

User's Manual



Full HD Outdoor IR Wireless IP Camera

▶ ICA-W3250V



Copyright

Copyright © 2015 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a 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. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance, for example, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it.

However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

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

WEEE Regulation



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; they should be collected separately.

Revision

User's Manual of PLANET Full HD Outdoor IR PoE IP Camera
Model: ICA-W3250V
Rev: 1.00 (January, 2015)
Part No. EM-ICA-W3250V_v1.0

Table of Contents

Chapter 1. Product Introduction	6
1.1 Package Contents.....	6
1.2 Overview.....	6
1.3 Features.....	8
1.4 Product Specifications.....	9
Chapter 2. Hardware Interface.....	12
2.1 Physical Descriptions.....	12
2.1.1 Identification of ICA-W3250V cable	12
2.1.2 I/O Control Instruction.....	13
2.2 Hardware Installation	13
2.3 Initial Utility Installation.....	16
2.4 Using UPnP of Windows XP or 7	18
2.4.1 Windows XP	18
2.4.2 Windows 7	22
2.5 Setting up ActiveX to use the Internet Camera	23
2.5.1 Internet Explorer 6 for Windows XP	23
2.5.2 Internet Explorer 7 for Windows XP.....	24
2.5.3 Internet Explorer 7 for Windows Vista.....	25
Chapter 3. Web-based Management.....	27
3.1. Introduction	27
3.2. Connecting to Internet Camera.....	27
3.3 Live Viewing.....	29
3.4 Configuration	31
3.5 System.....	31
3.5.1 System Information.....	32
3.5.2 User Management	33
3.5.3 System Update	34
3.6 Network.....	35
3.6.1 IP Setting	35
3.6.2 Advanced	38
3.6.3 PPPoE & DDNS.....	43
3.6.4 Mail & FTP & SAMBA	45
3.6.5 Wireless Setting.....	47
3.7 A/V Setting	49
3.7.1 Image Setting.....	50
3.7.2 Video Setting	51
3.7.3 Audio Setting	53
3.8 Event List.....	54
3.8.1 Event Setting	55
3.8.2 Schedule.....	57
3.8.3 I/O Setting.....	58
3.8.4 Log List.....	59
3.8.5 SD card.....	59
Appendix A. Factory Default.....	62
Appendix B. Ping IP Address.....	63
Appendix C. 3GPP Access	64
Appendix D. Planet DDNS Application.....	65
Appendix E. Configuring Port Forwarding Manually	66

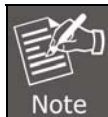
Appendix F. Troubleshooting & Frequently Asked Questions.....	68
Appendix G. Micro SD Card Compatibility	72

Chapter 1. Product Introduction

1.1 Package Contents

The package should contain the following items:

- Camera Unit x 1
- Power Adapter x 1
- User's Manual CD x 1
- Quick Installation Guide x 1
- Screw Package x 1
- Rubber Cover x 1
- Antenna x 1
- RJ45 Female to Female Connector x 1



1. If any of the above items are missing, please contact your dealer immediately.
2. Using the power supply that is not the one included in the Internet Camera packet will cause damage and void the warranty for this product.

1.2 Overview

Superb Full HD Outdoor Surveillance

PLANET ICA-W3250V IP Camera with IR Illuminator provides high-resolution images for the round-the-clock surveillance over IP networks. It supports H.264, and JPEG compression formats and delivers excellent picture quality in Full HD resolutions at 30 frames per second (fps). It is also equipped with a mounting bracket that conceals all cables within for easy management and waterproof purposes. The ICA-W3250V is an ideal solution for outdoor surveillance applications such as buildings, roads, parking areas, garages, railway stations and airports.

Full HD Resolution



Suitable for Various Applications

To adapt to different environments, the ICA-W3250V comes with corridor mode, which enables the camera to change video frame from horizontal to vertical, i.e. from 16:9 to 9:16. Corridor mode will maximize video surveillance in narrow situations. It also creates a perfect, high-quality vertical video when the ICA-W3250V is installed at hotel, hospital, roads, tunnels, and many other applications.



Normal Mode



Corridor Mode

Exceptional Image Quality with Vari-focal Lens

With 3-10.5mm vari-focal lens, the ICA-W3250V meets various demands of installation. For instance, traffic monitoring can be focused either on more than two lanes or just one specified lane, It brings an extremely clear and exquisite picture quality.



Advanced Event Management

The ICA-W3250V supports a number of advanced features to enhance surveillance flexibility and event management capabilities. The advanced features include auto-iris for improving the image quality to avoid overexposure, audio in/out interface for two-way audio function, and digital input/output for connecting to external devices such as door sensors and relays to activate light or close doors.

2-way Audio



Flexible Installation with 11n Wireless Connectivity

The ICA-W3250V adopts IEEE 802.11n wireless technology to communicate at up to 150Mbps wireless signal rate and ensures secure transmission with WEP and WPA encryptions. The wireless N functionality enables rapid integration into the wireless network and offers a flexible choice of the site.

Furthermore, the IP66-rated housing protects the ICA-W3250V against rain and dust and ensures stable operation under extreme weather conditions. The ICA-W3250V is indisputably the top choice for reliable and high-performance surveillance.



1.3 Features

➤ Camera

- 1/2.7" 2MP progressive scan CMOS sensor
- 3~10.5 mm vari-focal, DC auto-iris lens
- Minimum illumination at F1.2, 0.01 lux

- Maximum resolution 1920 x 1080
- Removable IR-cut filter for day & night function

➤ **Video / Audio**

- H.264 and M-JPEG video compression simultaneously
- Simultaneous multi-stream support
- H.264 high profile, main profile and baseline
- Up to 30fps for all resolutions
- 3DNR to improve picture quality at low lux
- WDR enhancement function strengthens visibility under extremely bright or dark environments
- Two-way audio support with enhanced audio quality
- Change video field to vertical in corridor mode
- Colorful video in dark conditions
- Anti fog and lens distortion correction

➤ **Network and Configuration**

- IEEE 802.11n wireless LAN capability
- Auto MDI/MDI-X supported
- Supports both IPv6 and IPv4 protocols
- RTSP / UPnP / 3GPP / HTTPS protocols selectable

➤ **Easy Installation & Management**

- ONVIF compliant for interoperability
- Built-in 35 IR Illuminators, effective up to 25 meters
- IP66 outdoor classifications with cable management bracket for rigorous environment
- Built-in Samba client for NAS
- 3GPP for 3G mobile remote applications
- Save files to SD card once network connection is lost
- Digital Input/Output for integration with sensors and alarms
- PLANET Smart Discovery Lite, Cam Viewer 3 central management software supported

1.4 Product Specifications

Model	ICA-W3250V
Camera	
Image Device	1/2.7" 2mega-pixel CMOS sensor
Effective Pixels	1920 x 1080@30fps
Sensitivity	Color: 0.05 lux (AGC ON) B / W: 0.01 lux (AGC ON)
Lens	3~10.5mm vari-focal lens with auto iris and IR-cut filter / F1.4
View Angle	H: 34.89~106.72 degrees V: 19.38~61.26 degrees

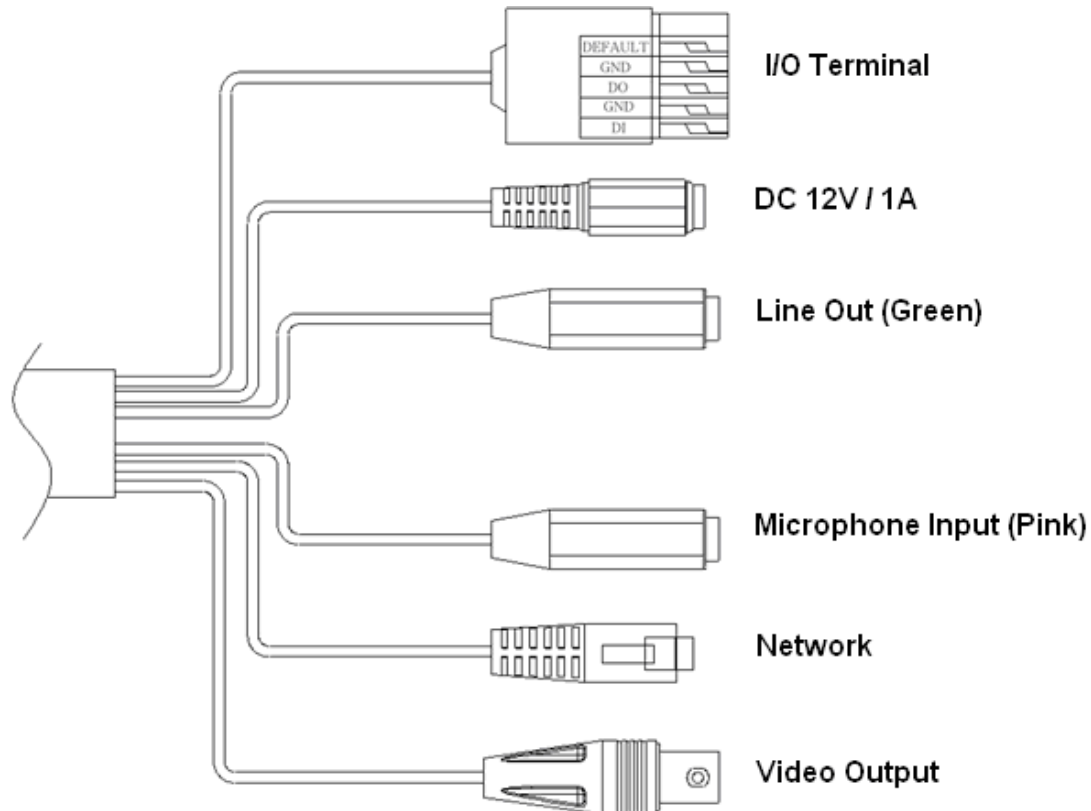
Video	
Video Encoder	H.264 and Motion JPEG simultaneously
Video Profile	- H.264 1080P / 720P / VGA / QVGA / QCIF - JPEG 1080P / 720P / VGA / QVGA / QCIF - 3GPP VGA / QVGA / QCIF
Frame Rate	HD-1080p / 720p / VGA / QVGA / QCIF up to 30fps
Image Setting	Brightness, Contrast, Hue, Saturation, Sharpness, AGC, Shutter Time, Sense-Up, WDR, Anti Fog, Lens Distortion Correction, Flip, Mirror, Noise Reduction, White Balance, Day & Night adjustable
Streaming	Simultaneous multi-profile streaming M-JPEG streaming over HTTP Supports 3GPP mobile surveillance Controllable frame rate and bandwidth Constant and variable bit rate (H.264)
Audio	
Audio Encoder	RTSP: G.711 / G.726
Audio Streaming	Two-way
Microphone	Phone jack
Audio Output	Phone jack
Network and Configuration	
Network Standard	IEEE 802.3 / IEEE 802.3u
Supported Protocols	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, SMTP, FTP, NTP, DNS, PLANET DDNS/ PLANET Easy DDNS, 802.1X, SNMP, DHCP, UPnP, RTSP, RTP, RTCP, PPPoE, 3GPP, ICMP
Security	Password protection, user access log, https
Users	10 simultaneous unicast users
Ethernet	10/100Mbps auto negotiation
Antenna	5dBi Dipole Antenna
Antenna Connector	RP-SMA Female
Frequency	2.4GHz
Wireless Channels	America / FCC: 2.414~2.462GHz (11 Channels) Europe / ETSI: 2.412~2.472GHz (13 Channels) Japan / TELEC: 2.412~2.484GHz (14 Channels)
RF Transmit Power	OFDM: 15 dBm CCK: 17 dBm
Output Power	802.11n: 14dBm (default) +/- 1dBm 802.11g: 14dBm (default) +/- 1dBm 802.11b: 17dBm (default) +/- 1dBm
Receiver Sensitivity	11b→1M: -83 11M: -76 11g→6M: -82 54M: -65 11n (BW20)→MCS0: -82 MCS7: -65 11n (BW40)→MCS0: -79 MCS7: -61

