netsys

Networking your world

1Megapixel Indoor Dome IP Camera

NC-11DF USER'S MANUAL

Http://www.netsys.com.tw

Copyright

Safety Warnings

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MISTURE.
DO NOT INSERT ANY METALLIC OBJECT THROUGH VENTILATION GRILLS.

Caution:

CAUTION

RISK OF ELECTRIC SHOCK
DO NOT OPEN

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.

The NC-11DF is for **indoor** applications only. This product does not have waterproof protection, please do not use in outdoor applications.

Table of Contents

Foreword

NC-11DF is a 1 / 2.7" 1 Mega-Pixel CMOS sensor IP camera with a built-in web server. The user can view real-time video via IE browser. It supports H.264 and M-JPEG video compression, providing smooth and high video quality. The video can be stored in Micro SD card and playback remotely. With a user friendly interface, it is an easy-to-use IP camera for security applications.

Outward

Chapter 1. Package Contents

1.1 Check List

Carefully unpack the package and check its contents against the checklist.

- NC-11DF (1 Megapixel Indoor Dome IP Camera)
- NV-202 / NV-202P (VDSL2 KIT with PoE), Optional
- Accessory: 8 x Rubber Feet , 1 x DC48V /1.875A Desktop Adapter, 1x AC to DC Power cord, 1 x DC12V Adapter, 1 x Ethernet Cable, 2 x Wall plug, 2 x Screw

Notes:

1. Please inform your dealer immediately for any missing or damaged parts. If possible, retain the carton including the original packing materials. Use them to repack the unit in case there is a need to return for repair.
2. If the product has any issue, please contact your local vendor.
3. The power supply included in the package is commercial-grade. Do not use in industrial-grade applications.
4. Please look for the QR code on the bottom of the product, the user can launch the QR code scanning program to scan and download the user's manual electronic format file.
5. Please scan the following QR code to view the NV-202 and NV-202P user's manual.
6. If user only purchase NC-11DF, the accessory only contain 2 x Wall plug and 2 x Screw.

NV-202 user's manual	NV-202P user's manual

Chapter 2. Product Specifications

Main Features

- Supports Real Time HD 720P
- Digital Wide Dynamic Range
- Adjustable Shutter Speed
- 3D+2D Digital Noise Reduction
- Adjustable Sense Up
- Day & Night Manual Switch Time Control
- Supports Power over Ethernet
- Built-in IR LED, 5M Available
- Supports 2-way Audio
- H.264/ M-JPEG Compression
- Micro SD Card Backup(Optional)
- Support iOS / Android / OS X / Windows
- SDK for Software Integration
- Free Bundle 36 ch Recording Software
- IR Distance up to 5M

Hardware	
CPU	Multimedia SoC
RAM	128MB
Flash ROM	16MB
Image Sensor	1 / 4" Mega-Pixel CMOS sensor
Sensitivity	**Color :** 0.2 Lux (AGC ON) **B / W:** 0.1 Lux (AGC ON)
Lens Type	2.8mm @ F1.8
View Angle	77.79°(**H**), 49.55°(**V**)
I/O	1 DI / 1 DO
ICR	Mechanism IR cut Filter
Audio	G.711(64K) and G.726(32K,24K) **Input :** Mic built-in **Output:** External Line out Support 2-way audio
Video Output	N/A
Power over Ethernet	Yes
Power Consumption	**DC 12V Max:** 2.52W(IR ON); 1.92W(IR Off) **PoE Max:** 802.3af, 3.36W (IR ON); 2.88W(IR Off)
Operating Temperature	0°C ~ 45°C

Dimensions	100mm (∅) x 49mm (H)
Weight	180g
IR LEDs	
LEDs	6 LEDs, 850nM,
IR distance	5M
Network	
Ethernet	10/ 100 Base-T
Network Protocol	IPv6, IPv4, HTTP, HTTPS, SNMP, QoS/DSCP, Access list, IEEE 802.1X, RTSP, TCP/ IP, UDP, SMTP, FTP, PPPoE, DHCP, DDNS, NTP, UPnP, 3GPP, SAMBA, Bonjour

System	
Video Resolution	1280x800@30fps,1280x720@30fps , 640x480@30fps, 320x240@30fps, 176x144@30fps
Video Adjust	Brightness, Contrast, Hue, Saturation, Sharpness, AGC, Shutter Time, Sense-up, D-WDR, Anti Fog, Lens Distortion Correction, Flip, Mirror, Day&Night adjustable, Red Gain and Blue Gain, Denoise
Triple Streaming	Yes
Image Snapshot	Yes
Full Screen Monitoring	Yes
Privacy Mask	Yes, 3 different areas
Compression Format	H.264/ M-JPEG
Video Bitrates Adjust	CBR, CVBR
Motion Detection	Yes, 3 Different Areas

Triggered Action	Mail, FTP, Save to SD card, SAMBA, DO
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
Micro SD card management	
Recording Trigger	Motion Detection, IP check, Network break down (wire only),Schedule, DI
Video Format	AVI, JPEG
Video Playback	Yes
Delete Files	Yes
Web browsing requirement	
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:** 1G **Graphic card:** 128MB

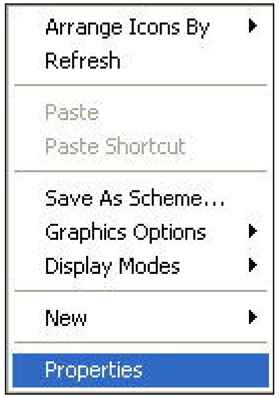
****SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTIFICATION.**

Chapter 3. Product Installation

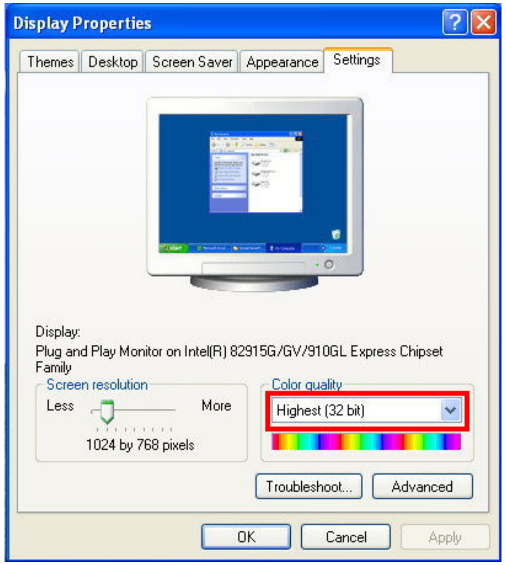
3.1 Monitor Settings

Step1 Right-Click on the desktop. Select **Properties**

Step2 Change color quality to highest (32bit).



.

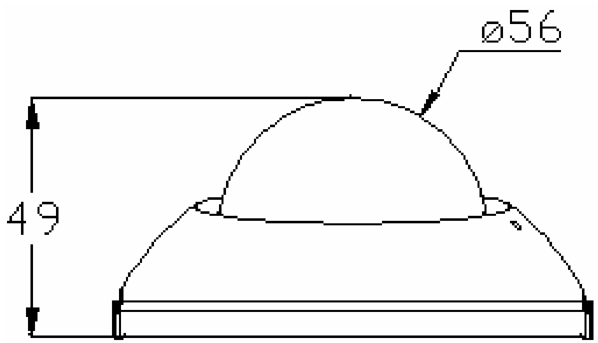


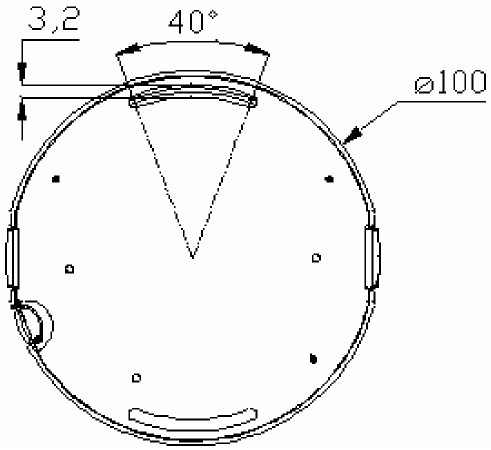
Display:
Plug and Play Monitor on Intel(R) 82915G/GV/910GL Express Chipset Family

Screen resolution
Less More
1024 by 768 pixels

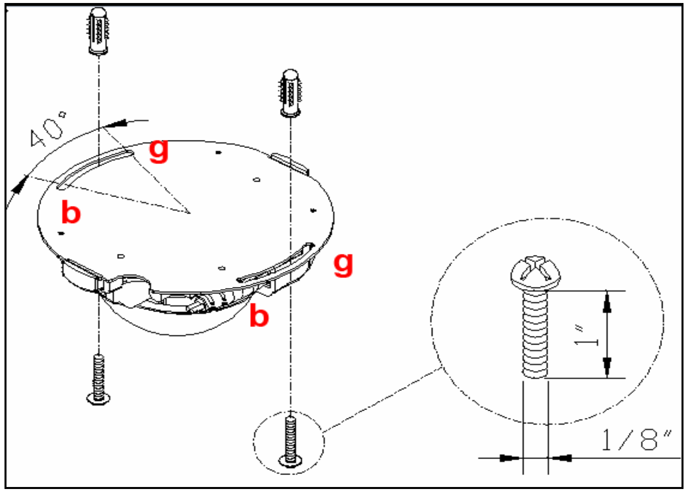
Color quality
Highest (32 bit)

3.2 Hardware Installation

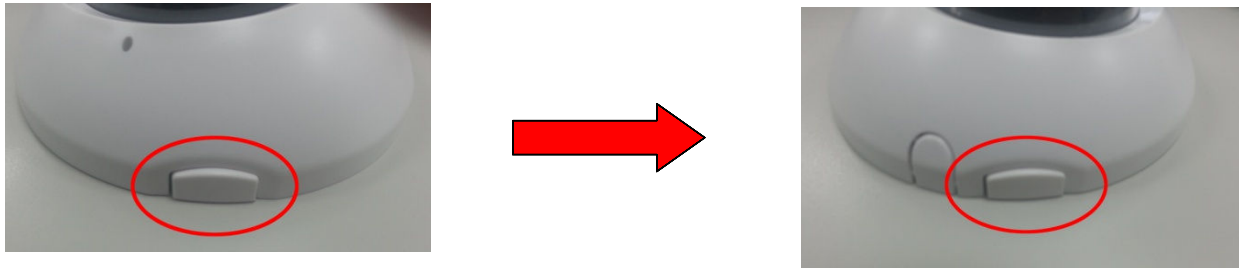




1. Dome Installation Steps

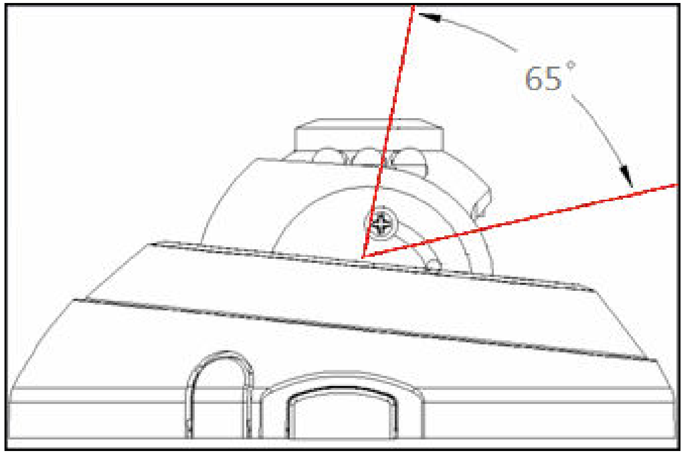


a. Open the dome by pressing the two sides shown in the following pictures:



b. Use screws to place the bottom of camera to the ceiling or the wall. Do not lock it completely because you might need to adjust the lens angle later.

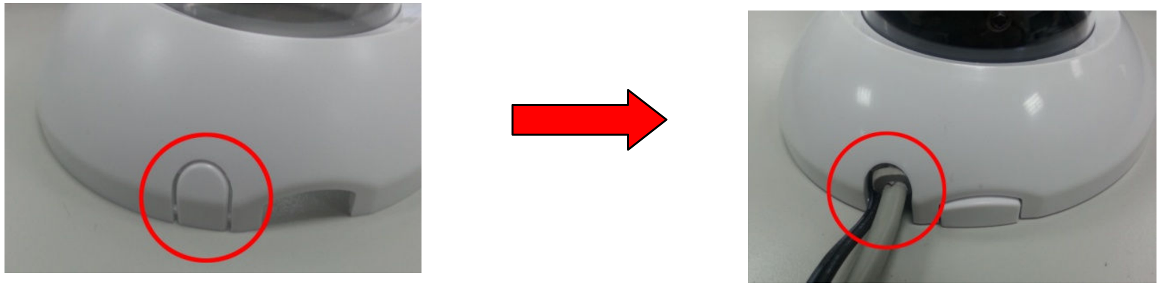
c. Unscrew the lens for adjust the angle.



d. After adjusting the lens tight the screw. Repeat steps b & C as many times you need during the whole process.

e. Connect the Ethernet and Power adaptor.

f. Carefully break the cover hole and plug-in the Ethernet and Power Adaptor.

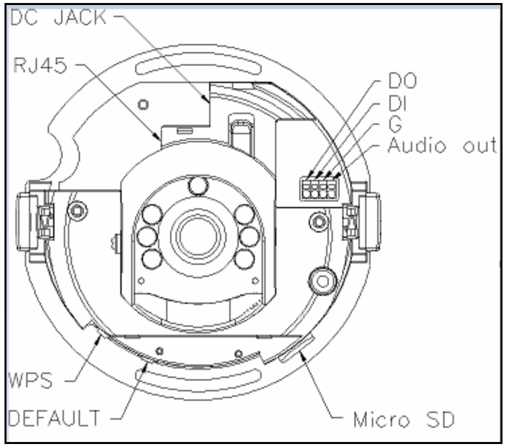


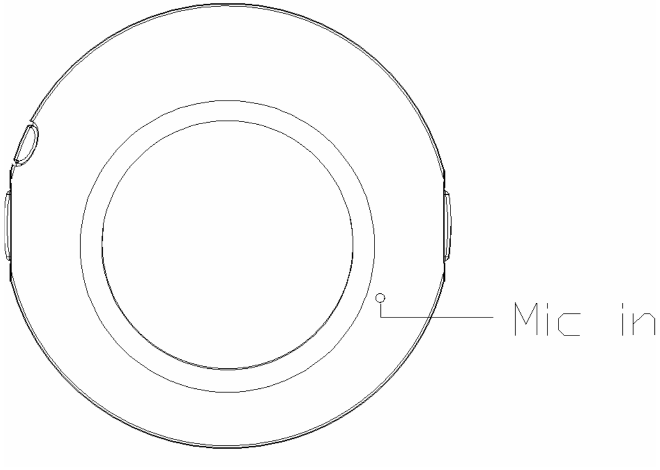
g. After finishing performing steps b & C close tight the screws on for locking the dome into the ceiling.

h. Close the dome cover.

2. Connectors

The camera connectors are as below.





3. PoE (Power Over Ethernet)(Optional) 802.3af, 15.4W / 802.3at, 30W max.

*NV-202P is recommended

Power over Ethernet (PoE) is a technology that integrates power into a standard LAN infrastructure. It enables power to be provided to a 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. NV-202P supports IEEE802.3af / IEEE 802.3at standard. (Figure 3.1)

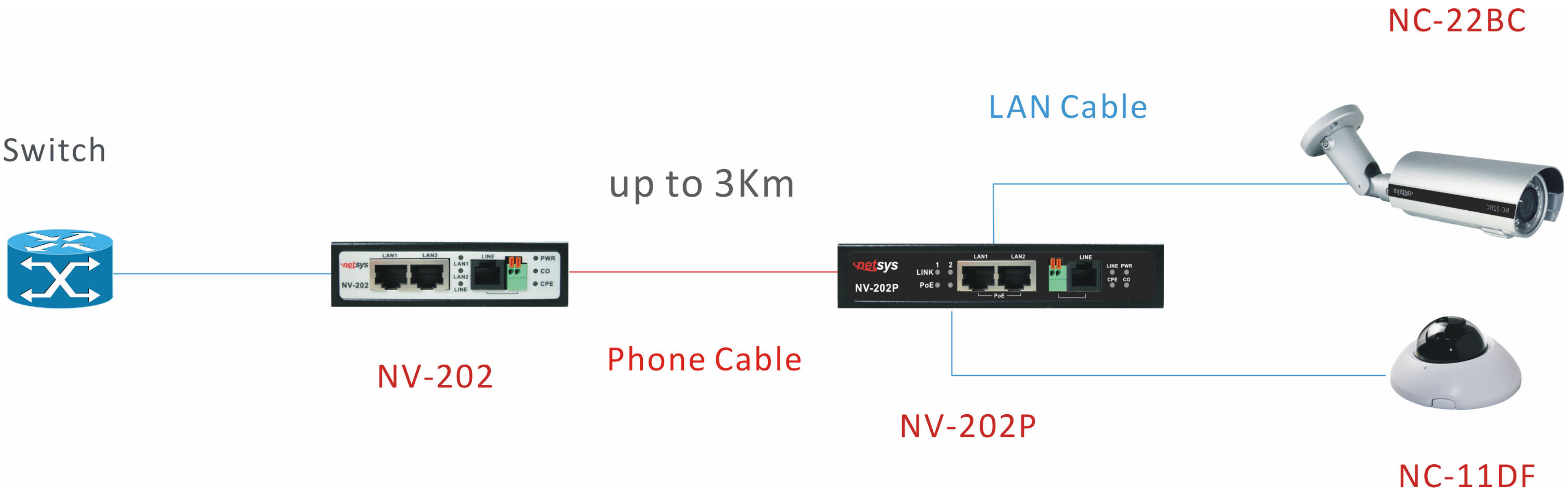


Figure 3.1 NV-202P KIT and IP-Camera applications

3.3 IP Assignment

1. Use the software **IP Installer** to assign the IP address of the IP Camera. User can download the software via http://www.netsys.com.tw/support/download.html

2. **IP installer** supports two languages:

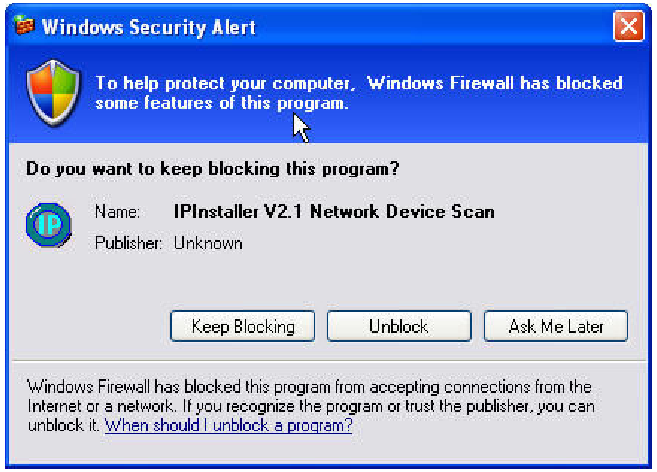
   a. IPInstallerCht.exe：Chinese version
   b. IPInstallerEng.exe：English version

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 Installer**

5. For Windows XP SP2 users, it may popup the following message box. Click **Unblock**.



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

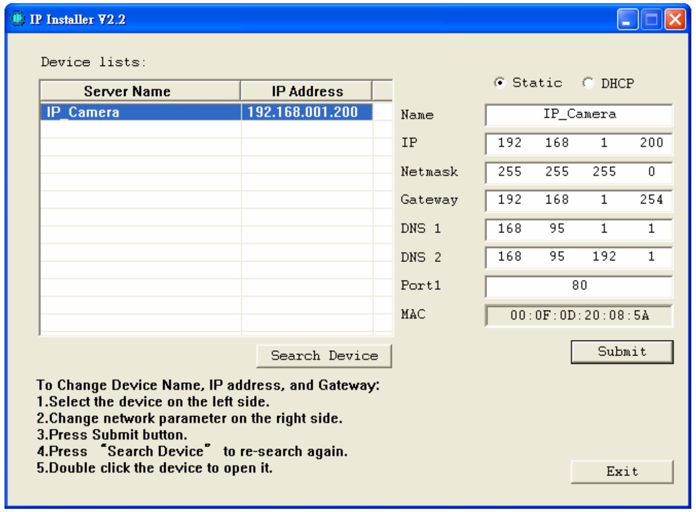
Do you want to keep blocking this program?

Name: IPInstaller V2.1 Network Device Scan

Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

6. **IP Installer** configuration:



IP Installer V2.2

Device lists:

Server Name	IP Address
IP_Camera	192.168.001.200

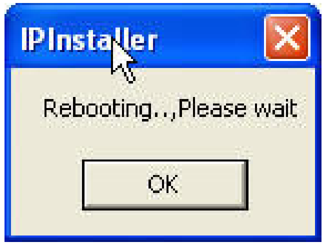
● Static ○ DHCP

Name	IP_Camera
IP	192 168 1 200
Netmask	255 255 255 0
Gateway	192 168 1 254
DNS 1	168 95 1 1
DNS 2	168 95 192 1
Port1	80
MAC	00:0F:0D:20:08:5A

To Change Device Name, IP address, and Gateway:
1.Select the device on the left side.
2.Change network parameter on the right side.
3.Press Submit button.
4.Press "Search Device" to re-search again.
5.Double click the device to open it.

7. **IP Installer** will search for all the IP Cameras connected on the LAN. The user can click **Search Device** to search again.

8. Click one of the IP Cameras listed on the left side. The network configuration of this IP camera will be shown on the right side. You can change the **name** of the IP Camera to your preference (e.g.: Office, warehouse). Change the parameters and click **Submit**, then click **OK**, it will apply the changes and reboot the device.



