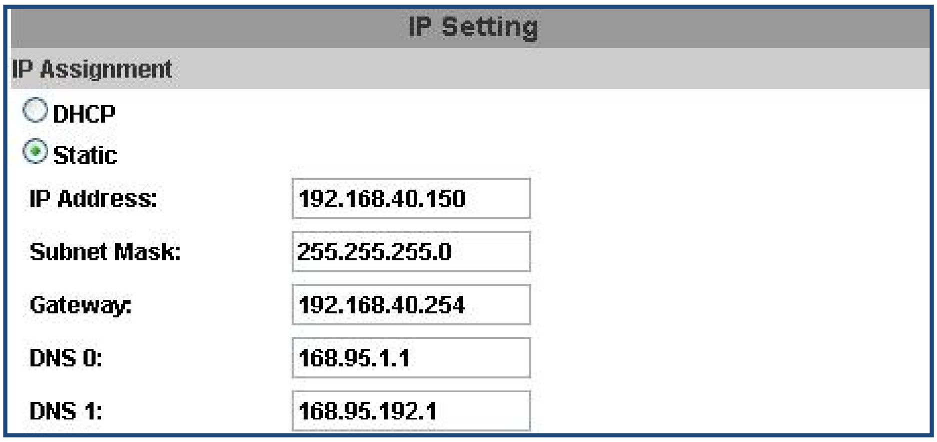
(ii) Upgrade from previous setting:

Browse → search previous setting → open → upgrade → Setting update confirm → click index.html. to return to main page

B. Network

1. IP Setting

a. IP Assignment



IP Setting

IP Assignment

○ DHCP

● Static

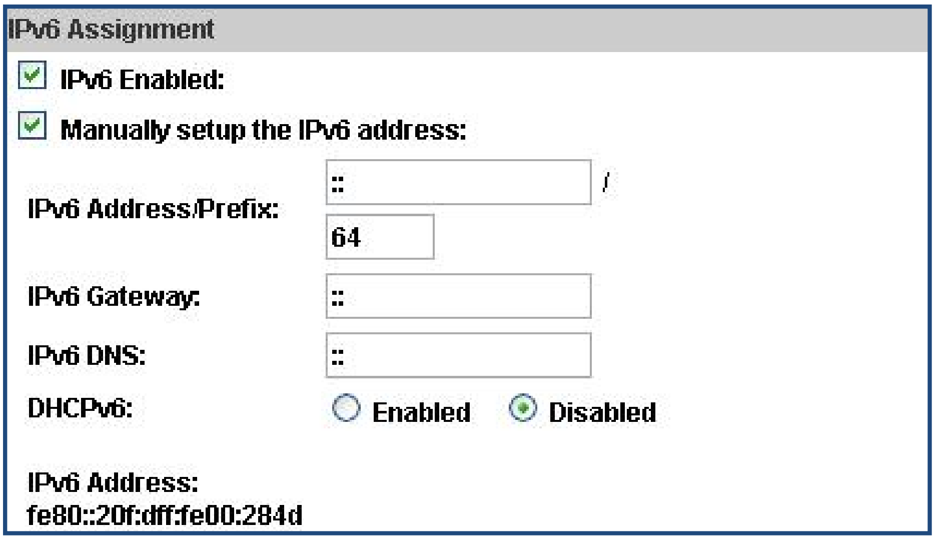
IP Address:	192.168.40.150
Subnet Mask:	255.255.255.0
Gateway:	192.168.40.254
DNS 0:	168.95.1.1
DNS 1:	168.95.192.1

IP Camera supports DHCP and static IP.

(i) DHCP: Using DHCP, IP CAMERA will get all the network parameters automatically.

(ii) Static IP: Please type in IP address, subnet mask, gateway, and DNS manually.

b. IPv6 Assignment



IPv6 Assignment

☑ IPv6 Enabled:

☑ Manually setup the IPv6 address:

IPv6 Address/Prefix:	:: / 64
IPv6 Gateway:	::
IPv6 DNS:	::
DHCPv6:	○ Enabled ● Disabled

IPv6 Address:
fe80::20f:dff:fe00:284d

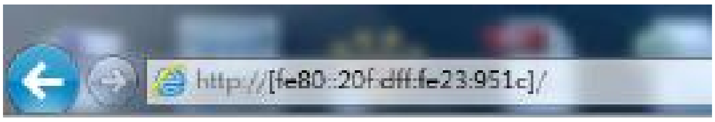
IPv6 is a newer numbering system that provides a much larger address pool than IPv4, which accounts for most of today’s Internet traffic. You can manually key-in IPv6 address, enable DHCPv6, and use automatically generated IPv6 address simultaneously.

(i) Manually setup the IPv6 address: Key-in Address, Gateway, and DNS.

(ii) DHCPv6: If you have a DHCPv6 server, enable it to assign the IPv6 automatically. The assigned IP address will be displayed beside the column.

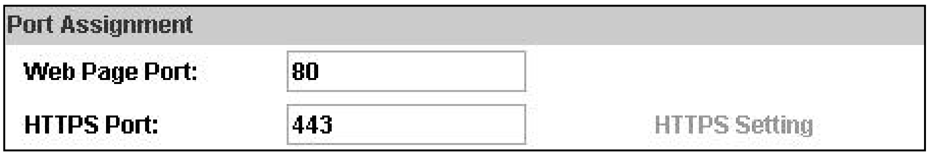
(iii) Automatically generated IPv6 Address: Here indicates a virtual IPv6 address generated automatically by IP camera. This virtual IPv6 address cannot use on WAN.

To use IPv6 address to access the IP camera, please open the web browser, and key-in [IPv6 address] in address bar. The [ ] parentheses mark is necessary.



http://[fe80::20f:dff:fe23:951c]/

c. Port assignment



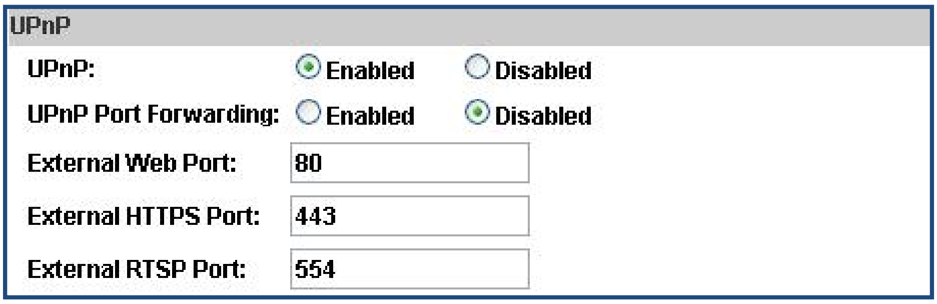
Port Assignment

Web Page Port:	80	
HTTPS Port:	443	HTTPS Setting

(i) Web Page Port: setup web page connecting port and video transmitting port (Default: 80)

(ii) HTTP Port: setup HTTPS connecting port (Default:443)

d. UPnP (Universal Plug and play)



UPnP

UPnP:	● Enabled	○ Disabled
UPnP Port Forwarding:	○ Enabled	● Disabled
External Web Port:	80	
External HTTPS Port:	443	
External RTSP Port:	554	

This IP camera supports UPnP, If this service is enabled on your computer, the camera will automatically be detected and a new icon will be added to "My Network Places."

(i) UPnP Port Forwarding:

When the camera is installed under a router, Enable UPnP Port Forwarding to let the router open ports so that the video streams can be sent out from a LAN. Set Web Port, Http Port, and RTSP port, and make sure your router supports UPnP and the function has been activated.

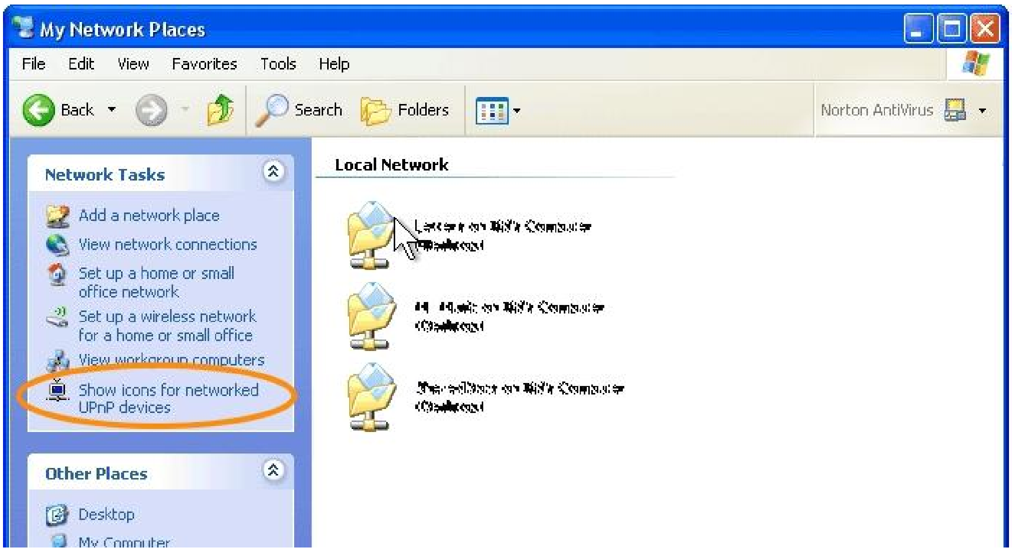
(ii) Note: UPnP must be enabled on your computer. Please follow the procedure to activate UPnP.

<Approach 1>

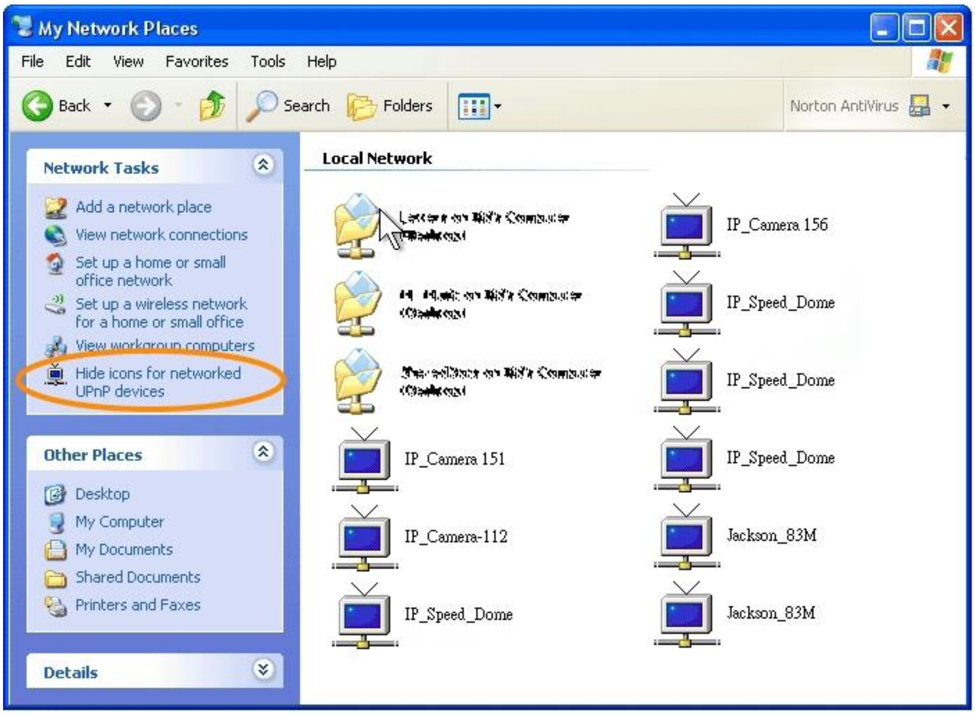
- Open the Control Panel from the Start Menu
- Select Add/Remove Programs
- Select Add/Remove Windows Components and open Networking
- Services section
- Click Details and select UPnP to setup the service
- The IP device icon will be added to “MY Network Places”
- User may double click the IP device icon to access IE browser

<Approach 2>

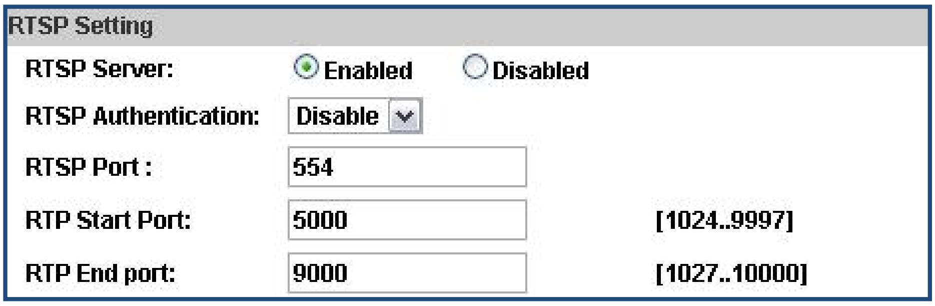
- Open "My Network Space", and click "Show icons for networked UPnP devices" in the tasks column on the left of the page. Windows may ask your confirmation for enabling the components. Click "Yes".



- Now you can see the IP device under the LAN. Double-click the icon to access the camera via web browser. To disable the UPnP click “Hide icons from networked UPnP devices” in the task column



e. RTSP setting



RTSP Setting

RTSP Server:	● Enabled ○ Disabled	
RTSP Authentication:	Disable	
RTSP Port :	554	
RTP Start Port:	5000	[1024..9997]
RTP End port:	9000	[1027..10000]

If you have a media player that supports RTSP protocol, you can use it to receive the video streaming from IP camera. The RTSP address can be set for two streamings respectively. Please jump to Chapter V-C:"Video Setting". There're setting field for RTSP address of two streamings.

(i) RTSP Server: enable or disable

(ii) RTSP Authentication:

"Disable" means everyone who knows your camera IP Address can link to your camera via RTSP. No username and password are required.

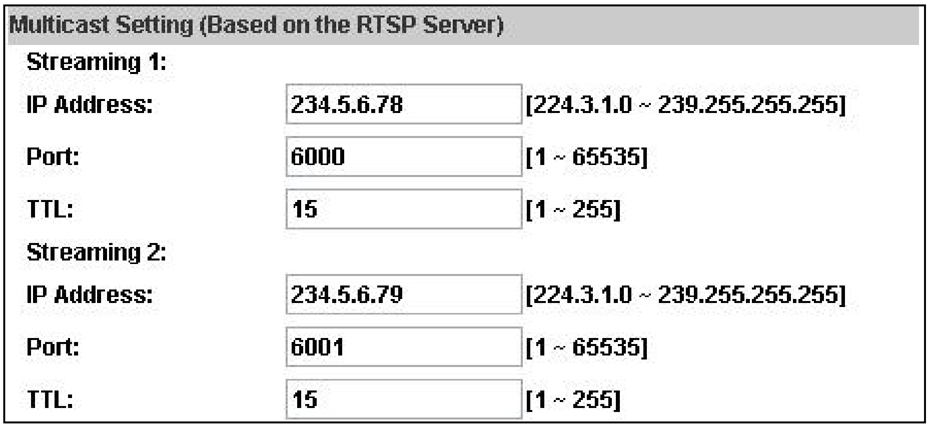
Under "Basic" and "Digest" authentication mode, the camera asks the user to give username and password before allows accessing. The password are transmitted as clear text under basic mode, which provides a lower level of security than under digest mode.

Make sure your media player supports the authenticaton schemes.

(iii) RTSP Port: setup port for RTSP transmitting (Default: 554)

(iv) RTSP Start and End Port: in RTSP mode, you may use TCP and UDP for connecting. TCP connection uses RTSP Port (554). UDP connection uses RTSP Start and End Port.

f. Multicast Setting (Based on the RTSP Server)



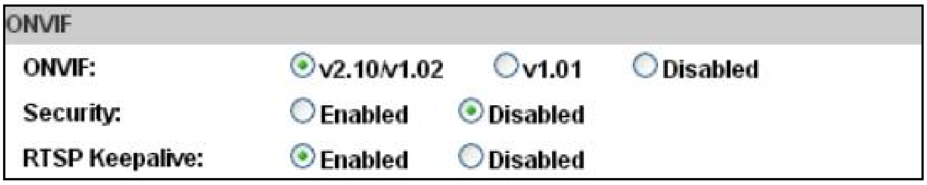
Multicast Setting (Based on the RTSP Server)

Streaming 1:		
IP Address:	234.5.6.78	[224.3.1.0 ~ 239.255.255.255]
Port:	6000	[1 ~ 65535]
TTL:	15	[1 ~ 255]
Streaming 2:		
IP Address:	234.5.6.79	[224.3.1.0 ~ 239.255.255.255]
Port:	6001	[1 ~ 65535]
TTL:	15	[1 ~ 255]

Multicast is a bandwidth conservation technology. This function allow several user to share the same packet sent from IP camera. To use Multicast, appoint IP Address and port here. TTL means the life time of packet, The larger the value is, the more user can receive the packet.

To use Multicast, be sure to enable the function "Force Multicast RTP via RTSP" in your media player. Then key-in the RTSP path of your camera: "rtsp://(IP address)/" to receive the multicast.

g. ONVIF



ONVIF

ONVIF:	● v2.10/v1.02	○ v1.01	○ Disabled
Security:	○ Enabled	● Disabled	
RTSP Keepalive:	● Enabled	○ Disabled	

(i) Choose your ONVIF version and settings.

Under ONVIF connection, the video will be transmitted by RTSP. Be sure to enable the RTSP server in IP setting, or you’re not able to receive the video via ONVIF.

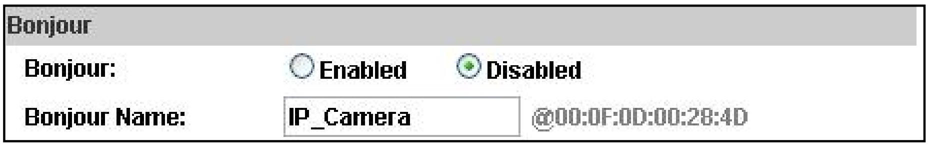
(ii) Security:

Select "Disable", then the username and password are not required when accessing the camera via ONVIF. Select "Enable", then username and password are necessary.

(iii) RTSP Keepalive:

When the function is enabled, the camera checks once in a while if the user who links to the camera via ONVIF still keeps connecting. If the connection had been broken, the camera stop transmitting video to user.

h. Bonjour



Bonjour

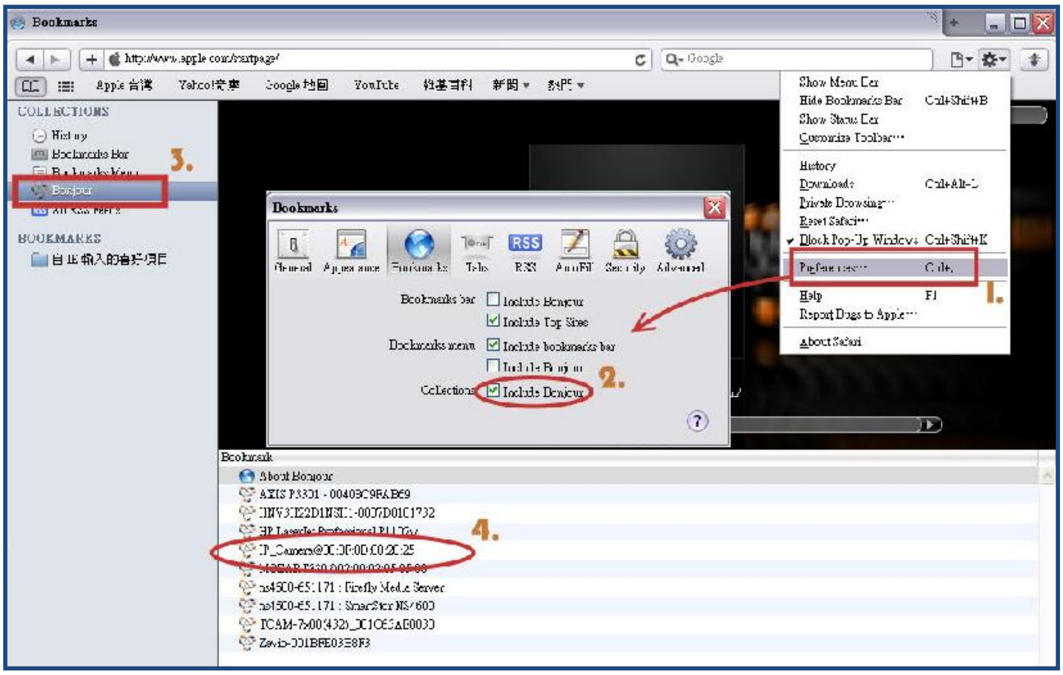
Bonjour: ○ Enabled ● Disabled

Bonjour Name: IP_Camera @00:0F:0D:00:28:4D

This function enables MAC systems to link to this IP camera. Key-in the name here.

The web browser "Safari" also has Bonjour function. Tick "Include Bonjour" in the bookmark setting, and you can see the IP camera appearing under the bonjour category. Click the icon to connect the IP camera.

So far the Bonjour function on Safari browser doesn’t support HTTPS protocol. If you select "https" mode for the camera, you can see the camera appearing on Safari’s bookmarks but cannot access camera via it.