Data Rate	IEEE 802.11b Standard Data Rates: 1, 2, 5.5 and 11Mbps IEEE 802.11g Standard Data Rates: 6, 9, 12, 18, 24, 36, 48, 54Mbps IEEE 802.11n Standard Data Rates: Legacy and High Throughput Modes, supporting 20 / 40MHz Bandwidth MCS0~7 (150Mbps PHY Rate Rate)
Wireless Security	WEP, WPA-PSK and WPA2-PSK encryptions
System Integration	
Application Programming Interface	Open API for software integration SDK ONVIF compliant
Alarm Triggering	Intelligent video motion detection and external input
Motion Detection	3-zone video motion detection
Alarm Events	File upload via FTP, email and SAMBA. External output activation Configurable pre/post alarm buffering
Video Buffer	Pre-5sec and post-10 sec alarm buffering
General	
Power Supply	12V DC external power adapter
PoE Consumption	12V DC: 4W (IR Off); 8W (IR On)
Illumination LED	IR LEDs
IR LED	Infrared LED × 35pcs
IR Wavelength	850nm
IR Distance	25m
Protection Class	IP-66 classification
Operating Temperature	-10 ~ 50 degrees C
Viewing System	
OS	Windows® XP, Vista 32bit, Win7 32bit, Server 2003
Browser	IE 8.0 or later
Cell Phone	With 3GPP player
Video Player	VLC, Quick Time, Real Player
Software	
Monitor / Recording / Management	PLANET CV3P (2-ch Cam Viewer Three Pro Trial Version) PLANET CV3L (64-ch Cam Viewer Three Lite Bundled Version)
Search & Installation	PLANET Smart Discovery Lite

Chapter 2. Hardware Interface

2.1 Physical Descriptions

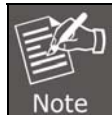
2.1.1 Identification of ICA-W3250V cable



1. RJ45 LAN socket: Connect to PC or Hub/Switch.

Connected to 10BASE-T Ethernet or 100Base-TX Fast Ethernet cabling, the ICA-W3250V with the Ethernet port built N-way protocol can detect or negotiate the transmission speed of the network automatically. Please use CAT-5 cable to connect the Network Camera to a 100Mbps Fast Ethernet network switch or hub.

2. Power Jack: The input power is DC 12V.



ONLY use package power adapter supplied with the Internet. Otherwise, the product may be damaged.

3. I/O Control Instruction

The I/O terminal connector is used for such applications as motion detection, event triggering, and alarm notification.

4. Video Output

The internet camera also provides composite video output. User can use BNC video cable to connect the internet camera with a TV monitor or VCR.

5. Microphone in (audio in)

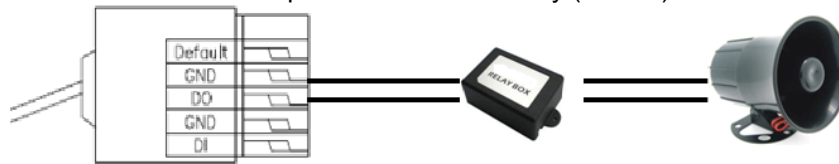
Connect a microphone to the network camera.

6. Line out (audio out)

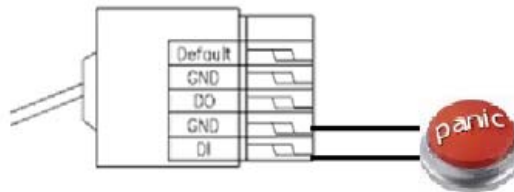
Connect a loud speaker to the network camera. This is for voice alert and two-way audio.

2.1.2 I/O Control Instruction

1) Please connect the GND and DO pin to the external relay (buzzer) device.



2) Please connect the GND and DI pin to the external trigger device.



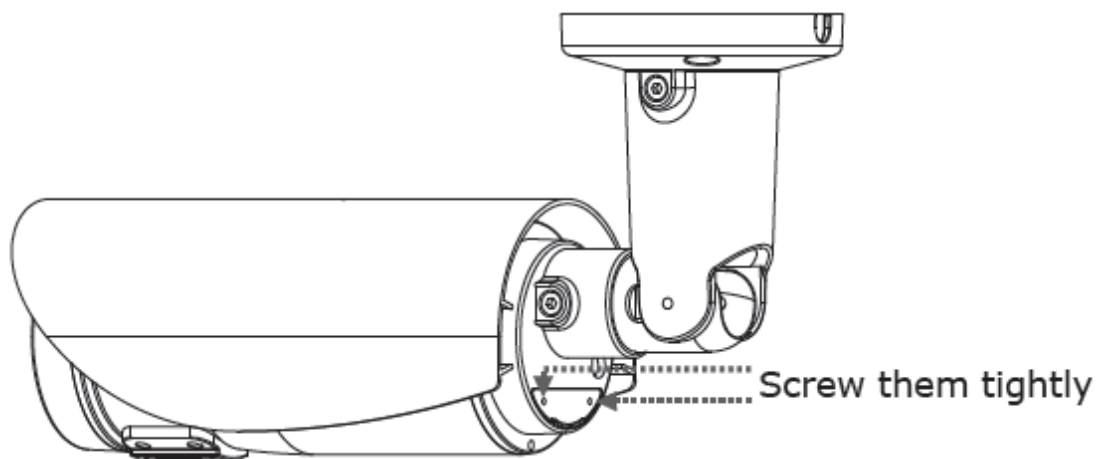
3) I/O Pin definition


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

2.2 Hardware Installation

1. Inserting Micro SD Card (optional)

If user needs to save video to SD card, please remove the micro SD card lid and insert your SD card. Then turn and lock the screws on the micro SD card lid tightly and make sure it's sealed.

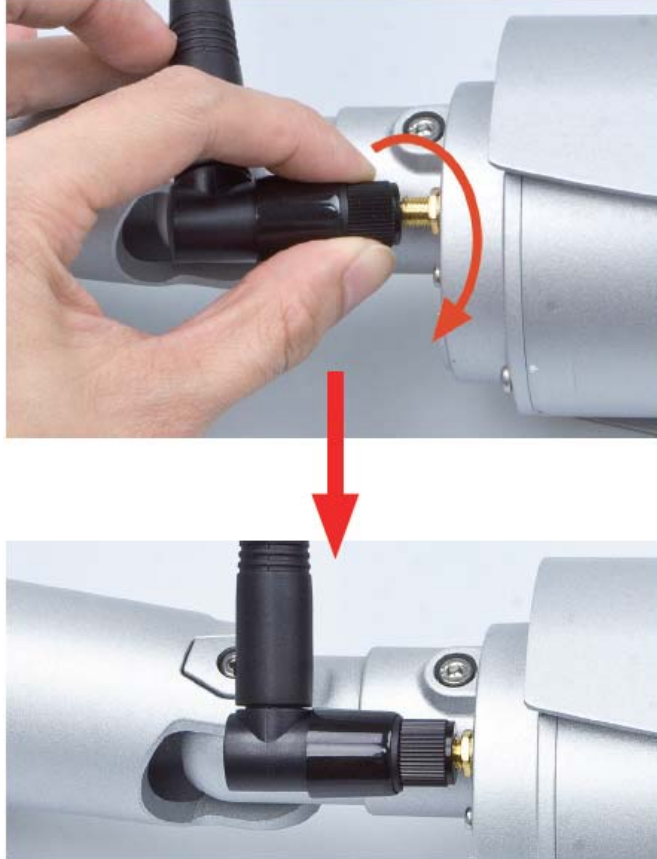


- | | |
|---|---|
| 
Note | <ol style="list-style-type: none"> 1. Please power off the device and then insert or remove the micro SD/SDHC card. 2. Please refer to Appendix G: Micro SD Card Compatibility to select your micro SD/SDHC card. 3. Be aware the waterproof rubber, improper placement or missing the rubber will cause seal malfunction. |
|---|---|

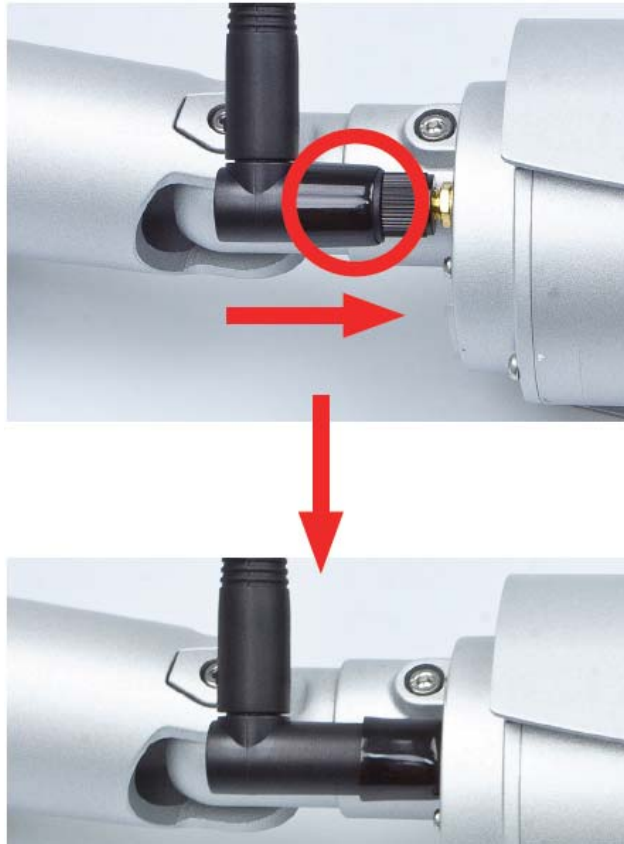
2. Installing the antenna

- a. Plug the antenna into the connector. Turn the lock nut to the right until it is totally locked.

Do not bend or try to straighten the antenna bar.



- b. Push the Rubber Cover until it totally covers the antenna connector. It certainly help to prevent water from seeping into the antenna.



3. Connecting an Ethernet cable

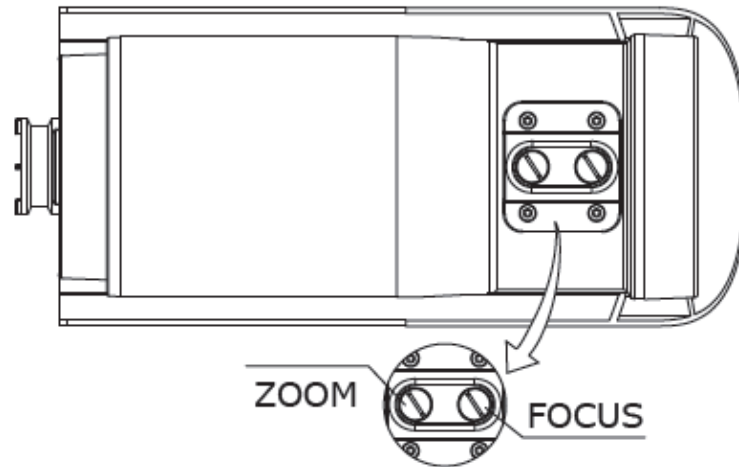
Connect the LAN cable on the camera to the network device (hub or switch).