Rebooting..,Please wait

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

The same Subnet:

IP Camera IP address: 192.168.1.200

PC IP address: 192.168.1.100

Different Subnets:

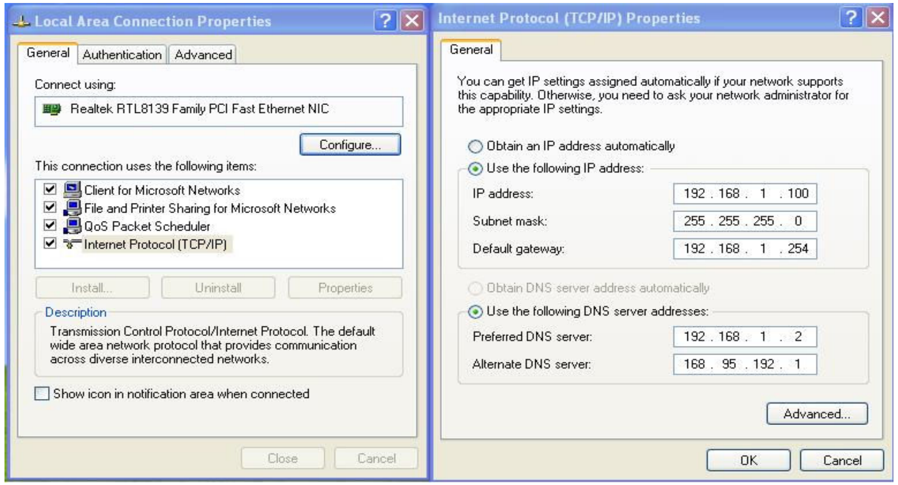
IP Camera IP address: 192.168.2.200

PC IP address: 192.168.1.100

To Change the PC IP address:

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

Make sure your IP Camera and PC are int the same Subnet. If not, change the IP Camera subnet or the PC IP subnet accordingly.



Local Area Connection Properties

Connect using:

Realtek RTL8139 Family PCI Fast Ethernet NIC

This connection uses the following items:

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

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

Internet Protocol (TCP/IP) Properties

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.

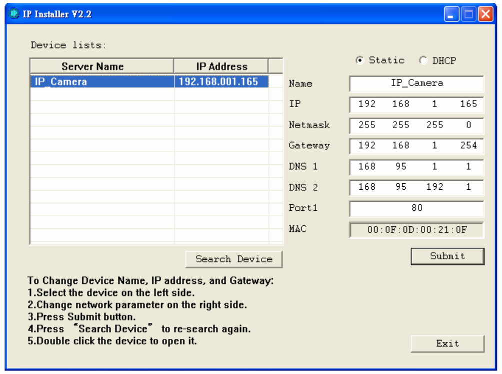
○ Obtain an IP address automatically
● Use the following IP address:

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

10. A quick way to access remote monitoring is to left-click the mouse twice, on a selected IP Camera, listed on **Device list** of **IP Installer**. An IE browser will be opened.



Device lists:

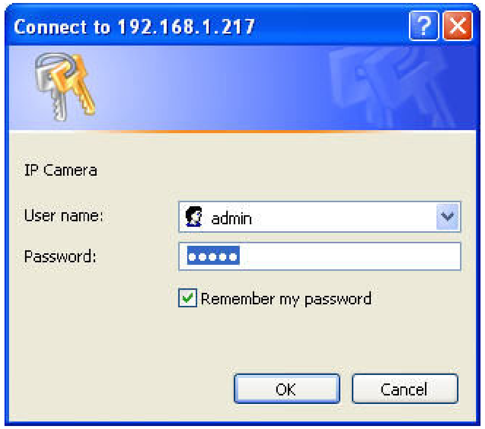
Server Name	IP Address
IP_Camera	192.168.001.165

● Static ○ DHCP

Name: IP_Camera
IP: 192 168 1 165
Netmask: 255 255 255 0
Gateway: 192 168 1 254
DNS 1: 168 95 1 1
DNS 2: 168 95 192 1
Port1: 80
MAC: 00:0F:0D:00:21:0F

To Change Device Name, IP address, and Gateway:
1.Select the device on the left side.
2.Change network parameter on the right side.
3.Press Submit button.
4.Press "Search Device" to re-search again.
5.Double click the device to open it.

11. Then, key-in the default **user name: admin** and **password: admin**.



IP Camera

User name: admin

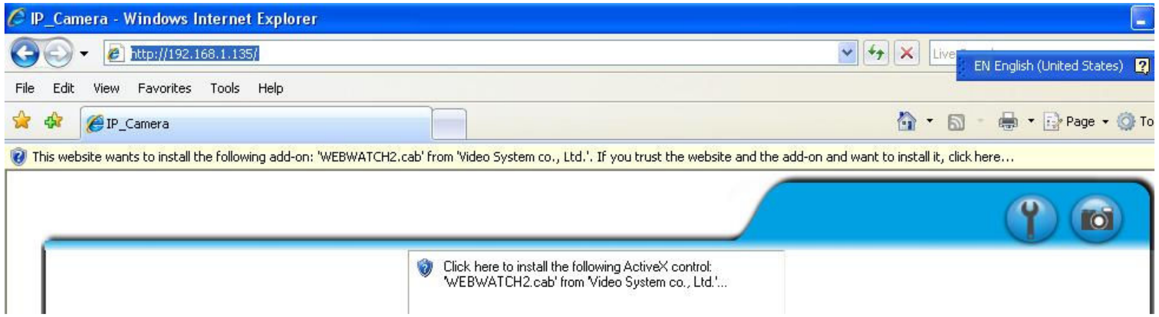
Password: •••••

☑ Remember my password

3.4 Install ActiveX Control

1. For users of IE 6.0 or above:

When viewing the camera video for the first time via IE, the browser will ask you to install the **ActiveX** component.



This website wants to install the following add-on: 'WEBWATCH2.cab' from 'Video System co., Ltd.'. If you trust the website and the add-on and want to install it, click here...

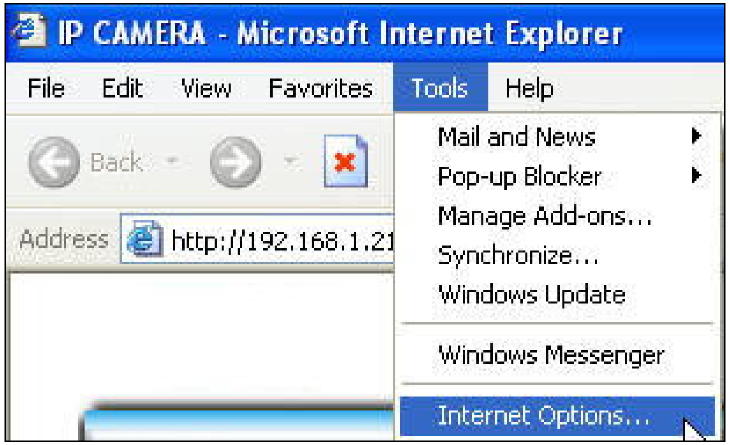
Click here to install the following ActiveX control: 'WEBWATCH2.cab' from 'Video System co., Ltd.'...

1. If the installation failed, please check the security settings in the IE browser.

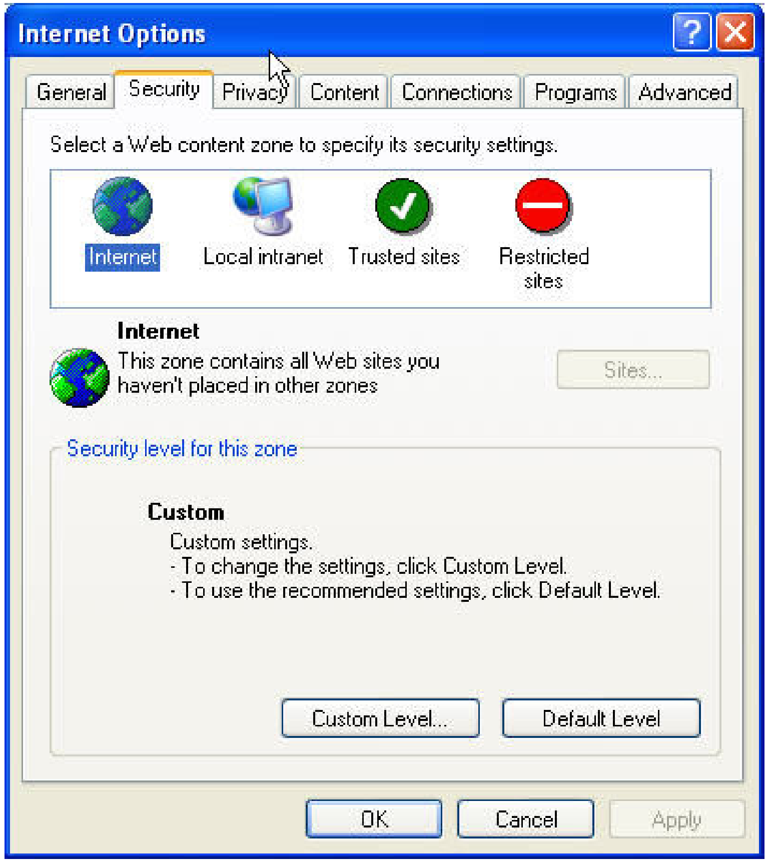
a. IE → Tools → Internet Options… → Security Tab → Custom Level… → Security Settings → Download unsigned ActiveX controls→ Select **Enable** or **Prompt**.

b. IE → Tools → Internet Options… → Security Tab → Custom Level… →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

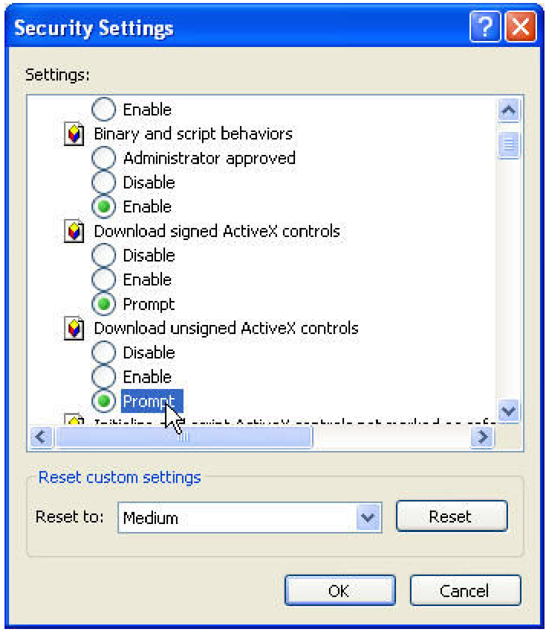
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom

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

3



Security Settings

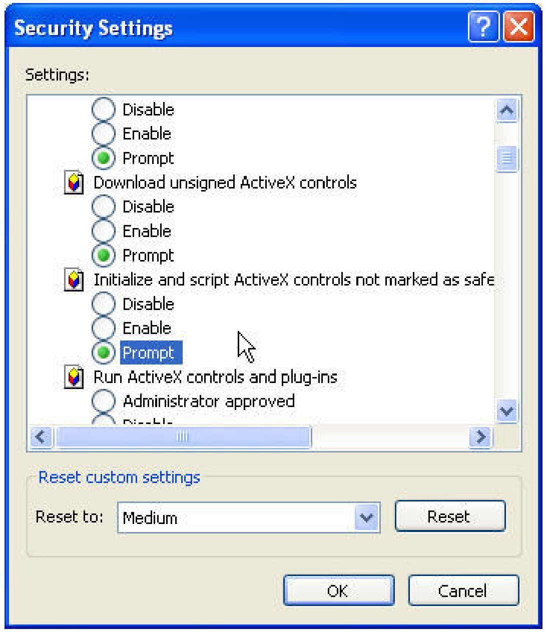
Settings:

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

Reset custom settings

Reset to: Medium

4



Security Settings

Settings:

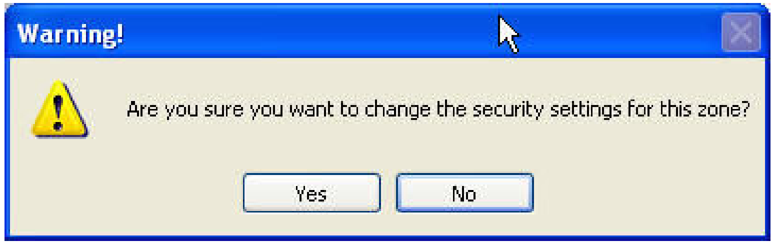
- ○ Disable
- ○ Enable
- ● Prompt
- Download unsigned ActiveX controls
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Initialize and script ActiveX controls not marked as safe
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Run ActiveX controls and plug-ins
  - ○ Administrator approved

Reset custom settings

Reset to: Medium

5

When popup the following dialogue box, click "Yes".



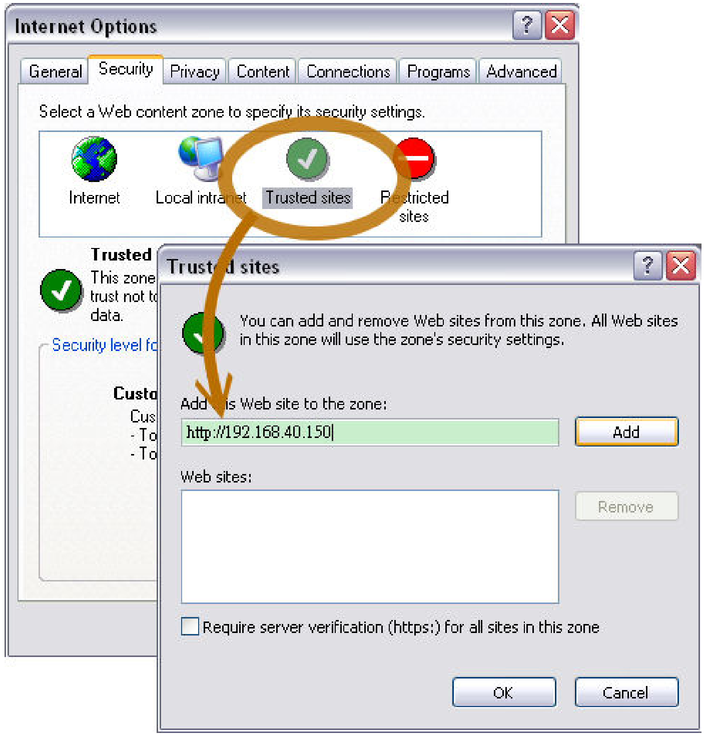
Warning!

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

2. 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.*** on the LAN will be regarded as trusted sites.



Internet Options

Select a Web content zone to specify its security settings.

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

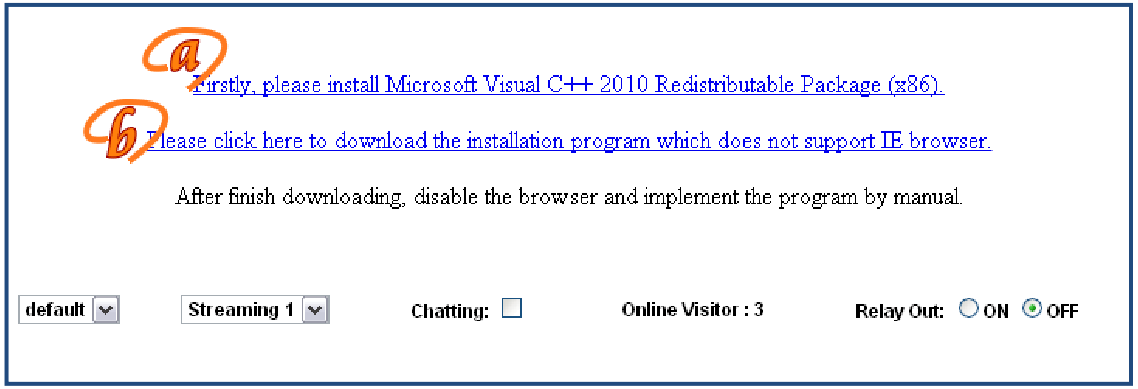
2. To Non-IE Web Browser Users

If you use Firefox or Google chrome to access the IP camera but fails 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. Click the link:

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

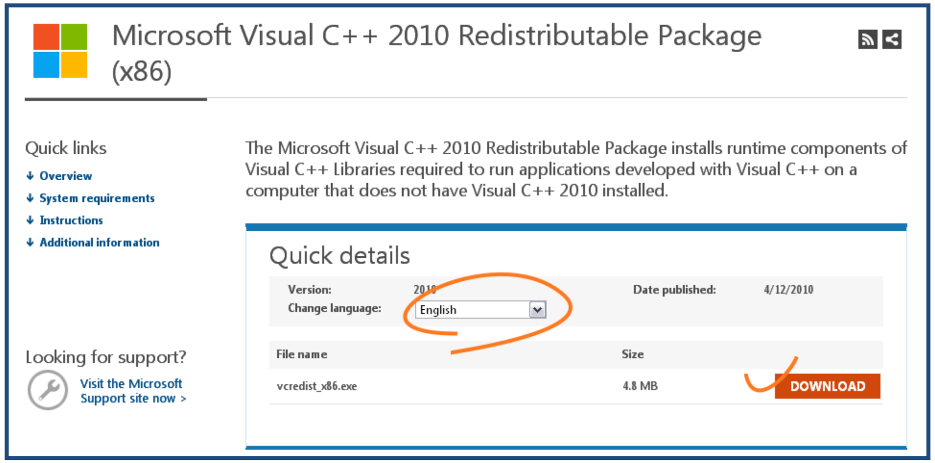


a Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86).

b 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.

The link will conduct you to the Microsoft official site where you can download the tools. Please select the language and click **download**.



Microsoft Visual C++ 2010 Redistributable Package (x86)

Quick links

- Overview
- System requirements
- Instructions
- Additional information

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 Date published: 4/12/2010

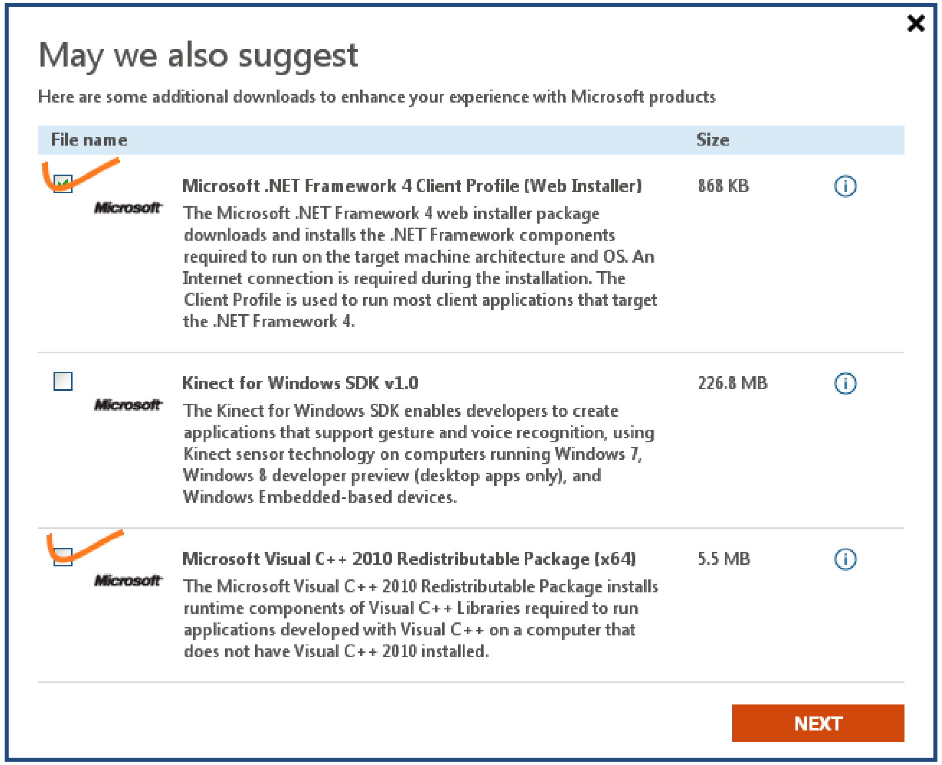
Change language: English

File name	Size	
vcredist_x86.exe	4.8 MB	DOWNLOAD

Looking for support?

Visit the Microsoft Support site now >

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)**.

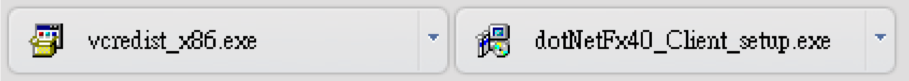


May we also suggest

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

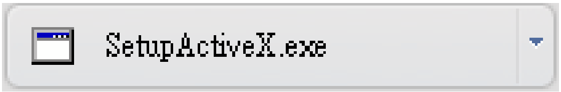
	File name	Size
☑	**Microsoft .NET Framework 4 Client Profile (Web Installer)** The Microsoft .NET Framework 4 web installer package downloads and installs the .NET Framework components required to run on the target machine architecture and OS. An Internet connection is required during the installation. 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

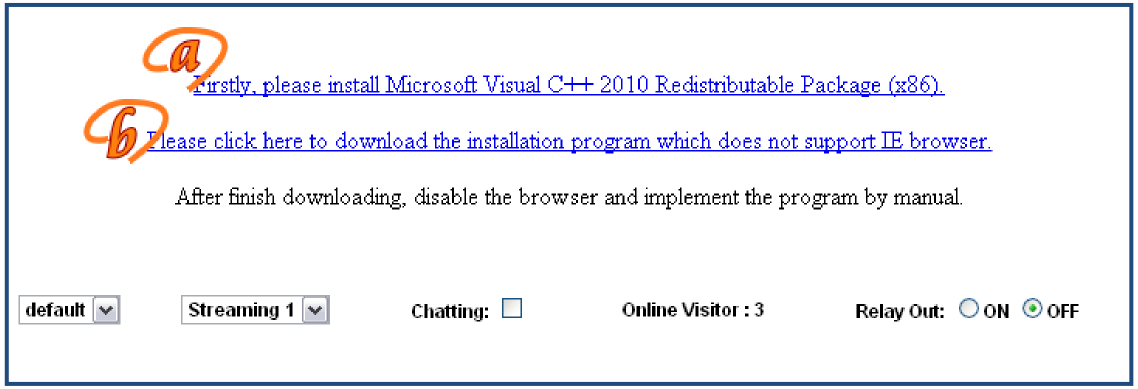
After finishing downloading, execute the two files respectively to install them. The windows may ask you to reboot the PC when the installation is finished.