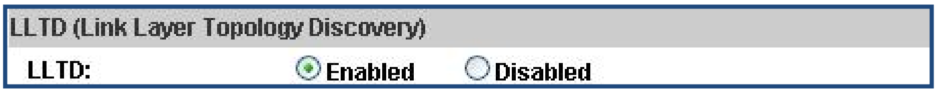


Bookmarks bar: □ Include Bonjour ☑ Include Top Sites

Bookmarks menu: ☑ Include bookmarks bar □ Include Bonjour

Collections: ☑ Include Bonjour

i. LLTD



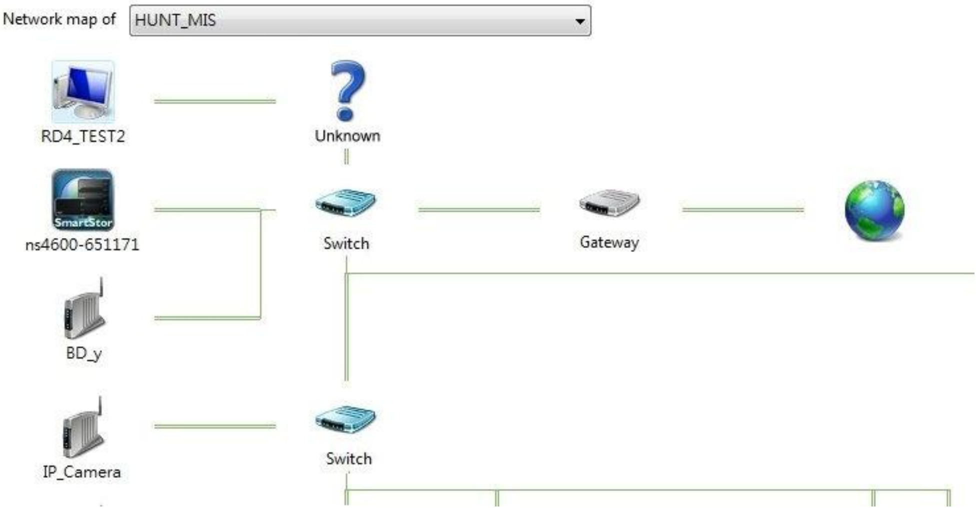
LLTD (Link Layer Topology Discovery)

LLTD: ● Enabled ○ Disabled

If your PC supports LLTD, enable this function then you can check the connection status, properties, and device position(like IP address) of this IP Camera in the network map.

In the computer running Windows Vista or Windows 7, you can find
LLTD through the path:

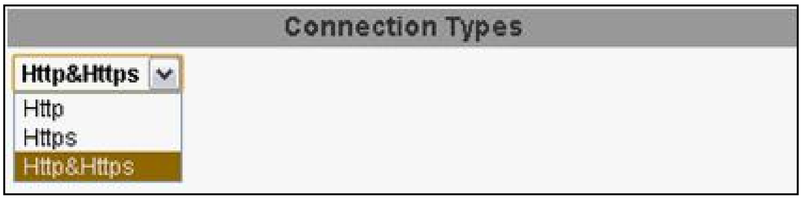
Call out the Control Panel → Network and Internet → Network and
Sharing Center → Click "See full map".



2. Advanced

a. Https (Hypertext Transfer Protocol Secure)

When the users access cameras via Https protocol, the transmitted information will be encrypted so that the security level is arisen.



You can select the connection type.

• Http: user can access the camera via Http path but cannot via Https path.

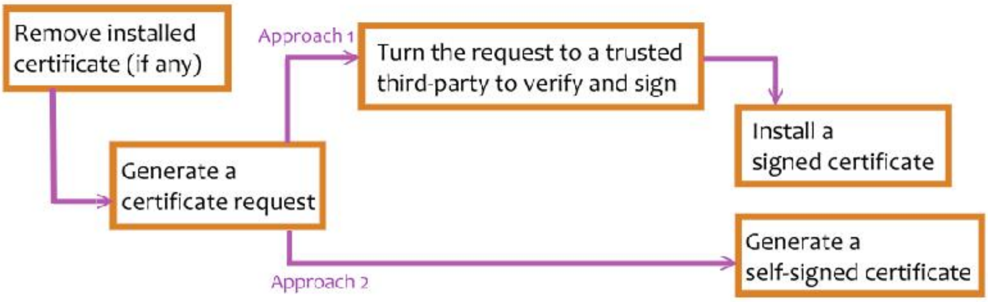
• Https: user can access the camera via Https path but cannot via Http path.

• Http & Https: Both the Http and Https path can be used to access the camera. When you change the setting of connection type, it may cause connection error or disconnection error if you switch the protocol directly. Therefore, Http & Https mode is necessary. If you want to change from Http to Https, please switch to

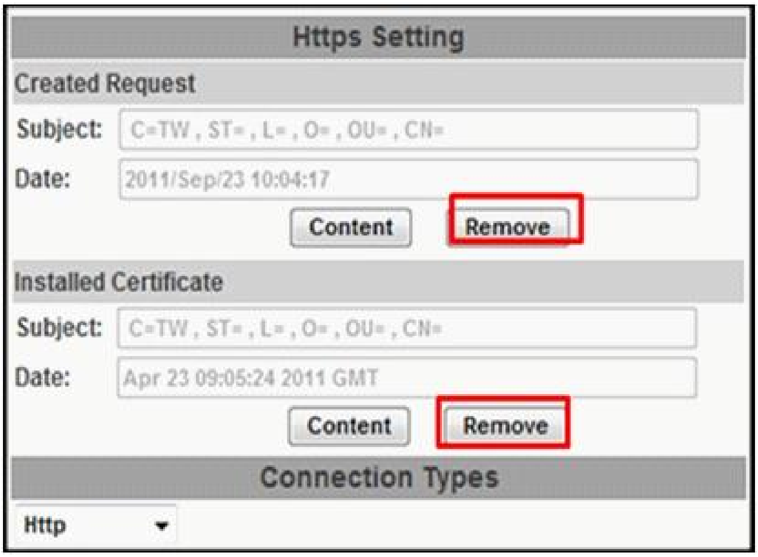
“Http & Https” mode first, and then switch to “Https” mode. Vise versa.

Https protocol has certificate verifying mechanism. When the user access a website via Https, the browser will check the certificate of that domain and verify its trustiness and secure.

Certificate generation process:


Remove installed certificate (if any)
Generate a certificate request
Approach 1
Turn the request to a trusted third-party to verify and sign
Install a signed certificate
Approach 2
Generate a self-signed certificate

(i) Remove the existing certificate: Before you generate a new certificate, please remove installed one. Select "Http" connection type and click "Remove". If a dialog box pops up to ask you to confirm, click “Yes”.



Https Setting

Created Request

Subject: C=TW , ST= , L= , O= , OU= , CN=

Date: 2011/Sep/23 10:04:17

Installed Certificate

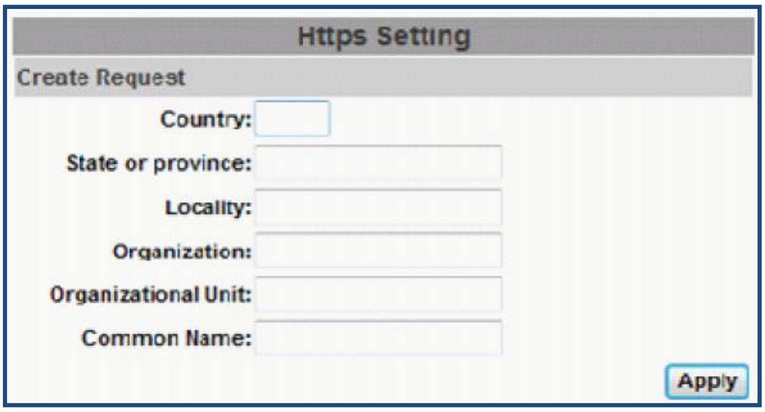
Subject: C=TW , ST= , L= , O= , OU= , CN=

Date: Apr 23 09:05:24 2011 GMT

Connection Types

Http

(ii) Created Request: Fill in the following form and click “apply”.



Https Setting

Create Request

Country:

State or province:

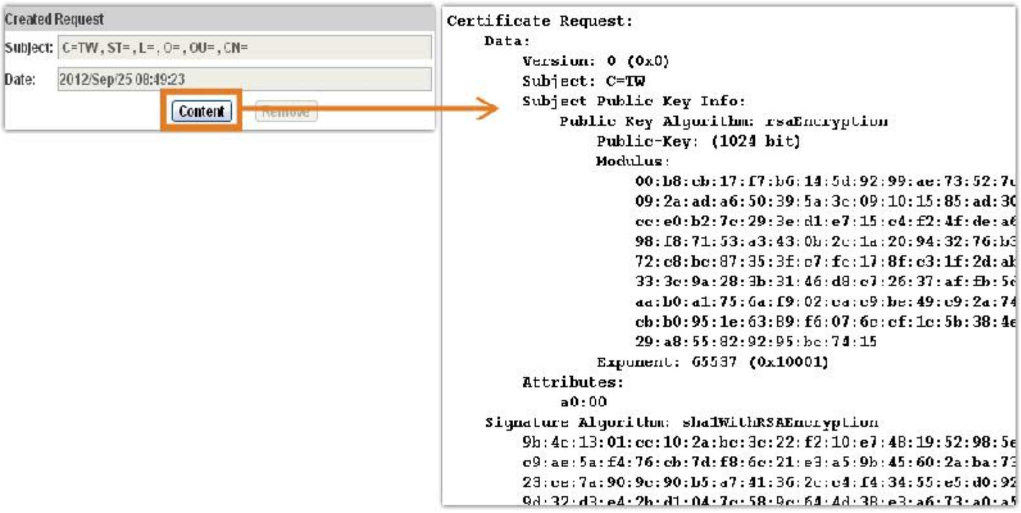
Locality:

Organization:

Organizational Unit:

Common Name:

(iii) After you generate a certificate request, if you choose to turn it to the trusted third-party to verify, please click “Content” and copy all the request content.



Created Request

Subject: C=TW, ST=, L=, O=, OU=, CN=

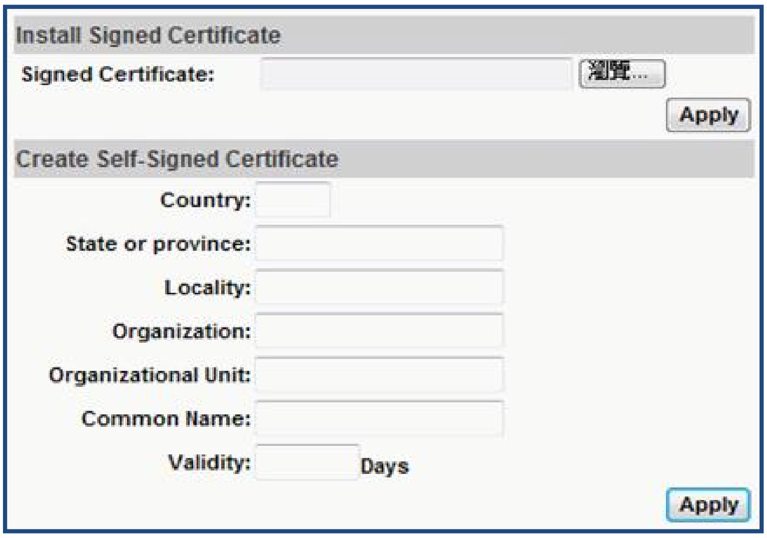
Date: 2012/Sep/25 08:49:23

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=TW
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b8:cb:17:f7:b6:14:5d:92:99:ae:73:52:7
                    09:2a:ad:a6:50:39:5a:3c:09:10:15:85:ad:3
                    cc:e0:b2:7c:29:3e:d1:e7:15:c4:f2:4f:de:a
                    98:f8:71:53:a3:43:0b:2c:1a:20:94:32:76:b
                    72:c8:bc:87:35:3f:c7:fc:17:8f:c3:1f:2d:a
                    33:3c:9a:28:3b:31:46:d8:c7:26:37:af:fb:5
                    aa:b0:a1:75:6a:f9:02:ca:c9:be:49:c9:2a:7
                    cb:b0:95:1e:63:89:f6:07:6c:cf:1c:5b:38:4
                    29:a8:55:82:92:95:bc:74:15
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        9b:4c:13:01:cc:10:2a:bc:3c:22:f2:10:e7:48:19:52:98:5
        c9:ae:5a:f4:76:cb:7d:f8:6c:21:e3:a5:9b:45:60:2a:ba:7
        23:ce:7a:90:9c:90:b5:a7:41:36:2c:c4:f4:34:55:e5:d0:9
        9d:32:d3:e4:2b:d1:04:7c:58:9c:64:4d:38:e3:a6:73:a0:a
```

(iv) According to the certificate source, there are two ways to install the certificate.

If you had sent the certificate request to do sign and received a signed certificate, please click” browse” and find the certificate file in your computer. Click “Apply” to install it.

If you choose to generate a self-signed certificate, fill in the following forms and set validity day, click “Apply” to finish installed it.



Install Signed Certificate

Signed Certificate:

Create Self-Signed Certificate

Country:

State or province:

Locality:

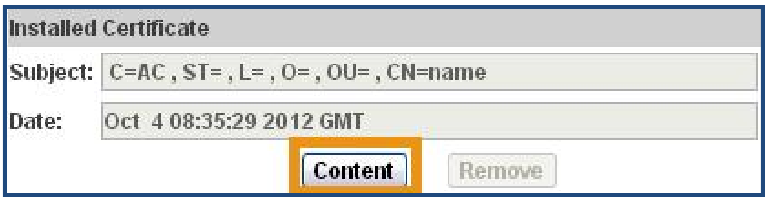
Organization:

Organizational Unit:

Common Name:

Validity: Days

After finishing installation, you can click “Content” to call out and check the certificate content.

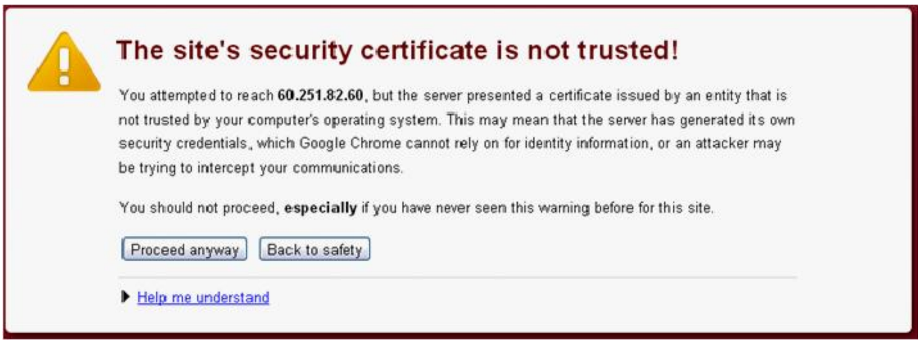


Installed Certificate

Subject: C=AC , ST= , L= , O= , OU= , CN=name

Date: Oct 4 08:35:29 2012 GMT

(v) To use Https to access camera, open your browser, and key-in "https:// (IP address)/" in the address bar. Now your data will be transmitted via encrypted communications, and the browser will check your certificate status. If it shows you a warning message:



The site's security certificate is not trusted!

You attempted to reach **60.251.82.60**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

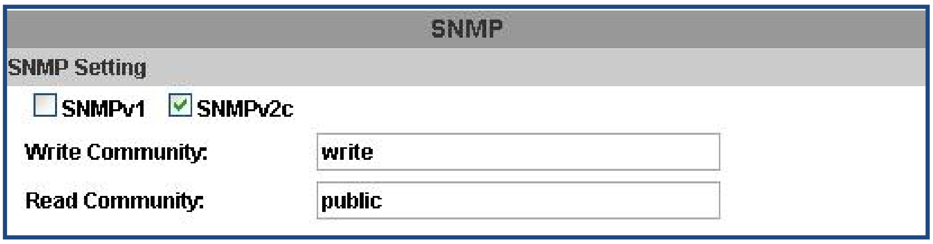
That means your certificate is self-signed or signed by distrusted institution. Click “Proceed anyway” and you can continue going to the camera page.

b. SNMP(Simple Network Management Protocol)

SNMP provides a simple framework for administering networked hardware. To manage the IP camera, you have to prepare a MIB browser or similar tools first. SNMPv1, SNMPv2c, and SNMPv3 can be enabled simultaneously.

The following examples are based on MG-SOFT MIB Browser. Depending on your MIS Browser, you may see different interface and options. Please refer to the user manual of your MIB Browser.

(i) SNMPv1 and SNMPv2:



SNMP

SNMP Setting

□ SNMPv1 ☑ SNMPv2c

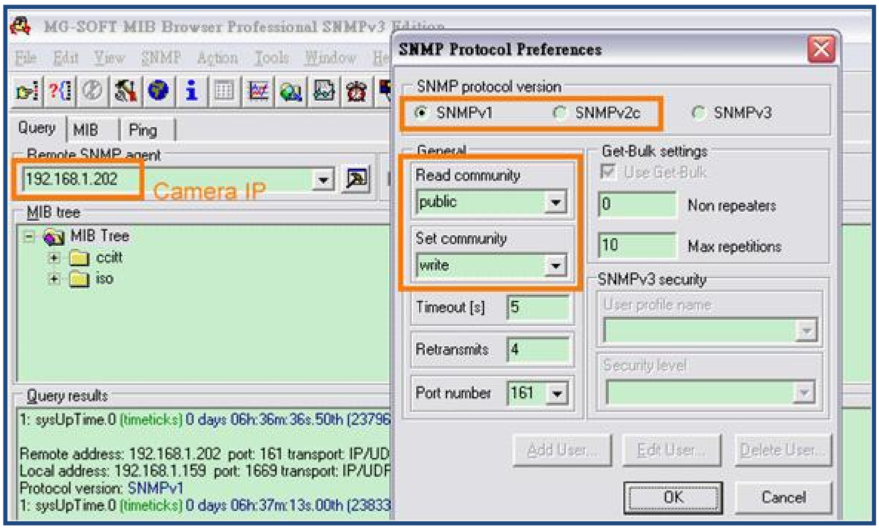
Write Community: write

Read Community: public

The term "Community name" in SNMPv1 and SNMPv2c can be roughly regarded as key. The person who has the community name has the authority to read or edit the information of IP camera via SNMP.

Tick the box to enable SNMPv1 or SNMPv2c protocal, and specify the community name for write(read and write) and read(read-only). The user who use read community name to access the IP camera cannot modify any data of this camera. The community name can be any English characters and numbers, and must be shorter than 31 bits.

Example:


MG-SOFT MIB Browser Professional SNMPv3 Edition
File Edit View SNMP Action Tools Window He
Query MIB Ping
Camera IP
MIB tree
MIB Tree
ccitt
iso
SNMP Protocol Preferences
Add User... Edit User... Delete User...
OK Cancel

Remote SNMP agent: 192.168.1.202

SNMP protocol version: ● SNMPv1 ○ SNMPv2c ○ SNMPv3

General
Read community: public
Set community: write
Timeout [s]: 5
Retransmits: 4
Port number: 161

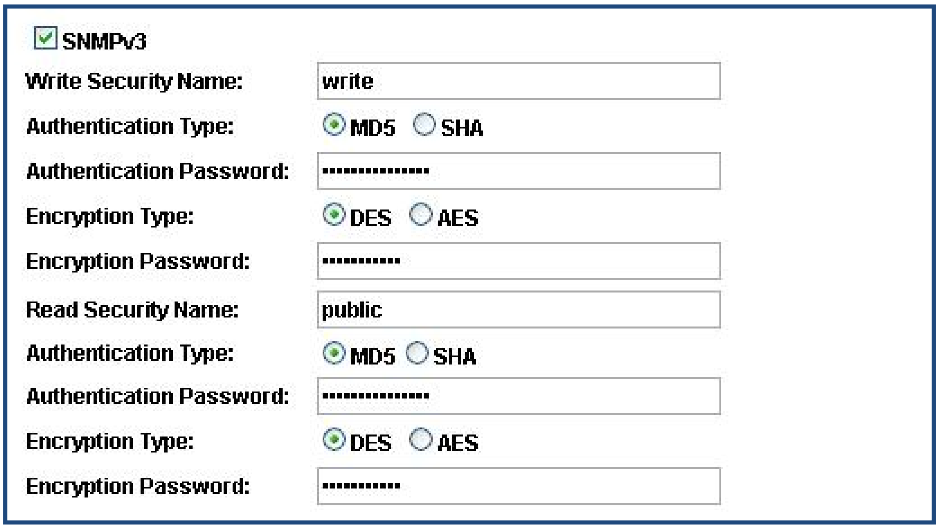
Get-Bulk settings
☑ Use Get-Bulk
0 Non repeaters
10 Max repetitions

SNMPv3 security
User profile name:
Security level:

Query results
```
1: sysUpTime.0 (timeticks) 0 days 06h:36m:36s.50th (23796
Remote address: 192.168.1.202  port: 161 transport: IP/UD
Local address: 192.168.1.159  port: 1669 transport: IP/UDF
Protocol version: SNMPv1
1: sysUpTime.0 (timeticks) 0 days 06h:37m:13s.00th (23833
```

Open the MIB Browser. Key-in camera IP address(192.168.1.202), select SNMPv1 or SNMPv2, and key-in the community name(Key-in the correct Read Community name “public”, the user has read authority to camera; key-in the correct Read Community name “public” and Key-in the correct Set community name “write”, the user has write authority to camera). Connection succeeds.

(ii) SNMPv3:



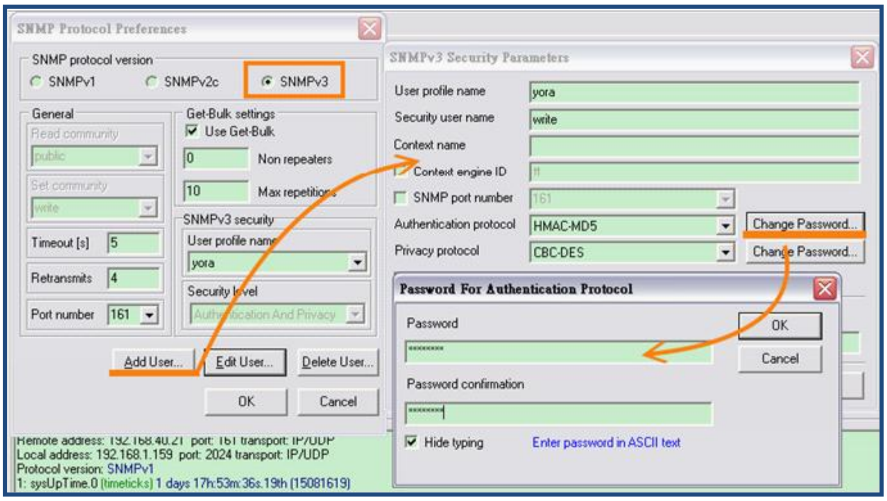
☑ SNMPv3

Write Security Name:	write
Authentication Type:	● MD5 ○ SHA
Authentication Password:	•••••••••••••••
Encryption Type:	● DES ○ AES
Encryption Password:	•••••••••••
Read Security Name:	public
Authentication Type:	● MD5 ○ SHA
Authentication Password:	•••••••••••••••
Encryption Type:	● DES ○ AES
Encryption Password:	•••••••••••

For data security reason, the authentication and encryption assurances are added when developing SNMPv3. The user has to give not only the security name(the same as "community name" in v1&v2c, or sometimes we call it "context name") but the password in order to access the IP camera. Please set security name, authentication type, authentication password, encryption type, encryption password of write and read respectively. The security name can be any English characters and numbers, and must be shorter than 31 bits. The password must be 8~64 bits in length.

Different from in SNMPv1 and v2c, the user have to create a account when using SNMPv3. In the account parameters, key-in the security name and password you set in the camera to get accessing.

<u>Example:</u>



SNMP Protocol Preferences

SNMP protocol version: ○ SNMPv1 ○ SNMPv2c ● SNMPv3

General
Read community: public
Set community: write
Timeout [s]: 5
Retransmits: 4
Port number: 161

Get-Bulk settings
☑ Use Get-Bulk
Non repeaters: 0
Max repetitions: 10

SNMPv3 security
User profile name: yora
Security level: Authentication And Privacy

SNMPv3 Security Parameters

User profile name: yora
Security user name: write
Context name:
☐ Context engine ID: ''
☐ SNMP port number: 161
Authentication protocol: HMAC-MD5
Privacy protocol: CBC-DES

Password For Authentication Protocol

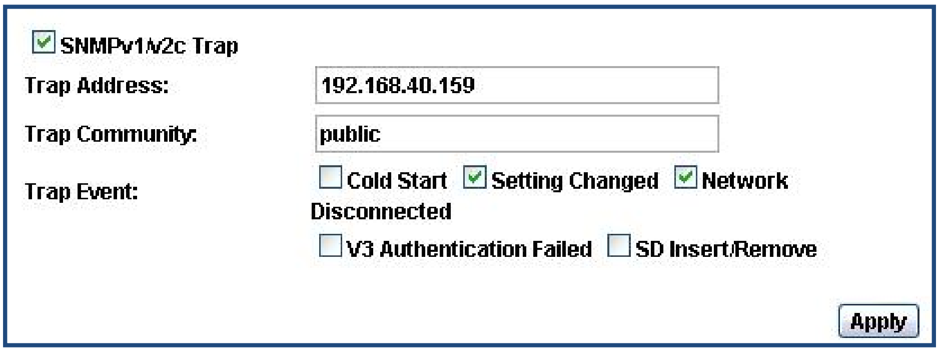
Password: ********
Password confirmation: ********
☑ Hide typing
Enter password in ASCII text

Remote address: 192.168.40.21 port: 161 transport: IP/UDP
Local address: 192.168.1.159 port: 2024 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTime.0 (timeticks) 1 days 17h:53m:36s.19th (15081619)

Select SNMPv3, add new user, and key-in correct security user name(write). Select the same authentication type with camera setting for authentication protocol(MD5), and key-in authentication password of write security. Select the same encryption type with camera setting for privacy protocol (DES), and key-in encryption password of write security. Click OK to add the user who has write authority to the camera. Connection succeeds.

If you want to add the new user who has read authority, key-in correct security user name(public), key-in authentication password of read security, and key-in encryption password of read security.

(iii) SNMPv1/SNMPv2 Trap:



☑ SNMPv1/v2c Trap

Trap Address: 192.168.40.159

Trap Community: public

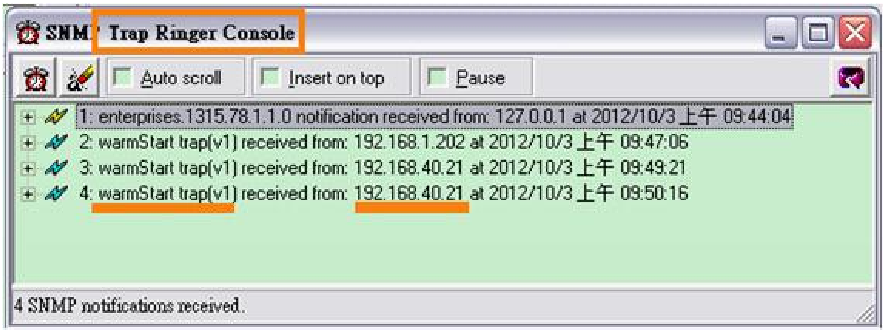
Trap Event: □ Cold Start ☑ Setting Changed ☑ Network Disconnected □ V3 Authentication Failed □ SD Insert/Remove

Trap is a mechanism that allows the managed device to send messages to manager instead of waiting passively for polling from the manager. Specify the trap event. When those events happen, the camera will send the ring message to the Trap Address, which is usually the manager's IP address. Trap Community means the community that can receive the trap message.

Note: Trap Address must be under the same LAN with IP camera.

- Cold Start: The camera starts up or reboots.
- Setting changed: The SNMP setting is changed.
- Network Disconnected: The network connection was broken down. (The camera will send trap messages after the network being connected again)
- V3 Authentication Failed: A SNMPv3 user account tries to get authentication but failed. (Due to incorrect password or community)
- SD Insert / Remove: A Micro SD card is inserted or removed.

Example:

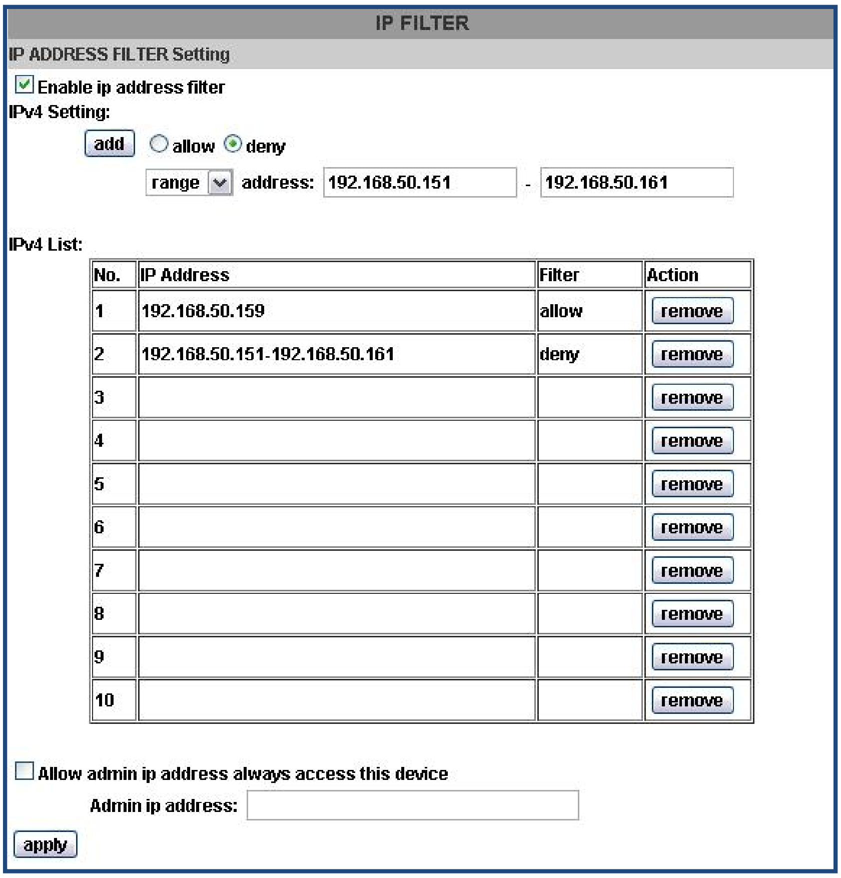