4. Attaching BNC connector (optional)

Connect the video BNC connector to a monitor set if necessary. It is helpful to check camera viewing angle and focus.

5. Adjusting zoom and focus (optional)

This IP camera is equipped with an external vari-focal lens controller. Please adjust “ZOOM” and then FOCUS” as shown in the following picture until the image gets clear.




6. Attaching Speaker/microphone to camera (optional)

If user needs both video and audio streams, a speaker/ microphone should be attached to camera.

7. Attaching the power supply

Plug in power adapter and connect to power source. After power on, the camera will start to operate.

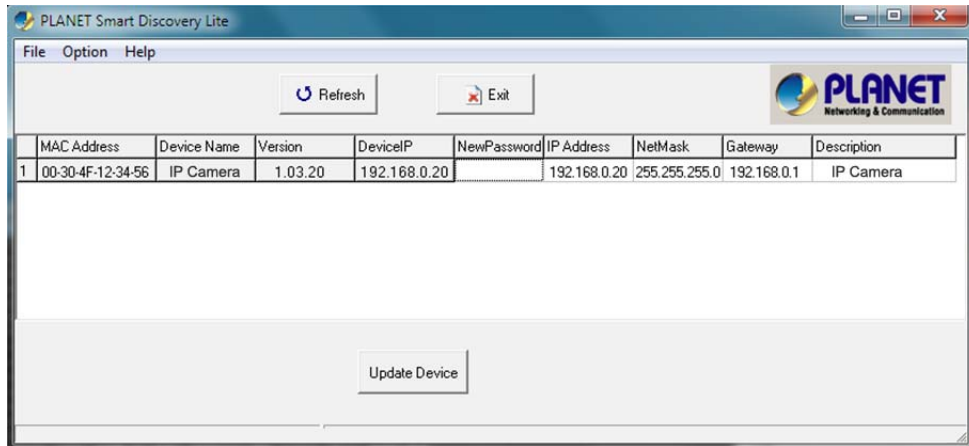
 Note	1. Only use the power adapter supplied with Internet camera. Otherwise, the product may be damaged.
---	---

2.3 Initial Utility Installation

This chapter shows how to quickly set up your H.264 camera. The camera is with the default settings. However, to help you find the networked camera quickly the windows utility PLANET Smart Discovery Lite can search the cameras in the network that will help you to configure some basic settings before you start advanced management and monitoring.

1. Insert the bundled CD into the CD-ROM drive to launch the auto-run program. Once completed, a welcome menu screen will appear.




- Click the “Utility” hyperlink; you will see the dialog box as shown below.



- OS: Windows XP SP2 or above. If the following “Windows Security Alert” pops up, please click “Unblock”.




- When you install the Internet Camera in a LAN environment, you may execute PLANET Smart Discovery Lite to discover the camera’s IP address and set up related parameters in the camera.

Item	Description
	Smart Discovery Lite will search all IP cameras connected to LAN. The user can click “ Refresh ” to search again.
	You can move your mouse to IP Address, NetMask and Gateway column to change parameters and then just click the “ Update Device ” button. Enter password to complete network configuration settings.
	Close Smart Discovery Lite.

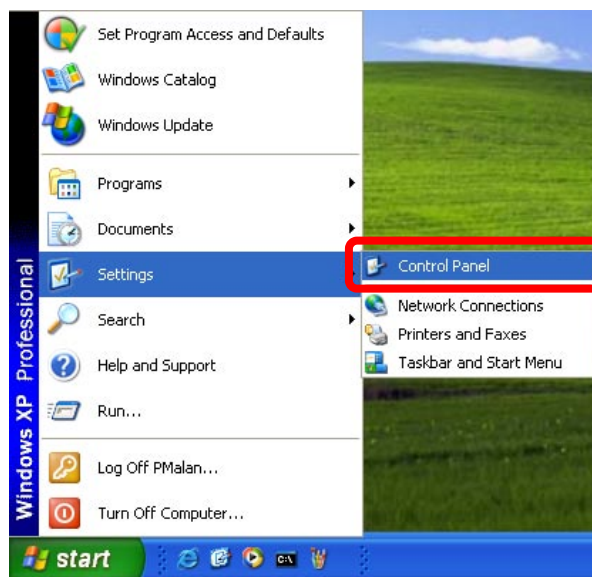
2.4 Using UPnP of Windows XP or 7

2.4.1 Windows XP

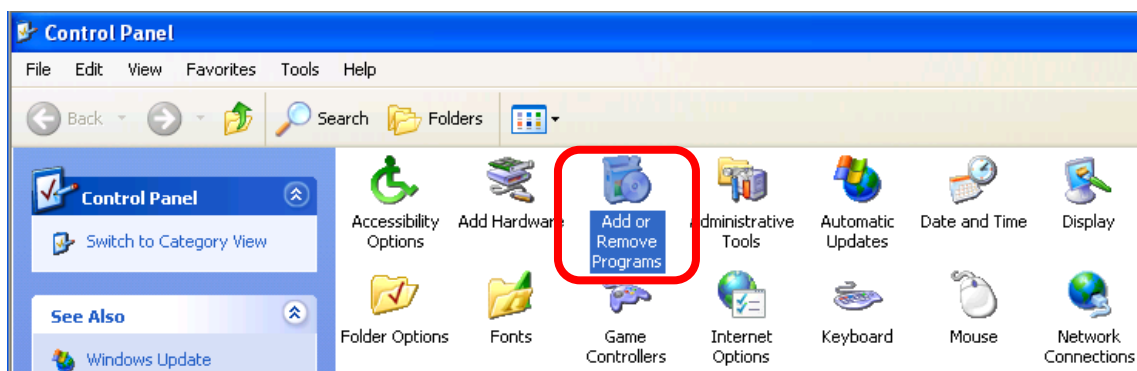
UPnP™ is short for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This device is an UPnP enabled device. If the operating system, Windows XP, of your PC is UPnP enabled, the device will be very easy to configure. Use the following steps to enable UPnP settings only if your operating system of PC is running Windows XP.

 Please note that MS Windows 2000 does not support UPnP feature.

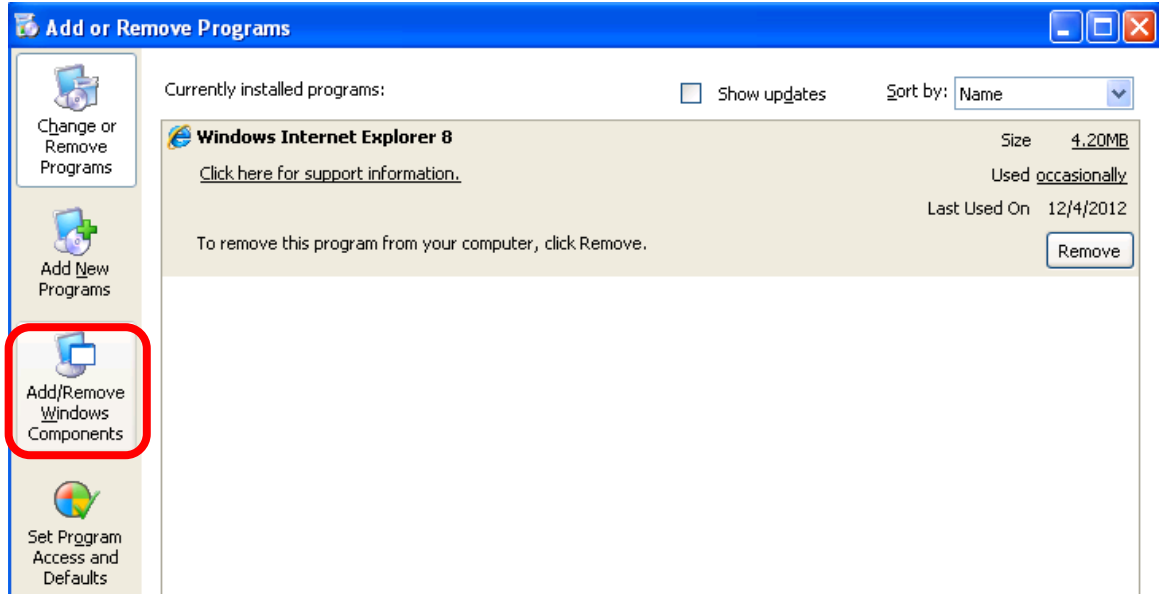
Go to **Start > Settings**, and click **Control Panel**.



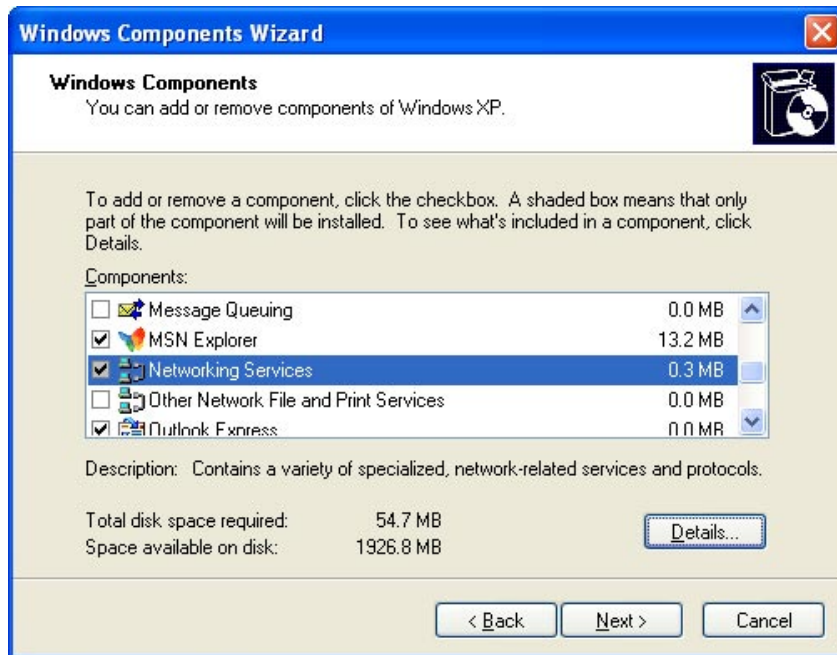
The **“Control Panel”** will display on the screen and double-click **“Add or Remove Programs”** to continue.



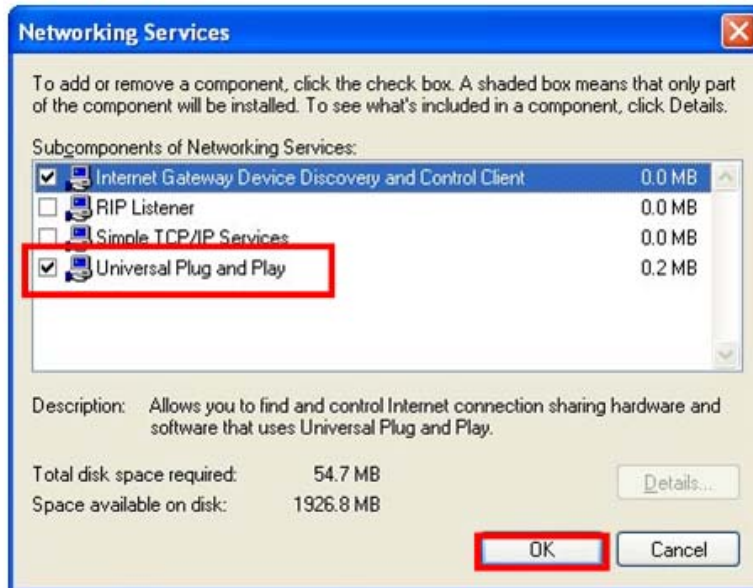
The “Add or Remove Programs” will display on the screen and click **Add/Remove Windows Components** to continue.