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

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



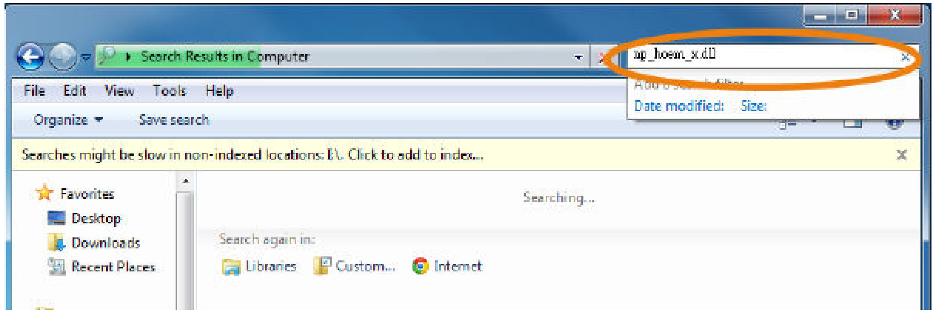

a
b
Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86).
Please click here to download the installation program which does not support IE browser.

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

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

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

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.


Search Results in Computer
File Edit View Tools Help
Organize Save search
Date modified: Size:
Favorites
Desktop
Downloads
Recent Places
Libraries Custom... Internet

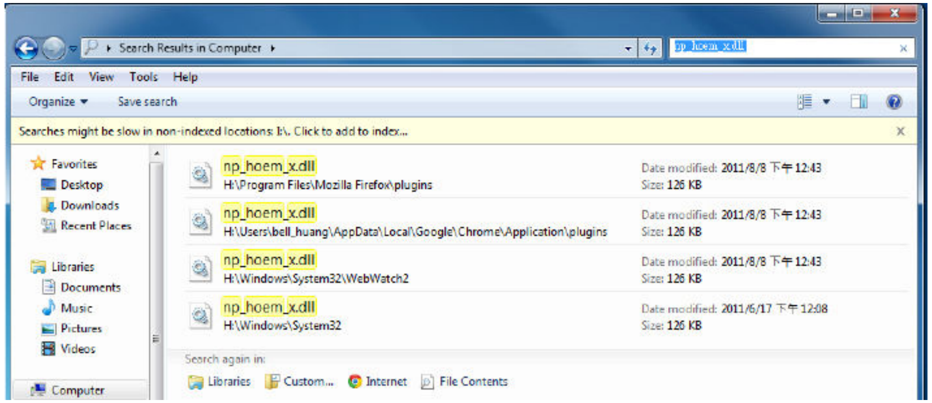
np_hoem_x.dll

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

Searching...

Search again in:

Delete all the files named **np_hoem_x.dll**. They're the **ActiveX** control tools installed in your computer, but the old version of **ActiveX** might not be compatible with the new version of the browser. Therefore, they need to be deleted in order to install the latest **ActiveX** control.



np_hoem_x.dll

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

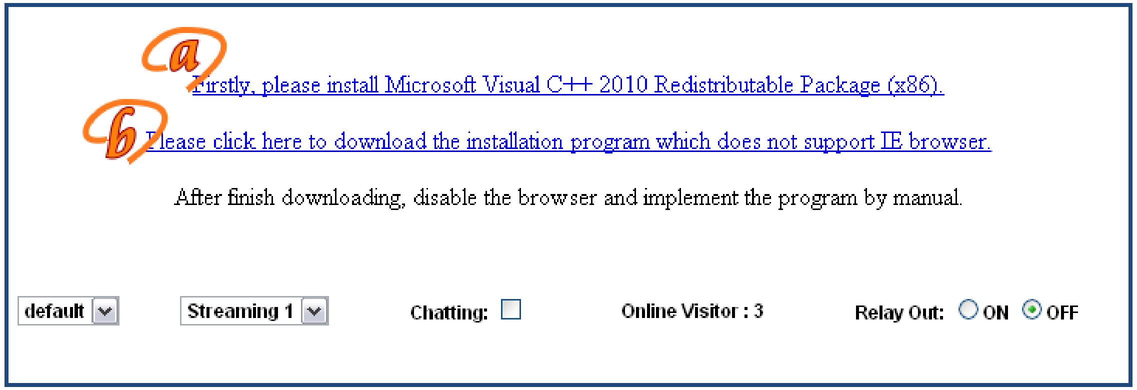
np_hoem_x.dll
H:\Users\bell_huang\AppData\Local\Google\Chrome\Application\plugins
Date modified: 2011/8/8 下午 12:43
Size: 126 KB

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

Search again in:

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**.



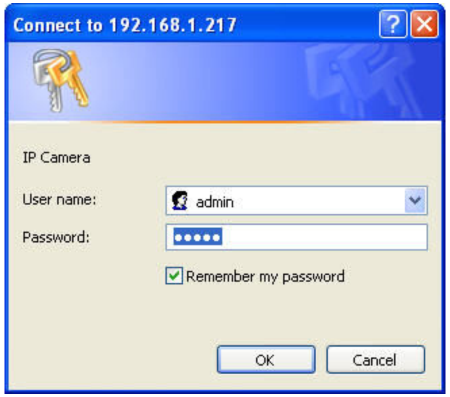
a Firstly, please install Microsoft Visual C++ 2010 Redistributable Package (x86).

b 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.

Chapter 4. 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: **admin** and password: **admin**.



Connect to 192.168.1.217

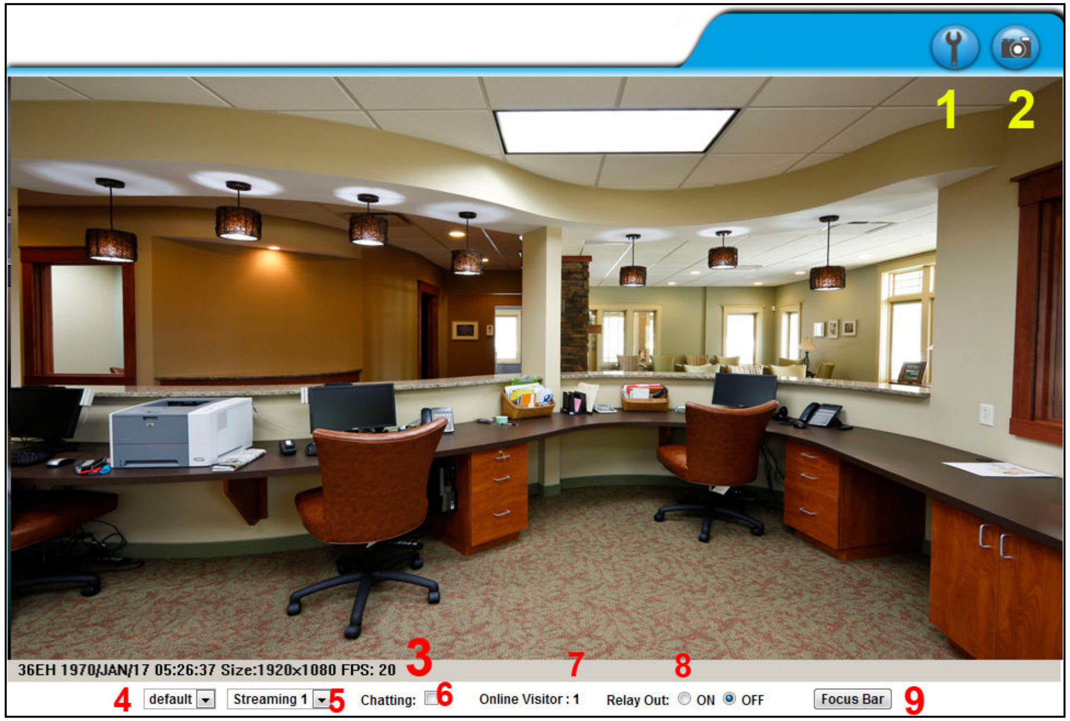
IP Camera

User name: admin

Password: ●●●●●

☑ Remember my password

When the IP Camera is successfully connected it shows the following interface.



36EH 1970/JAN/17 05:26:37 Size:1920x1080 FPS: 20

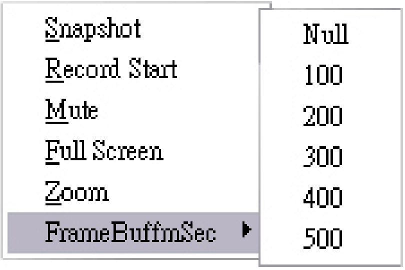
default ▾ Streaming 1 ▾ Chatting: □ Online Visitor : 1 Relay Out: ○ ON ● OFF

1. Get into 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. Streaming source: If the streaming 2 is closed, this function will not be displayed.
6. Tick on **Chatting** for enabling two-way audio.

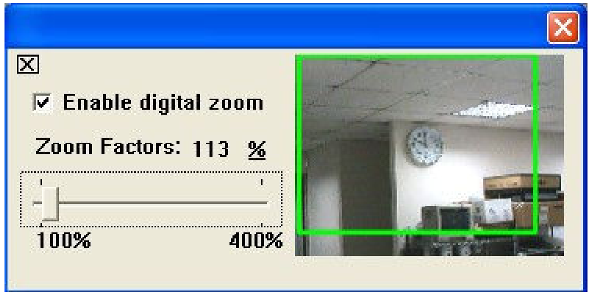
7. Shows how many people are connected to this IP camera.
8. Control the relay output connected to this camera.

Double-clicking on the video will change the view to full screen mode. Press **Esc** or double-click the video again for changing back to normal mode.

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 where to save the video. To stop recording, right-click again and 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.
4. Full Screen: Full-screen mode.
5. Zoom: Enable the zoom-in and zoom-out functions. First, select **Enable digital zoom** option within the pop-up dialogue box and then drag and drop the bar to adjust the zoom factors.



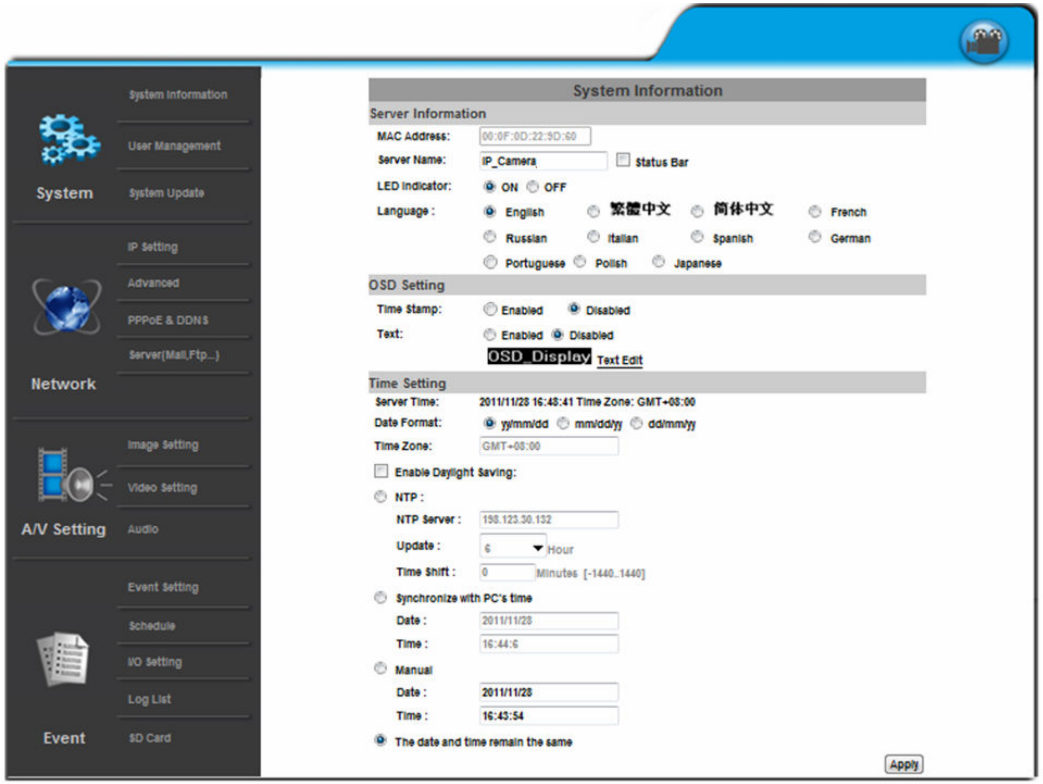
☑ Enable digital zoom

Zoom Factors: 113 %

6. Frame Buffer Sec: This function builds a temporary buffer to accumulate several video frames. This function can make video smooth-going when the Network speed is slow and lag. If you select **100**, the camera plays video 100 mSec after receiving images from camera. The slower the Network is the bigger value should be selected. The available values are: **NULL, 100, 200, 300, 400, and 500**. The default value is null.

Chapter 5. Camera Configuration

Click to get into the administration page. Click to go back to the live video page



System Information

Server Information

MAC Address: 00:0F:0D:22:9D:60

Server Name: IP_Camera □ Status Bar

LED Indicator: ● ON ○ OFF

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: 2011/11/28 16:48:41 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 : 198.123.30.132

Update : 6 Hour

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

○ Synchronize with PC's time

Date : 2011/11/28

Time : 16:44:6

○ Manual

Date : 2011/11/28

Time : 16:43:54

● The date and time remain the same

Apply

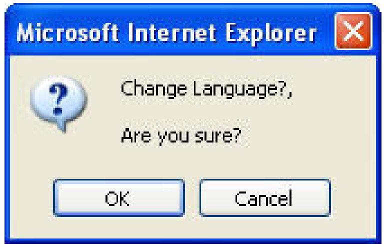
5.1. System

I. System Information

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

1. Server Name: This is the Camera name. This name will be shown on the IP Installer.

2. Select language: English, Traditional Chinese, and Simplified Chinese can be selected. When it changes, it will show the following dialogue box to confirm the language changing.

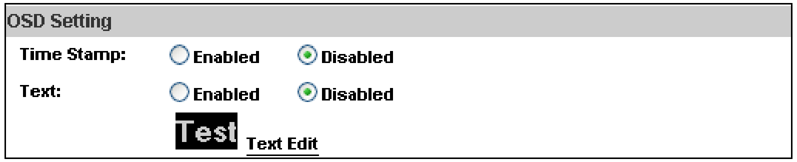


Microsoft Internet Explorer

Change Language?,

Are you sure?

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

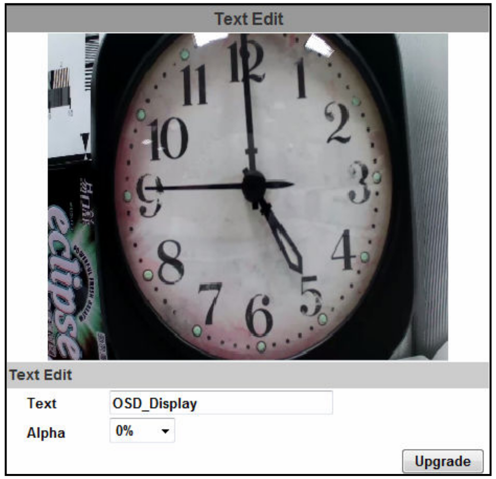


OSD Setting

Time Stamp: ○ Enabled ● Disabled

Text: ○ Enabled ● Disabled

Moreover, click **Text Edit** for changing the OSD content, including text size and alpha. Finally, click the Upgrade button to keep the settings.



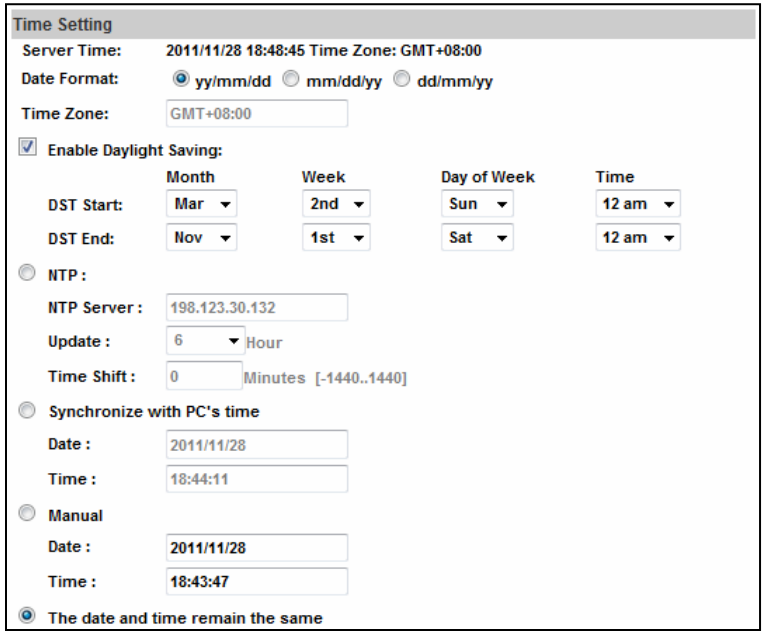
Text Edit

Text Edit

Text: OSD_Display

Alpha: 0%

c. Server time setting: Select between the options **NTP**, **Synchronize with PC's time**, **Manual**, **The date and time remain the same** for setting the time.



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

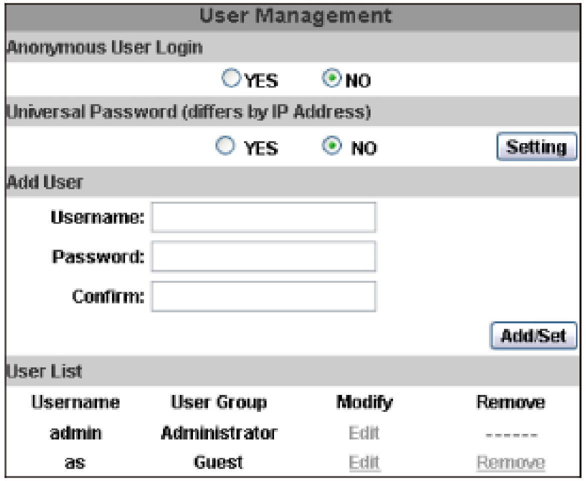
Date : 2011/11/28

Time : 18:43:47

● The date and time remain the same

II. User Management

The IP Camera supports three different users: **administrator**, **general**, and **anonymous** user.



User Management

Anonymous User Login

○ YES ● NO

Universal Password (differs by IP Address)

○ YES ● NO [Setting]

Add User

Username:

Password:

Confirm:

[Add/Set]

User List

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

a. Anonymous User Login:

Select "**Yes**" for allowing everybody to watch 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.

Select "**No**" for requiring a username and login to access the camera.

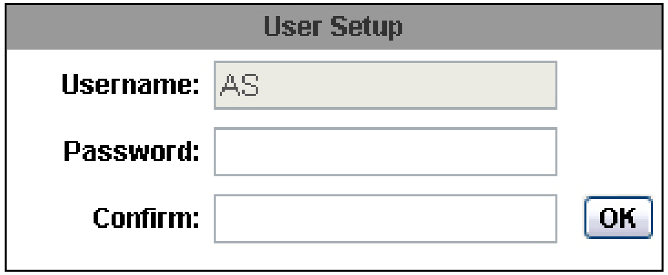
b. Universal Password:

Select "**Yes**" for allowing login to this IP Cam by universal password. Please refer to **Universal Password** chapter for more explanations. Select "**No**" for disabling universal password.

c. **Add user**

Type the user name and password, then click **Add/Set**. The guest user can only browse 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.



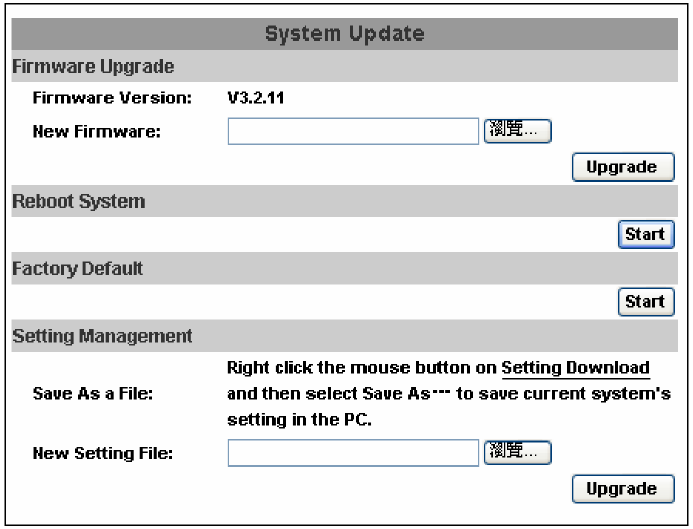
User Setup

Username: AS

Password:

Confirm:

III. System update



System Update

Firmware Upgrade

Firmware Version: V3.2.11

New Firmware:

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:

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

b. Reboot system: re-start the IP camera

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

d. Setting Management: The user can download the current settings to PC, or upgrade from previous saved settings.