```
1: enterprises.1315.78.1.1.0 notification received from: 127.0.0.1 at 2012/10/3 上午 09:44:04
2: warmStart trap(v1) received from: 192.168.1.202 at 2012/10/3 上午 09:47:06
3: warmStart trap(v1) received from: 192.168.40.21 at 2012/10/3 上午 09:49:21
4: warmStart trap(v1) received from: 192.168.40.21 at 2012/10/3 上午 09:50:16
```

4 SNMP notifications received.

Open the MIB Browser. Use SNMPv1 or SNMPv2 to access the camera. When the SNMP setting is edited, Manager's MIB Browser (192.168.40.159) will receive the trap message of "setting change"from IP Camera (192.168.40.21).

c. Access List



IP FILTER

IP ADDRESS FILTER Setting

☑ Enable ip address filter

IPv4 Setting:

add ○ allow ● deny

range address: 192.168.50.151 - 192.168.50.161

IPv4 List:

No.	IP Address	Filter	Action
1	192.168.50.159	allow	remove
2	192.168.50.151-192.168.50.161	deny	remove
3			remove
4			remove
5			remove
6			remove
7			remove
8			remove
9			remove
10			remove

☐ Allow admin ip address always access this device

Admin ip address:

apply

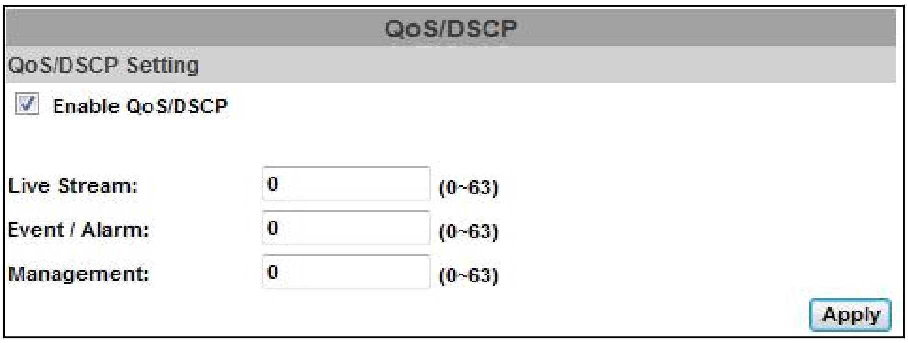
You can deny an IP address or a range of IP address so that they cannot access the IP camera. Tick the "enable" box, key-in the IP address you want to deny, select “deny" then click “Add" to add it to the list.

You can also choose to deny a range of IP address but allow one or several IP address of them. Take the picture above for example, IP address 192.168.50.151~161 are not allowed to connect to the camera, but only 192.168.50.159 can access. Note: In the list "allow" condition must be ranked before "deny" condition.

For example, if we exchange the sequence, set "Deny: 192.168.50.151~192.168.50.161" for the first item and "Allow:
192.168.50.159" for the second item in the list, the IP "192.168.50.159" turns out to be denied by the camera because the "deny" condition has the priority according to our ranking way.

As for those IP addresses not included in the list, the default is “allow”.

d. QoS/DSCP(Quality of Server/Differentiated Services Code-point)



QoS/DSCP

QoS/DSCP Setting

☑ Enable QoS/DSCP

Live Stream: 0 (0~63)

Event / Alarm: 0 (0~63)

Management: 0 (0~63)

DSCP specifies a simple mechanism for classifying and managing network traffic and provide QoS on IP networks. DSCP is a 6-bit in the IP header for packet classification purpose.

Set up instruction:

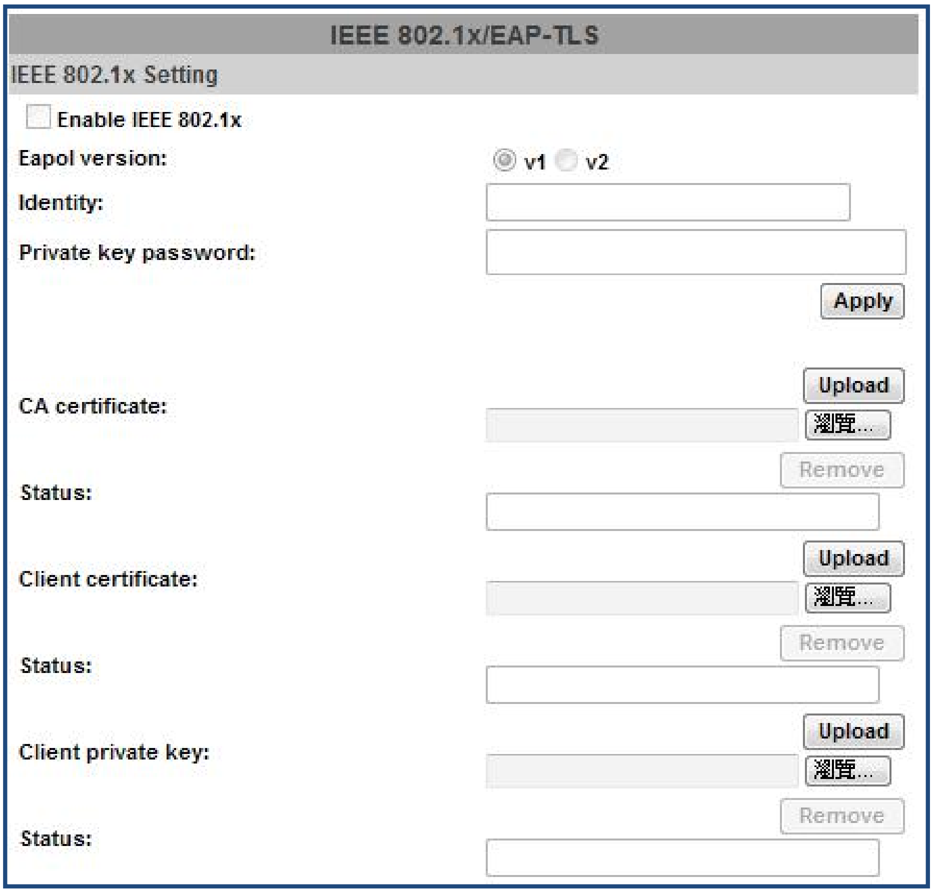
The number 0~63 for Live Stream, Event / Alarm, and Management represent the ratio that the bandwidth is divided. For example, if you set 5, 10, and 20 for the three items, then the bandwidth of the three item is 5:10:20. The item getting more bandwidth has lower probability to be delayed. There is no difference between setting "0, 0, 0" or "63, 63, 63" because under these two setting the three items will get equal bandwidth (1/3).

The three stream control the protocols respectively:

- Live Stream (Video and audio): RTP / RTSP
- Event/Alarm: FTP / SMTP / SAMBA / SIP
- Management: HTTPS / HTTP / SNMP

Note: The "Management" stream handles both the live view and the setting area of the web page on which the data is transferred via http/https protocol. If you prefer to distribute more bandwidth when using the web browser to watch the live video, please adjust the Management Stream instead of Live Stream.

e. IEEE 802.1x



IEEE 802.1x/EAP-TLS

IEEE 802.1x Setting

□ Enable IEEE 802.1x

Eapol version: ● v1 ○ v2

Identity:

Private key password:

CA certificate:

Status:

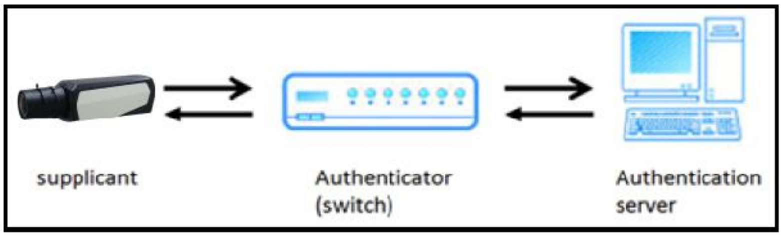
Client certificate:

Status:

Client private key:

Status:

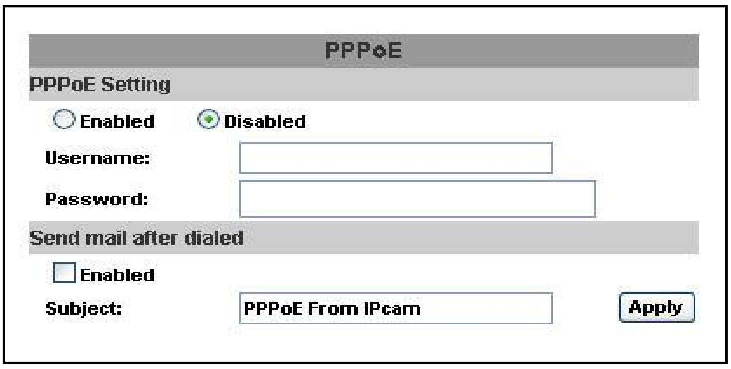
IEEE 802.1x is an IEEE standard for port-based Network Access Control. It provides an authentication mechanism to device wishing to attach to a LAN or WLAN. To use this function, you need a device to build IEEE 802.1x LAN at first. The EAPOL protocol support service identification and optional point to point encryption over the local LAN segment.



Please check what version of the authenticator and authentication server support. This camera supports EAP-TLS method. Please enter ID, password issued by the CA, then upload related certificates.

3. PPPoE & DDNS

a. PPPoE: Select “Enabled” to use PPPoE. Key-in Username and password for the ADSL connection. Send mail after dialed: When connect to the internet, it will send a mail to a specific mail account. For the mail setting, please refer to Server settings.



PPPoE

PPPoE Setting

○ Enabled ● Disabled

Username:

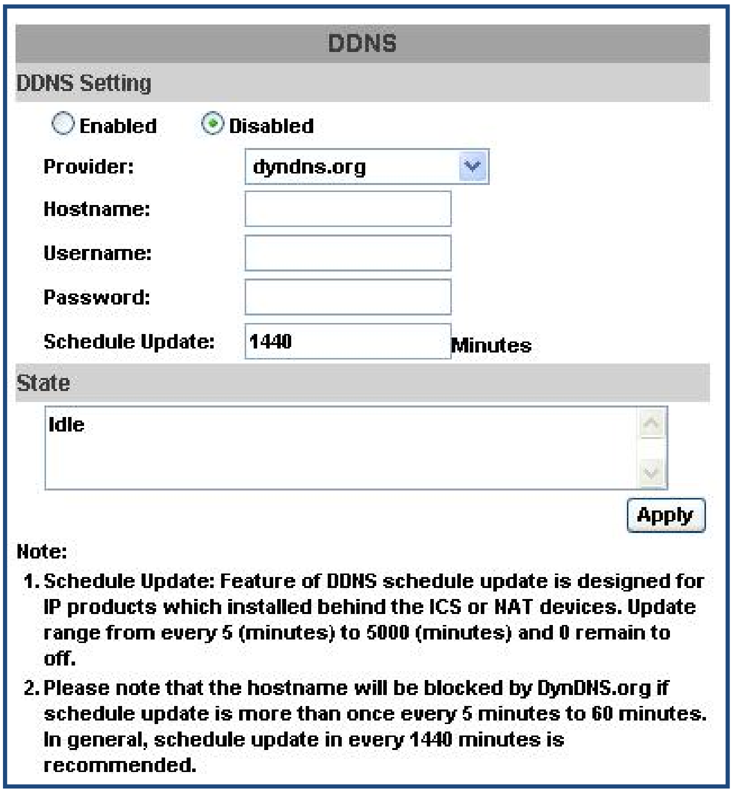
Password:

Send mail after dialed

□ Enabled

Subject: PPPoE From IPcam

b. DDNS:



DDNS

DDNS Setting

○ Enabled ● Disabled

Provider: dyndns.org

Hostname:

Username:

Password:

Schedule Update: 1440 Minutes

State

Idle

Note:

1. Schedule Update: Feature of DDNS schedule update is designed for IP products which installed behind the ICS or NAT devices. Update range from every 5 (minutes) to 5000 (minutes) and 0 remain to off.
2. Please note that the hostname will be blocked by DynDNS.org if schedule update is more than once every 5 minutes to 60 minutes. In general, schedule update in every 1440 minutes is recommended.

(i) It supports DDNS (Dynamic DNS) service.

(ii) Enable this service

(iii) Key-in the DynDNS server name, user name, and password.

(iv) Set up the IP Schedule update refreshing rate.

(v) Click “Apply”

(vi) If setting up IP schedule update too frequently, the IP may be blocked. In general, schedule update every day (1440 minutes) is recommended

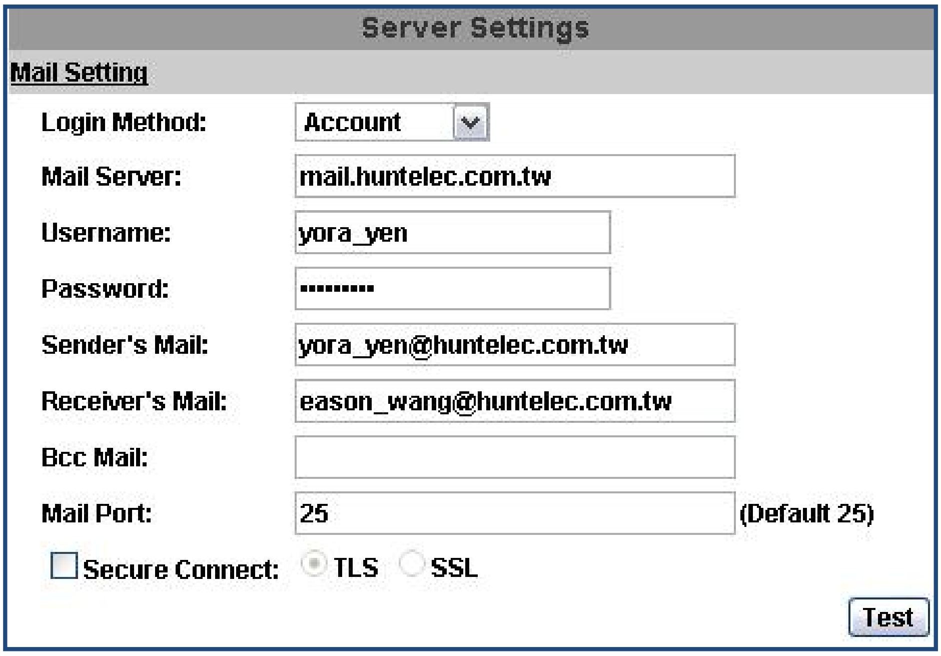
(vi) DDNS Status

- **Updating:** Information update
- **Idle:** Stop service
- **DDNS registration successful:** can now log by http://<username>. ddns.camddns.com: Register successfully.
- **Update Failed:** the name is already registered: The user name has already been used. Please change it.
- **Update Failed:** please check your internet connection: Network connection failed.
- **Update Failed:** please check the account information you provide: The server, user name, and password may be wrong.

4. Server Settings

The settings of Email, FTP and SAMBA are used when the event happens, schedule snapshot executes, or the alarm input is triggered. Select the item to display the detailed configuration options. You can configure either one or all of them.

a. Mail Settings



Server Settings

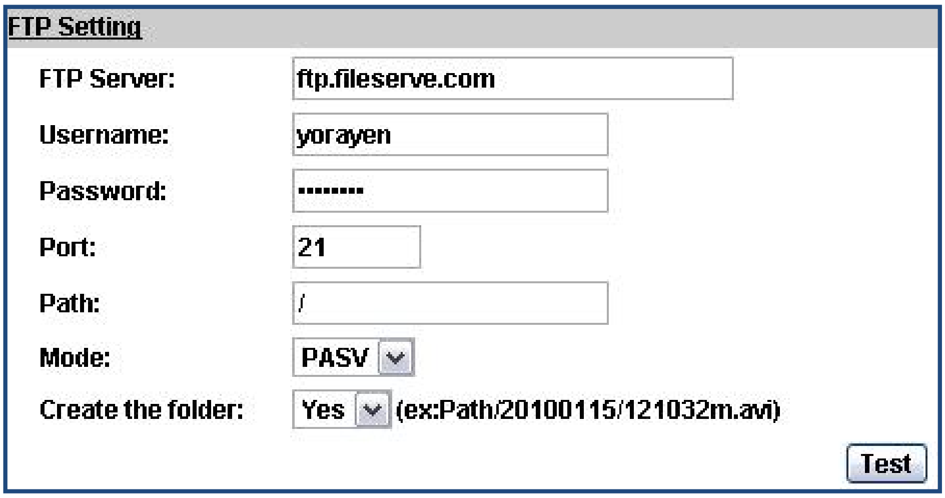
Mail Setting

Login Method:	Account	
Mail Server:	mail.huntelec.com.tw	
Username:	yora_yen	
Password:	•••••••••	
Sender's Mail:	yora_yen@huntelec.com.tw	
Receiver's Mail:	eason_wang@huntelec.com.tw	
Bcc Mail:		
Mail Port:	25	(Default 25)

☐ Secure Connect: ● TLS ○ SSL

Set up the server address and account information of your e-mail. Click “Apply” to save the setting, then use “Test” button to test the server connection. A message box will tell you “OK!” if it works, and a test e-mail will be sent to receiver’s mail address.

b. FTP



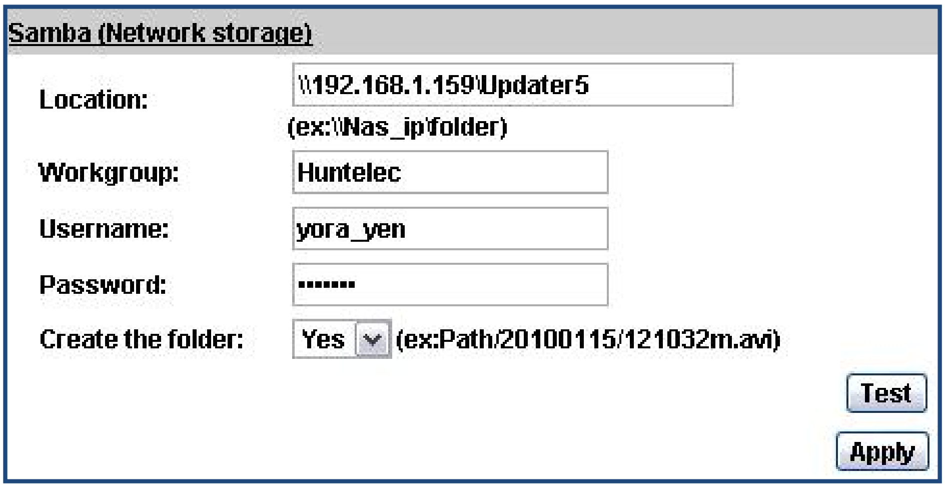
FTP Setting

FTP Server:	ftp.fileserve.com
Username:	yorayen
Password:	••••••••
Port:	21
Path:	/
Mode:	PASV
Create the folder:	Yes (ex:Path/20100115/121032m.avi)

Set up the server address and account information of your FTP. Click “Apply” to save the setting, then use “Test” button to test the server connection. A message box will tell you “OK!” if it works, and a test file will be uploaded to FTP space.

In PORT mode, the FTP server builds the connection to the user’s data port actively. However, from the user-side firewall’s standpoint, the action of connecting from FTP server is often considered to be dangerous and should be blocked. In PASV mode, the problem is solved: The FTP server waits for the data transmission connection built by the user. Make sure that the server supports the mode you select.

c. Samba:

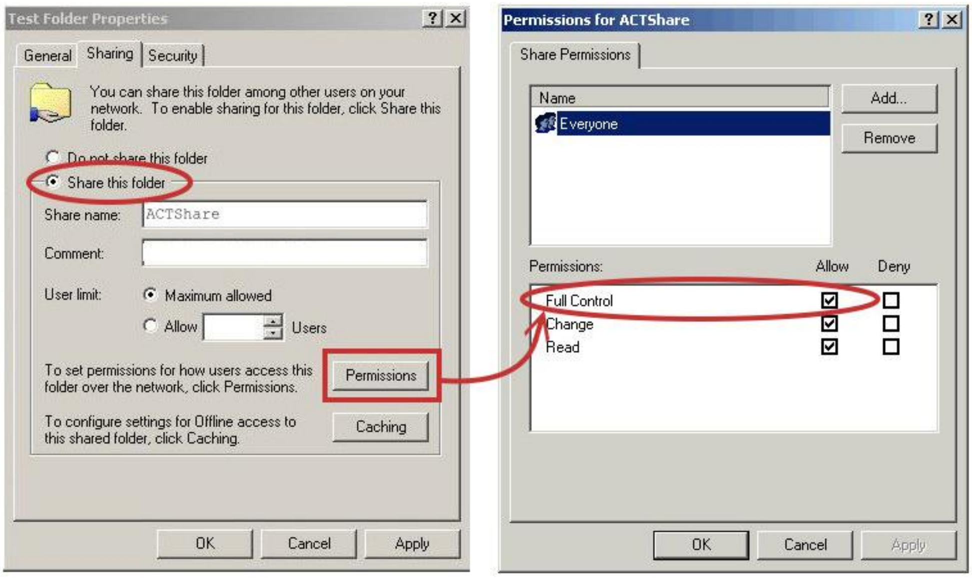


Samba (Network storage)

Location:	\\192.168.1.159\Updater5 (ex:\\Nas_ip\folder)
Workgroup:	Huntelec