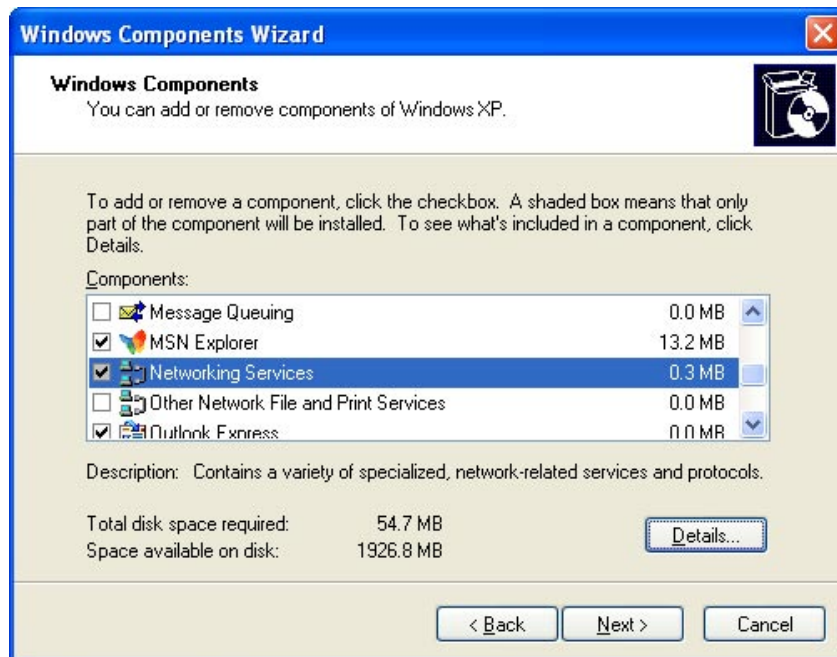
The following screen will appear. Select “**Networking Services**” and click “**Details**” to continue.



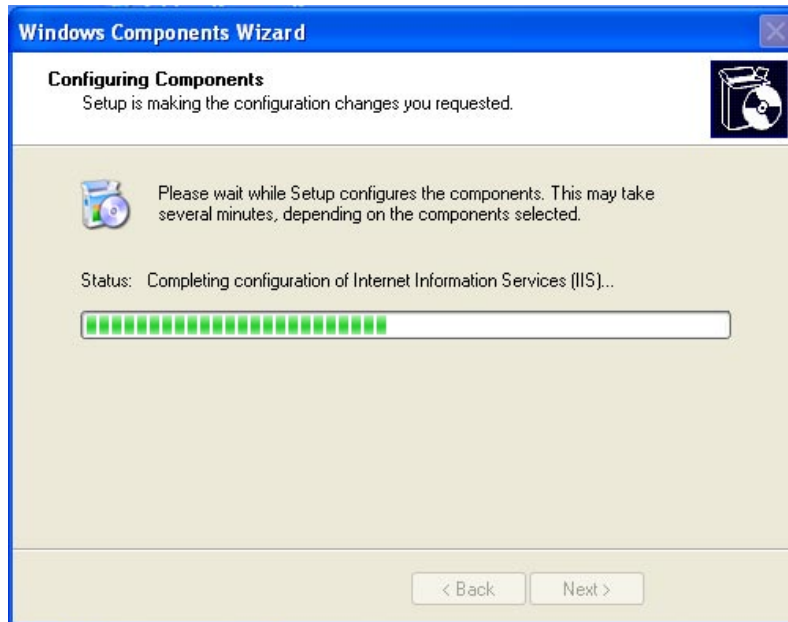
The “Networking Services” will display on the screen. Select “**Universal Plug and Play**” and click “**OK**” to continue.



Please click “**Next**” to continue.



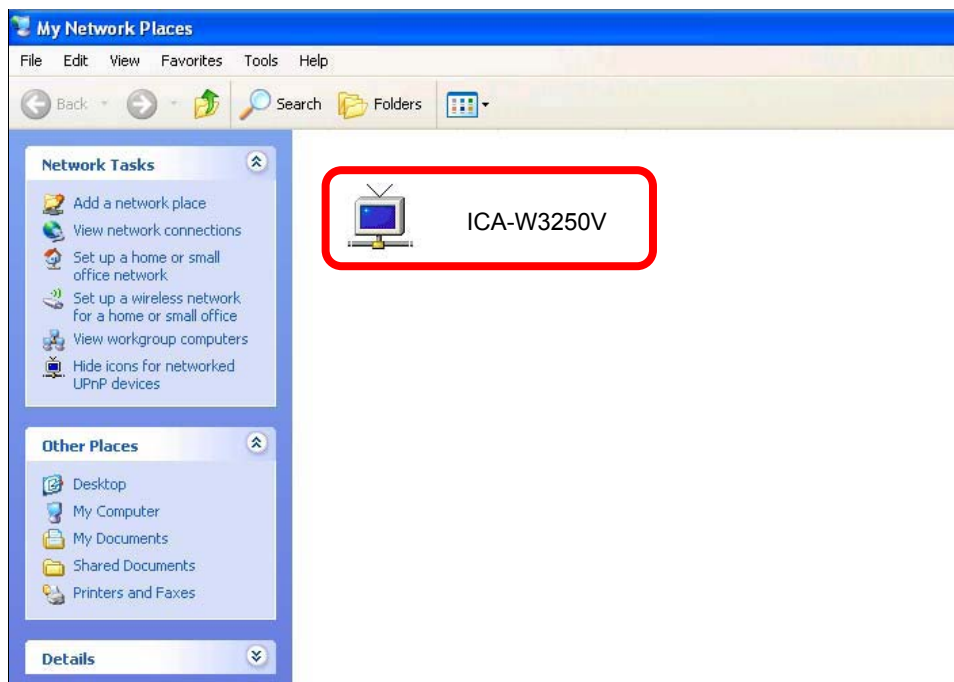
The program will start installing the UPnP automatically. You will see the pop-up screen below. Please wait while Setup configures the components.



Please click **Finish** to complete the UPnP installation.




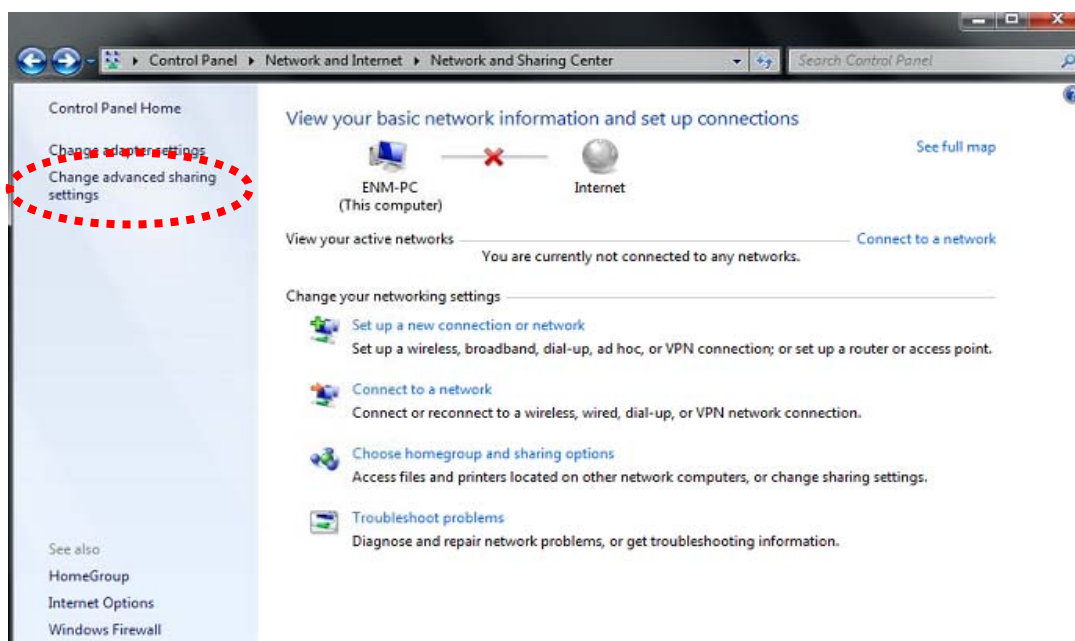
Double-click **"My Network Places"** on the desktop, and the "My Network Places" will display on the screen. Double-click the UPnP icon with Internet Camera to view your device in an internet browser.

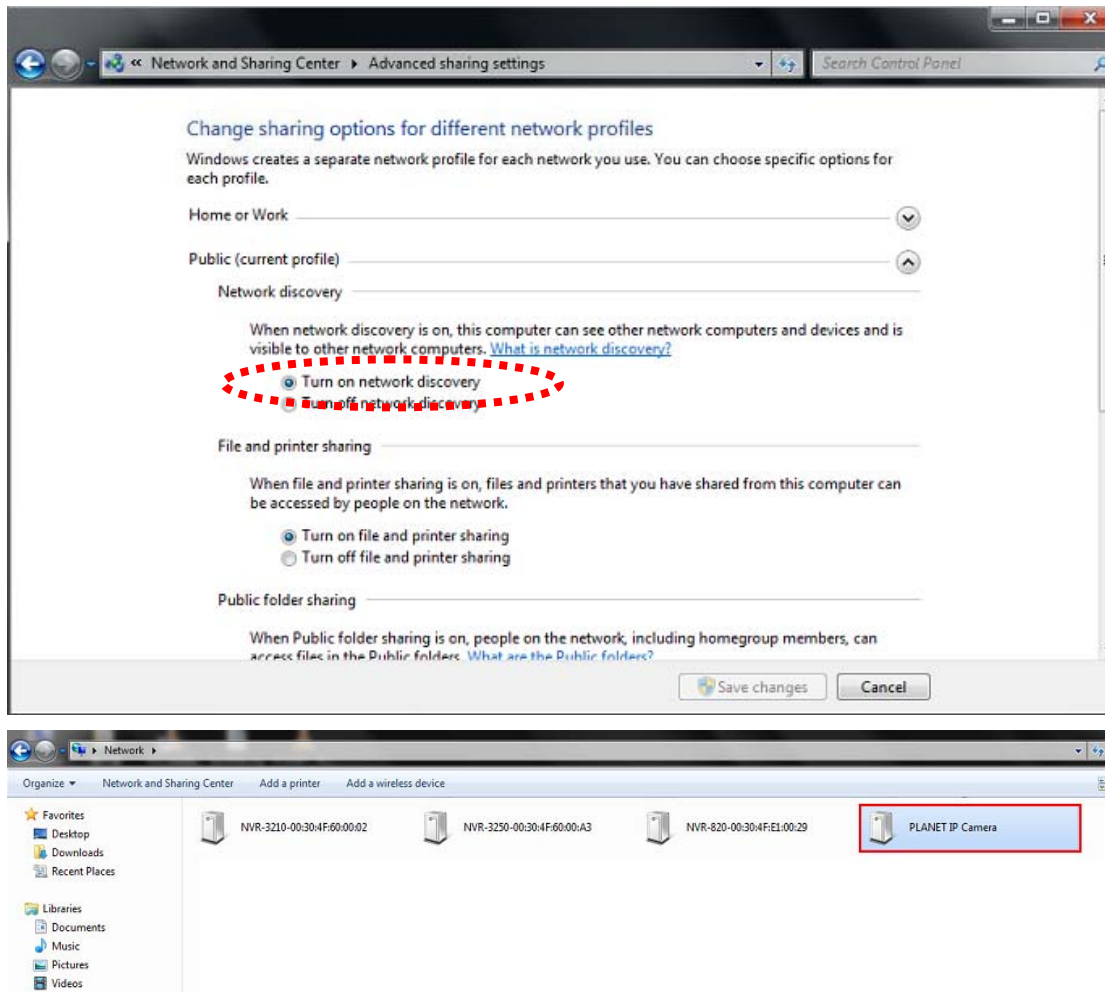


2.4.2 Windows 7

Go to **Start > Control Panel > Network and Internet > Network and Sharing Center**, if network discovery is off; click the arrow button  to expand the section.