1. Settings download:

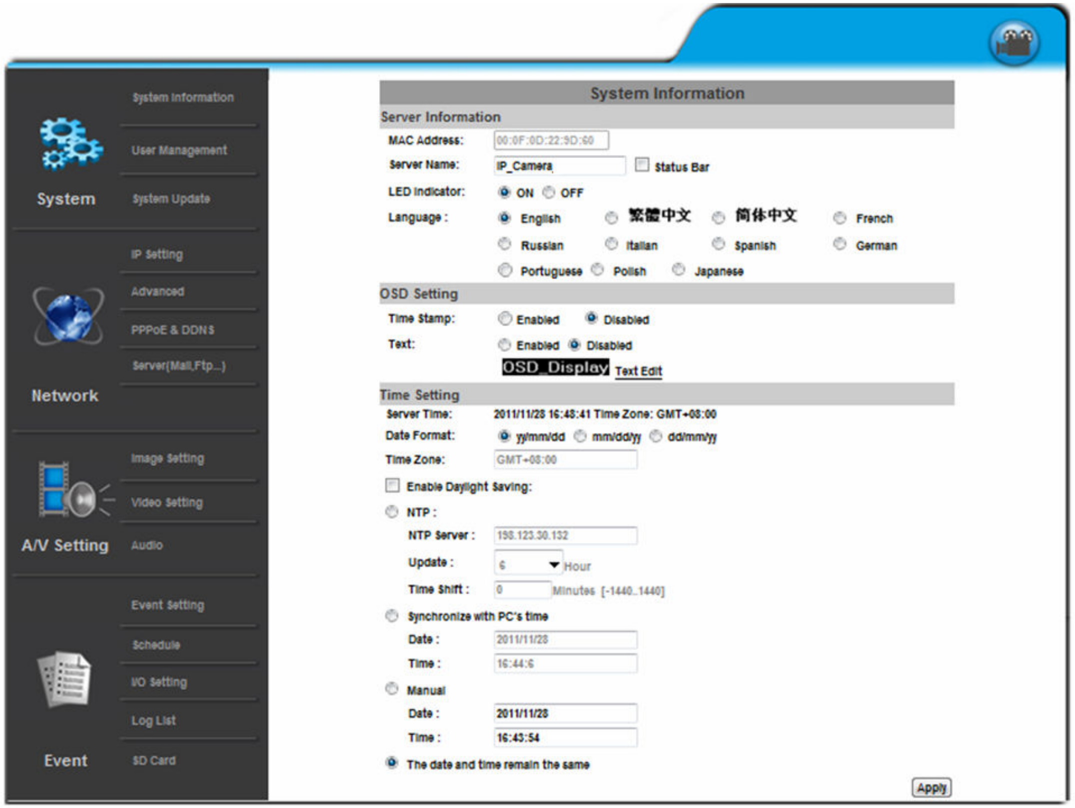
   Right-click the mouse button on Setting Download → Select **Save AS…** to save current IP Camera settings in PC → Select saving directory → Save

2. Upgrade from previous settings

   Browse → search previous settings → open → upgrade → Settings update confirm → click **index.html**. for returning to the main page

5.2. Network

Click to get into the administration page. Click to go back to the live video page.



System Information

Server Information

MAC Address: 00:0F:0D:22:9D:60

Server Name: IP_Camera □ Status Bar

LED Indicator: ● ON ○ OFF

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: 2011/11/28 16:48:41 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 : 198.123.30.132

Update : 6 Hour

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

○ Synchronize with PC's time

Date : 2011/11/28

Time : 16:44:6

○ Manual

Date : 2011/11/28

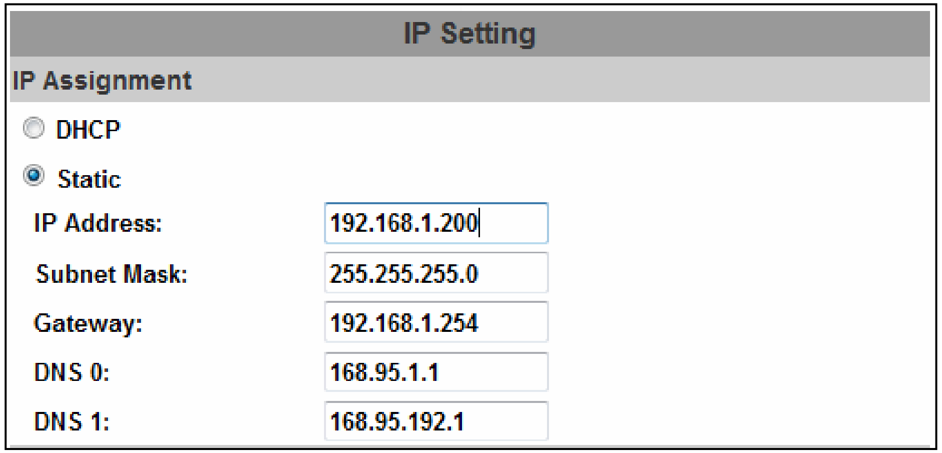
Time : 16:43:54

● The date and time remain the same

Advanced IP Settings

IP Assignment

The IP Camera supports DHCP and static IP



IP Setting

IP Assignment

○ DHCP

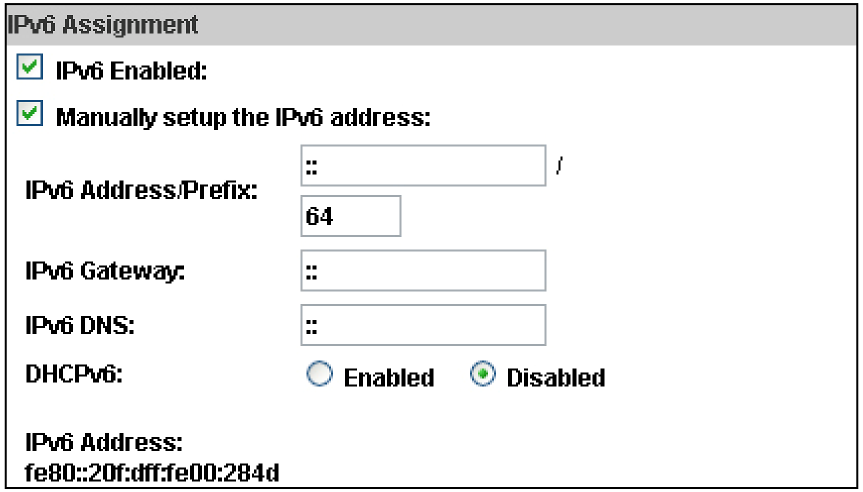
● Static

IP Address:	192.168.1.200
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.254
DNS 0:	168.95.1.1
DNS 1:	168.95.192.1

a. DHCP: The IP Camera will get all the network parameters automatically.

b. Static IP: Type-in the IP address subnet mask, gateway, and DNS.

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

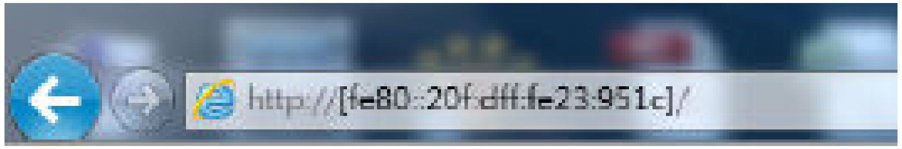
By enabling DHCPv6 you can configure the following IPv6 address settings:

✓ Manually setup the IPv6 address: Key-in the Address, Gateway, and DNS.

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

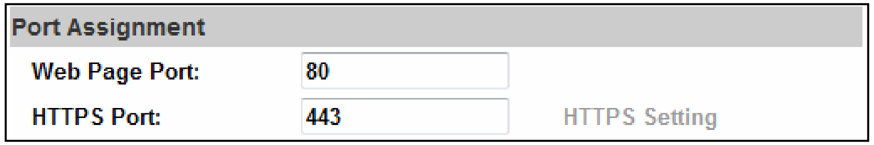
✓ Automatically generated IPv6 Address: Indicates a virtual IPv6 address generated automatically by the IP camera. This virtual IPv6 address cannot be used on WAN.

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



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

a. Port Assignment: The user might need to assign a different port to avoid conflicts when setting up the IP.



Port Assignment

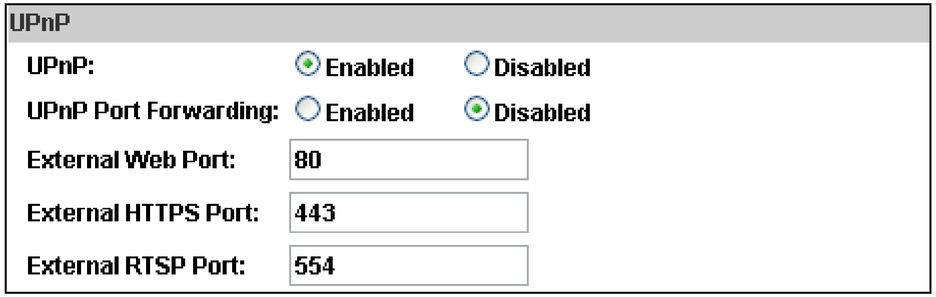
Web Page Port: 80

HTTPS Port: 443 HTTPS Setting

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

c. HTTPs Port: setup the https port(Default: 443)

UPnP



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**.

UPnP Port Forwarding：Enable UPnP Port Forwarding for accessing the IP Camera from the Internet; this option allows the IP Camera to open ports on the router automatically so that video streams can be sent out from a LAN. There are three external ports for being set: **Web Port**, **Http Port** and **RTSP** port. To utilize of this feature, make sure that your router supports **UPnP** and is activated.

Note: *UPnP must be enabled on your computer.*

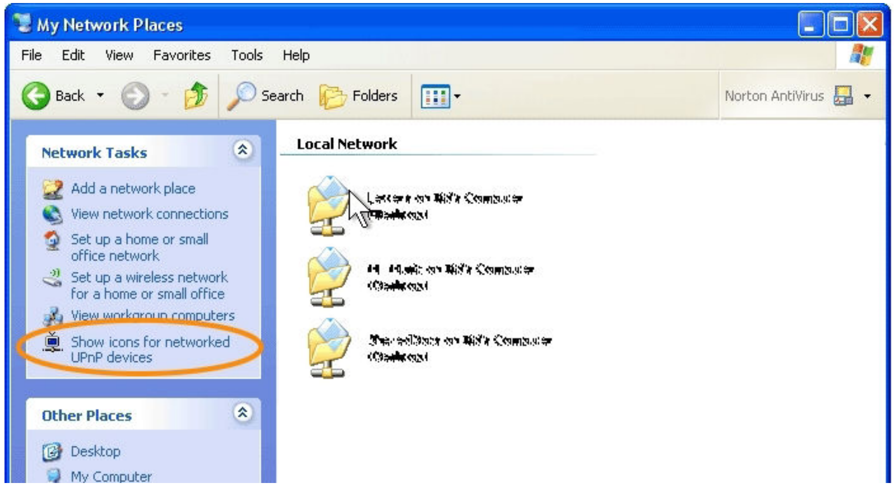
**Please follow the procedure to activate UPnP:

Approach 1

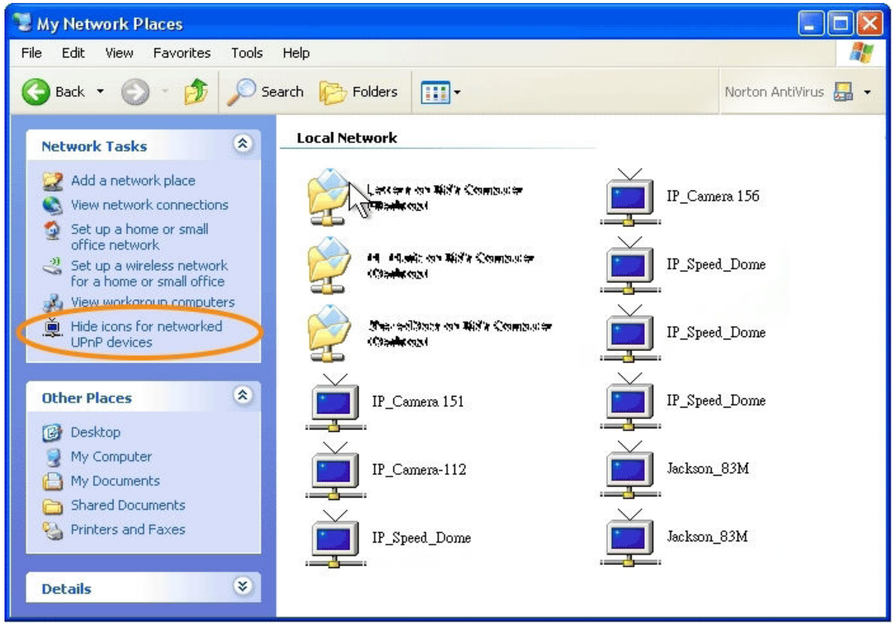
1. Open the **Control Panel** from the **Start Menu.**
2. Select **Add/Remove Programs.**
3. Select **Add/Remove Windows Components** and open **Networking Services** section.
4. Click **Details** and select **UPnP** to setup the service.
5. The IP device icon will be added to **My Network Places.**
6. The user may double click the IP device icon to access IE browser.

Approach 2

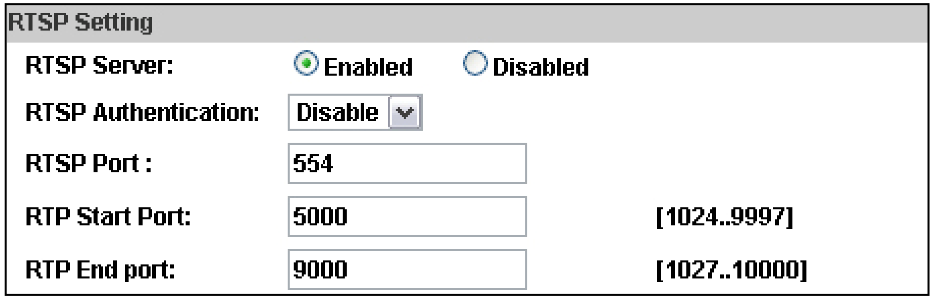
1. Open My **Network Space.**
2. Click **Show icons for networked UPnP devices** in the tasks column on the left of the page.
3. Windows might ask your confirmation for enabling the components. Click **Yes.**



4. Now the IP device is displayed under the LAN. Double-click the icon to access the camera via web browser. To disable the UPnP, click **Hide icons for networked UPnP devices** in the tasks column.



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 video streaming from the IP camera. The RTSP address can be set for two streaming respectively.

1. RTSP Server: enable or disable

✓**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 for a username and password before allows access.

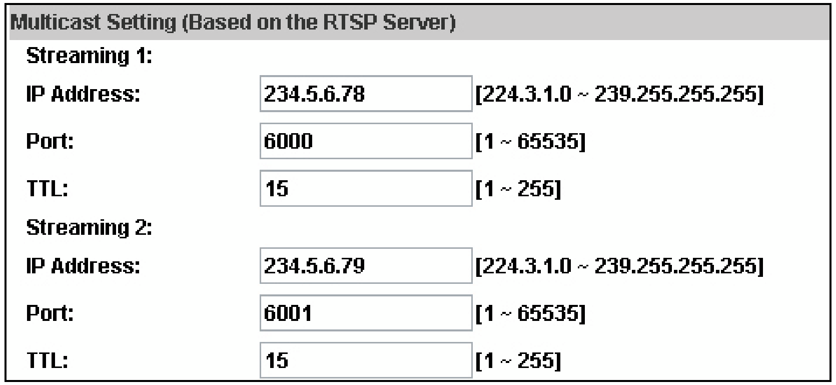
✓The password is transmitted as a clear text under basic mode, which provides a lower level of security than under **digest** mode.

✓Make sure your media player supports the authentication schemes.

2. RTSP Port: setup port for RTSP transmitting (Default: 554)

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

Multicast Setting (Based on the RTSP Server)

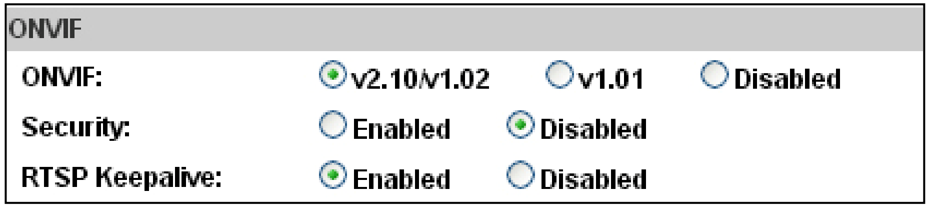


Multicast Setting (Based on the RTSP Server)

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 allows several users to share the same packet sent from the IP camera.
- ✓ For using Multicast, appoint here an IP Address and port. TTL means the life time of packet, the larger the value is, the more users can receive the packet.
- ✓ For using 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.

ONVIF



ONVIF

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

1. 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, otherwise the IP Camera will not be able to receive the video via ONVIF.

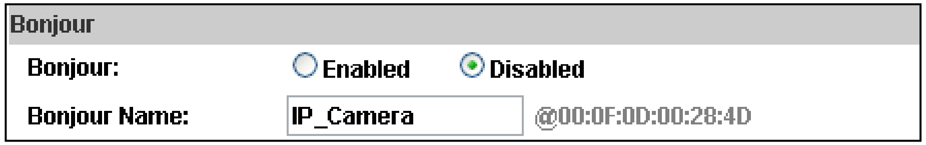
2. Security

   By selecting **Disable**, the username and password are not required for accessing the camera via ONVIF. By selecting **Enable** the username and password are necessary.

3. RTSP Keepalive:

   When the function is enabled, the camera checks once in a while if the user who is connected to the camera via ONVIF is still connected. If the connection has been broken the camera will stop transmitting video to the user

Bonjour



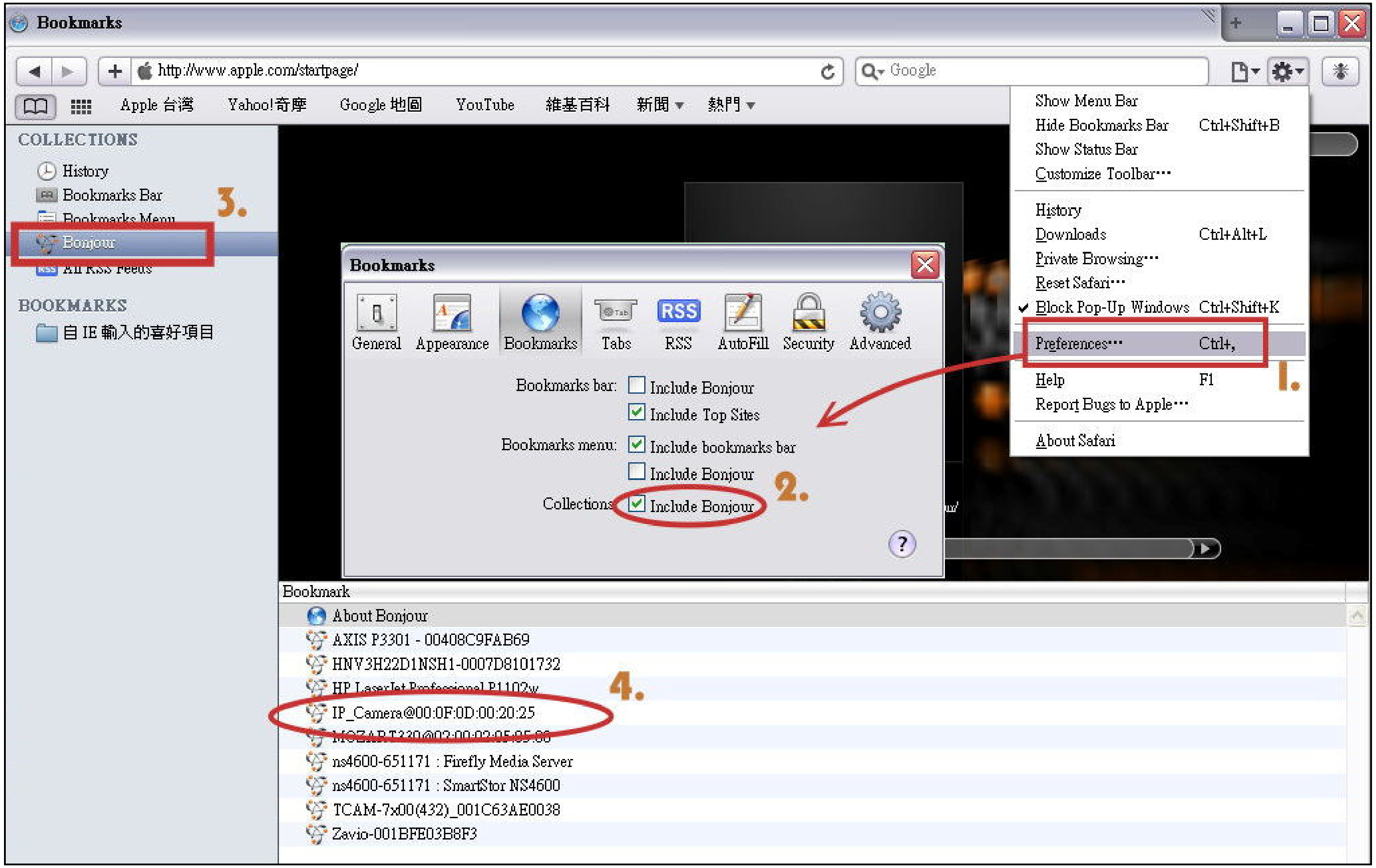
Bonjour

Bonjour: ○ Enabled ● Disabled

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

- ✓ This function allows Apple systems to connect to this IP camera. On **Bonjour Name** key-in the name here
- ✓ The web browser **Safari** also has a Bonjour function. Tick **Include Bonjour** in the bookmark setting, for the IP camera to appear under the bonjour category. Click the icon to connect to the IP camera

- ✓ The Bonjour function on Safari browser doesn't support HTTPS protocol. If on the camera you select **https**, the camera will appear on Safari's bookmarks but it cannot be accessed
- ✓ Take as a reference the following image:



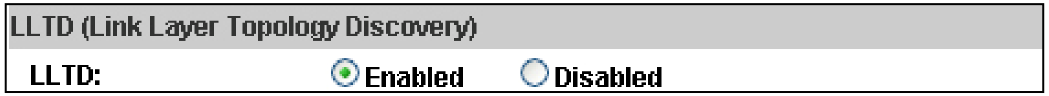
Bookmarks bar: ☐ Include Bonjour
☑ Include Top Sites

Bookmarks menu: ☑ Include bookmarks bar
☐ Include Bonjour

Collections: ☑ Include Bonjour

Bookmark
- About Bonjour
- AXIS P3301 - 00408C9FAB69
- HNV3H22D1NSH1-0007D8101732
- HP LaserJet Professional P1102w
- IP_Camera@00:0F:0D:00:20:25
- MOZART330@02:00:02:05:05:00
- ns4600-651171 : Firefly Media Server
- ns4600-651171 : SmartStor NS4600
- TCAM-7x00(432)_001C63AE0038
- Zavio-001BFE03B8F3

LLTD

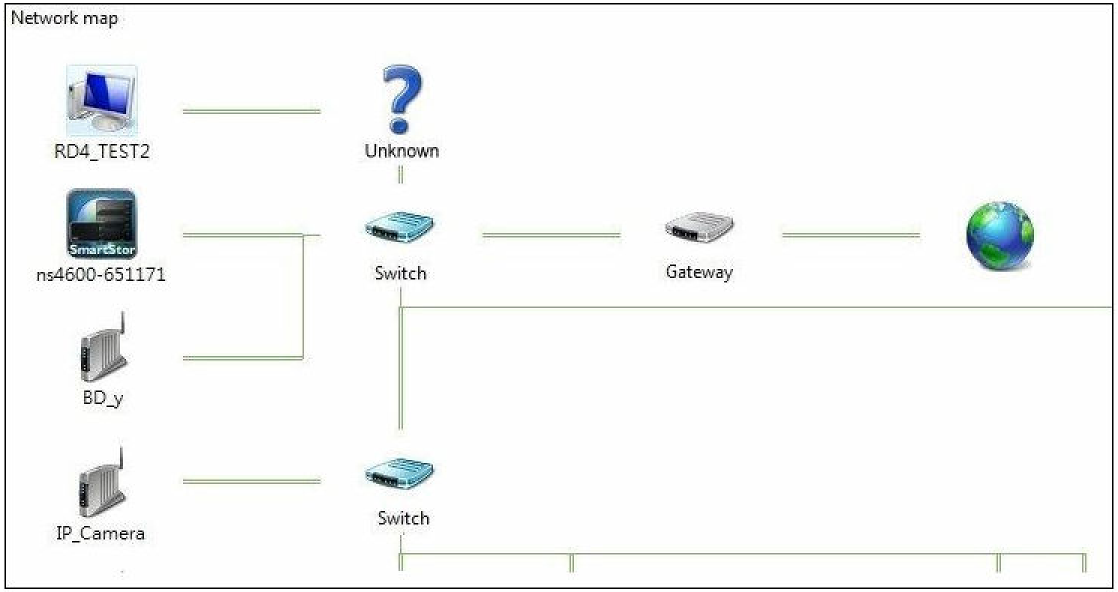


LLTD (Link Layer Topology Discovery)

LLTD: ● Enabled ○ Disabled

- ✓ If your PC supports LLTD, enable this function for allowing checking the connection status, properties, and device location (IP address) in the network map.
- ✓ If the computer is running Windows Vista or Windows 7, you can find LLTD through the path:

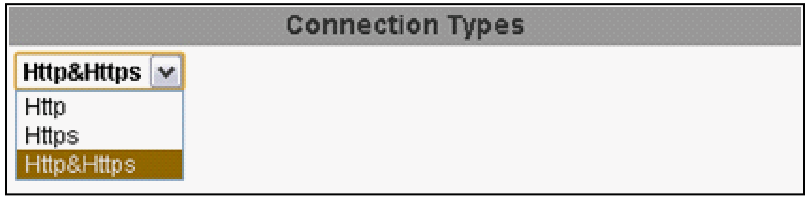
Control Panel → Network and Internet → Network and Sharing Center → Click **See full map**



II. Advanced

a. Https (Hypertext Transfer Protocol Secure

When the users access cameras via Https protocol, the transmitted information will be encrypted, increasing the security level.


Connection Types

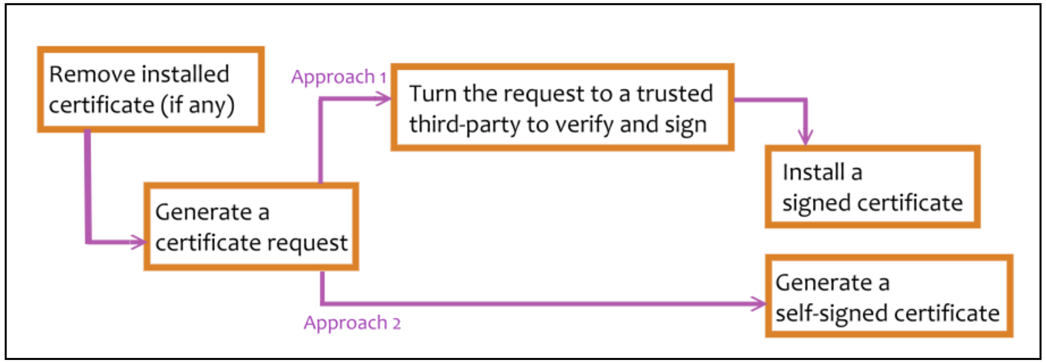
Select the connection type:

- ✓ Http: the user can access the camera via the Http path but cannot access it via the Https path.
- ✓ Https: the user can access the camera via the Https path but cannot access it via the Http path.
- ✓ Http & Https: Both the Http and Https path can be used to access the camera. When you change the connection type settings, it may cause connection error or disconnection error if you switch the protocol directly. Therefore, **Http & Https** mode is necessary.

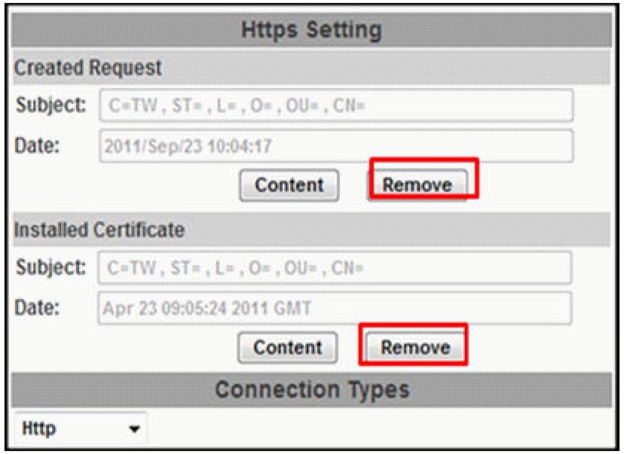
If you want to change from Http to Https, please switch to **Http & Https** mode first, and then switch to **Https** mode and vice versa.

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

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

Remove the existing certificate: Before you generate a new certificate, please remove the installed one. Select the **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

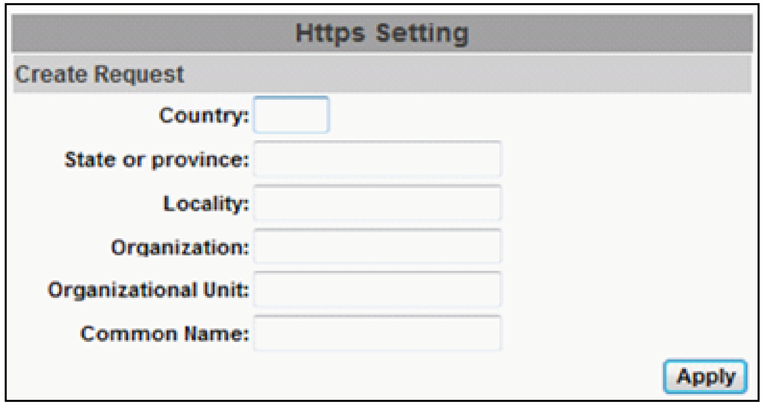
Subject: C=TW , ST= , L= , O= , OU= , CN=

Date: Apr 23 09:05:24 2011 GMT

Connection Types

Http

Created Request: Fill-in the following form and click **apply.**



Https Setting

Create Request

Country:

State or province:

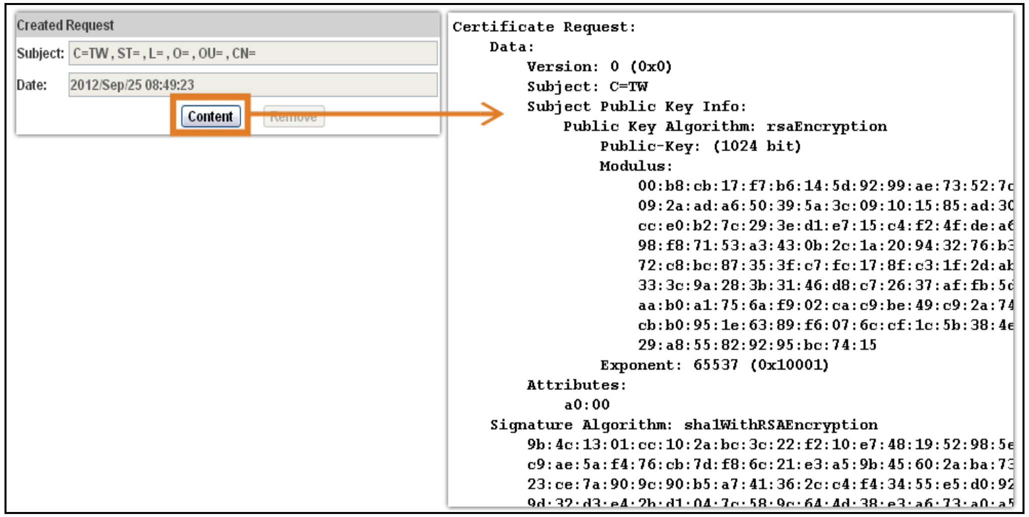
Locality:

Organization:

Organizational Unit:

Common Name:

After generating a certificate request, if you choose to turn it and verified by a trusted third-party, click **Content** and copy all the request content.



Created Request

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

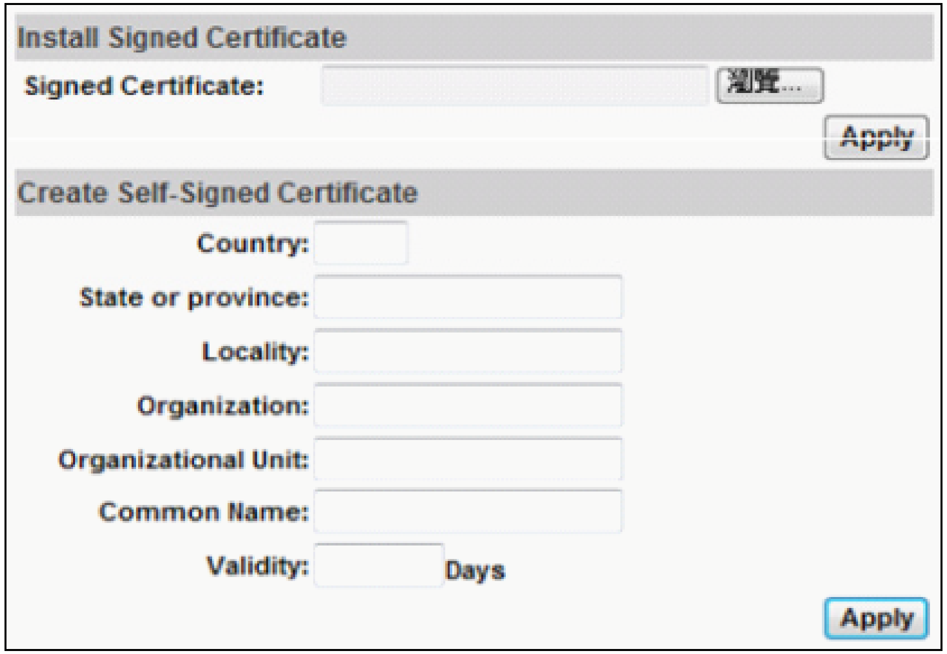
Date: 2012/Sep/25 08:49:23

```
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:73:52:7c
                    09:2a:ad:a6:50:39:5a:3c:09:10:15:85:ad:30
                    cc:e0:b2:7c:29:3e:d1:e7:15:c4:f2:4f:de:a6
                    98:f8:71:53:a3:43:0b:2c:1a:20:94:32:76:b3
                    72:c8:bc:87:35:3f:c7:fc:17:8f:c3:1f:2d:ab
                    33:3c:9a:28:3b:31:46:d8:c7:26:37:af:fb:5c
                    aa:b0:a1:75:6a:f9:02:ca:c9:be:49:c9:2a:74
                    cb:b0:95:1e:63:89:f6:07:6c:cf:1c:5b:38:4e
                    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:e7:48:19:52:98:5e
        c9:ae:5a:f4:76:cb:7d:f8:6c:21:e3:a5:9b:45:60:2a:ba:73
        23:ce:7a:90:9c:90:b5:a7:41:36:2c:c4:f4:34:55:e5:d0:92
        9d:32:d3:e4:2b:d1:04:7c:58:9c:64:4d:38:e3:a6:73:a0:a5
```

According to the certificate source, there are two ways to install the certificate:

If you had sent the certificate request for signing and receiving a signed certificate, 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 the validity day, click **Apply** to finish installed it.



Install Signed Certificate

Signed Certificate:

Create Self-Signed Certificate

Country:

State or province:

Locality:

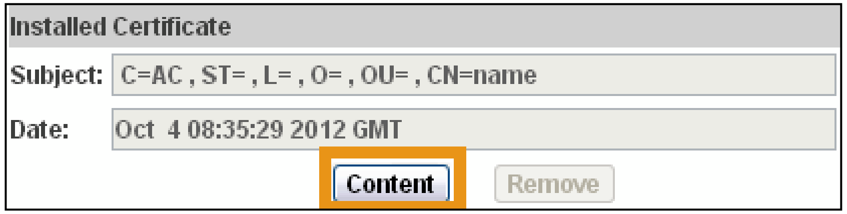
Organization:

Organizational Unit:

Common Name:

Validity: Days

After finishing the installation, click on **Content** to call out and check the certificate content

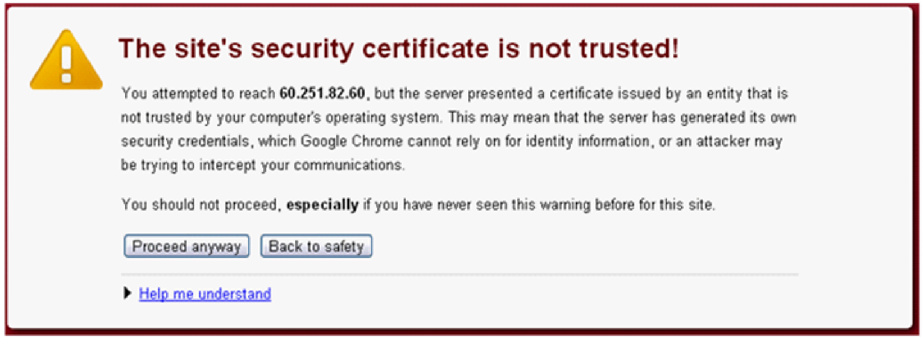


Installed Certificate

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

Date: Oct 4 08:35:29 2012 GMT

To use Https to access the camera, open your browser, and key-in **https:// (IP address)/** in the address bar. Now your data will be transmitted via encrypted communications. The browser will check your certificate status. It might show the following warning message:



The site's security certificate is not trusted!

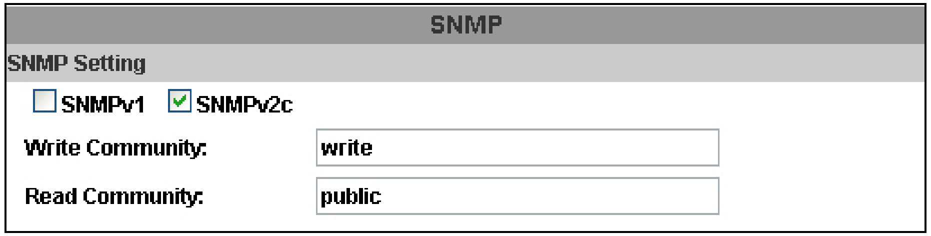
You attempted to reach **60.251.82.60**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker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

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

Meaning that certificate is self-signed or signed by a distrusted institution. Click **Proceed anyway** for continuing to the camera page.

b. SNMP (Simple Network Management Protocol)

1. **SNMPv1** or **SNMPv2**: write the name of both **Write Community** and **Read Community.**



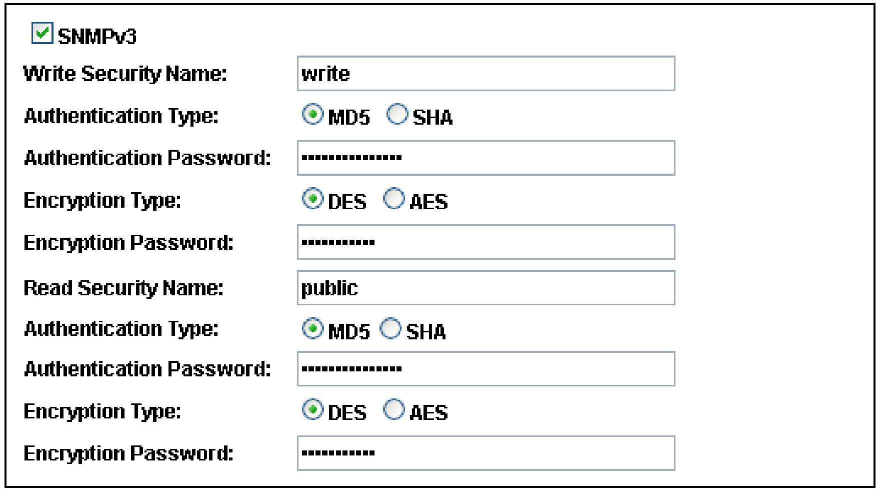
SNMP

SNMP Setting

□ SNMPv1 ☑ SNMPv2c

Write Community:	write
Read Community:	public

2. SNMPv3: Set the Security Name, Authentication Type, Authentication Password, Encryption Type, Encryption Password of Write mode and Read mode

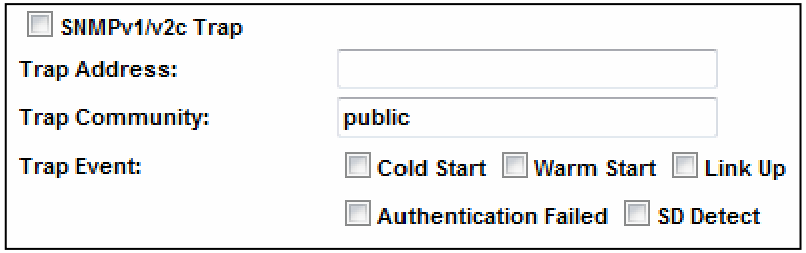


☑ SNMPv3

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:	***********

3. Enable SNMPv1/SNMPv2 Trap for detecting the Trap server

Please set what event needs to be detected.



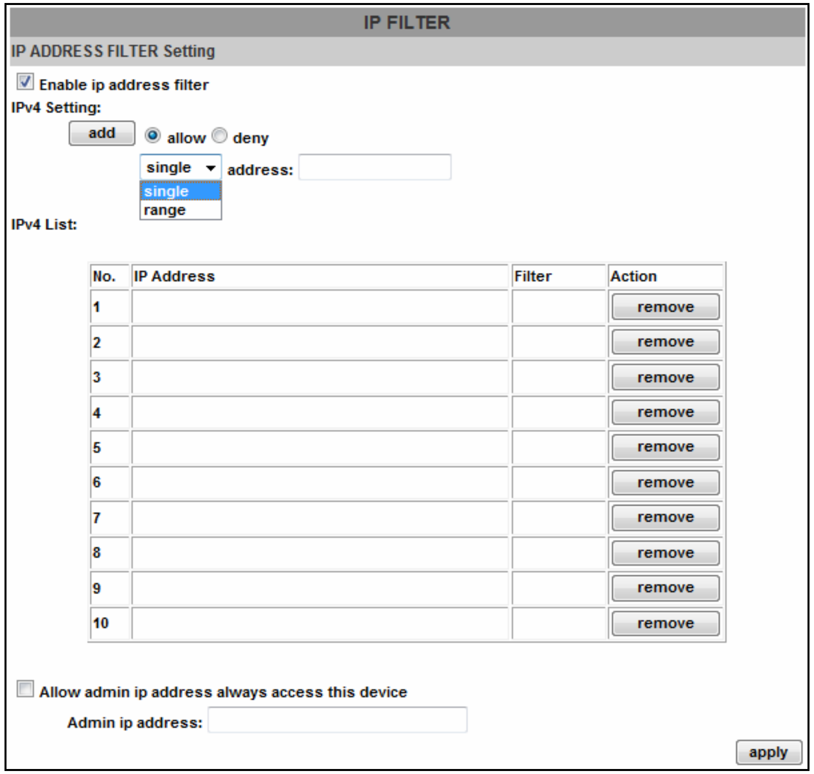
☐ SNMPv1/v2c Trap

Trap Address:	
Trap Community:	public
Trap Event:	☐ Cold Start ☐ Warm Start ☐ Link Up ☐ Authentication Failed ☐ SD Detect

- ✓ Cold Start: The camera starts up or reboots.
- ✓ Setting changed: The SNMP settings have been changed.
- ✓ Network Disconnected: The network connection was broken down (The camera will send trap messages after the network is 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.

c. Access list:

Enable IP address filter for setting the IP addresses which allows or denies this camera. There are two options: **single** and **range**.