Username:	yora_yen
Password:	•••••••
Create the folder:	Yes (ex:Path/20100115/121032m.avi)

Select this option to send the media files via a network neighborhood when an event is triggered. Click “Apply” to save the setting, then use “Test” button to test the server connection. A message box will tell you “OK!” if it works, and a test document will be created in the location.

If the test failed, check the sharing setting of your location folder. The folder properties must be “shared” and the permissions must be “Full Control” as the picture.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder
● Share this folder

Share name: ACTShare

Comment:

User limit: ● Maximum allowed
○ Allow Users

To set permissions for how users access this folder over the network, click Permissions. Permissions

To configure settings for Offline access to this shared folder, click Caching. Caching

Everyone

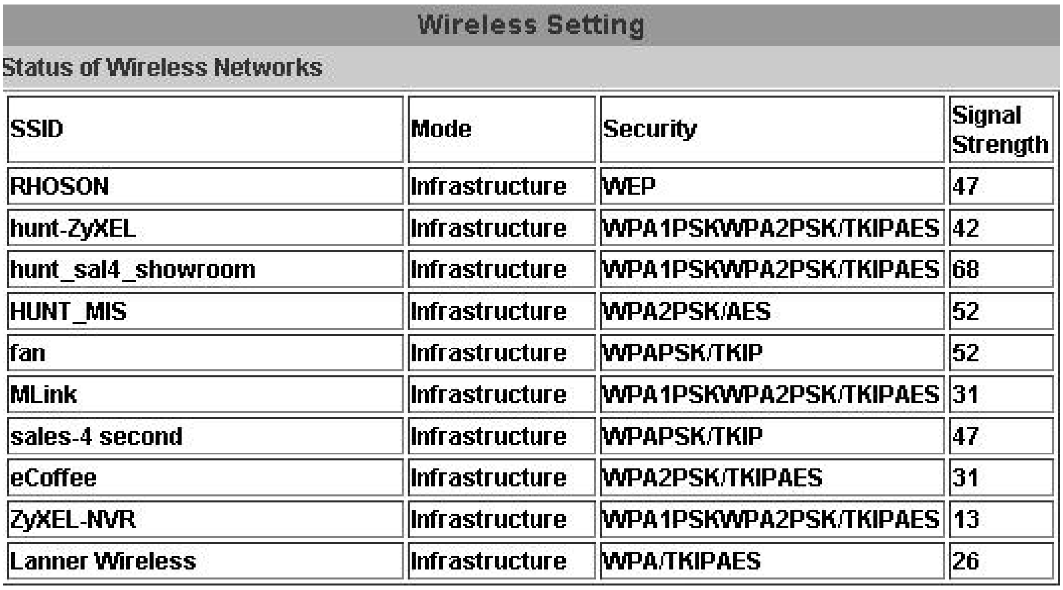
Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

5. Wireless Settings: Support 802.11 b/g/n

To set up the IP camera via wireless network, use ethernet cable to connect the camera first. After you finish the wireless setting and save it, remove the ethernet cable.

Note: The IP address is the same under both wireless and wired network. If the Ethernet cable is plugged in the camera, the IP camera will use it to link to the Internet instead of wireless router.

a. Status of Wireless Networks



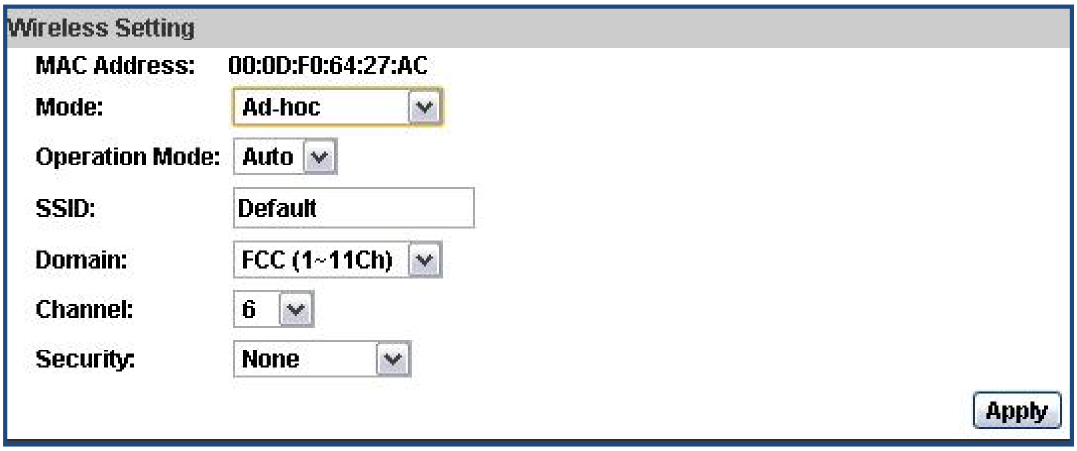
Wireless Setting

Status of Wireless Networks

SSID	Mode	Security	Signal Strength
RHOSON	Infrastructure	WEP	47
hunt-ZyXEL	Infrastructure	WPA1PSKWPA2PSK/TKIPAES	42
hunt_sal4_showroom	Infrastructure	WPA1PSKWPA2PSK/TKIPAES	68
HUNT_MIS	Infrastructure	WPA2PSK/AES	52
fan	Infrastructure	WPAPSK/TKIP	52
MLink	Infrastructure	WPA1PSKWPA2PSK/TKIPAES	31
sales-4 second	Infrastructure	WPAPSK/TKIP	47
eCoffee	Infrastructure	WPA2PSK/TKIPAES	31
ZyXEL-NVR	Infrastructure	WPA1PSKWPA2PSK/TKIPAES	13
Lanner Wireless	Infrastructure	WPA/TKIPAES	26

The camera scans and shows the SSID, Mode, Security, and Signal Strength of wireless network here.

b. Wireless Setting



Wireless Setting

MAC Address: 00:0D:F0:64:27:AC

Mode: Ad-hoc

Operation Mode: Auto

SSID: Default

Domain: FCC (1~11Ch)

Channel: 6

Security: None

(i) Mode: Infrastructure mode is used to link to the wireless router. Ad-hoc mode is used to link to the PC directly. "Domain" and "Channel" options appear only in the Ad-hoc mode.

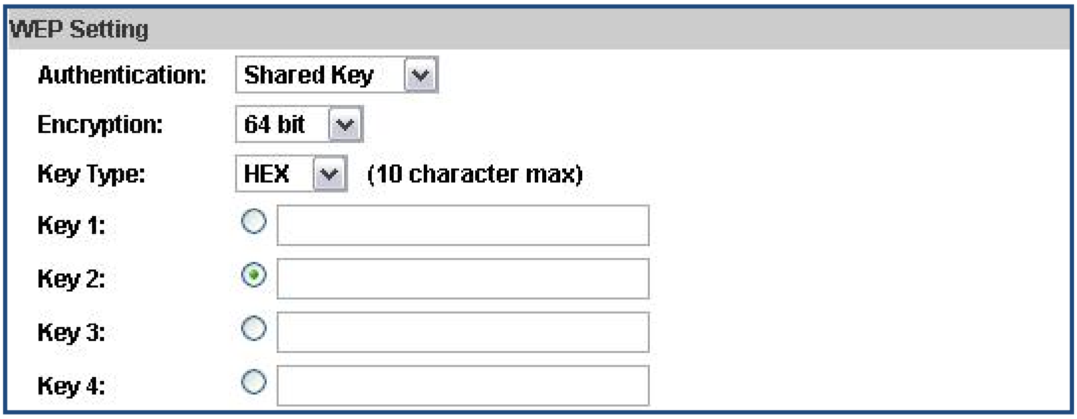
(ii) SSID: The ID of wireless network service.

(iii) Domain: The wireless network standards are different in each region.

Please select as the wireless system in your location. FCC is American standard. ETSI is European standard. JP is Japan standard.

(iv) Channel: Assign a channel for the camera in order to avoid interference. Security: Select WEP, WPA-PSK, or WPA2-PSK according to your wireless router setting.

c. WEP Setting



WEP Setting

Authentication:	Shared Key
Encryption:	64 bit
Key Type:	HEX (10 character max)
Key 1:	○
Key 2:	●
Key 3:	○
Key 4:	○

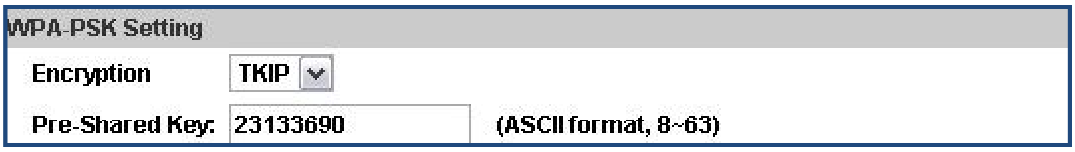
(i) Authentication: Open System or Shared Key, according to your wireless router.

(ii) Encryption: The option determine the length of key password. In HEX type, 10 characters are allowed if you select 64 bit while 26 characters are allowed if selecting 128bit; In ASCII type, 5 characters are allowed if you select 64 bit while 13 characters are allowed if selecting 128bit.

(iii) Key Type: In HEX type, the key password can only be hexadecimal numbers. In ASCII type, the key password can be any letters and numbers. (Capital and lowercase letters are regarded as different.)

(iv) Key 1~4: Key-in the key password. The length and type must be consistent with the settings above.

d. WPA-PSK Setting



WPA-PSK Setting

Encryption TKIP

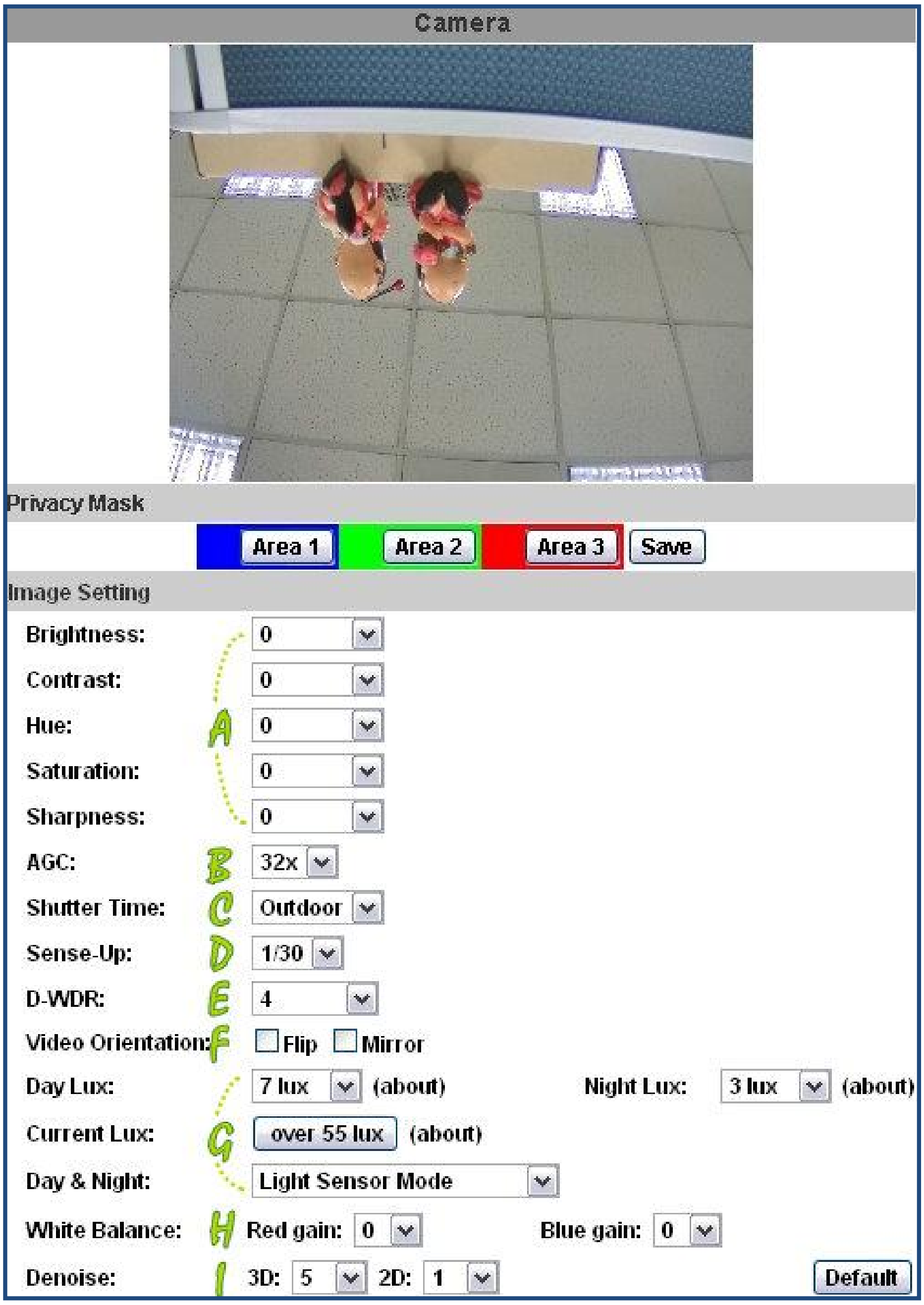
Pre-Shared Key: 23133690 (ASCII format, 8~63)

(i) Encryption: TKIP or AES, according to your wireless router.

(ii) Pre-Shared Key: Key-in the key password here. Any letters and numbers are allowed. (Capital and lowercase letters are regarded as different.)

C. A/V Settings

1. Image Setting



Camera

Privacy Mask

Area 1 | Area 2 | Area 3 | Save

Image Setting

Brightness: 0

Contrast: 0

Hue: 0

Saturation: 0

Sharpness: 0

AGC: 32x

Shutter Time: Outdoor

Sense-Up: 1/30

D-WDR: 4

Video Orientation: □ Flip □ Mirror

Day Lux: 7 lux (about) Night Lux: 3 lux (about)

Current Lux: over 55 lux (about)

Day & Night: Light Sensor Mode

White Balance: Red gain: 0 Blue gain: 0

Denoise: 3D: 5 2D: 1 Default

For the security and privacy purpose, there are three areas can be setup for privacy mask. Click Area button first and drag an area on the above image, and remember to save your setting. The masked area will not show on both the live view and recording.

Please refer to the details below for Image setting:

a. Brightness, Contrast, Hue, Saturation, Sharpness can be adjusted here.

b. AGC: Automatic gain control. The gain level of camera amplifier can adjusts with the environmental light. Enable this function and the brighter image can be got under dim light, but the level of noise may also increase.

c. Shutter Time: Choose as the location of your camera or fixed shutter time.
The shorter the shutter time is, the less light the camera receives and the image becomes darker.

d. Sense-Up: This function makes the shutter slower to get brighter image at night. The bigger the value you select, the slower the shutter speed becomes so that the image will get brighter, and moving subjects might be blurred.

Sense-Up option is only enabled when users select "outdoor" or "indoor" in shutter time option.

e. D-WDR: Digital wide dynamic range. This function enables the camera to reduce the contrast in the view to avoid the dark zones resulting from over and under exposure.

f. Video Orientation: Flip or mirror the image as your requirement.

g. Day & Night: The camera can detect the light level of environment. If you choose "Light Sensor Mode", the image will be turned to black and white at night in order to keep clear. To set light sensor mode, appoint a lux standard of switching D/N here. Current lux value is provided for reference. Under "Times Mode" the switch time of Color / Black and white is according to the given time. You can also control it by choosing "Color" or "B/W".

h. White Balance: Enhance red / blue color in the image.

i. Denoise: This function is able to filter the noise and blur from the image and show a clearer view. "3D" and "2D" are two different denoising approaches.

3D denoise analyzes successive pictures to detect the noise places while 2D denoise analyzes only single picture.

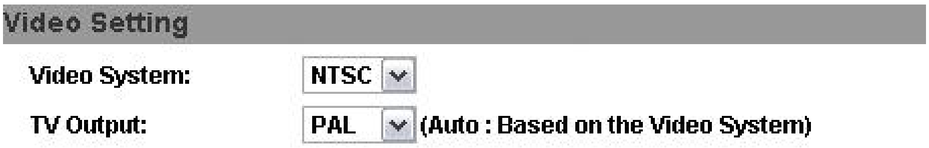
Note: When you select a number in "Shutter Time", actually the shutter time varies in a range and controlled by camera automatically. Following table shows the shutter time option and corresponding range.

Option	Shutter Time Range (sec.)
Outdoor	1/10000 ~ Selected number in "Sense-up"
Indoor	NTSC: 1/120 ~ Selected number in "Sense-up" PAL: 1/100 ~ Selected number in "Sense-up"
1/30	1/10000 ~ 1/30
1/50	1/10000 ~ 1/50
1/60	1/10000 ~ 1/60
1/100	1/10000 ~ 1/100
1/125	1/10000 ~ 1/125
1/250	1/10000 ~ 1/250
1/500	1/10000 ~ 1/500
1/1000	1/10000 ~ 1/1000
1/10000	1/10000
* Sense-up options: 1/30, 1/15, 1/10, 1/5	

2. Video Setting

a. Video System Settings:

Choose the Video System (digital signal) and TV Output (analog signal).

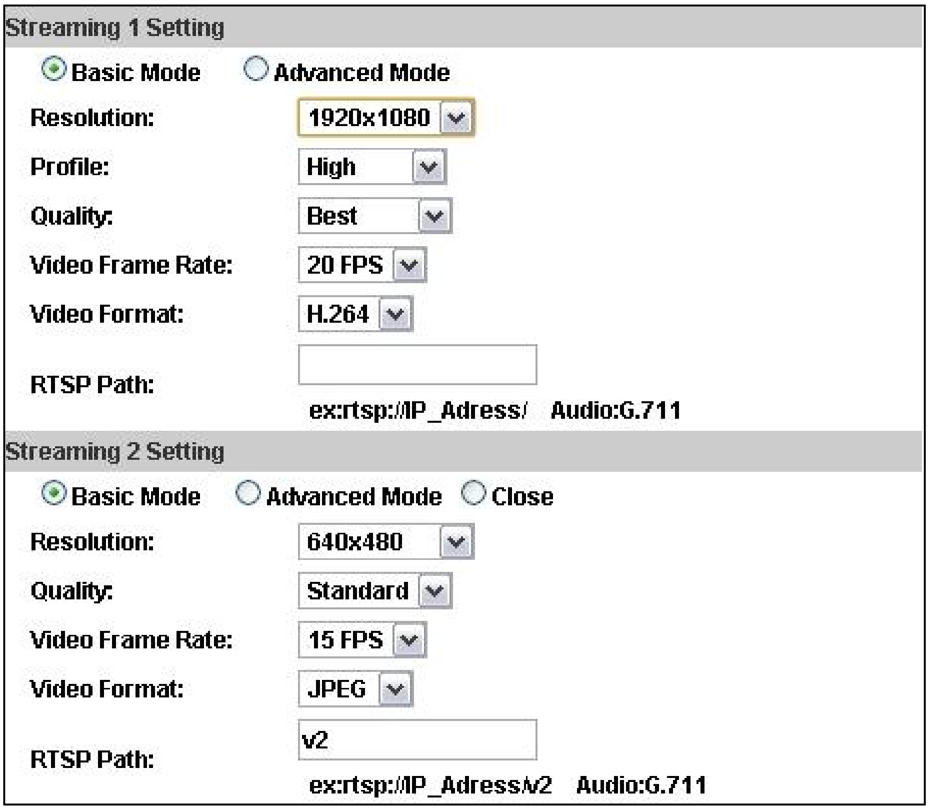


Video Setting

Video System: NTSC

TV Output: PAL (Auto : Based on the Video System)

b. Basic Mode of Streaming 1 and Streaming 2:



Streaming 1 Setting

● Basic Mode ○ Advanced Mode

Resolution: 1920x1080

Profile: High

Quality: Best

Video Frame Rate: 20 FPS

Video Format: H.264

RTSP Path:

ex:rtsp://IP_Adress/ Audio:G.711

Streaming 2 Setting

● Basic Mode ○ Advanced Mode ○ Close

Resolution: 640x480