Click Turn on network discovery, and then click Apply.  If you are prompted for an administrator password or confirmation, type the password or provide confirmation.





2.5 Setting up ActiveX to use the Internet Camera

The Internet Camera web pages communicate with the Internet Camera using an ActiveX control. The ActiveX control must be downloaded from the Internet Camera and installed on your PC. Your Internet Explorer security settings must allow for the web page to work correctly. To use the Internet Camera, user must set up his IE browser as follows:

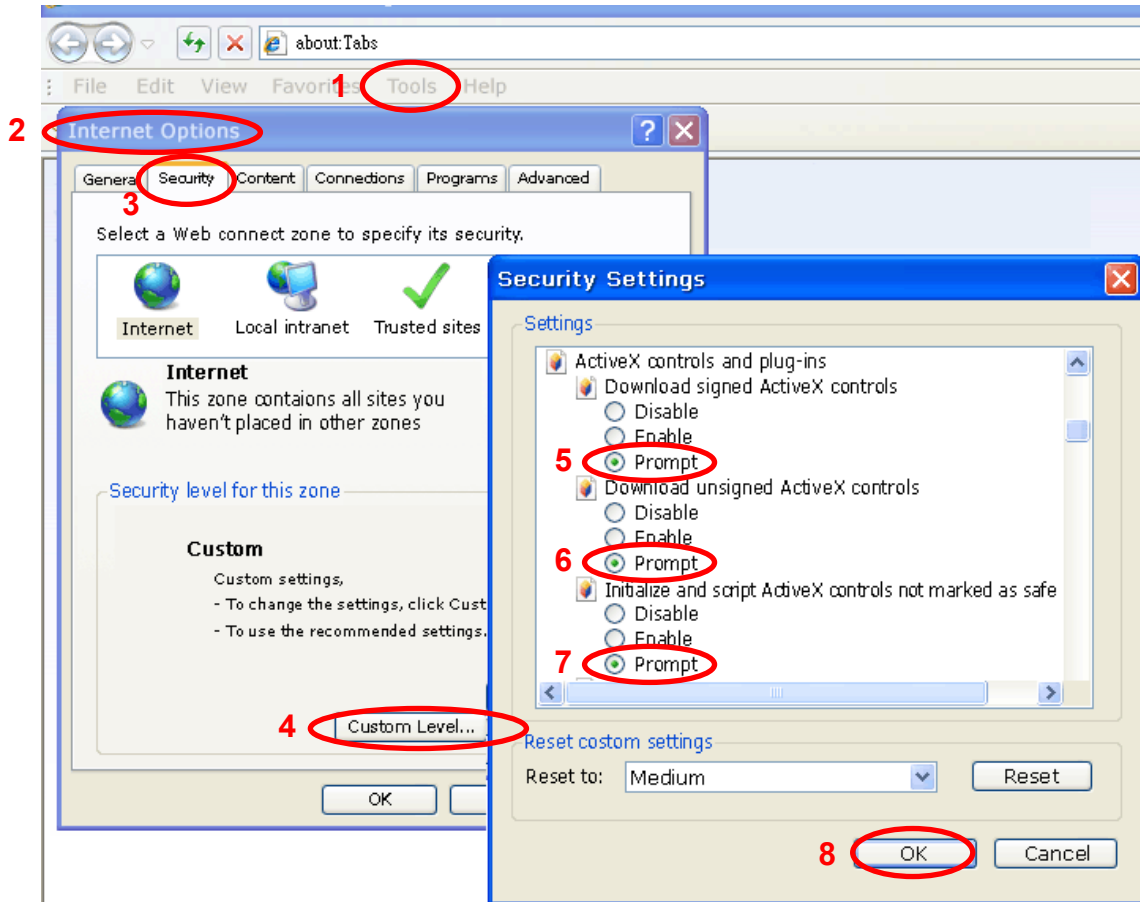
2.5.1 Internet Explorer 6 for Windows XP

From your IE browser → "Tools" → "Internet Options..." → "Security" → "Custom Level...", please set up your "Settings" as follows:

Set up the first 3 items

- Download the signed ActiveX controls
- Download the unsigned ActiveX controls

- Initialize and script the ActiveX controls not masked as safe to Prompt



By now, you have finished your entire PC configuration for Internet Camera.

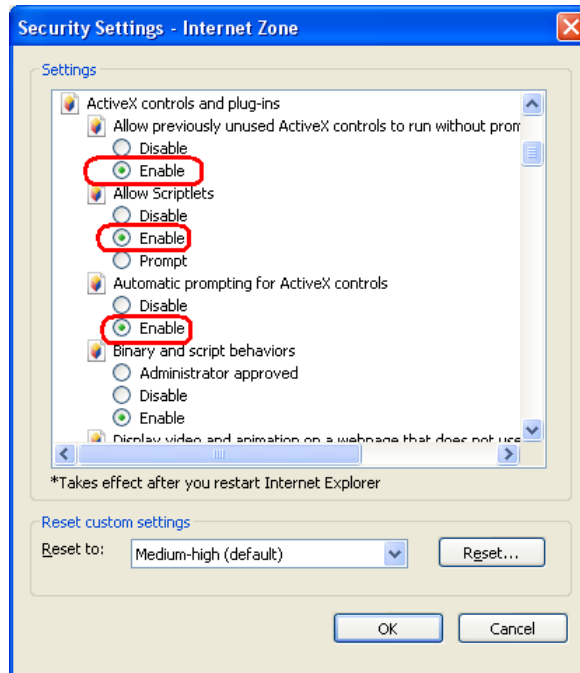
2.5.2 Internet Explorer 7 for Windows XP

From your IE browser → "Tools" → "Internet Options..." → "Security" → "Custom Level...", please set up your "Settings" as follows:

Set up the first 3 items

- Allow previously unused ActiveX control to run...
- Allows Scriptlets

- Automatic prompting for ActiveX controls

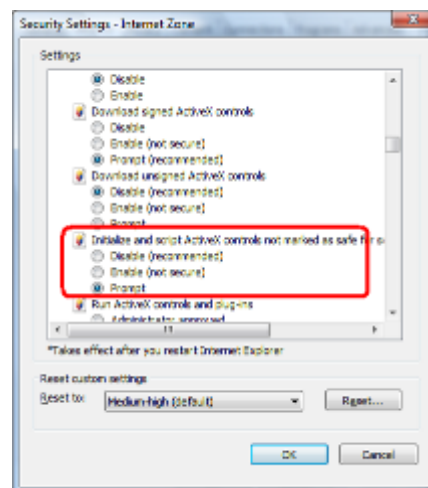
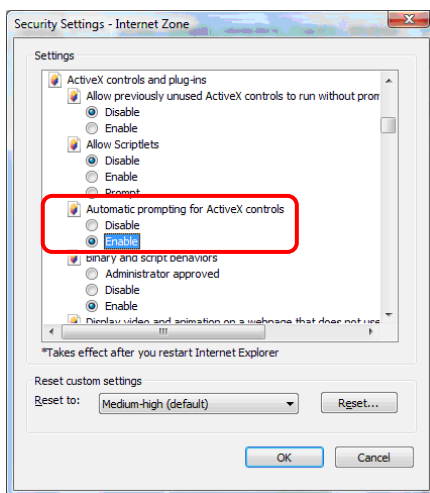


By now, you have finished your entire PC configuration for Internet Camera.

2.5.3 Internet Explorer 7 for Windows Vista

From your IE browser → "Tools" → "Internet Options..." → "Security" → "Internet" → "Custom Level...", please set up your "Settings" as follows:

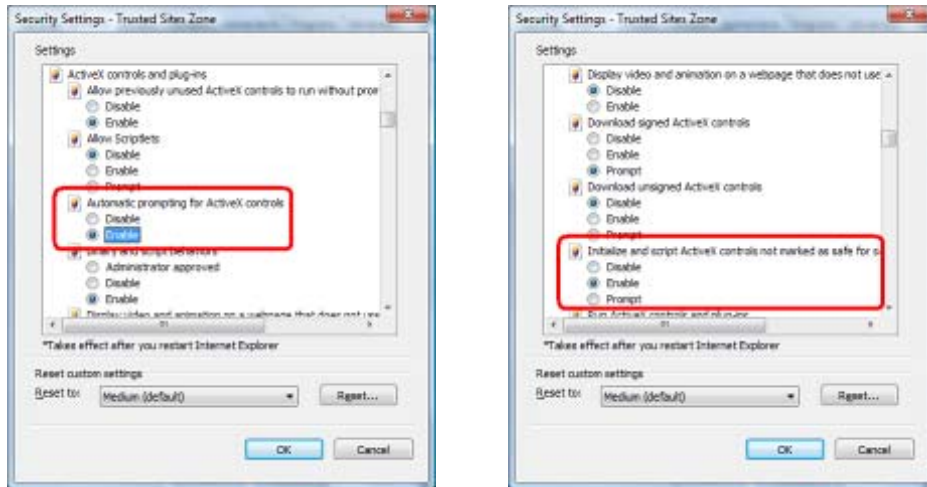
- Enable "Automatic prompting for ActiveX controls"
- Prompt "Initialize and script active controls not marked as safe for scripting"



From your IE browser → "Tools" → "Internet Options..." → "Security" → "Trusted Sites" → "Custom Level...", please set up your "Settings" as follows:

- Enable "Automatic prompting for ActiveX controls"

- Prompt “Initialize and script active controls not marked...”



By now, you have finished your entire PC configuration for Internet Camera.

Chapter 3. Web-based Management

This chapter provides setup details of the Internet Camera's Web-based Interface.

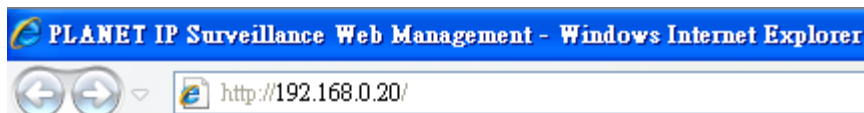
3.1. Introduction

The Internet Camera can be configured with your Web browser. Before configuring, please make sure your PC is under the same IP segment as Internet Camera.