IP FILTER

IP ADDRESS FILTER Setting

☑ Enable ip address filter

IPv4 Setting:

add ● allow ○ deny

single address:

IPv4 List:

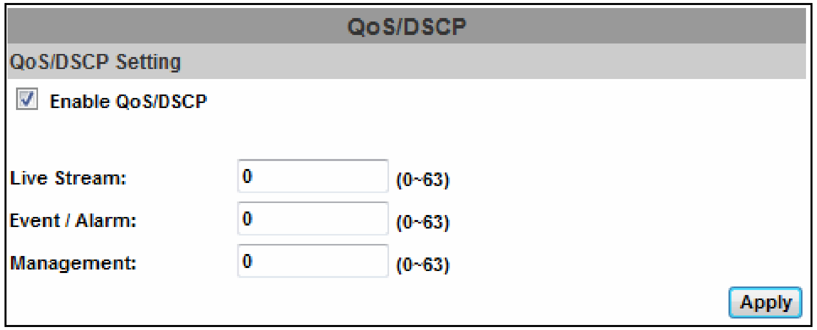
No.	IP Address	Filter	Action
1			remove
2			remove
3			remove
4			remove
5			remove
6			remove
7			remove
8			remove
9			remove
10			remove

□ Allow admin ip address always access this device

Admin ip address:

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

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. Please define it for **Live Stream**, **Event / Alarm and Management**



QoS/DSCP

QoS/DSCP Setting

☑ Enable QoS/DSCP

Live Stream: 0 (0~63)

Event / Alarm: 0 (0~63)

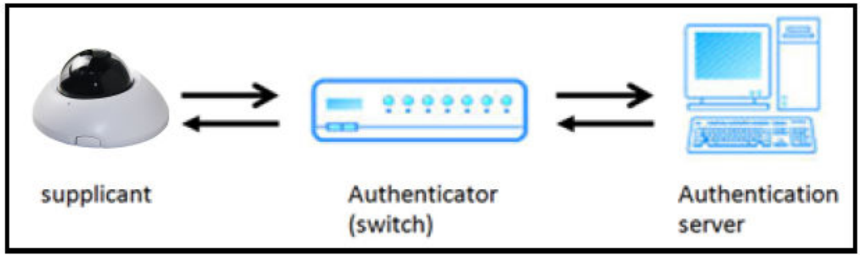
Management: 0 (0~63)

Apply

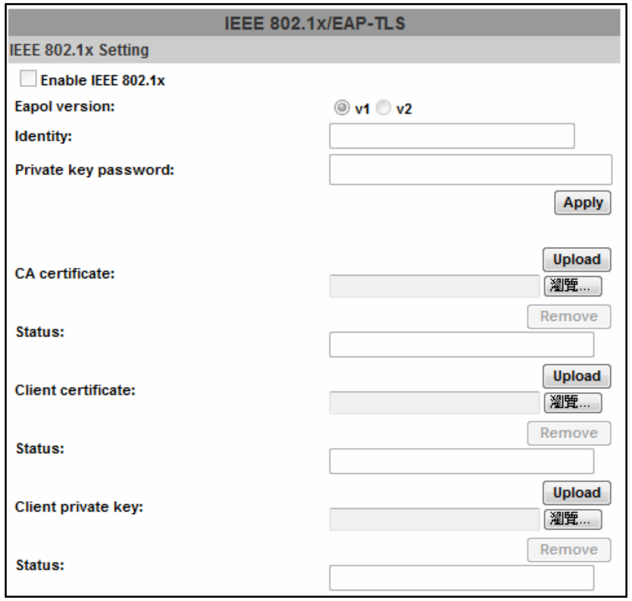
e. IEEE 802.1x:

IEEE 802.1x is an IEEE standard for port-based Network Access Control. It provides an authentication mechanism to a device on a LAN or WLAN.

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 is supported. This camera supports EAP-TLS method. Please enter the ID, password issued by the CA, then upload related certificates.



IEEE 802.1x/EAP-TLS

IEEE 802.1x Setting

□ Enable IEEE 802.1x

Eapol version: ● v1 ○ v2

Identity:

Private key password:

CA certificate:

Status:

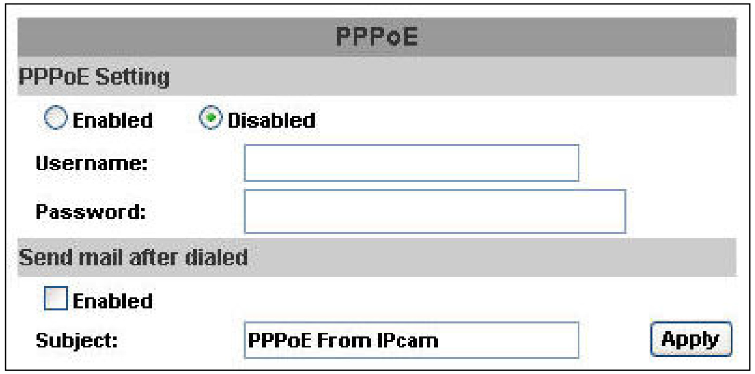
Client certificate:

Status:

Client private key:

Status:

III. PPPoE & DDNS



PPPoE

PPPoE Setting

○ Enabled ● Disabled

Username:

Password:

Send mail after dialed

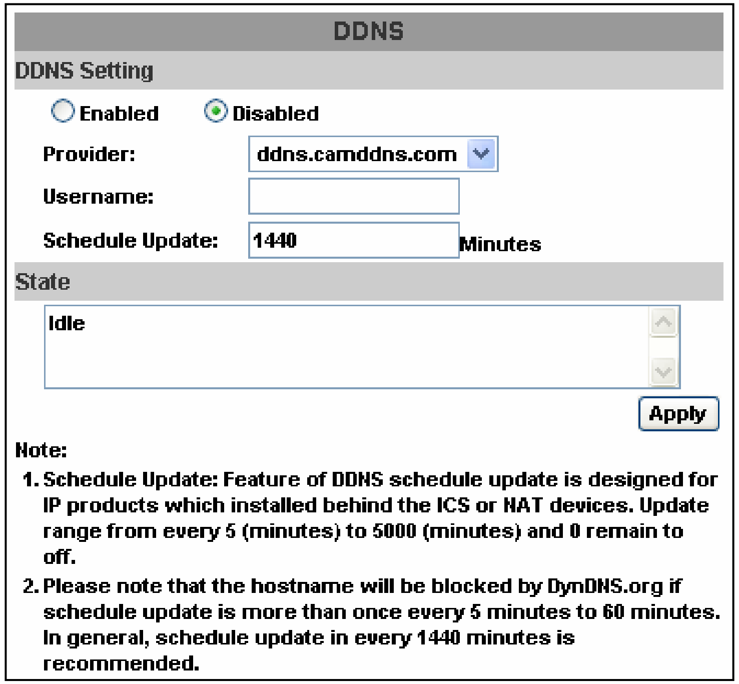
□ Enabled

Subject: PPPoE From IPcam

a. PPPoE: Select **Enabled** to use PPPoE. Key-in the the Username and password for VDSL connection.

Send mail after dialed: When connected to the internet, the camera will send a mail to a specific mail account.

b. DDNS (camddns example):



DDNS

DDNS Setting

○ Enabled ● Disabled

Provider: ddns.camddns.com

Username:

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.

1. Enable this service.
2. Key-in the username.
3. IP schedule update. Default: 5 minutes.
4. Click **Apply**.

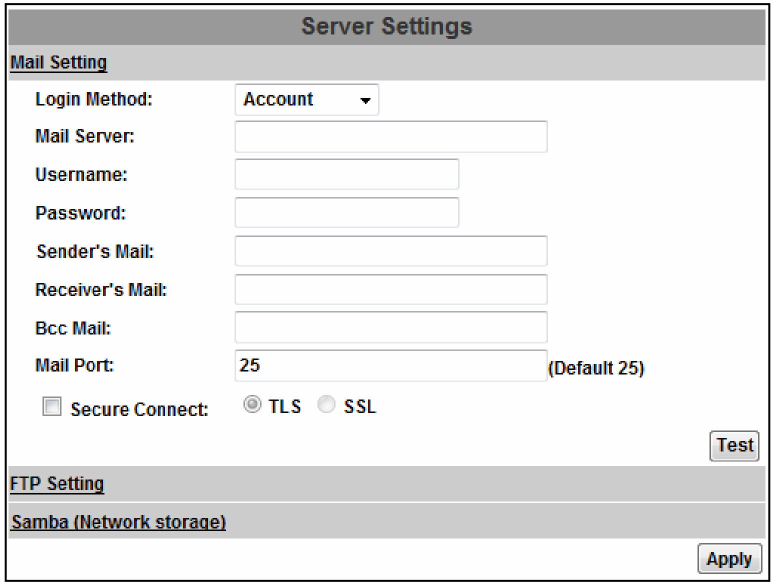
DDNS Status

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

IV. Server settings

There are three server types available: **Email**, **FTP** and **SAMBA**. Select the item for display detailed configuration options. You can configure either one or all of them.

To send out the video via mail of FTP, please set up the configuration first.



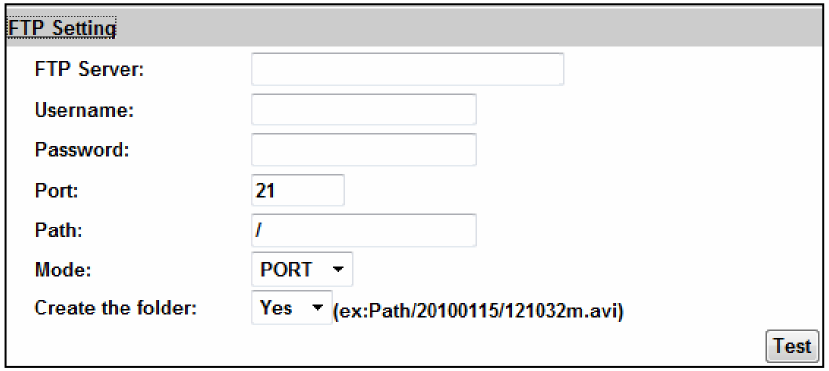
Server Settings

Mail Setting

Login Method:	Account
Mail Server:	
Username:	
Password:	
Sender's Mail:	
Receiver's Mail:	
Bcc Mail:	
Mail Port:	25 (Default 25)
□ Secure Connect:	● TLS ○ SSL

FTP

To send out the video via mail of FTP, please set up the configuration.

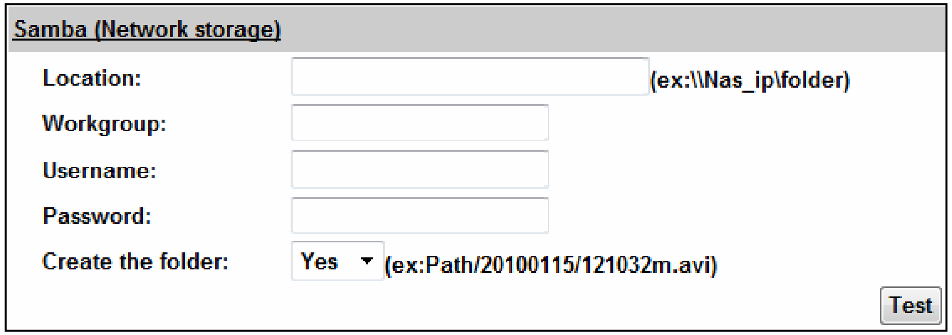


FTP Setting

FTP Server:	
Username:	
Password:	
Port:	21
Path:	/
Mode:	PORT
Create the folder:	Yes (ex:Path/20100115/121032m.avi)

Samba

Select this option to send the media files via a neighbor network when an event is triggered.



Samba (Network storage)

Location: (ex:\\Nas_ip\folder)

Workgroup:

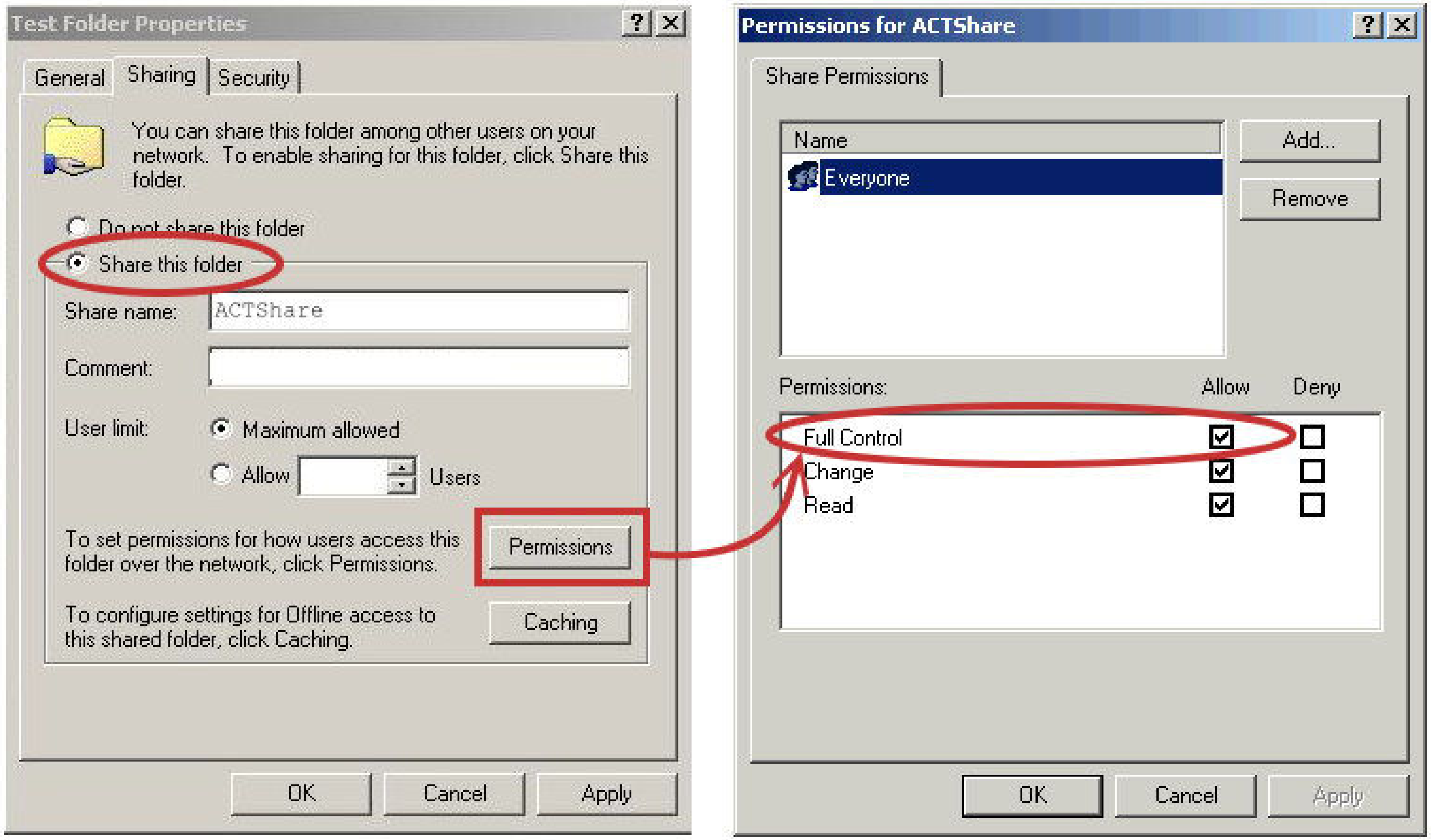
Username:

Password:

Create the folder: Yes (ex:Path/20100115/121032m.avi)

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.

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

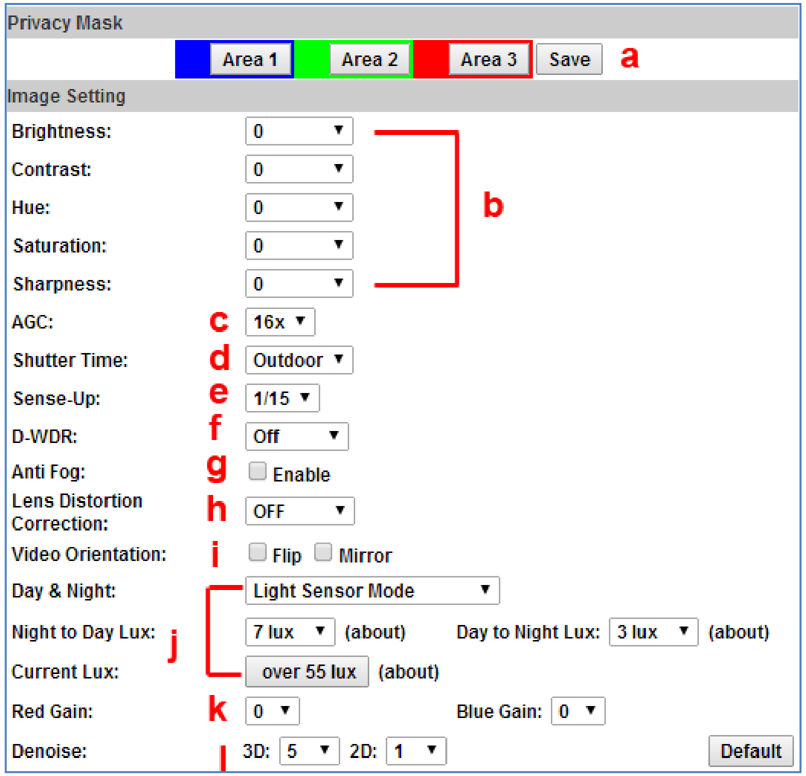
Name: Everyone

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

5.3. A / V Setting

1. Image Setting

Please refer to the details below for image settings:



Privacy Mask

Area 1 Area 2 Area 3 Save

Image Setting

Brightness: 0

Contrast: 0

Hue: 0

Saturation: 0

Sharpness: 0

AGC: 16x

Shutter Time: Outdoor

Sense-Up: 1/15

D-WDR: Off

Anti Fog: □ Enable

Lens Distortion Correction: OFF

Video Orientation: □ Flip □ Mirror

Day & Night: Light Sensor Mode

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

Current Lux: over 55 lux (about)

Red Gain: 0 Blue Gain: 0

Denoise: 3D: 5 2D: 1

Default

a. For security and privacy purposes, there are three areas that can be set up for privacy. Click the Area button first, and then drag an area on the above image. Remember to save your settings. The masked area will not be shown on both live view and recording image.

b. Brightness, Contrast, Hue, Saturation, Sharpness can be adjusted here. The available values are: **-4, -3, -2, -1, 0, 1, 2, 3, 4.**

c. AGC: The sensitivity of the camera can be adjusted to the environmental lighting. By enabling this function the camera will get brighter images on low light, but the level of noise may also increase. The available values are: **16x, 24x, 32x, 48x, 64x.**

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

Note: When you select a number in **Shutter Time**, the shutter time will vary in a range and be controlled by camera automatically. The following table shows the shutter time options and corresponding range.

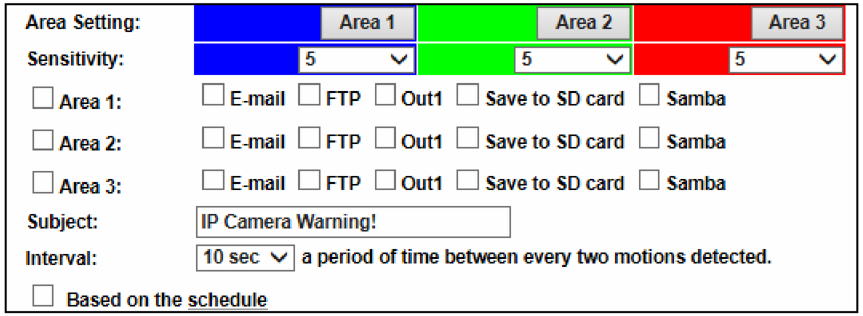
Option	Shutter Time Range (sec.)
Outdoor	1/33000 ~ Selected number in **Sense-up**
Indoor	NTSC: 1/120 ~ Selected number in **Sense-up** PAL: 1/100 ~ Selected number in **Sense-up**
1/30	1/33000 ~ 1/30
1/50	1/33000 ~ 1/50
1/60	1/33000 ~ 1/60
1/100	1/33000 ~ 1/100
1/125	1/33000 ~ 1/125
1/250	1/33000 ~ 1/250
1/500	1/33000 ~ 1/500
1/1000	1/33000 ~ 1/1000
1/33000	1/33000
* **Sense-up options:** 1/30, 1/15, 1/10	

5.4. Event List

The IP Camera provides multiple event settings.

1. Event Setting

a. 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

Subject: IP Camera Warning!

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

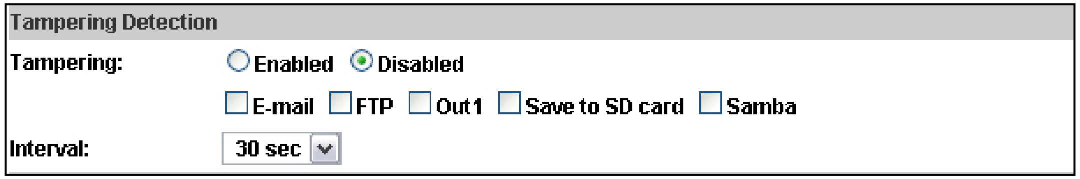
□ Based on the schedule

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

By selecting **save to SD card**, the video or snapshot will be saved to the Micro SD card. Also, by ticking **E-mail/ FTP/ Samba** on the **Log** option, the motion detection log will be sent to **E-mail/ FTP/ Samba** simultaneously.