Quality: Standard

Video Frame Rate: 15 FPS

Video Format: JPEG

RTSP Path: v2

ex:rtsp://IP_Adress/v2 Audio:G.711

(i) Resolution: 1920x1080,1280x720 , 640x480, 320x240, or 176x144

(ii) Profile: Profiles are different compression way of H.264. High profile provides better coding efficiency. Note that some devices do not support every profile. For example, iPhone4 only supports Main profile.

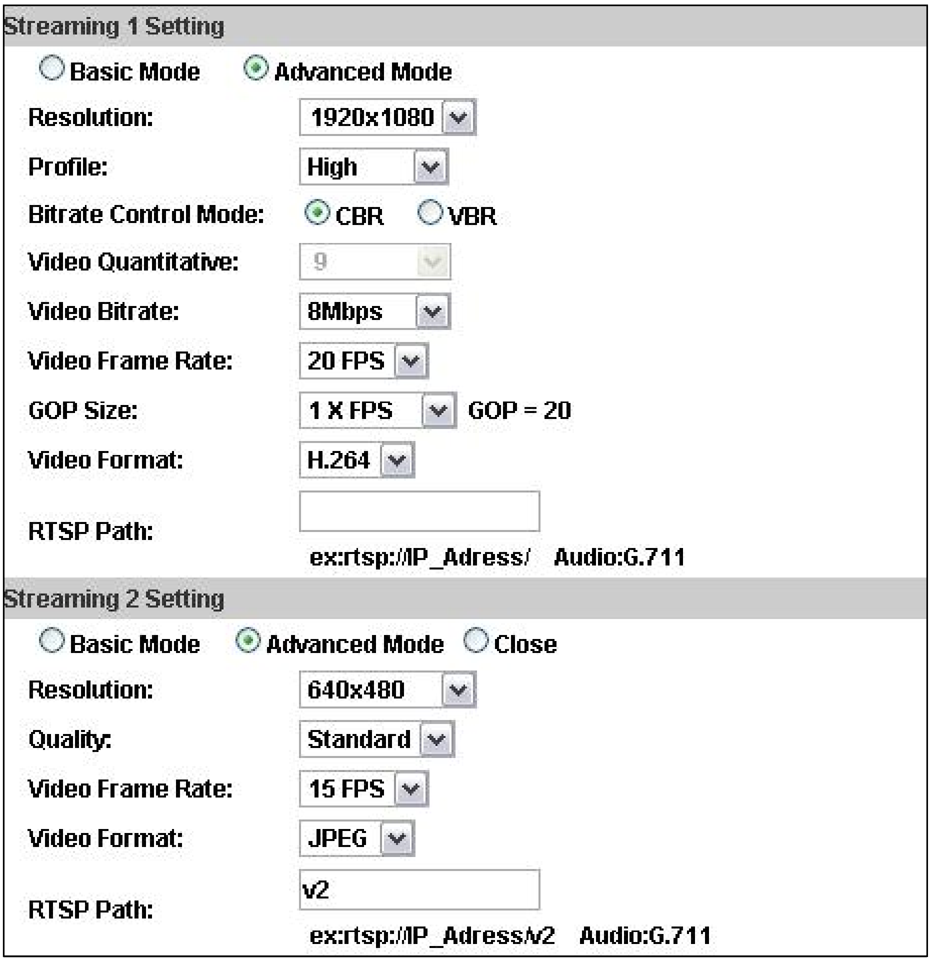
(iii) Quality: The higher the quality is, the bigger the file size is. It might affect Internet transmitting speed if the file gets too large.

(iv) Video Frame Rate: The video refreshing rate per second. The max value is affected by the input resolution you choose.

(v) Video Format: H.264 or M-JPEG

(vi) RTSP Path: Set the RTSP output connecting route

c. Advanced Mode of Streaming 1 and Streaming 2:



Streaming 1 Setting

○ Basic Mode ● Advanced Mode

Resolution:	1920x1080
Profile:	High
Bitrate Control Mode:	● CBR ○ VBR
Video Quantitative:	9
Video Bitrate:	8Mbps
Video Frame Rate:	20 FPS
GOP Size:	1 X FPS GOP = 20
Video Format:	H.264
RTSP Path:	 ex:rtsp://IP_Adress/ Audio:G.711

Streaming 2 Setting

○ Basic Mode ● Advanced Mode ○ Close

Resolution:	640x480
Quality:	Standard
Video Frame Rate:	15 FPS
Video Format:	JPEG
RTSP Path:	v2 ex:rtsp://IP_Adress/v2 Audio:G.711

(i) Resolution: 1920x1080,1280x720 , 640x480, 320x240, or 176x144

(ii) Profile: High profile provides better coding efficiency. Note that some devices do not support every profile. For example, iPhone4 only supports Main profile.

(iii) Bitrate Control Mode: In CBR(Constant Bit Rate) mode, the bitrate keeps consistent all over the video. In VBR(Variable Bit Rate) mode, the bitrate changes with the complexity extent of the video data.

VBR provides a better compression way and the file may be smaller. However, the VBR file size cannot be predicted. The image may become broken or lagged when your bandwidth is not enough for the data quantity you selected.

(iv) Video Quantitative: The quality parameter of VBR. The higher the value is, the higher the image quality is.

(v) Video Bitrate: The quality parameter of CBR. You can choose 32kbps~10Mkbps. The higher the value is, the higher the image quality is.

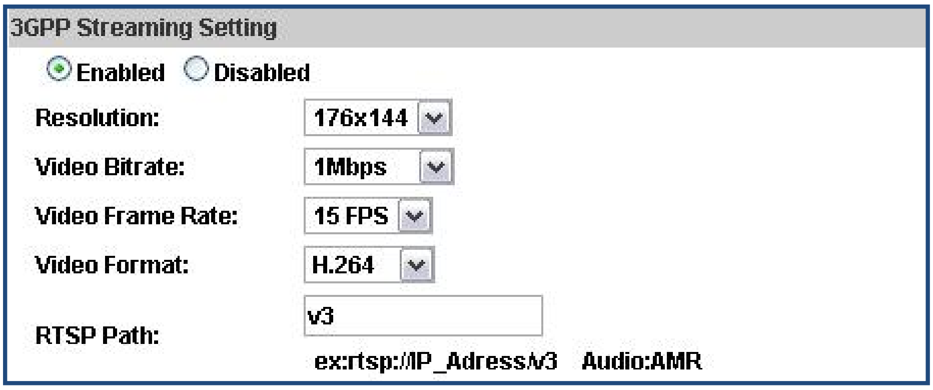
(vi) Video Frame Rate: The video refreshing rate per second. The max value is affected by the input resolution you choose.

(vii) GOP Size: It means “Group of Pictures”. The higher the GOP is, the better the quality is.

(viii) Video Format: H.264 or M-JPEG.

(ix) RTSP Path: RTSP output connecting route.

d. 3GPP Streaming mode:



3GPP Streaming Setting

● Enabled ○ Disabled

Resolution:	176x144
Video Bitrate:	1Mbps
Video Frame Rate:	15 FPS
Video Format:	H.264
RTSP Path:	v3 ex:rtsp://IP_Adress/v3 Audio:AMR

3GPP Streaming is designed for mobile viewing. Please lower the resolution, bitrate, or frame rate if the image flow isn't smooth when you use the mobile phone.

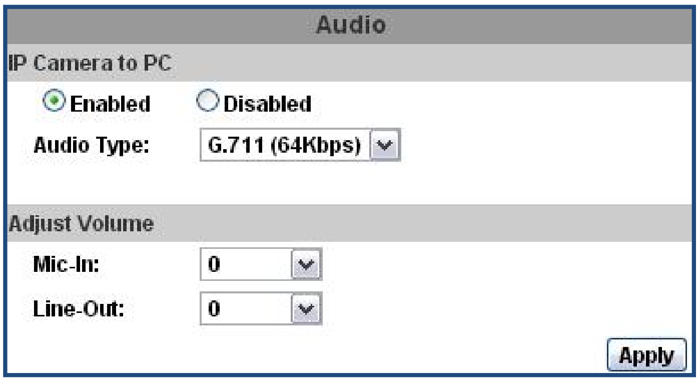
(i) <u>Resolution:</u> 640x480, 320x240, or 176x144
(ii) <u>Video Bitrate:</u> The higher the value is, the higher the image quality is.
(iii) <u>Video Frame Rate:</u> The video refreshing rate per second.
(iv) <u>Video Format:</u> H.264 or MPEG4
(v) <u>3GPP Path:</u> 3GPP output connecting route. If the IP address of your camera is 192.168.40.150, and you key-in "3g" in the column, the 3GPP path will be rtsp://192.168.40.150/3g.

To receive video via 3gpp, please remember to enable rtsp server in the "IP Settings" page.

3. Audio:

The IP Camera supports 2-way audio. Audio can be receive by the mic connected with the IP camera and transmitted to remote PC. User can also send audio from remote PC mic to IP Camera's external speaker.

a. IP Camera to PC



Audio

IP Camera to PC

● Enabled ○ Disabled

Audio Type: G.711 (64Kbps)

Adjust Volume

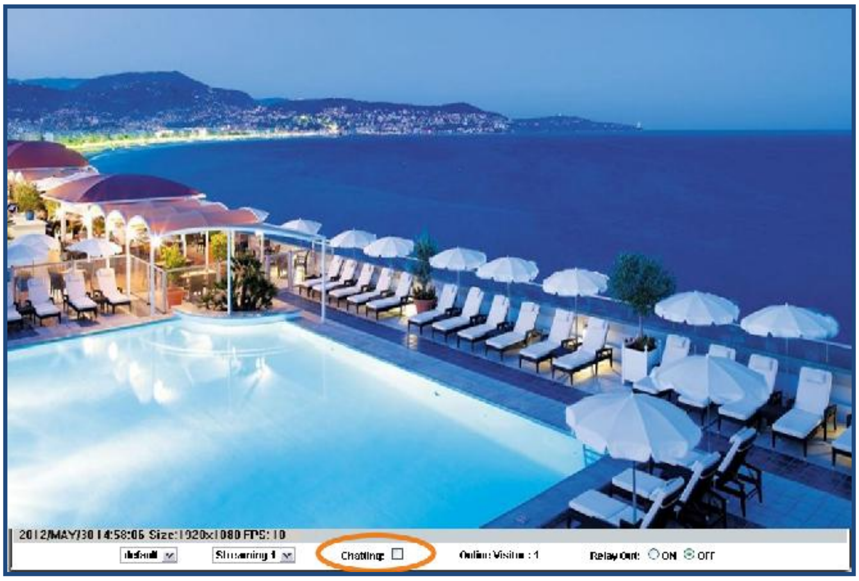
Mic-In: 0

Line-Out: 0

To receive Audio from IP camera, select “Enable” to start this function. The Audio compression format can be chosen from 3 options. You can also adjust the volume of 2-way audio.

b. PC to IP Camera

Tick “chatting” box in the browsing page, then your voice can be propagated from PC to camera.



2012/MAY/30 14:58:06 Size:1920x1080 FPS:10

default

Streaming 1

Chatting: □

Online Visitor : 1

Relay Out: ○ ON ● OFF

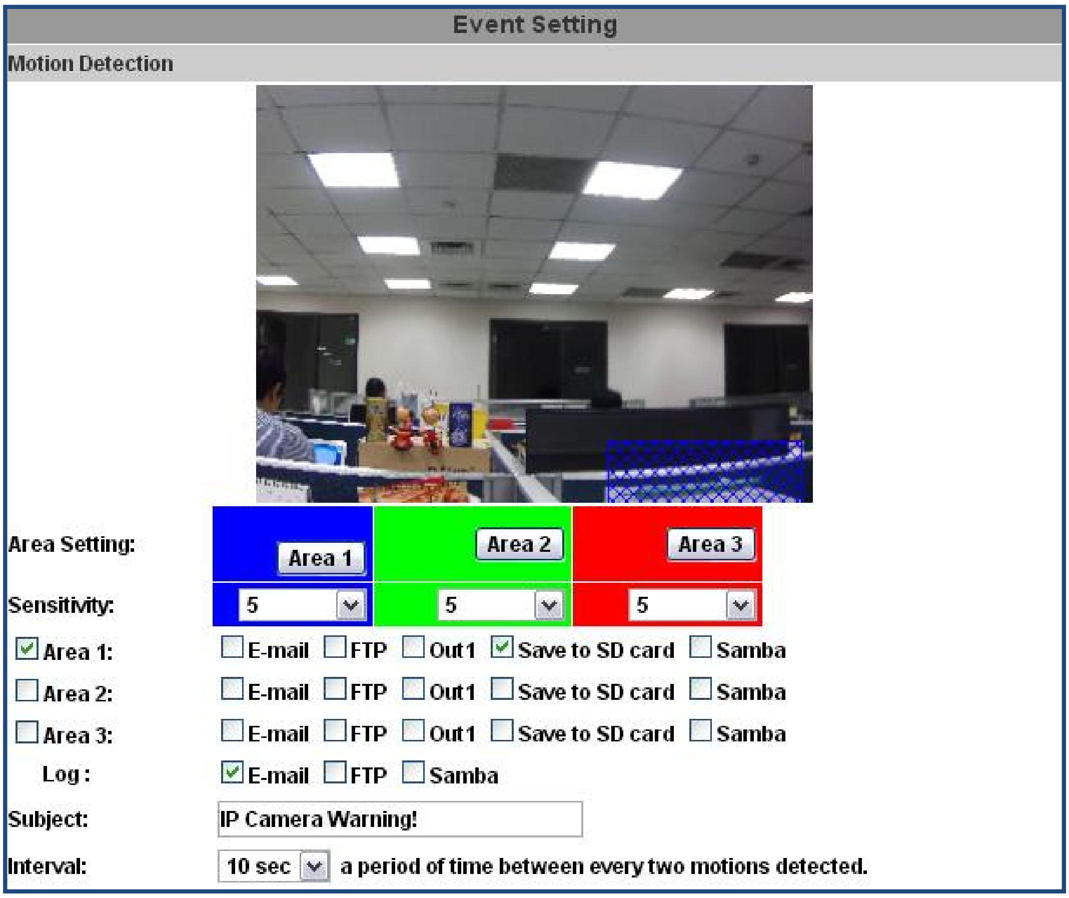
If "Chatting" and "Save to SD card" are enabled simultaneously, the sound quaily might be affected and becomes not smooth.

D. Event List

IP Camera provides multiple event settings.

1. Event Setting

a. Motion Detection



Event Setting

Motion Detection

Area Setting:	Area 1	Area 2	Area 3		
Sensitivity:	5	5	5		
☑ Area 1:	□ E-mail	□ FTP	□ Out1	☑ Save to SD card	□ Samba
□ Area 2:	□ E-mail	□ FTP	□ Out1	□ Save to SD card	□ Samba
□ Area 3:	□ E-mail	□ FTP	□ Out1	□ Save to SD card	□ Samba
Log :	☑ E-mail	□ FTP	□ Samba		

Subject: IP Camera Warning!

Interval: 10 sec a period of time between every two motions detected.

To enable motion detection, please tick "Area 1/2/3". Click "Area 1/2/3" in Area Setting, and draw an area on the preview screen. When motion in the area is detected, "Motion!" word will be marked on the live screen, and the camera can send video or snapshot to specific mail addresses, trigger the output device, or save video to FTP/ SD card/ Samba.

If you select "save to SD card", the video or snapshot will be saved to SD card. If you also tick E-mail/ FTP/ Samba of "Log" option, the motion detection log will be sent to E-mail/ FTP/ Samba simultaneously.

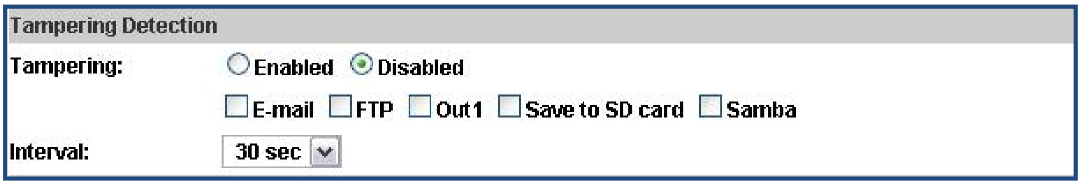
- Interval:

For example, if you select "10 sec" here, once the motion is detected and action is triggered, it cannot be triggered again within 10 seconds.

- Based on the schedule:

When the option box is ticked, only during the selected schedule time the motion detection is enabled. That is, for example, the 11th hour of Monday has not been colored in the schedule table, then no action will be triggered even the camera detects motion during 11:00~12:00 on Monday.

b. Tampering Detection



Tampering Detection

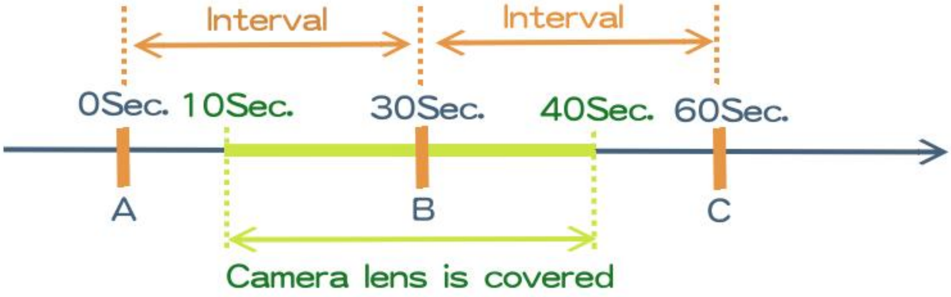
Tampering: ○ Enabled ● Disabled

□ E-mail □ FTP □ Out1 □ Save to SD card □ Samba

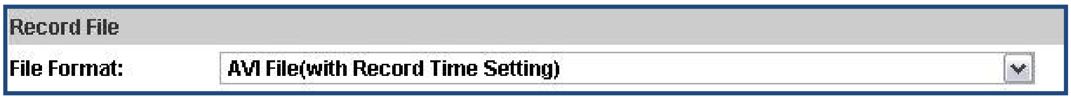
Interval: 30 sec

When the camera view is covered, moved, shot by strong light, or out of focus, the tampering detection will be triggered, and send snapshot or video to mail/FTP/Samba/SD card, or trigger the external alarm. Please select the alarm action.

- Interval: The tampering detecting interval. Take the diagram for example, we set interval as 30 second, and the camera lens is covered during 10- 40 sec. At time point B, the camera compares the view with time point A, and sends alarm when it found that the lens is covered. At time point C, the camera compares the view with time point B, and send alarm when it found that the lens is uncovered.



c. Record File


Record File

File Format:	AVI File(with Record Time Setting)

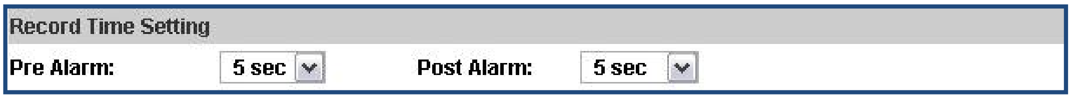
When an event happens, the IP camera can record a video clip or take snapshot, and then send to mail/ FTP/ Samba. Select what format you want to save.

• AVI File (with Record Time Setting): Save AVI video file. The video length is according to the value you set in Record Time Setting.

• JPEG File (Single File with Interval Setting): Save single JPEG picture file when event happens.

• JPEG Files (with Record Time Setting): Only when you select "JPEG" in streaming 1 video format of Video Setting, this option can be enabled. Select this option to save several JPEG picture files, and the successive picture files cover a period of time according to the value you set in Record Time Setting.

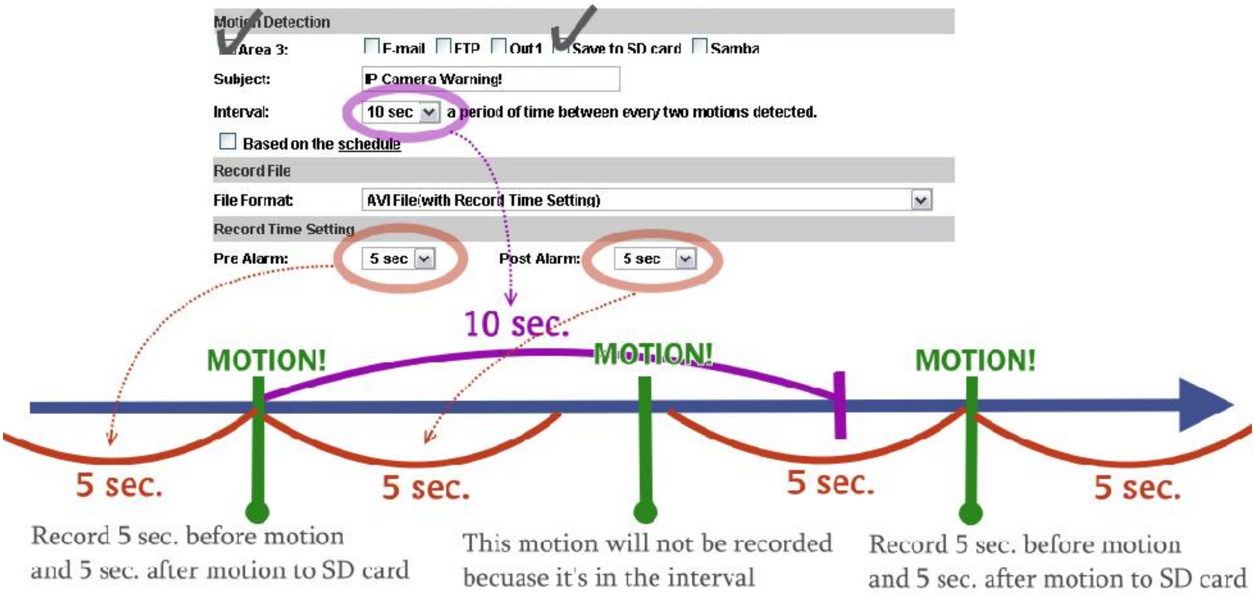
d. Record Time Setting


Record Time Setting

Pre Alarm:	5 sec	Post Alarm:	5 sec