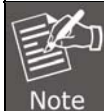
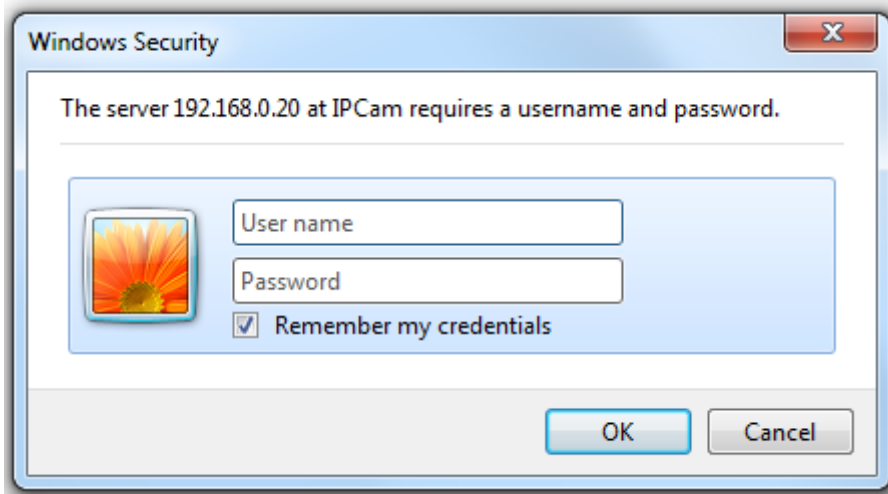
3.2. Connecting to Internet Camera

- A. Use the following procedures to establish a connection from your PC to the Internet Camera.
- B. Once connected, you can add the camera to your browser's Favorites or Bookmarks.

Start the web browser on the computer and type the IP address of the camera.
The default IP: "<http://192.168.0.20/>"

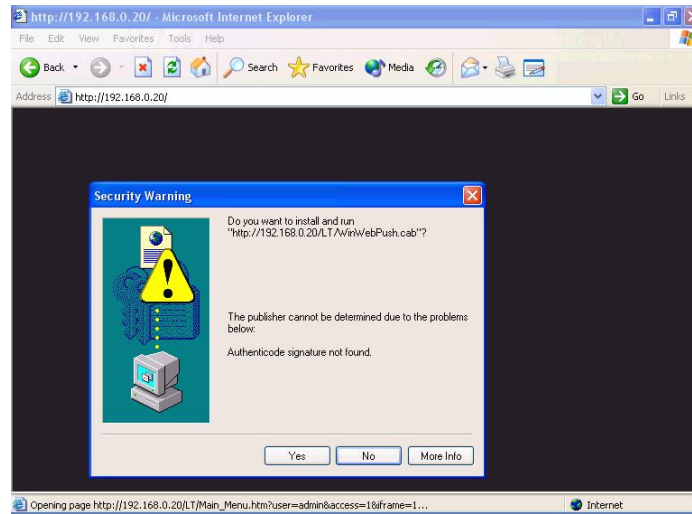


The login window of Internet Camera will appear,
Default login **username** and **password** are both **admin**.

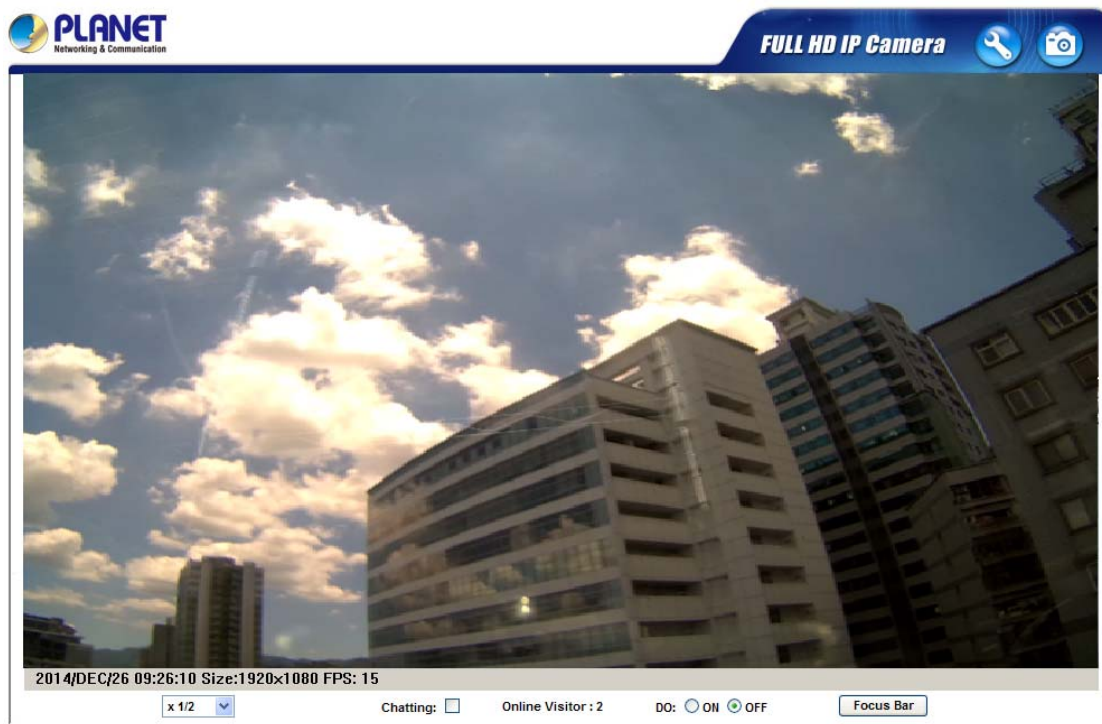



If the User Name and Password have been changed before, please enter the new User Name and Password here.

Web browser may display the “**Security Warning**” window. Select “**Yes**” to install and run the ActiveX control into your PC.



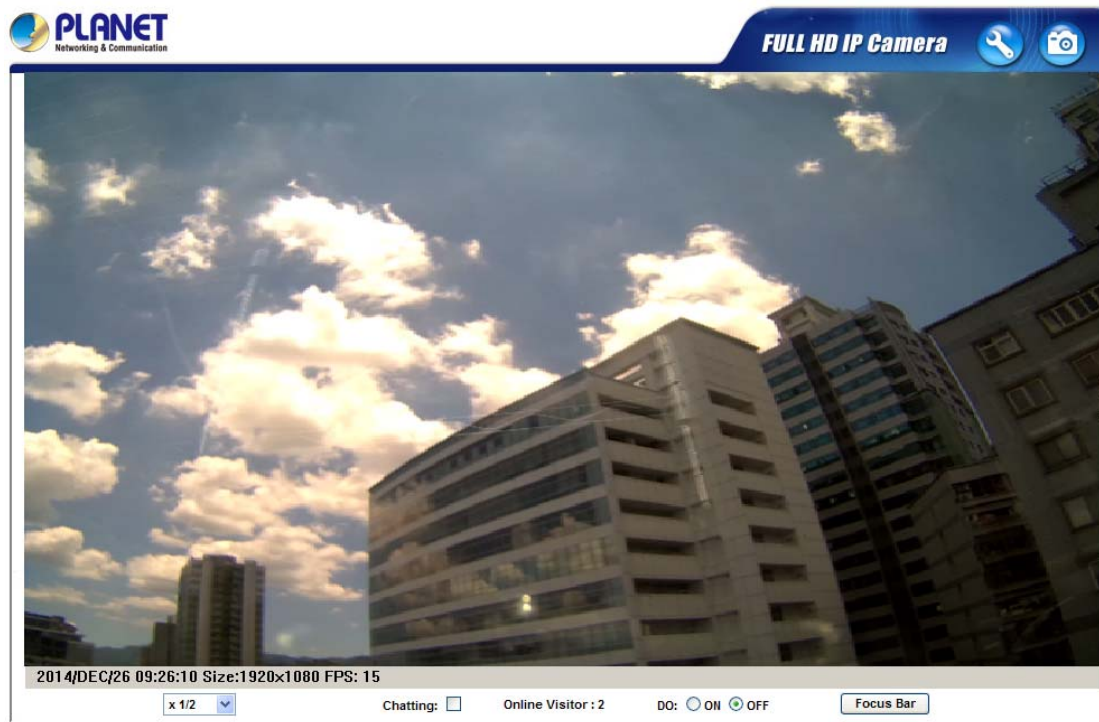
After the ActiveX control is installed and run, the first image will be displayed.





 **Note** If you log in the camera as an ordinary user, setting function will be not available. If you log in the camera as the administrator, you can perform all the settings provided within the device.

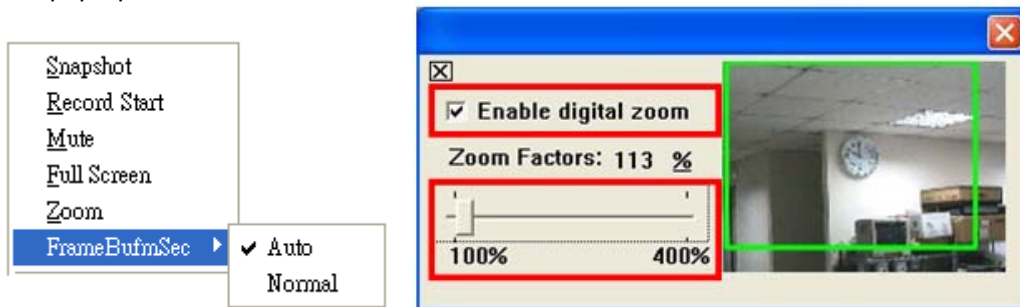
3.3 Live Viewing

Start-up screen is shown below whether you are an ordinary user or an administrator.



Configure	 Get into the administration page.
Snapshot	 Video Snapshot
Status Bar	Show system time, video resolution, and video refreshing rate
Screen Size	Select video screen “ default, 1/2x, 1x, 2x ” for view with current camera screen size
Chatting	IP Camera supports 2-way audio. Click the “ Chatting ” check box. Then you can use microphone which connects to the PC to talk to server side, which is IP Camera side
Online Visitor	Shows how many people are connected to this IP camera
DO(on/off)	Control the relay which is connected to this camera
Focus Bar	Show the Focus Bar


Double-click the video and it will change to full screen mode. Press “**Esc**” or double-click the video again. It will change back to normal mode. Right-click the mouse on the video, it will show a pop-up menu.




Snapshot	Save a JPEG picture.
Record Start	Record the video in the local PC. It will ask you where to save the video. To stop recording, right-click the mouse again. Select “ Record Stop ”. The video format is AVI. Use Microsoft Media Player to play the recorded file.
Mute	Turn off the audio. Click again to turn it on.
Full Screen	Full-screen mode.
Zoom	Enable zoom-in and zoom-out functions. Select “ Enable digital zoom ” option first within the pop-up dialogue box and then drag and drop the bar to adjust the zoom factors.
FrameBufferSec	Build a buffer to accumulate several video frames and play at a regular interval. This function can make video smooth-going when the Network speed is slow and lag. The default value is “Auto”.