- Interval: For example, when selecting "10 sec", once the motion is detected and the 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.

b. Tampering Detection



Tampering Detection

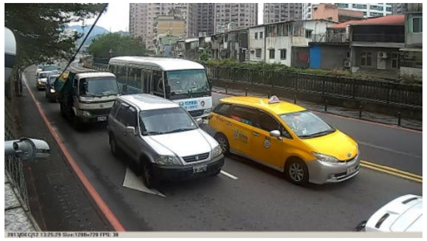
Tampering:	○ Enabled ● Disabled
	□ E-mail □ FTP □ Out1 □ Save to SD card □ Samba
Interval:	30 sec

When the camera view is covered, moved, hit by strong light, or out of focus, the tampering detection will be triggered, and send snapshots to mail/FTP/Samba/SD card, or trigger the external alarm. For example:

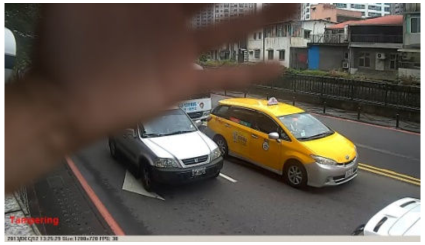
Before Tampering Detection

Tampering Triggered (Defocused)

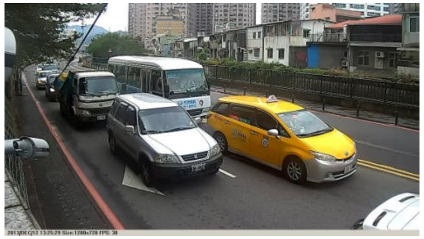
Before Tampering Detection



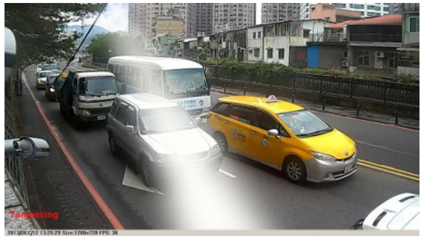
Tampering Triggered (Lens Covered)



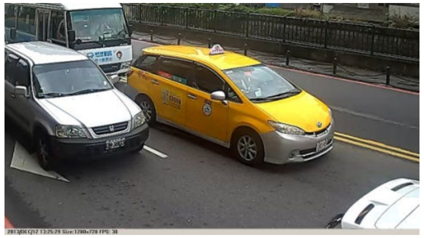
Before Tampering Detection



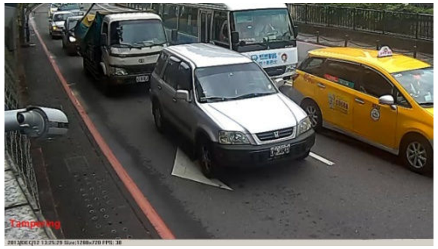
Tampering Triggered (Glare)



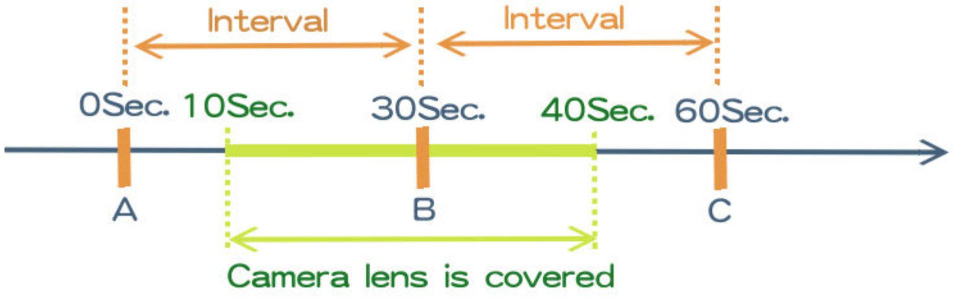
Before Tampering Detection



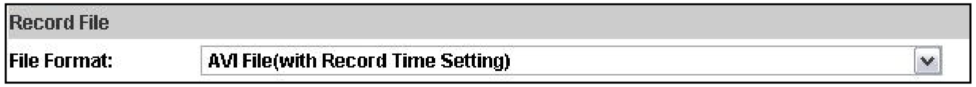
Tampering Triggered (Camera Moved)



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



c. Record File



Record File

File Format: AVI File(with Record Time Setting)

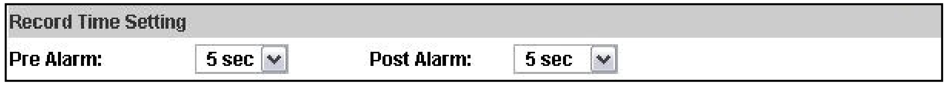
When an event occurs, the IP camera will record a video clip or take snapshot, and then send to mail/ FTP/ Samba. Select the file format to be saved.

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

• JPEG Files (with Record Time Setting): This option is enabled when selecting **JPEG** video format in **streaming 1** on **Video Setting**, this option can be enabled. Select this option to save several JPEG picture files. The successive picture files cover a period of time according to the value set in **Record Time Setting**.

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

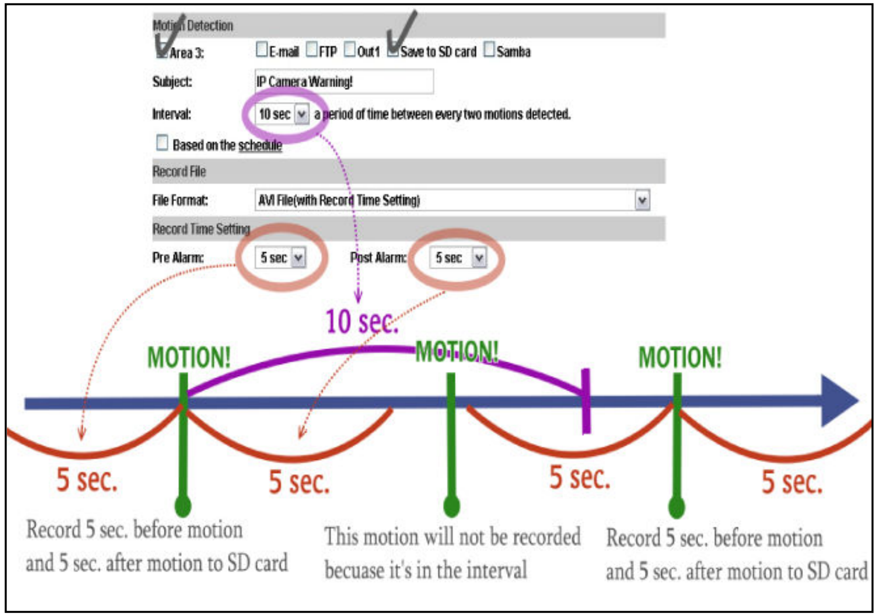
d. Record Time Setting



Record Time Setting

Pre Alarm: 5 sec Post Alarm: 5 sec

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



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

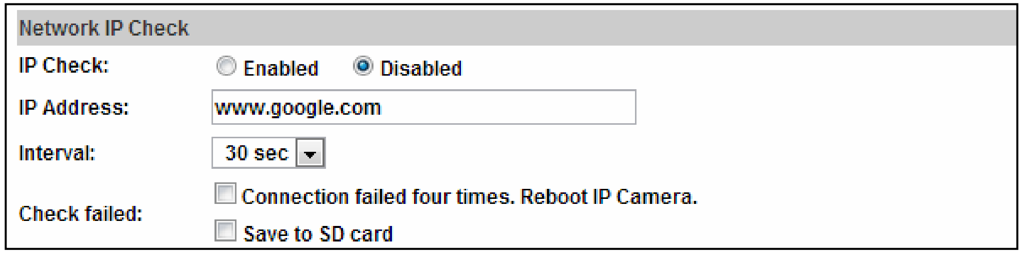
Record 5 sec. before motion and 5 sec. after motion to SD card

e. Network Dis-connected:

The IP Camera will scan the network. The image will be record to the SD card after the IP Camera detects network dis-connected, if set **Save to SD card**.

f. Network IP check:

After enabling IP Check, the IP camera can check if the network server is connecting. If the IP camera checking failed, the image will be recorded into the SD card.



Network IP Check

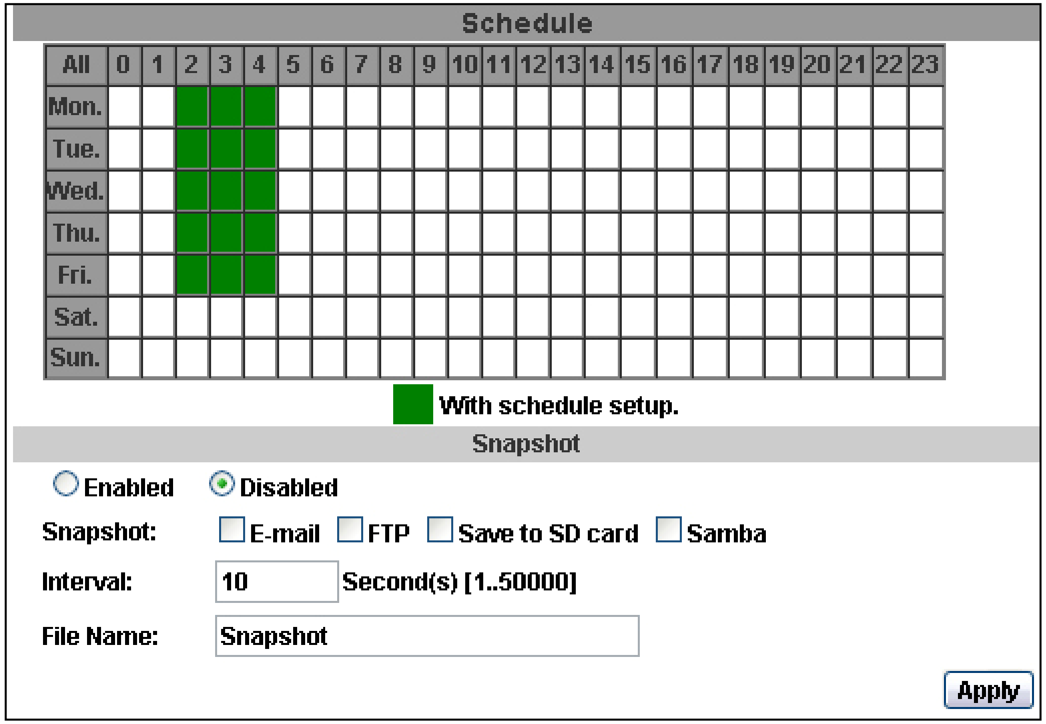
IP Check: ○ Enabled ● Disabled

IP Address: www.google.com

Interval: 30 sec

Check failed: □ Connection failed four times. Reboot IP Camera.
□ Save to SD card

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]

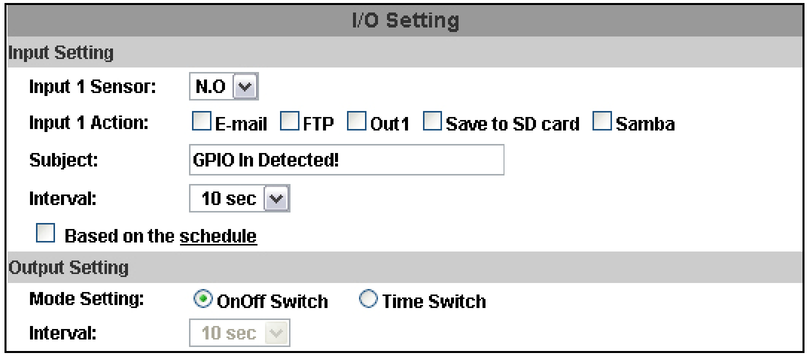
File Name: Snapshot

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

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

The IP Cam supports input and output. When the input condition is triggered the camera will trigger the relay; send video to mail addresses or /FTP server / SAMBA.

- Interval:

For example, when selecting **10 sec**, once the motion is detected and the action is triggered, it cannot be triggered again within 10 seconds.

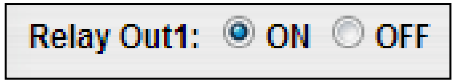
- Based on the schedule:

Only when the option box is ticked, the selected schedule time for I/O is enabled. For example, if the 11th hour of Monday has not been colored in the schedule table, then no action will be triggered even if 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.

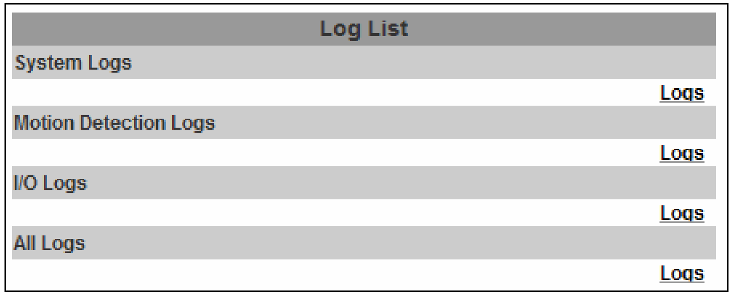
- ON/Off Switch: The camera triggers the external device and lasts for 10 seconds. You can turn off the alarm manually by clicking **off** at the right bottom of the live video page.



Relay Out1: ● ON ○ OFF

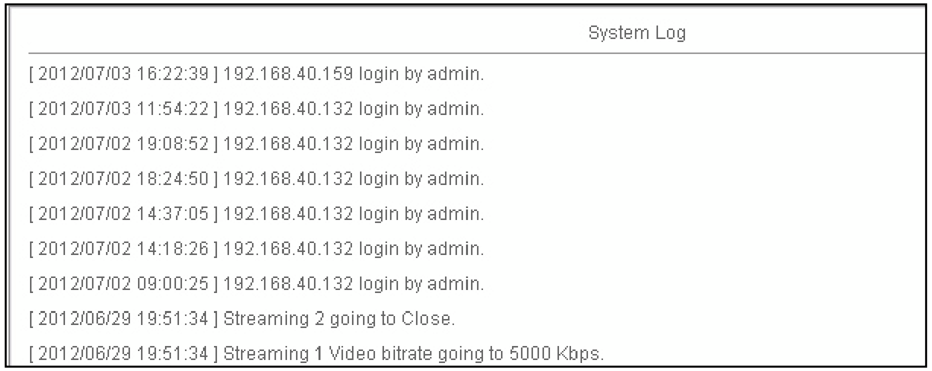
- Time Switch: The camera triggers the external device and lasts for certain time according to the internal setting, and the user is not allowed to break off the alarm manually.

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.