When an event happens, the IP camera can record a video clip or take snapshot, and then send to mail/ FTP/ Samba. Select the video recording length before and after event happens.

- Diagram example of "Interval" and "Pre/ Post Alarm":



Motion Detection

Area 3: ☐E-mail ☐FTP ☐Out1 ☑Save to SD card ☐Samba

Subject: IP Camera Warning!

Interval: 10 sec a period of time between every two motions detected.

☐ Based on the schedule

Record File

File Format: AVI File(with Record Time Setting)

Record Time Setting

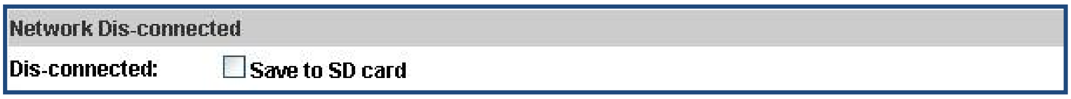
Pre Alarm: 5 sec Post Alarm: 5 sec

Record 5 sec. before motion and 5 sec. after motion to SD card

This motion will not be recorded becuase it's in the interval

Record 5 sec. before motion and 5 sec. after motion to SD card

e. Network Dis-connected



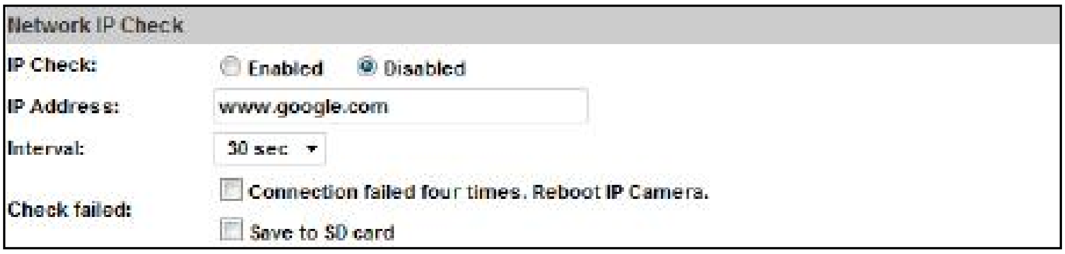
Network Dis-connected

Dis-connected: ☐Save to SD card

To avoid video loss, the camera will start to save the video to local SD card when it detect Ethernet cable is unplugged. The video recording will continuously be saved into SD card and divided into every 5 minutes a file until the network is reconnected successfully. The oldest file will be deleted if the capacity of SD card is full.

This function is only enabled under wire connection.

f. Network IP check

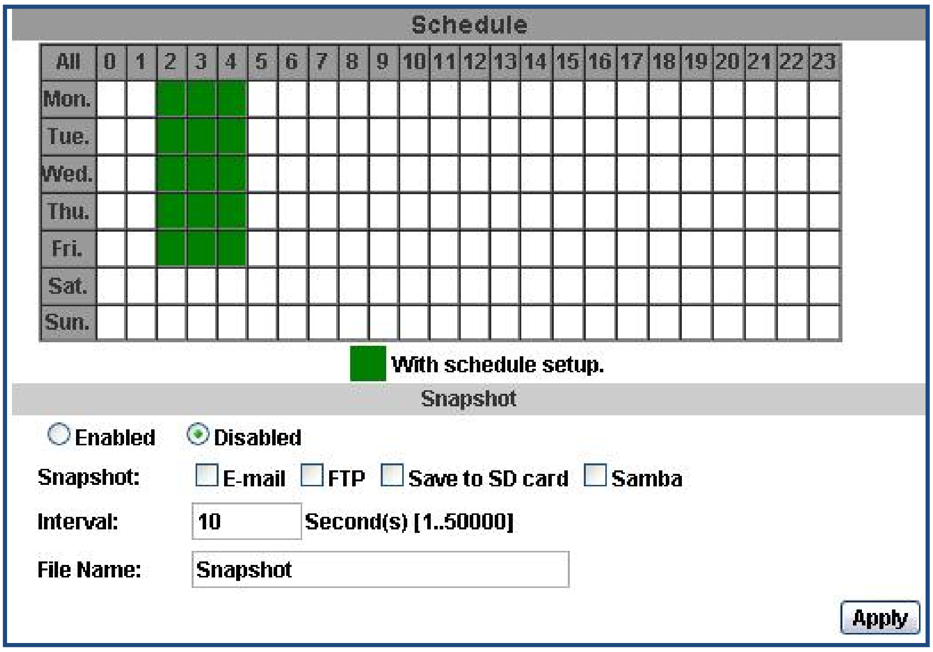


Network IP Check

IP Check:	○ Enabled ● Disabled
IP Address:	www.google.com
Interval:	30 sec ▾
Check failed:	□ Connection failed four times. Reboot IP Camera. □ Save to SD card

The same with "Network Disconnected" function, Network IP check is designed for avoiding video loss. Even when the Ethernet cable is plugged, the network might be sometimes not stable. Key-in the target IP address and interval. The camera checks once in a while according to the setting interval time if it can access the target IP address. If PIN failed, the camera can start saving the video to SD card. If PIN failed four times successively, the camera can reboot itself.

2. Schedule



Schedule

All	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon.			🟩	🟩	🟩																			
Tue.			🟩	🟩	🟩																			
Wed.			🟩	🟩	🟩																			
Thu.			🟩	🟩	🟩																			
Fri.			🟩	🟩	🟩																			
Sat.																								
Sun.																								

🟩 With schedule setup.

Snapshot

○ Enabled ● Disabled

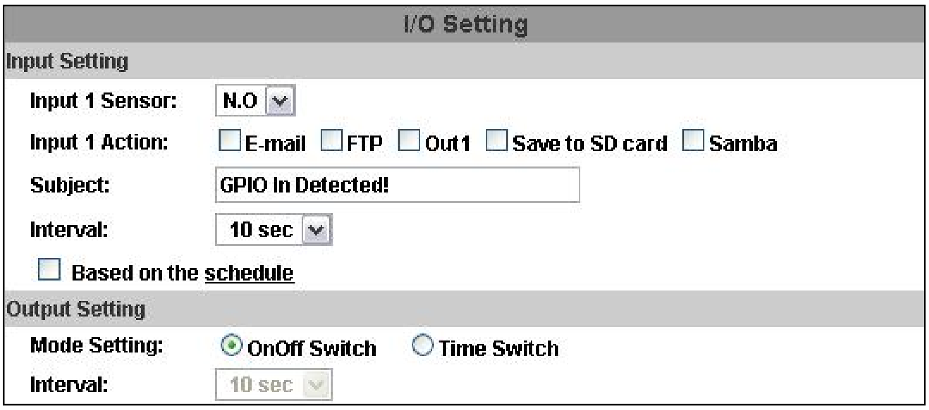
Snapshot:	□ E-mail □ FTP □ Save to SD card □ Samba
Interval:	10 Second(s) [1..50000]
File Name:	Snapshot

a. Schedule: After complete the schedule setup, the camera data will be recorded according to the schedule setup.

b. Snapshot: After enable the snapshot function, user can select the storage position of snapshot file, the interval time of snapshot and the reserved file name of snapshot.

c. Interval: The interval between two snapshots.

3. I/O Setting



I/O Setting

Input Setting

Input 1 Sensor: N.O

Input 1 Action: □ E-mail □ FTP □ Out1 □ Save to SD card □ Samba

Subject: GPIO In Detected!

Interval: 10 sec

□ Based on the schedule

Output Setting

Mode Setting: ● OnOff Switch ○ Time Switch

Interval: 10 sec

a. Input Setting:

IP Camera supports input and output. When the input condition is triggered, it can trigger the relay, send the video to mail addresses /FTP server / SAMBA.

- Interval:

For example, if you select "10 sec" here, once the external alarm is triggered and action is triggered, it cannot be triggered again within 10 seconds.

- Based on the schedule:

When the option box is ticked, only during the selected schedule time the I/O is enabled. That is, for example, the 11th hour of Monday has not been colored in the schedule table, then no action will be triggered even the camera detects input signal during 11:00~12:00 on Monday.

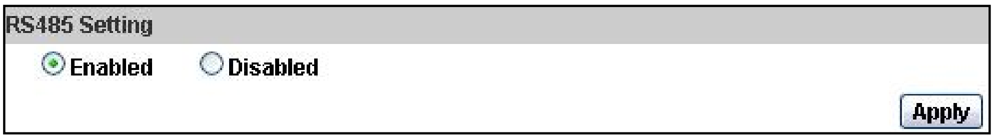
b. Output Setting:

The output mode affects the DO or relay out duration.

(i) On/Off Switch: The camera triggers the external device and lasts for certain of time according to the event "interval" setting. If it's triggered by motion detection, the triggering time is according to "interval" setting of motion detection. If it's triggered by external input alarm, the triggering time is according to input "interval" setting. It triggers the external device and lasts for 10 seconds if you select "10" in interval setting. You can turn off the alarm manually by click "off" at the right bottom of the live video page.

(ii) Time Switch: The camera triggers the external device and lasts for certain of time according to the output "interval" setting, and the user is not allowed to break off the alarm manually.

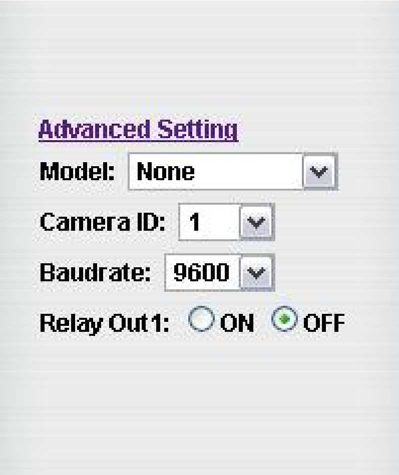
c. RS485 Setting



RS485 Setting

● Enabled ○ Disabled

If the RS485 is enabled, the related options will be shown in the live video page.



Advanced Setting

Model: None

Camera ID: 1

Baudrate: 9600

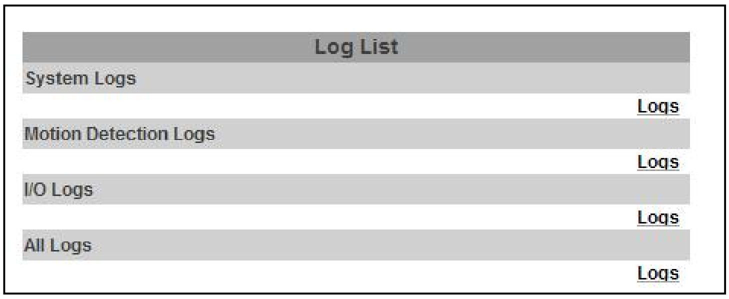
Relay Out1: ○ ON ● OFF

(i) Model: Select the model of the connected device.

(ii) Camera ID: To connect successfully, the ID must be the same with the connected device.

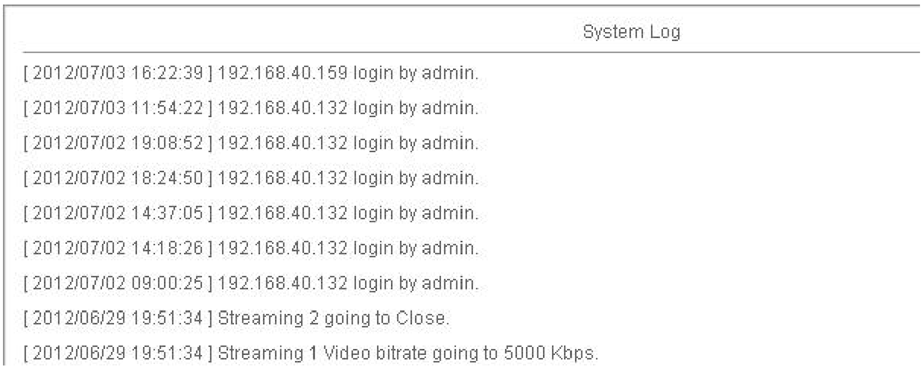
(iii) Baudrate: It means the data transfer rate. The Baudrate must be the same with the connected device.

4. Log List



Log List	
System Logs	
	Logs
Motion Detection Logs	
	Logs
I/O Logs	
	Logs
All Logs	
	Logs

Sort by System Logs, Motion Detection Logs and I/O Logs. In addition, System Logs and I/O Logs won’t lose data due to power failure.



System Log

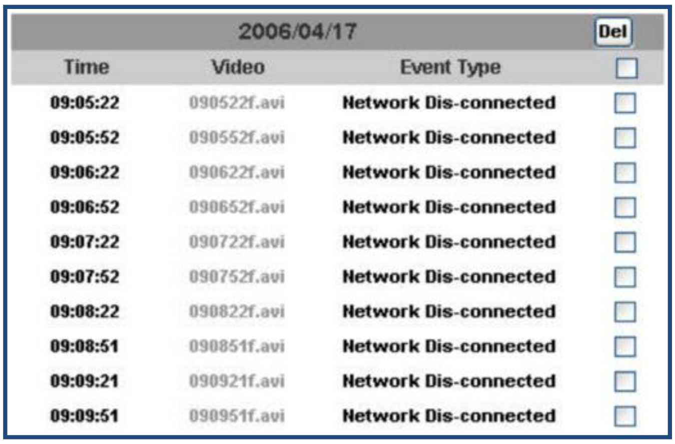
```
[ 2012/07/03 16:22:39 ] 192.168.40.159 login by admin.
[ 2012/07/03 11:54:22 ] 192.168.40.132 login by admin.
[ 2012/07/02 19:08:52 ] 192.168.40.132 login by admin.
[ 2012/07/02 18:24:50 ] 192.168.40.132 login by admin.
[ 2012/07/02 14:37:05 ] 192.168.40.132 login by admin.
[ 2012/07/02 14:18:26 ] 192.168.40.132 login by admin.
[ 2012/07/02 09:00:25 ] 192.168.40.132 login by admin.
[ 2012/06/29 19:51:34 ] Streaming 2 going to Close.
[ 2012/06/29 19:51:34 ] Streaming 1 Video bitrate going to 5000 Kbps.
```

5. SD card

a. Playback

Please Insert SD card before use it. Make sure pushing SD card into the slot completely.

Click the date listed on this page, and it shows the list of the video. The video format is AVI. Click the video to start Microsoft Media Player to play it. To delete the video, check it, and then click "Del".



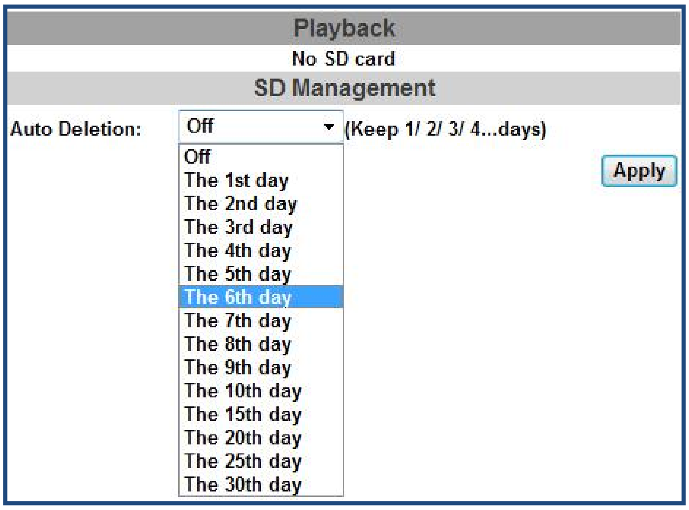
2006/04/17 Del

Time	Video	Event Type	□
09:05:22	090522f.avi	Network Dis-connected	□
09:05:52	090552f.avi	Network Dis-connected	□
09:06:22	090622f.avi	Network Dis-connected	□
09:06:52	090652f.avi	Network Dis-connected	□
09:07:22	090722f.avi	Network Dis-connected	□
09:07:52	090752f.avi	Network Dis-connected	□
09:08:22	090822f.avi	Network Dis-connected	□
09:08:51	090851f.avi	Network Dis-connected	□
09:09:21	090921f.avi	Network Dis-connected	□
09:09:51	090951f.avi	Network Dis-connected	□

b. SD Management

Choose “The 1st day” means the recoding file will be keep one day. Example: It is five o’clock now. Choose “The 1st day”. The files will be kept from five o’clock yesterday to five o’clock today.

The oldest file will be deleted if the SD card is full.



Playback

No SD card

SD Management

Auto Deletion: Off (Keep 1/ 2/ 3/ 4...days)

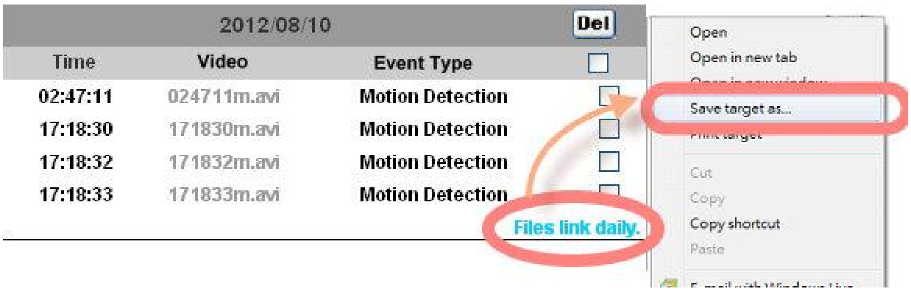
Note：The use of the SD card will affect the operation of the IP Camera slightly, such as affecting the frame rate of the video.

c. Copy to PC

You can insert the SD card to PC and read the files directly, or use FlashGet instead to download the files from IP camera. (In this way you do not need to pull out SD card from the camera.)

To use FlashGet for downloading the image and video data from the SD card, please follow the steps:

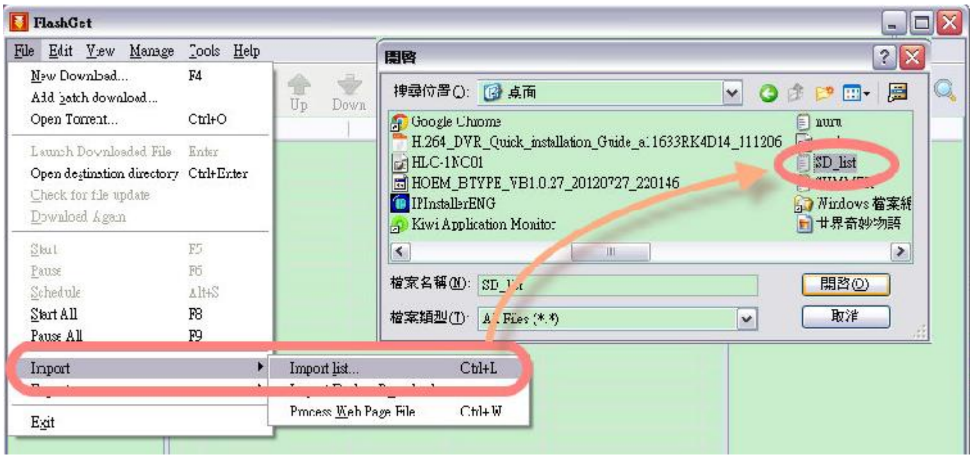
(i) Enter the data list and right-click "Files link daily", select "save target as..." to save the link list to PC.



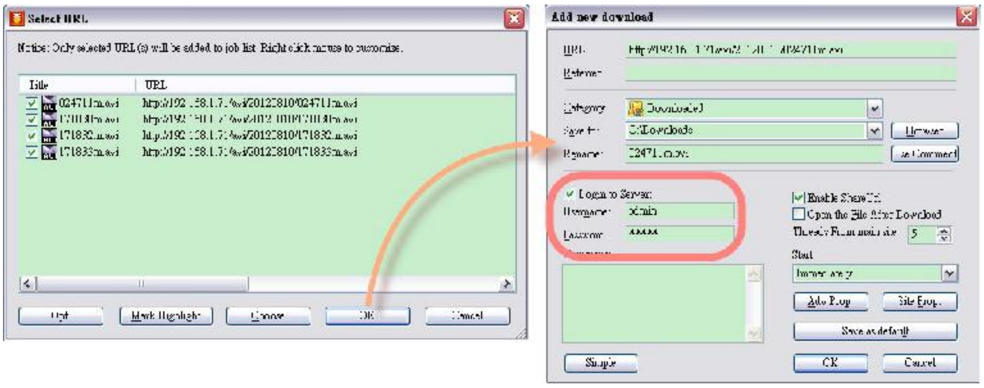
2012/08/10			Del
Time	Video	Event Type	□
02:47:11	024711m.avi	Motion Detection	□