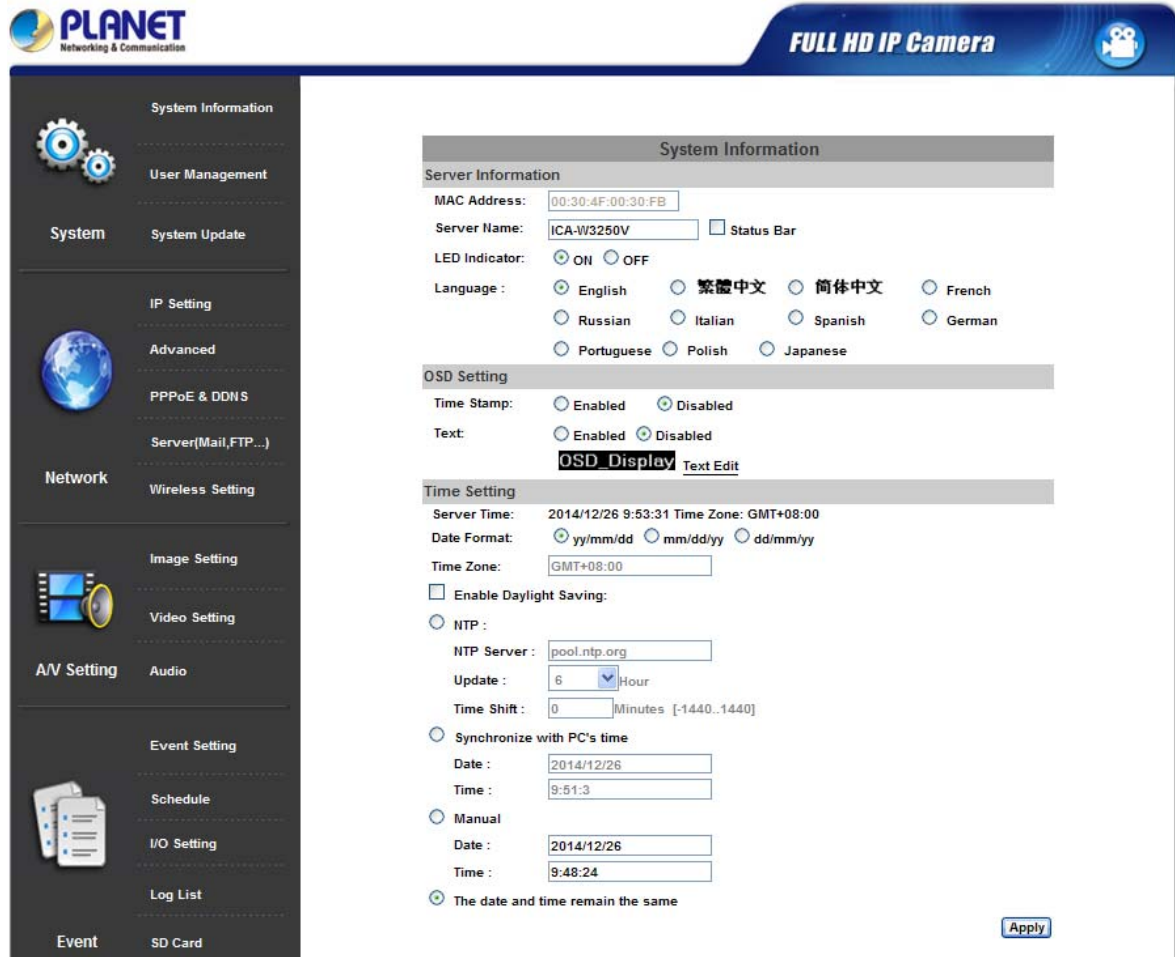
3.4 Configuration



Click  to get into the administration page.



Click  to go back to the live video page.




The screenshot shows the configuration web interface for the IP camera. The left sidebar contains a menu with categories: System Information, User Management, System, System Update, IP Setting, Advanced, PPPoE & DDNS, Server(Mail,FTP...), Network, Wireless Setting, Image Setting, Video Setting, A/V Setting, Audio, Event Setting, Schedule, I/O Setting, Log List, Event, and SD Card. The main content area is titled 'System Information' and contains the following settings:

- Server Information:**
 - MAC Address: 00:30:4F:00:30:FB
 - Server Name: ICA-W3250V 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: 2014/12/26 9:53:31 Time Zone: GMT+08:00
 - Date Format: yy/mm/dd mm/dd/yy dd/mm/yy
 - Time Zone: GMT+08:00
 - Enable Daylight Saving:
 - NTP:
 - NTP Server: pool.ntp.org
 - Update: 6 Hour
 - Time Shift: 0 Minutes [-1440..1440]
 - Synchronize with PC's time
 - Date: 2014/12/26
 - Time: 9:51:3
 - Manual
 - Date: 2014/12/26
 - Time: 9:48:24
 - The date and time remain the same

An 'Apply' button is located at the bottom right of the configuration area.

3.5 System



This block shows a thumbnail of the configuration menu items: System Information, User Management, System, and System Update.

3.5.1 System Information

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

System Information	
Server Information	
MAC Address:	<input type="text" value="00:30:4F:00:30:FB"/>
Server Name:	<input type="text" value="ICA-W3250V"/> <input type="checkbox"/> Status Bar
LED Indicator:	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Language :	<input checked="" type="radio"/> English <input type="radio"/> 繁體中文 <input type="radio"/> 简体中文 <input type="radio"/> French <input type="radio"/> Russian <input type="radio"/> Italian <input type="radio"/> Spanish <input type="radio"/> German <input type="radio"/> Portuguese <input type="radio"/> Polish <input type="radio"/> Japanese

Server Name	This is the Camera name. This name will show on the IP Installer.
Select language	There are English, Traditional Chinese, Simplified Chinese, French, Russian, Italian, Spanish, German, Portuguese and Polish to select. When changed, it will show the following dialogue box for the confirmation of changing language.



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

OSD Setting	
Time Stamp:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Text:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
	Test <u>Text Edit</u>

Moreover, click Text Edit to enter to adjust the OSD contents which include Size and Alpha of text. Finally, click the "Upgrade" button to reserve the setting.

Text Edit	
Text	<input type="text" value="OSD_Display"/>
Size	<input type="text" value="12"/> ▼
Transparency	<input type="text" value="100%"/> ▼
<input type="button" value="Upgrade"/>	

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

Time Setting

Server Time: 2014/8/25 16:32:43 Time Zone: GMT+08:00

Date Format: yy/mm/dd mm/dd/yy dd/mm/yy

Time Zone:

Enable Daylight Saving:

NTP :

NTP Server :

Update : Hour

Time Shift : Minutes [-1440..1440]

Synchronize with PC's time

Date :

Time :

Manual

Date :

Time :

The date and time remain the same

3.5.2 User Management

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

User Management

Anonymous User Login

YES NO

Add User

Username:

Password:

Confirm:

User List

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


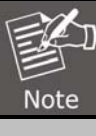
Anonymous User Login	Yes : Allow anonymous login No : Need user name & password to access this IP camera
Add user	Type the user name and password, and then click “Add/Set”.

Click “edit” or “delete” to modify the user



3.5.3 System Update

System Update	
Firmware Upgrade	
Firmware Version:	VC1.0.18_PL
New Firmware:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>	
Reboot System	
<input type="button" value="Start"/>	
Factory Default	
<input type="button" value="Start"/>	
Setting Management	
Save As a File:	Right click the mouse button on <u>Setting Download</u> and then select Save As to save current system's setting in the PC.
New Setting File:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>	

Firmware Upgrade	<p>To update the firmware online, click “Browse...” to select the firmware. Then click “Upgrade” to proceed.</p> <div style="border: 1px solid black; padding: 5px;"> <p> Note</p> <ol style="list-style-type: none"> 1. Upgrading firmware procedure cannot be interrupted. If the power or network connection is broken during the download procedure, the device might be damaged. 2. User must make sure that the firmware only applies to this device. Furthermore, do not try to upgrade new firmware if not necessary. </div>
Reboot System	Re-start the IP camera.
Factory default	<p>Delete all the settings in this IP camera.</p> <div style="border: 1px solid black; padding: 5px;"> <p> Note</p> <p>IP address is not included.</p> </div>
Setting Management	User may download the current setting to PC, or upgrade from previous saved setting.

Setting download:

Right-click the mouse button on Setting Download → Select “**Save AS...**” to save current IP CAM setting in PC → Select saving directory → Save

Upgrade from previous setting:

Browse → search previous setting → open → upgrade → Setting update confirm → click [index.html](#) to return to main page

3.6 Network



3.6.1 IP Setting

IP camera supports DHCP and static IP.

IP Setting	
IP Assignment	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IP Address:	192.168.0.20
Subnet Mask:	255.255.255.0
Gateway:	192.168.0.1
DNS 0:	168.95.1.1
DNS 1:	168.95.1.2
IPv6 Assignment	
<input checked="" type="checkbox"/> IPv6 Enabled:	
<input type="checkbox"/> Manually setup the IPv6 address:	
DHCPv6:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IPv6 Address:	fe80::20f:dff:fe24:933e
Port Assignment	
Web Page Port:	80
HTTPS Port:	443 HTTPS Setting
UPnP	
UPnP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
UPnP Port Forwarding:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
External Web Port:	80
External HTTPS Port:	443

RTSP Setting

RTSP Server: Enabled Disabled

RTSP Authentication:

RTSP Port:

RTP Start Port: [1024..9997]

RTP End port: [1027..10000]

Multicast Setting (Based on the RTSP Server)

Streaming 1:

IP Address: [224.3.1.0 ~ 239.255.255.255]

Port: [1 ~ 65535]

TTL: [1 ~ 255]

Streaming 2:

IP Address: [224.3.1.0 ~ 239.255.255.255]

Port: [1 ~ 65535]

TTL: [1 ~ 255]

ONVIF

ONVIF: V2.20 V1.01 Disabled

Security: Enabled Disabled

RTSP Keepalive: Enabled Disabled

Bonjour


Bonjour: Enabled Disabled

Bonjour Name: @00:30:4F:00:30:FB

LLTD (Link Layer Topology Discovery)

LLTD: Enabled Disabled

DHCP	Using DHCP, IP camera will get all the network parameters automatically.
Static IP	Please type in IP address, subnet mask, gateway, and DNS manually.
IPv6 Assignment	IPv6 is a newer numbering system that provides a much larger address pool than IPv4, which accounts for most of today's Internet traffic. You can set up IPv6 manually by keying in Address, Gateway, and DNS, or enabling DHCP to assign the IP automatically.
Port Assignment	User may need to assign a different port to avoid conflict when setting up IP assignment. (1) Web Page Port: setup web page connecting port and video transmitting port (Default: 80) (2) RTSP Port: setup port for RTSP transmitting (Default: 554) (3) RTP Start and End Port: in RTSP mode, you may use TCP and UDP for connecting. TCP connection uses RTSP Port (554). UDP connection uses RTP Start and End Port.
UPnP	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." Note: UPnP must be enabled on your computer.
UPnP Port Forwarding	When the camera is installed under a router, enable UPnP Port Forwarding to let the router open ports so that the video streams can be sent out from a LAN. Set Web Port, Http Port, and RTSP port, and make sure your router supports UPnP and the function has been activated.