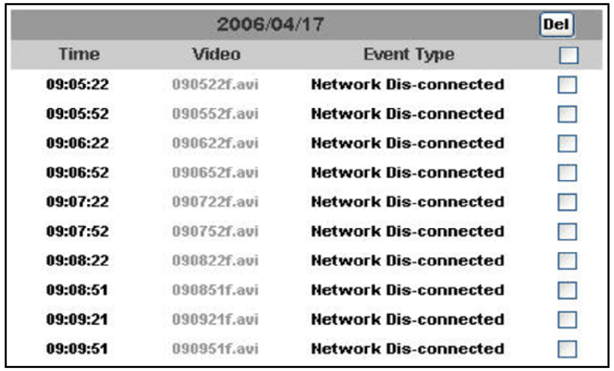
System Log

```
[ 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

Insert the Micro SD card before using it. Make sure to push the Micro SD card completely into the slot. Click the date listed on this page for showing the video list. 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**.



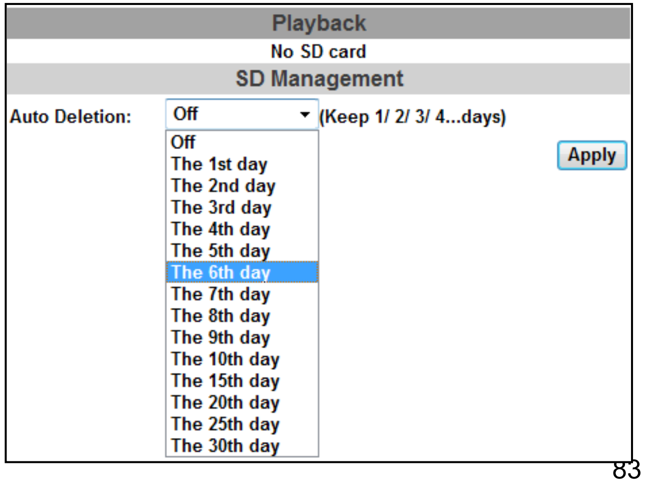
2006/04/17 Del

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

When choosing **The 1st day** the recoding file will be kept for one day.

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



Playback

No SD card

SD Management

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

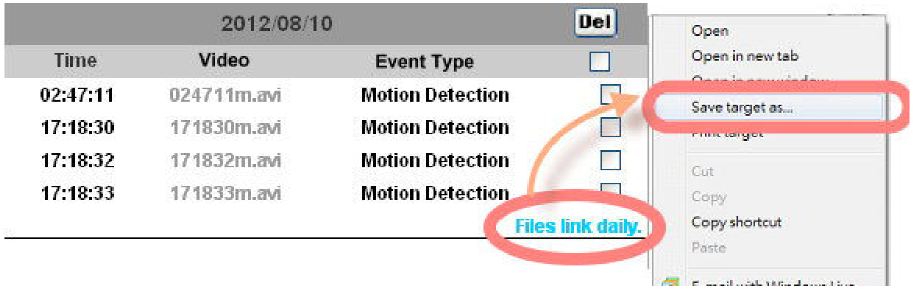
Note: The use of the SD card will slightly affect the operation of the IP Camera, such as affecting the frame rate of the video.

c. Copy to PC

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

For using **FlashGet** to download image and video data from the Micro SD card, please follow the steps:

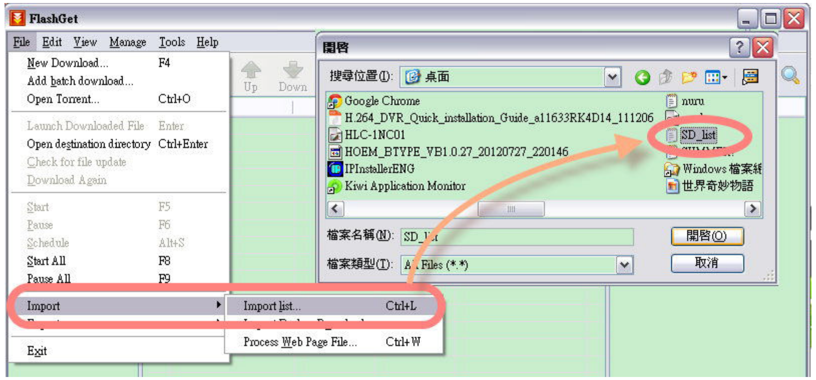
(i) Enter data list and right-click **Files link daily**, select **save target as…** then save the link list to PC.



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	□

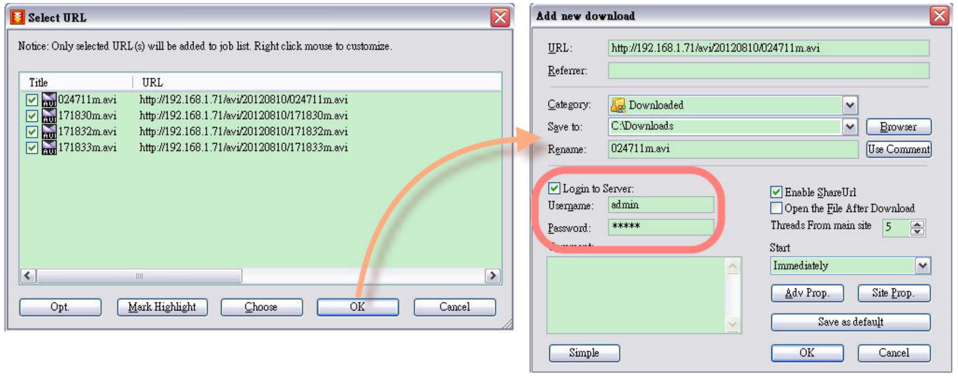
(ii) Open FlashGet, select **File** → **Import** → **Import list**, and find the link list file you just saved. The file name may be called **SD_list**.



檔案名稱(N): SD_list

檔案類型(T): All Files (*.*)

(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.



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

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: *****

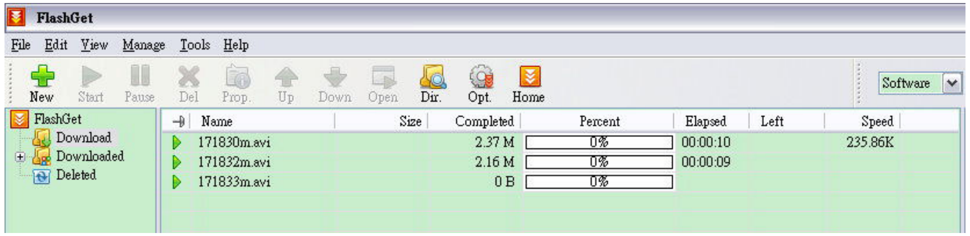
☑ Enable ShareUrl

□ Open the File After Download

Threads From main site 5

Start: Immediately

(iv) Click **OK** to start download.

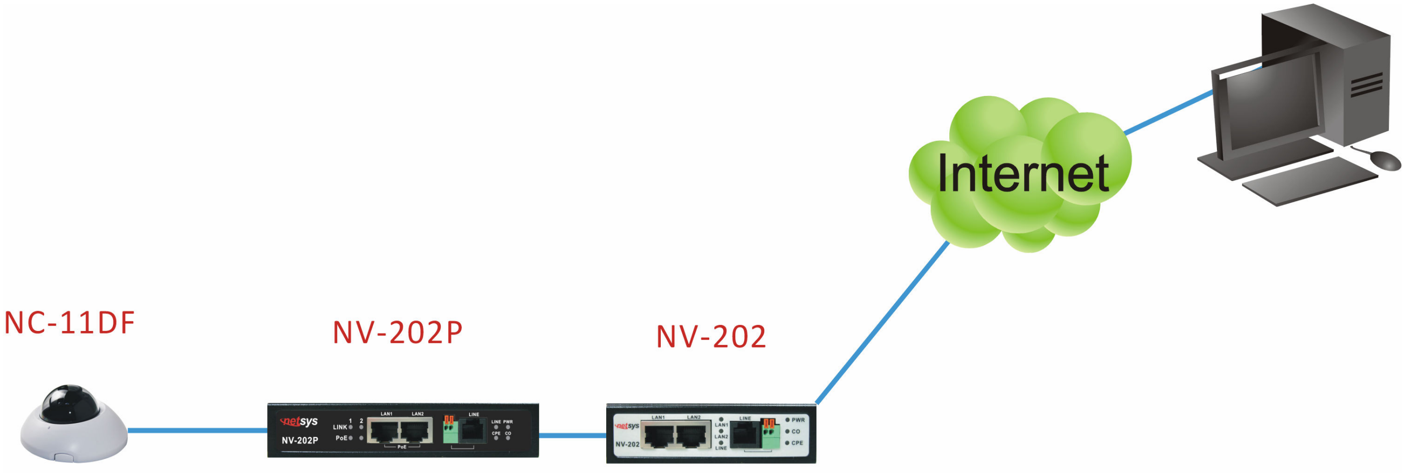


Name	Size	Completed	Percent	Elapsed	Left	Speed
171830m.avi		2.37 M	0%	00:00:10		235.86K
171832m.avi		2.16 M	0%	00:00:09		
171833m.avi		0 B	0%			

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

Chapter 6. Network Configuration

I. Configuration 1:



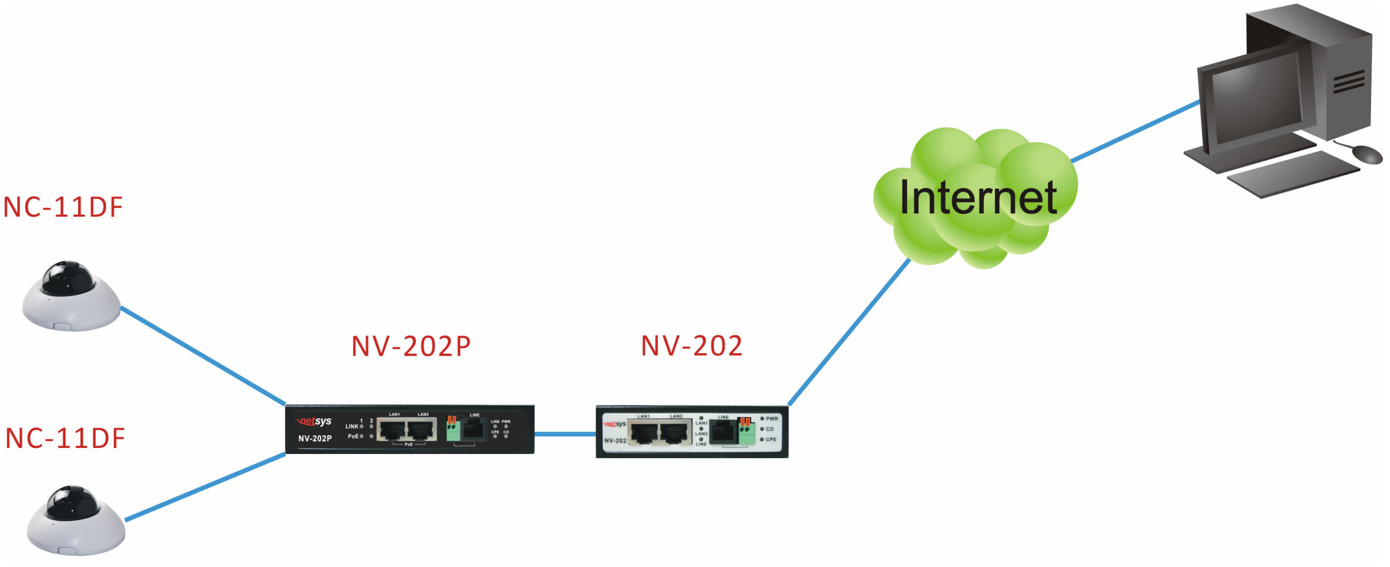
a. Internet Access: NV-202 and NV-202P(Ethernet Extender)

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

c. Only the IP Camera is connected to the internet.

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

II. Configuration 2:



a. Internet Access: NV-202 and NV-202P(Ethernet Extender)

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

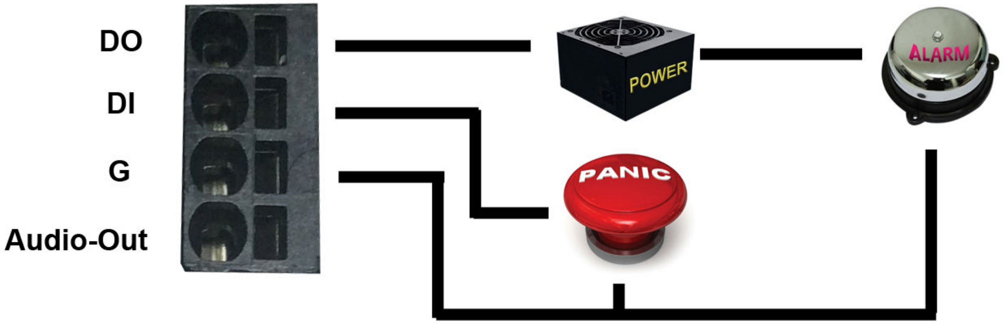
c. IP Camera and PC connect to the internet

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

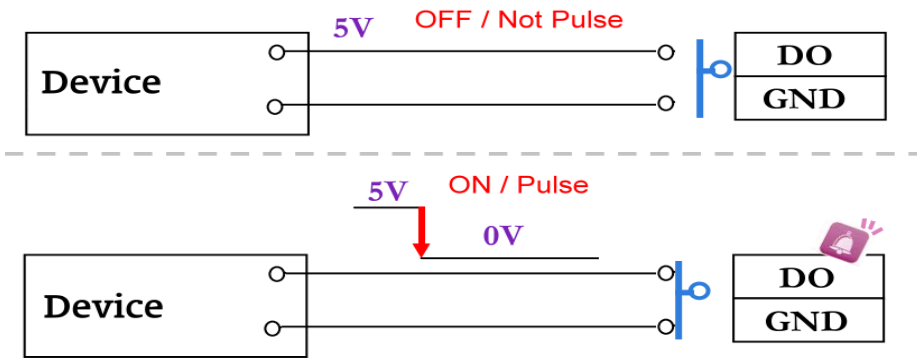
Chapter 7. I/O Configuration

1. I/O Connection

a. Connect the **G (GND)** & **DO** pin to the external relay (buzzer) device.
b. Connect the **G (GND)** & **DI** pin to the external trigger device.

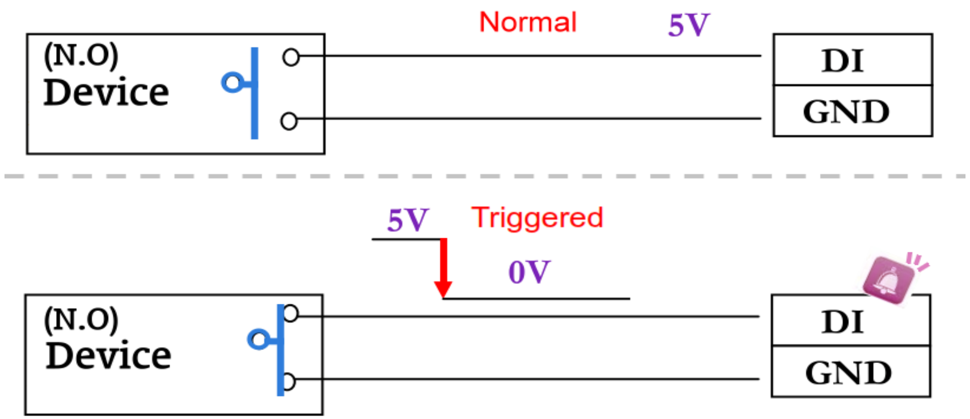


When no event occurs, the DO output is 5V (DO and GND are disconnected). When the camera detects events it will trigger and external alarm, DO output is 0V (DO and GND are connected).



If you select **N.O** on **Input sensor setting**, when the switch contacts are opened, the camera input alarm will be triggered and will execute the action user has set, for example, send a snapshot to E-mail address.

If you select **N.C** in **Input sensor setting**, when the switch contacts are closed, the camera input alarm will be triggered and will execute the action user has set, for example, send a snapshot to E-mail address.

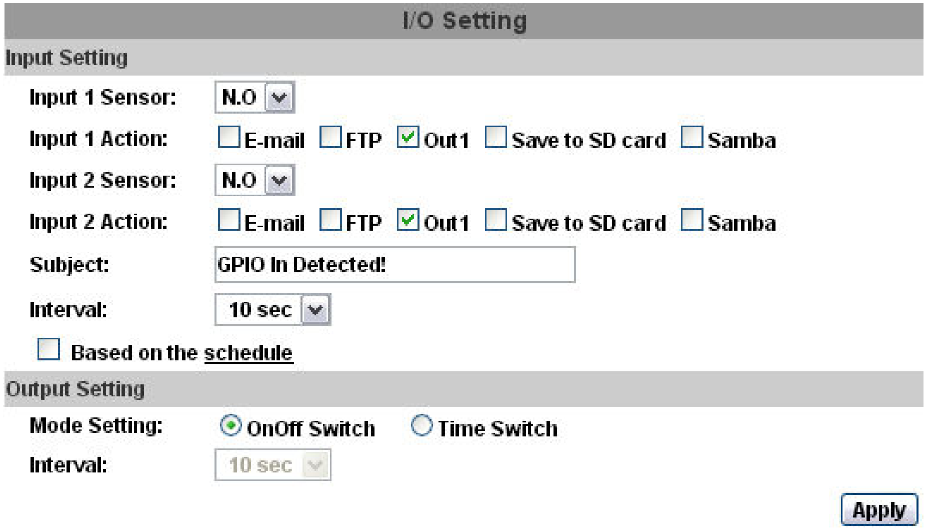


c. I/O PIN definition

- **GND (Ground):** Initial state is LOW
- **DO (Digital Output):** DC 5V
- **DI (Digital Input):** Max. 50mA, DC 5V

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

Input 2 Sensor: N.O

Input 2 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

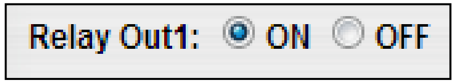
Interval: 10 sec

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:

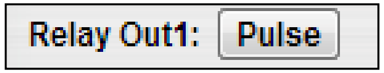
Clicking **ON** will trigger the external output device for 10 seconds. For example, your alarm buzzer will continuously ring for 10 seconds. After 10 seconds the buzzer stops ringing, or you can manually break off the output signal by clicking **OFF**



Relay Out1: ● 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.

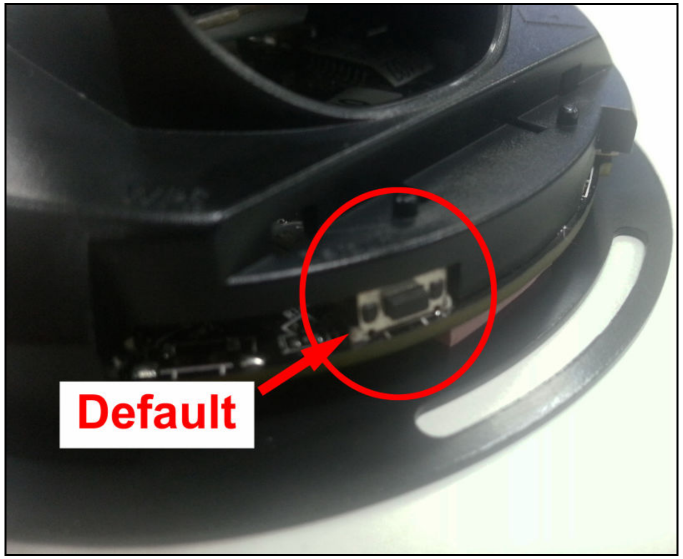


Relay Out1:

Chapter 8. Factory Default

If you forget your password, please follow the steps to set back the IP Camera to its factory default state.

- Remove the power and Ethernet cable. Open the dome and press and hold the button as shown in the picture below.



- Connect the power back to the camera, and do not release the button during the system booting. It will take around 30 seconds to boot the camera.

- Release the button when the camera finishes booting.

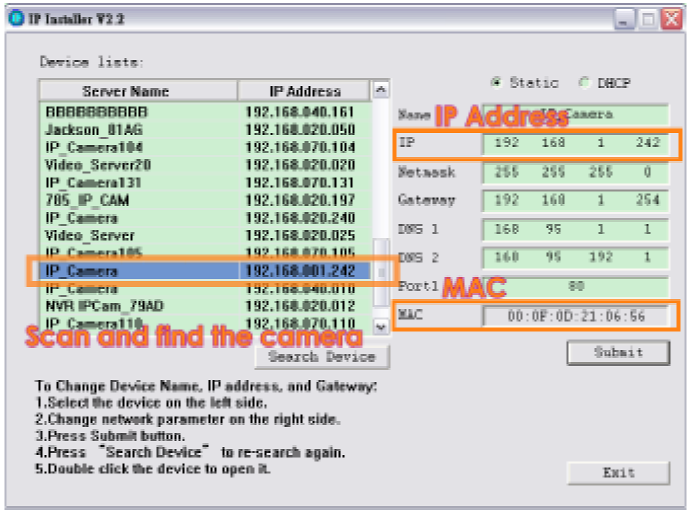
- Plug-in the Ethernet cable. Re-login the camera using the default IP (**http://192.168.1.200**), and user name: **admin**, password: **admin**.

Chapter 9. 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.**

Step1 First, you need to know the IP address and MAC address of your IP camera. You can use **IP installer** to scan the LAN, and see the IP address and MAC address on the side column.



Device lists:

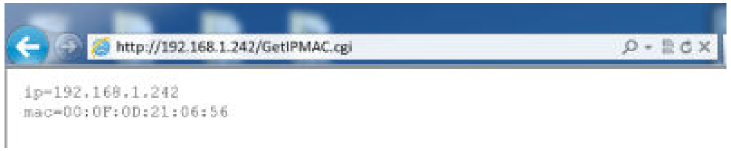
Server Name	IP Address
BBBBBBBBBBB	192.168.040.161
Jackson_01AG	192.168.020.050
IP_Camera104	192.168.070.104
Video_Server20	192.168.020.020
IP_Camera131	192.168.070.131
705_IP_CAM	192.168.020.197
IP_Camera	192.168.020.240
Video_Server	192.168.020.025
IP_Camera105	192.168.070.105
IP_Camera	192.168.001.242
IP_Camera	192.168.040.010
NVR IPCam_79AD	192.168.020.012
IP_Camera110	192.168.070.110

● Static ○ DHCP

Name: IP_Camera
IP: 192 168 1 242
Netmask: 255 255 255 0
Gateway: 192 168 1 254
DNS 1: 168 95 1 1
DNS 2: 168 95 192 1
Port1: 80
MAC: 00:0F:0D:21:06:56

To Change Device Name, IP address, and Gateway:
1.Select the device on the left side.
2.Change network parameter on the right side.
3.Press Submit button.
4.Press "Search Device" to re-search again.
5.Double click the device to open it.

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 address will be displayed on browser.



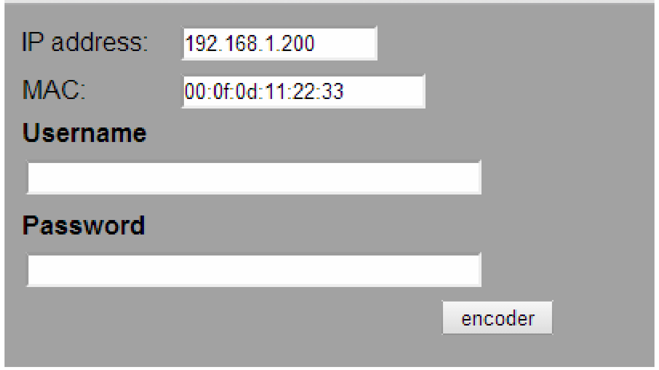
http://192.168.1.242/GetIPMAC.cgi

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

Step2 Find the .html file named **Universal Password** in CD-ROM. Click to open it.

Universal Password_V1.1
Chrome HTML Document
10 KB

Step3 Key in the camera IP address **IP Address** column and MAC address in **MAC** column, and then click **encoder**, a set of username and password will appear, as shown in the picture below:



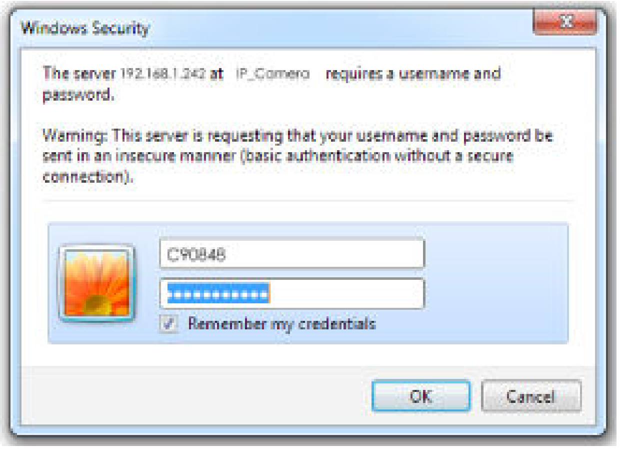
IP address:	192.168.1.200
MAC:	00:0f:0d:11:22:33

Username

Password

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

Step4 Take the generated username and password. Use them to log into the camera.



Windows Security

The server 192.168.1.242 at IP_Camera requires a username and password.

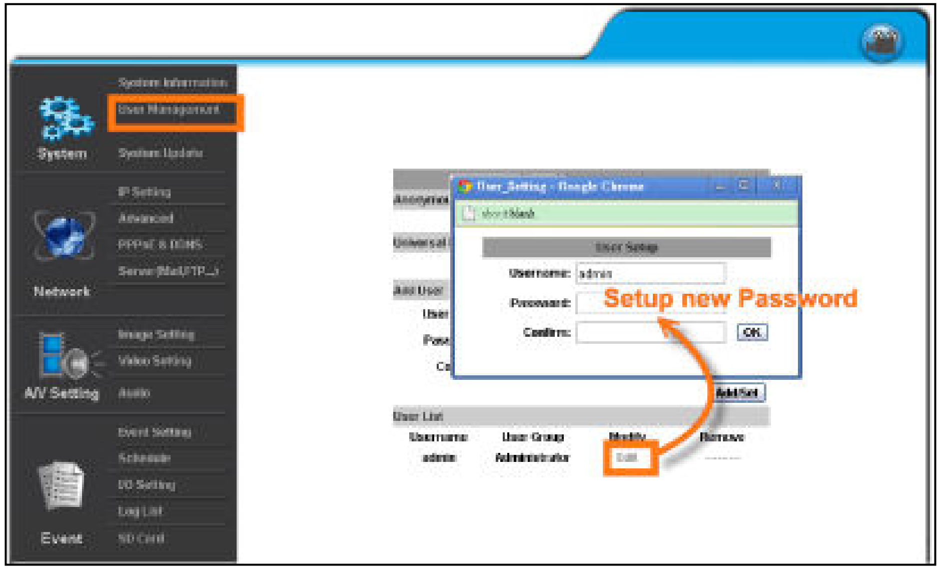
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

C90848

●●●●●●●●●●●●

☑ Remember my credentials

Step5 Now you can login 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	------

Appendix A. Micro SD Card Compatibility (Optional)

The following are the recommended Micro SD Cards:

Transcend	SDHC	class4	16GB
	SDHC	class4	32GB
	SD	class4	16GB
	SD	class4	32GB
	SDHC	class6	4GB
	SDHC	class6	8GB
	SDHC	class6	16GB
	SD	class6	4GB
	SD	class6	8GB
	SD	class6	16GB
SanDisk	SDHC	class4	4GB
	SDHC	class4	8GB
	SDHC	class4	16GB

Appendix B: Compliance Information

FCC Radio Frequency Interference Statement

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

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. The equipment and the receiver should be connected to outlets on separate circuits.
4. Consult the dealer or an experienced radio/television technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

If this telephone equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance in order for you to make necessary modifications to maintain uninterrupted service.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

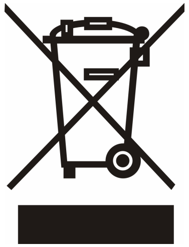
FCC Warning

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment can generate, use, and radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at owner's expense.

CE Mark Warning

In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Warranty

The original product that the owner delivered in this package will be free from defects in material and workmanship for one year parts after purchase.

There will be a minimal charge to replace consumable components, such as fuses, power transformers, and mechanical cooling devices. The warranty will not apply to any products which have been subjected to any misuse, neglect or accidental damage, or which contain defects which are in any way attributable to improper installation or to alteration or repairs made or performed by any person not under control of the original owner.

The above warranty is in lieu of any other warranty, whether express, implied, or statutory, including but not limited to any warranty of merchantability, fitness for a particular purpose or any warranty arising out of any proposal, specification or sample. We shall not be liable for incidental or consequential damages. We neither assume nor authorize any person to assume for it any other liability.

Chinese SJ/T 11364-2014

部件名称	有毒有害物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬[Cr(VI)]	多溴联苯(PBB)	多溴二苯醚(PBDE)
结构壳体	○	○	○	○	○	○
电路组	○	○	○	○	○	○
电源供应器	○	○	○	○	○	○
线材	○	○	○	○	○	○
包装及配件	○	○	○	○	○	○

○：表示该有毒物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。

╳：表示该有毒物质至少在该部件的某依均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

上述规范仅适用於中国法律