17:18:30	171830m.avi	Motion Detection	□
17:18:32	171832m.avi	Motion Detection	□
17:18:33	171833m.avi	Motion Detection	□

Files link daily.

(ii) Open FlashGet, select "File" → "Import" → "Import list", and find the link list file you just saved. The file name may be called "SD_list".



(iii) FlashGet will show you the link list, and you can tick the files you want to copy to your PC. Give the directory path in the new download window, and remember to enable "Login to Server": key-in the IP Camera username and password.



Select URL

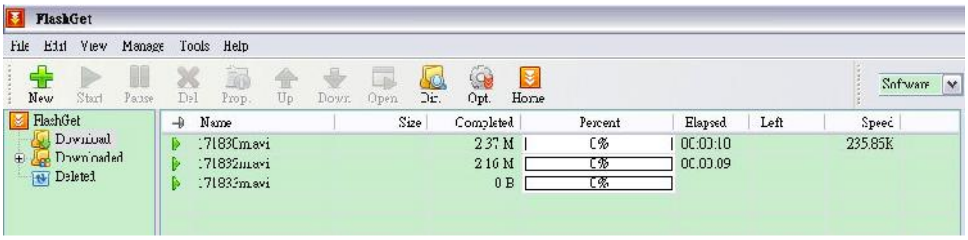
Notice: Only selected URL(s) will be added to job list. Right click mouse to customize.

	Title	URL
☑	024711m.avi	http://192.168.1.71/avi/20120810/024711m.avi
☑	171830m.avi	http://192.168.1.71/avi/20120810/171830m.avi
☑	171832m.avi	http://192.168.1.71/avi/20120810/171832m.avi
☑	171833m.avi	http://192.168.1.71/avi/20120810/171833m.avi

Add new download

URL: http://192.168.1.71/avi/20120810/024711m.avi
Referrer:
Category: Downloaded
Save to: C:\Downloads
Rename: 024711m.avi
☑ Login to Server
Username: admin
Password: *****
Comment:
☑ Enable ShareUrl
□ Open the File After Download
Thread's Fragment's size: 5
Start: Immediately

(iv) Click OK to start download.

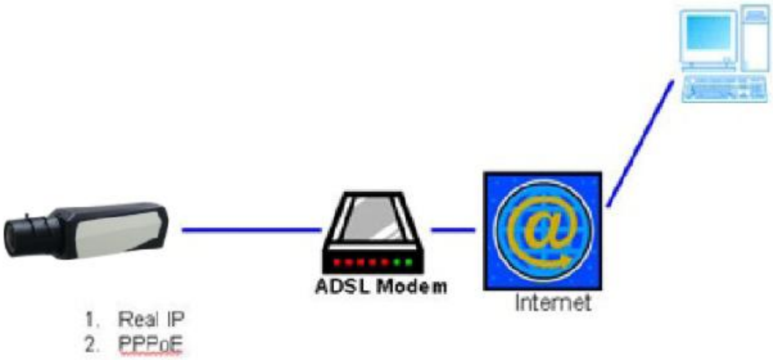


Name	Size	Completed	Percent	Elapsed	Left	Speed
:7183Cm.avi		2.37 M	0%	00:00:10		235.85K
:71832m.avi		2.16 M	0%	00:00:09		
:71833m.avi		0 B	0%			

• FlashGet is a free software that can be downloaded from FlashGet official website. The example above is based on FlashGet ver.1.9.6.

VI. Network Configuration

• Configuration 1:



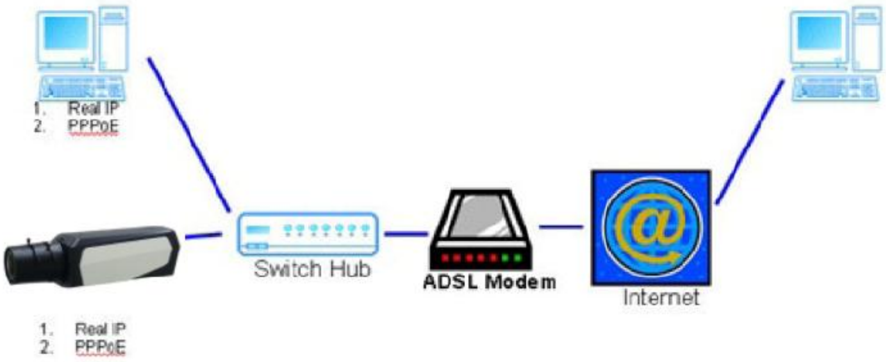
a. Internet Access: ADSL or Cable Modem

b. IP address: One real IP or one dynamic IP

c. Only the IP Camera connects to the internet

d. For fixed real IP, set up the IP into IP Camera. For dynamic IP, start PPPoE.

- **Configuration 2:**



a. Internet Access: ADSL or Cable Modem

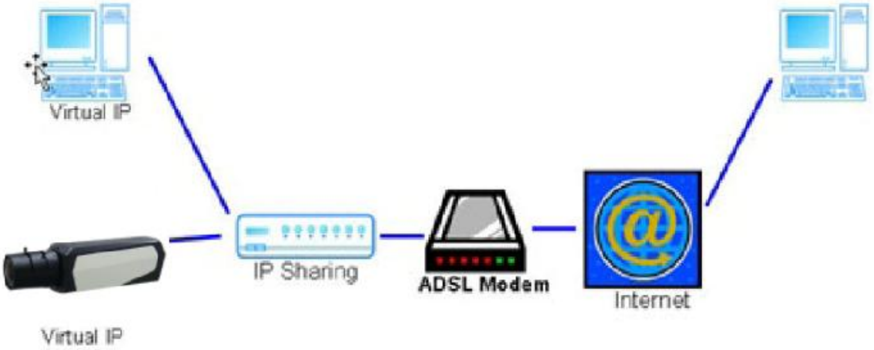
b. IP address: More than one real IP or one dynamic IP

c. IP Camera and PC connect to the internet

d. Device needed: Switch Hub

e. For fixed real IP, set up the IP into IP Camera and PC. For dynamic IP, start PPPoE

- **Configuration 3:**



a. Internet Access: ADSL or Cable Modem

b. IP address: one real IP or one dynamic IP

c. IP Camera and PC connect to the internet d. Device needed: IP sharing

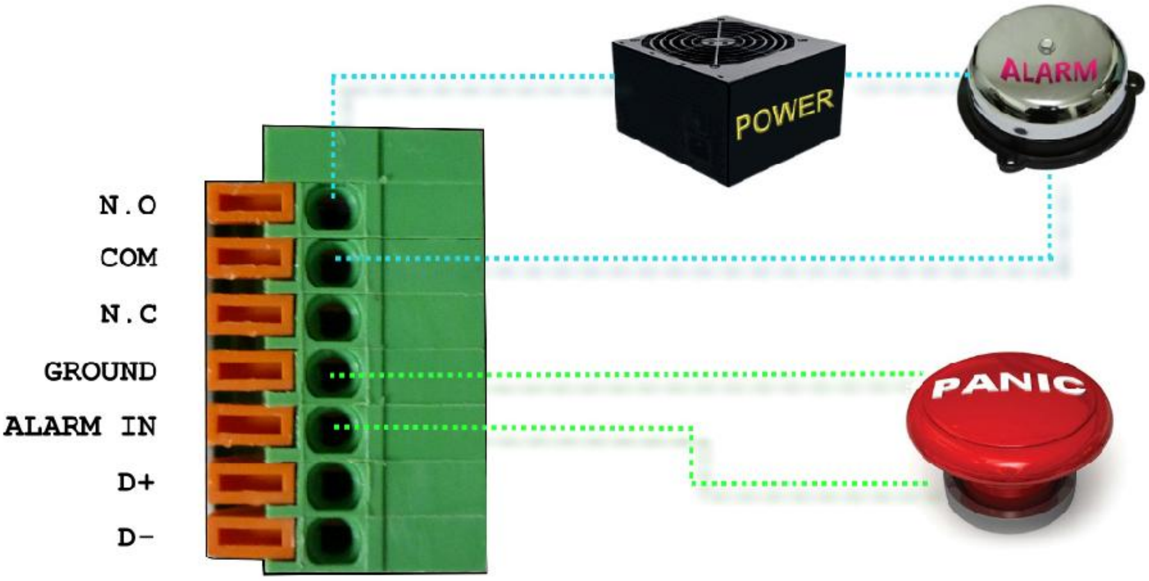
e. Use virtual IP, set up port forwarding in IP sharing.

VII. I/O Configuration

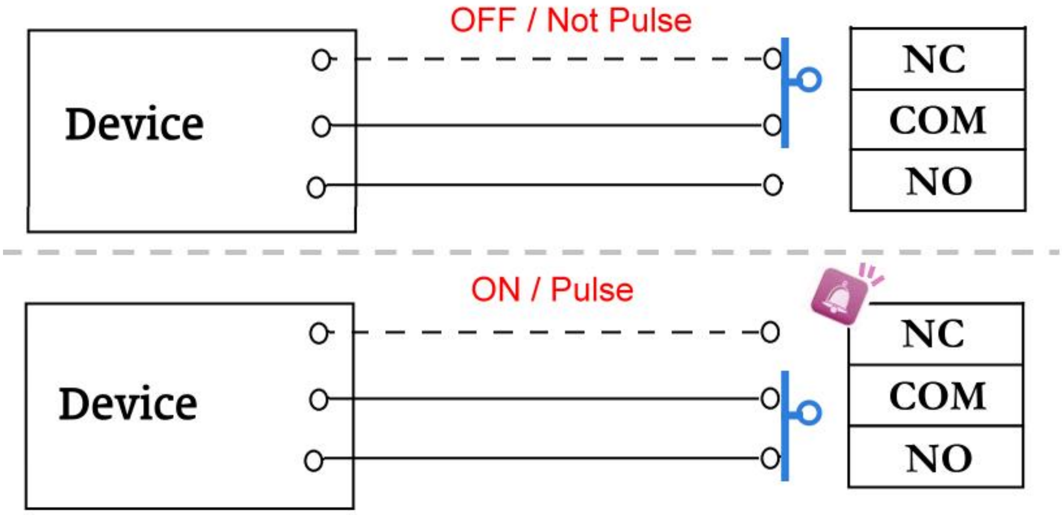
1. I/O Connection

a. Please connect the external output device (ex. siren) to N.O & COM or N.C & COM. (Depends on the output device)

b. Please connect the external trigger device to the GND & Alarm In.

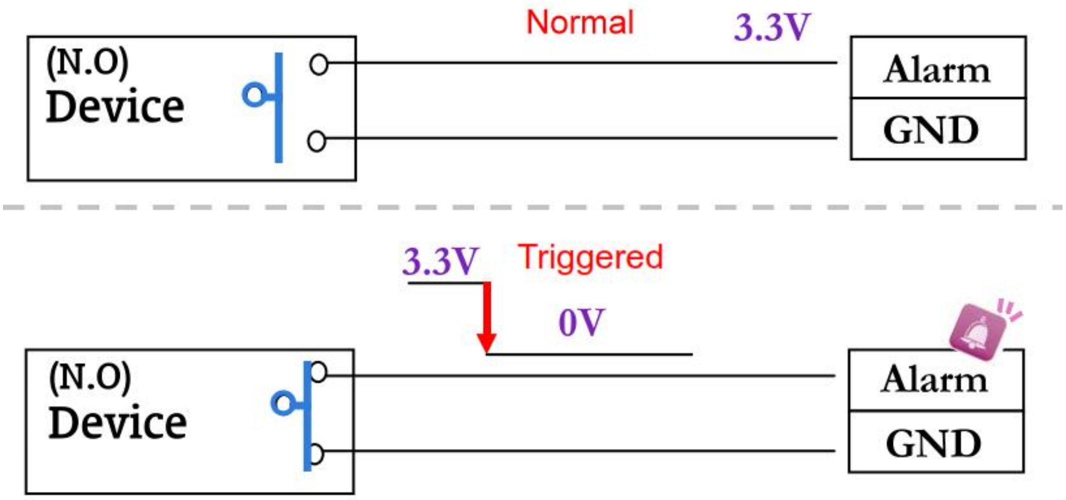


When no event is detected, NC and COM are connected. When the camera detects an event it triggers the external alarm.



If you select "N.O" in "Input sensor setting", when the external device or circuit makes is connected to Alarm and GND pins, the camera input alarm is triggered, and then camera will execute the action user has set, for example, sending snapshot to E-mail address.

If you select "N.C" in "Input sensor setting", when the external device or circuit mare connected to Alarm and GND pins, the camera input alarm is triggered, and then camera will execute the action the user has set, for example, sending snapshot to E-mail address.

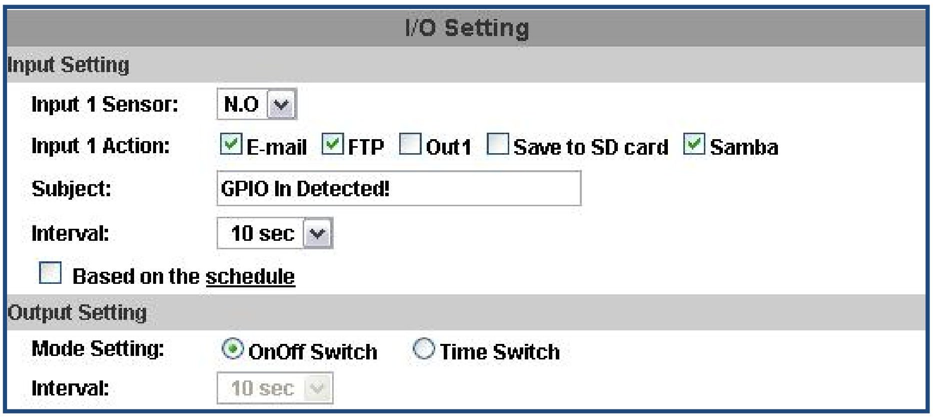


c. I/O PIN definition

- GND (Ground): Initial state is LOW
- Alarm In: Max. 50mA, DC 3.3V
- N.C. (Normally Close): Max. 1A, 24VDC or 0.5A, 125VAC
- COM (Common)
- N.O. (Normally Open): Max. 1A, 24VDC or 0.5A, 125VAC

2. I/O Setup

a. Click I/O Setting from the system setup page via IE, and check “Out1” to enable I/O signal.



I/O Setting

Input Setting

Input 1 Sensor:	N.O
Input 1 Action:	☑ E-mail ☑ FTP □ Out1 □ Save to SD card ☑ Samba
Subject:	GPIO In Detected!
Interval:	10 sec

□ Based on the schedule

Output Setting

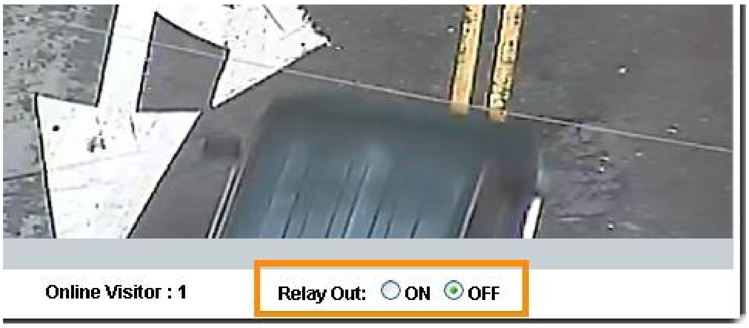
Mode Setting:	● OnOff Switch ○ Time Switch
Interval:	10 sec

b. Output Test

After the external input and output hardware is installed, you can use the "Relay Out" bottom on the live video page to test if DO / Relay Out works.

(i) On/Off Switch mode:

Click "ON", the camera will trigger the external output device. For example, your alarm buzzer will continuously ring. You can manually break off the output signal by clicking "OFF".

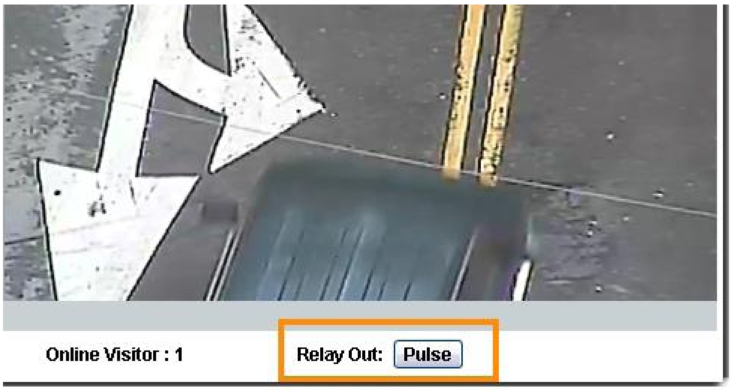


Online Visitor : 1

Relay Out: ○ ON ● OFF

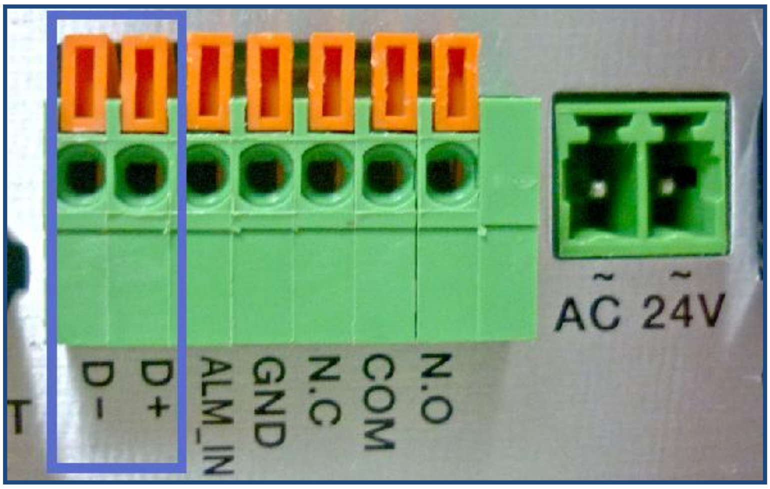
(ii) Time Switch mode:

Click "Pulse", the camera will trigger the external output device for several seconds; the duration length is according to the "interval" setting in Output Setting.

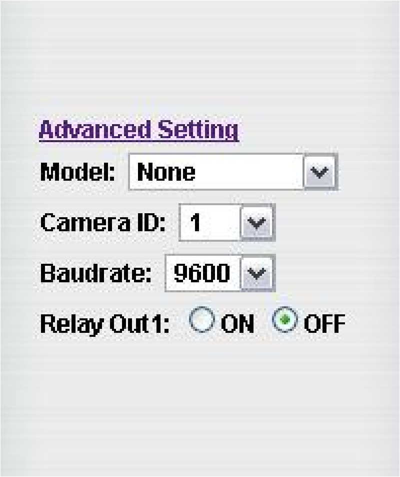


3. RS485:

You can link the IP camera to DVR/NVR, cradle head, or joystick controller by RS-485. Please use cable to connect D+ with D+ of two device, and connect D- with D-.



After the RS485 Setting in I/O Setting is enabled, you can turn to the live video page and check the related options.



Advanced Setting

Model: None

Camera ID: 1

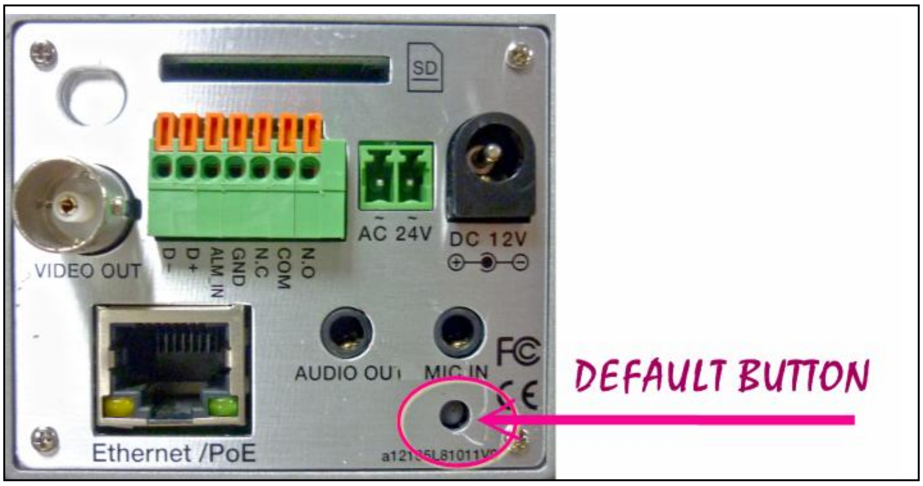
Baudrate: 9600

Relay Out1: ○ ON ● OFF

VIII. Factory Default

If you forget your password, please follow the steps to revert back to default value.

- Remove the power and Ethernet cable. Press and hold the button as the picture below.



- Connect power to the camera again, and do not release the button during the system booting.

- It will take around 30 seconds to boot the camera.

- Release the button when camera finishes proceed.

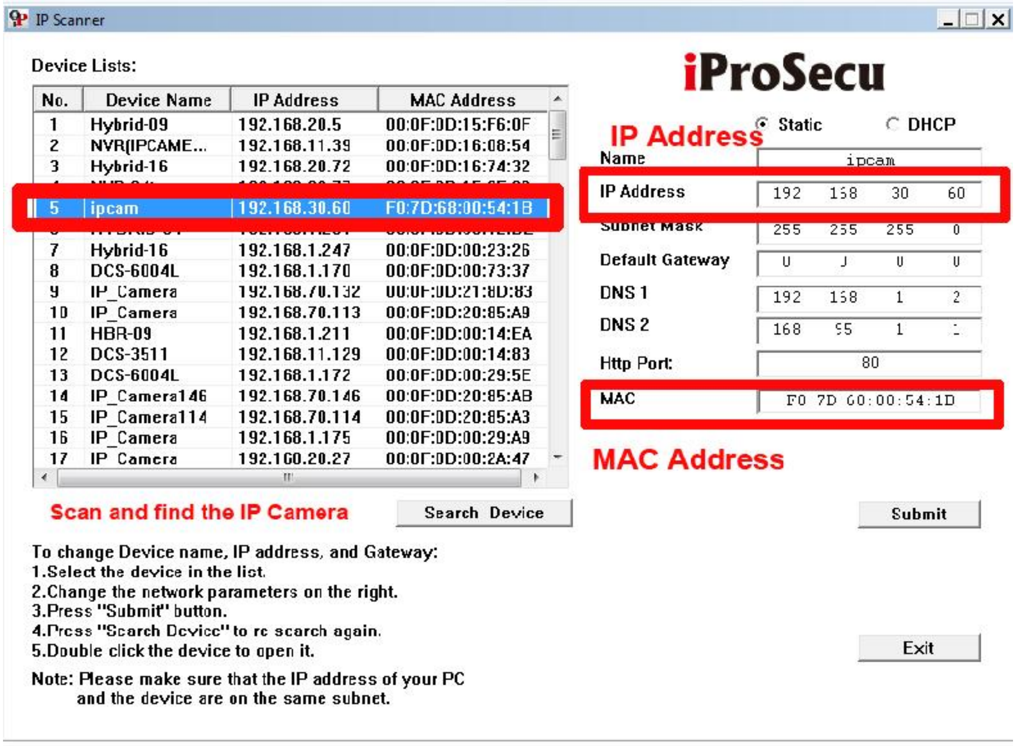
- Plug in the Ethernet cable. Re-login the camera using the default IP (http://192.168.1.200), and user name (admin), password (admin)

IX. Universal Password

If you forgot the password of your IP camera, you can reset the camera to factory default, or follow the procedure below to generate a universal password.

Note: Universal password will be valid only when you enable the function in User Management.

1. First, you need to know the IP address and MAC of your IP camera. You can use IP Scanner to scan the LAN, and see the IP address and MAC on the side column.



IP Scanner

Device Lists:

No.	Device Name	IP Address	MAC Address
1	Hybrid-09	192.168.20.5	00:0F:0D:15:F6:0F
2	NVR(IPCAME...	192.168.11.39	00:0F:0D:16:08:54
3	Hybrid-16	192.168.20.72	00:0F:0D:16:74:32
4	[illegible]	[illegible]	[illegible]
5	ipcam	192.168.30.60	F0:7D:68:00:54:1B
6	[illegible]	[illegible]	[illegible]
7	Hybrid-16	192.168.1.247	00:0F:0D:00:23:26
8	DCS-6004L	192.168.1.170	00:0F:0D:00:73:37
9	IP_Camera	192.168.70.132	00:0F:0D:21:8D:83
10	IP_Camera	192.168.70.113	00:0F:0D:20:85:A9
11	HBR-09	192.168.1.211	00:0F:0D:00:14:EA
12	DCS-3511	192.168.11.129	00:0F:0D:00:14:83
13	DCS-6004L	192.168.1.172	00:0F:0D:00:29:5E
14	IP_Camera146	192.168.70.146	00:0F:0D:20:85:AB
15	IP_Camera114	192.168.70.114	00:0F:0D:20:85:A3
16	IP_Camera	192.168.1.175	00:0F:0D:00:29:A9
17	IP_Camera	192.160.20.27	00:0F:0D:00:2A:47

Scan and find the IP Camera

To change Device name, IP address, and Gateway:
1.Select the device in the list.
2.Change the network parameters on the right.
3.Press "Submit" button.
4.Press "Search Device" to re search again.
5.Double click the device to open it.

Note: Please make sure that the IP address of your PC
and the device are on the same subnet.

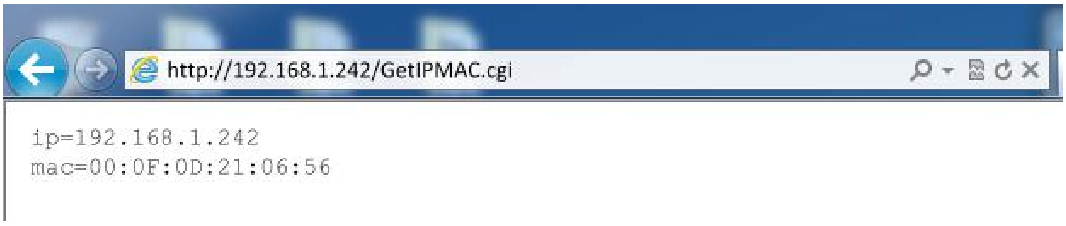
IP Address

● Static ○ DHCP

Name	ipcam
IP Address	192 168 30 60
Subnet Mask	255 255 255 0
Default Gateway	0 0 0 0
DNS 1	192 168 1 2
DNS 2	168 95 1 1
Http Port:	80
MAC	F0 7D 60:00:54:1D

MAC Address

Or, if you already know the IP address of camera: Open the web browser, key-in “http:// (IP address) /GetIPMAC.cgi” and press enter. The IP address and MAC will be displayed on browser.



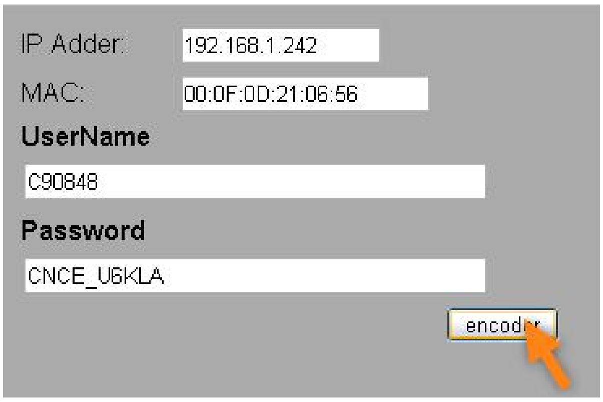
http://192.168.1.242/GetIPMAC.cgi

```
ip=192.168.1.242
mac=00:0F:0D:21:06:56
```

2. Find the .html file named “Universal Password” in CD-ROM. Click to open it.

Universal Password_V1.1
Chrome HTML Document
10 KB

3. Key-in the camera IP address in “IP Adder.” column and MAC in “MAC” column, and then click “encoder”. You will see a set of username and password appears, as below:



IP Adder: 192.168.1.242

MAC: 00:0F:0D:21:06:56

UserName

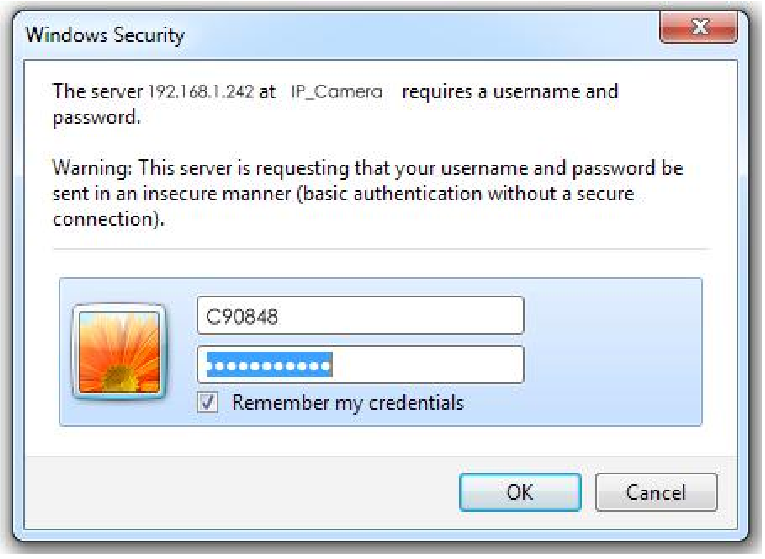
C90848

Password

CNCE_U6KLA

The universal username and password are generated from the IP address and MAC you key-in, so if you change the camera IP address, the universal password changes, too.

4. Take the picture for example, the universal username is “C90848” and password is “CNCE_U6KLA”. Use them to log in the camera.



Windows Security

The server 192.168.1.242 at IP_Camera requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

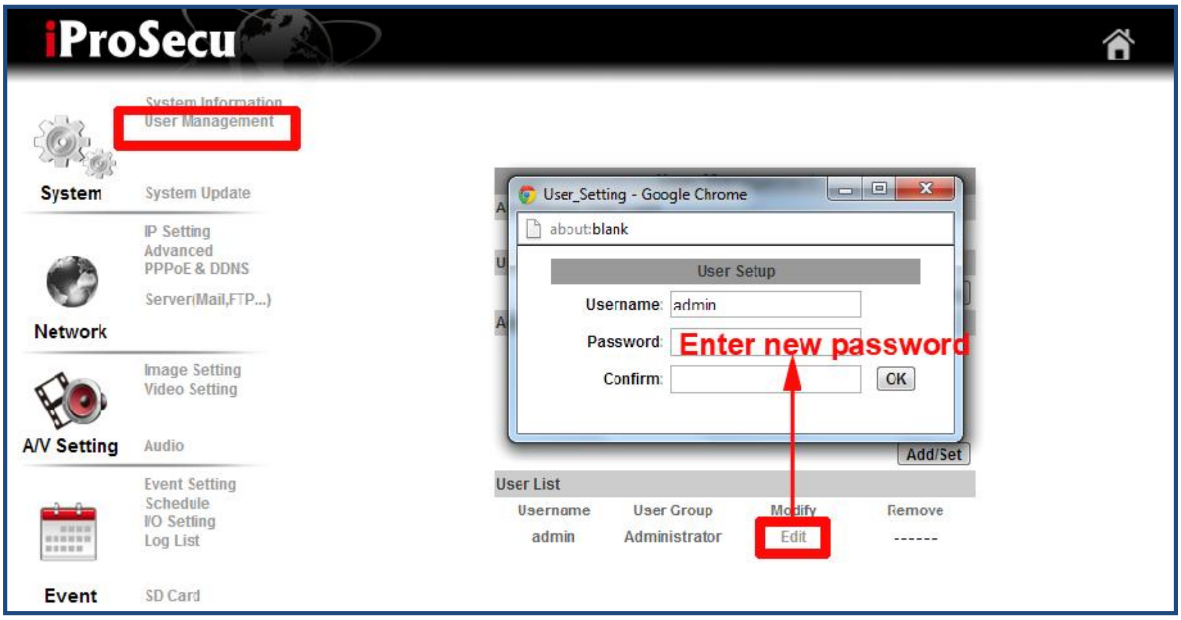
C90848

●●●●●●●●●●

☑ Remember my credentials

5. Now you are logging in as administrator. Turn to User Management page.

The use of universal password does not affect the previous user setting, so the administrator account password does not change until you edit it. Please click "Edit" to give a new administrator password.



Username: admin

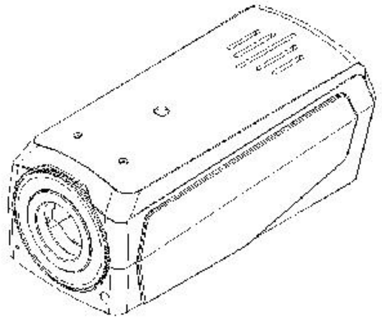
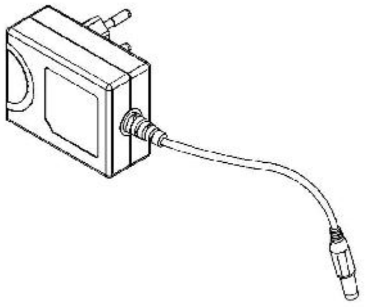
Password:

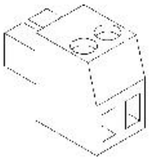
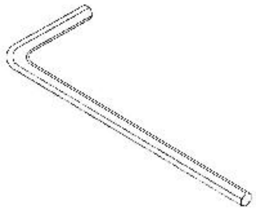
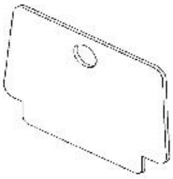
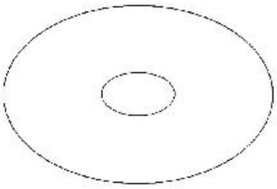
Confirm:

User List

Username	User Group	Modify	Remove
admin	Administrator	Edit	------

X. Package Content

IP Camera	Adapter	Quick Installation Guide
		

2P Terminal block	Hex wrench	Plates for turning the CS ring	CD
			

- Adaptor: AC100-240V DC12V/1A
- The CD includes User manual and software tools.

XI. SD Card Compatibility

The following is the compatible SD Card, and those in red are especially recommended:

SD CARD	
ADATA 4G	SanDisk 512M
ADATA 512M	SanDisk 8G
Blast 128M	SiliconPower 128M
GiGATEK 128M	SiliconPower 256M
Kingmax 256M	TEKQ 128M
Kingston 128M	TEKQ 256M
Kingston 1G	Toshiba 128M
Kingston 256M	Toshiba 256M
Kingston 32G	Toshiba 4GB
Kingston 512M	Tracend 128M 80X
Phast 256M	Tracend 1G 80X
Photofast 256M	Tracend 256M 80X
PK 128M	Tracend 2G 150X
PRETEC 128M	Tracend 4G 150X
READY 128M	Tracend 512M 80X
SanDisk 128M	Transcend 16G
SanDisk 16G	Transcend 32G
SanDisk 1G	Transcend 4GB
SanDisk 256M	Transcend 8G
SanDisk 2G	TwinMOS 128M
SanDisk 32G	TwinMOS 256M
SanDisk 4GB	UMAX 128M
	U-TEK 128M
SDHC CARD	
SanDisk 4GB	Transcend 4GB
SanDisk 8G	Transcend 8G
SanDisk 16G	Transcend 16G
SanDisk 32G	Transcend 32G
Toshiba 4GB	Kingston 32G