RTSP Server	enable or disable RTSP server
RTSP Authentication	<p>"Disable" means everyone who knows your camera IP Address can link to your camera via RTSP. No username and password are required.</p> <p>Under "Basic" and "Digest" authentication mode, the camera asks the user to give username and password before allows accessing. The password is transmitted as clear text under basic mode, which provides a lower level of security than under digest mode.</p> <p>Make sure your media player supports the authentication schemes</p>
RTSP port	<p>RTSP Port: setup port for RTSP transmitting (Default: 554)</p> <p>RTSP Start and End Port: in RTSP mode, you may use TCP and UDP for connecting. TCP connection uses RTSP Port (554). UDP connection uses RTSP Start and End Port.</p>
Multicast Setting (Based on the RTSP Server)	<p>Multicast is a bandwidth conservation technology. This function allows several users to share the same packet sent from IP camera. To use Multicast, appoint IP Address and port here. TTL means the life time of packet, The larger the value is, and the more users can receive the packet.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note To use Multicast, be sure to enable the function "Force Multicast RTP via RTSP" in your media player. Then key in the RTSP path of your camera: "rtsp://(IP address)/" to receive the multicast.</p> </div>
ONVIF	<p>The IP camera supports ONVIF v1.01 / v2.20 standard for to integration.</p> <p>Under ONVIF connection, the video will be transmitted by RTSP. Be sure to enable the RTSP server in IP setting, or you're not able to receive the video via ONVIF.</p>
RTSP Keepalive	<p>When the function is enabled, the camera checks once in a while if the user who links to the camera via ONVIF still keeps connecting. If the connection is broken, the camera will stop transmitting video to user.</p>
Bonjour	<p>This function enables MAC systems to link to this IP camera. Key in the name here.</p> <p>The web browser "Safari" also has Bonjour function. Tick "Include Bonjour" in the bookmark setting, and you can see the IP camera appearing under the bonjour category. Click the icon to connect the IP camera.</p>
LLTD	<p>If your PC supports LLTD, enable this function and then you can check the connection status, properties, and device position (like IP address) of this IP Camera in the network map.</p> <p>In the computer running Windows Vista or Windows 7, you can find LLTD through the path: Call out the Control Panel → Network and Internet → Network and Sharing Center → Click "See full map"</p>

3.6.2 Advanced

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS Setting

Created Request

Subject:

Date:

Installed Certificate

Subject:

Date:

Connection Types

▼

-
-
-

Https can help protect streaming data transmission over the Internet on the higher security level. You can select the connection type. "Https" means user cannot connect the camera via Http protocol. The Https path will be: "https :// (IP address)". If you select "Http & Https", both the Http and Https path can be used to access the camera.

Remove the existing setting: Before setting new request, please remove old secure identification. Select "Http" connection type and click "Remove".

Https Setting

Created Request

Subject:

Date:

Installed Certificate

Subject:

Date:

Connection Types

▼

Created Request: Setting the secure identification and apply it

Https Setting

Create Request

Country:

State or province:

Locality:

Organization:

Organizational Unit:

Common Name:

There are two ways to set Certificate -- Install Signed Certificate or Create Self-Signed Certificate.

SNMP (Simple Network Management Protocol)

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

SNMPv1 and SNMPv2:

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

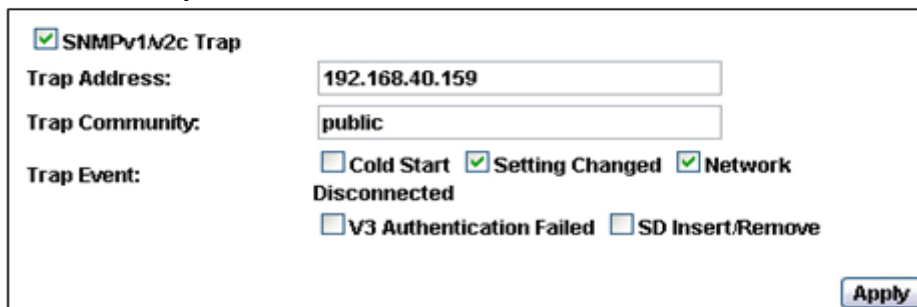
Tick the box to enable SNMPv1 or SNMPv2c protocol, and specify the community name for write (read and write) and read (read-only). The user who use read community name to access the IP camera cannot modify any data of this camera.

SNMPv3:

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

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

SNMPv1/SNMPv2 Trap:



The form contains the following fields and options:

- SNMPv1/v2c Trap
- Trap Address:
- Trap Community:
- Trap Event:
 - Cold Start
 - Setting Changed
 - Network Disconnected
 - V3 Authentication Failed
 - SD Insert/Remove
-

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

- Cold Start: The camera starts up or reboots.
- Setting changed: The SNMP setting is changed.
- Network Disconnected: The network connection is 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.

Access List

IP FILTER

IP ADDRESS FILTER Setting

Enable ip address filter

IPv4 Setting:

allow deny

address: -

IPv4 List:

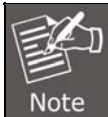
No.	IP Address	Filter	Action
1	192.168.50.159	allow	<input type="button" value="remove"/>
2	192.168.50.151-192.168.50.161	deny	<input type="button" value="remove"/>
3			<input type="button" value="remove"/>
4			<input type="button" value="remove"/>
5			<input type="button" value="remove"/>
6			<input type="button" value="remove"/>
7			<input type="button" value="remove"/>
8			<input type="button" value="remove"/>
9			<input type="button" value="remove"/>
10			<input type="button" value="remove"/>

Allow admin ip address always access this device

Admin ip address:

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

You can also choose to deny a range of IP addresses but allow one or several of them. Take the the above picture for example, IP address 192.168.50.151~161 is not allowed to connect to the camera, but only 192.168.50.159 can access.



In the list "allow" condition must be ranked before "deny" condition.

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

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

QoS/DSCP

QoS/DSCP Setting

Enable QoS/DSCP

Live Stream: (0~63)

Event / Alarm: (0~63)


Management: (0~63)

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

The number 0~63 for Live Stream, Event / Alarm, and Management represent the ratio that

the bandwidth is divided. For example, if you set 5, 10, and 20 for the three items, then the bandwidth of the three items is 5:10:20. There is no difference between setting "0, 0, 0" or "63, 63, 63" because under these two settings, the three items will get equal bandwidth (1/3). The three stream control protocols are as follows:

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



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

IEEE 802.1x

IEEE 802.1x/EAP-TLS

IEEE 802.1x Setting

Enable IEEE 802.1x

Eapol version: v1 v2

Identity:

Private key password:

CA certificate:

Status:

Client certificate:

Status:

Client private key:

Status:

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

The EAPOL protocol supports service identification and optional point to point encryption over the local LAN segment.

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

3.6.3 PPPoE & DDNS

PPPoE & DDNS

PPPoE Setting

Enabled Disabled

Username:

Password:

Send mail after PPPoE dialed

Enabled

Subject:

DDNS Setting

Enabled Disabled

Provider:

Username:

Schedule Update: Minutes

State

Idle

Note:

1. Schedule Update: Depends on the input time of Schedule Update, it will update DDNS's web site automatically. The time range is from 5 to 5000 minutes.
*0: It will not update.
2. dyndns.org & 3322.org: Update once per day is recommended (1440 minutes per day). If updated too frequently, it will be blocked.

PPPoE: Stands for Point to Point Protocol over Ethernet

A standard builds on Ethernet and Point-to-Point network protocol. It allows Internet camera to connect to Internet with xDSL or cable connection; it can dial up your ISP and get a dynamic IP address. For more PPPoE and Internet configuration, please consult your ISP.

It can directly connect to the xDSL; however, it should be set up in a LAN environment to program the PPPoE information first, and then connect to the xDSL modem. Power on again to enable the device to dial on to the ISP connection to the WAN through the xDSL modem.

The procedures are:

- (1) Select "**Enabled**" to use PPPoE.
- (2) Key-in username and password for the ADSL connection.
- (3) Send mail after dialing : When connecting to the Internet, it will send a mail to a specific mail account. For the mail setting, please refer to "**Mail and FTP**" settings.

DDNS: Stands for Dynamic Domain Name Server

The device supports DDNS If your device is connected to xDSL directly; you might need this feature. However, if your device is behind a NAT router, you will not need to enable this feature. Because DDNS allows the device to use an easier way to remember naming format rather than an IP address. The name of the domain is like the name of a person, and the IP address is like his phone number. On the Internet we have IP numbers for each host (computer, server,

router, and so on), and we replace these IP numbers to easily remember names, which are organized into the domain name. As to xDSL environment, most of the users will use dynamic IP addresses. If users want to set up a web or a FTP server, then the Dynamic Domain Name Server is necessary. For more DDNS configuration, please consult your dealer.

Your Internet Service Provider (ISP) provides you with at least one IP address which you use to connect to the Internet. The address you get may be static, meaning it never changes, or dynamic, meaning it's likely to change periodically. Just how often it changes, it depends on your ISP. A dynamic IP address complicates remote access since you may not know what your current WAN IP address is when you want to access your network over the Internet. The solution to the dynamic IP address problem comes in the form of a dynamic DNS service.

The Internet uses DNS servers to lookup domain names and translates them into IP addresses. Domain names are just easy to remember aliases for IP addresses. A dynamic DNS service is unique because it provides a means of updating your IP address so that your listing will remain current when your IP address changes. There are several excellent DDNS services available on the Internet and best of all they're free to use. One such service you can use is www.DynDNS.org. You'll need to register with the service and set up the domain name of your choice to begin using it. Please refer to the home page of the service for detailed instructions or refer to Appendix E for more information.

DynDns.org, the procedures are:

- (1) Enable this service
- (2) Key-in the DynDNS server name, user name, and password.
- (3) Set up the IP Schedule update.
- (4) Click "**Apply**"
- (5) If setting up IP schedule update too frequently, the IP may be blocked. In general, schedule update every day (1440 minutes) is recommended.

DDNS Setting

Enabled Disabled

Provider:

Hostname:

Username:

Password:

Schedule Update: Minutes

State

Note:

1. Schedule Update: Depends on the input time of Schedule Update, it will update DDNS's web site automatically. The time range is from 5 to 5000 minutes.
*0: It will not update.
2. dyndns.org & 3322.org: Update once per day is recommended (1440 minutes per day). If updated too frequently, it will be blocked.

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 provide: The server, user name, and password may be wrong.

This model adds Planet easy DDNS that when this function enable will occur hostname with PLANET Easy DDNS and end six of MAC automatically. User doesn't have to go to www.planetddns.com to register a new account.

DDNS Setting

Enabled Disabled

Provider:

Hostname:

Schedule Update: Minutes

3.6.4 Mail & FTP & SAMBA

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

Mail Setting:

Server Settings

Mail Setting

Login Method:

Mail Server:

Username:

Password:

Sender's Mail:

Receiver's Mail:

Bcc Mail:

Mail Port: (Default 25)

Secure Connect: TLS SSL

FTP Setting

Samba (Network storage)

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

FTP Setting:

Server Settings	
Mail Setting	
FTP Setting	
FTP Server:	<input type="text" value="192.168.0.174"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••"/>
Port:	<input type="text" value="21"/>
Path:	<input type="text" value="/VOLUME2/ADMIN/test"/>
Mode:	<input type="button" value="PORT"/>
Create the folder:	<input type="button" value="Yes"/> (ex:Path/20100115/121032m.avi)
<input type="button" value="Test"/>	
Samba (Network storage)	
<input type="button" value="Apply"/>	

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

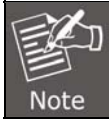
In PORT mode, the FTP server builds the connection to the user’s data port actively. However, from the user-side firewall’s standpoint, the action of connecting from FTP server is often considered to be dangerous and should be blocked. In PASV mode, the problem is solved: The FTP server waits for the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

Samba Setting:

Server Settings	
Mail Setting	
FTP Setting	
Samba (Network storage)	
Location:	<input type="text" value="192.168.0.124\share"/> (ex:\\Nas_ip\folder)
Workgroup:	<input type="text" value="workgroup"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••"/>
Create the folder:	<input type="button" value="Yes"/> (ex:Path/20100115/121032m.avi)
<input type="button" value="Test"/>	
<input type="button" value="Apply"/>	

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

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



Samba only supports one layer folder.

3.6.5 Wireless Setting

To connect the camera to wireless AP/router, please set up the configuration first.

Wireless Setting			
Status of Wireless Networks			
SSID	Mode	Security	Signal Strength
Test8888	Infrastructure	WPA2P SK/AES	90
ADN-4100_ENM	Infrastructure	WPA2P SK/AES	67
Wireless Setting			
MAC Address:	00:30:4F:00:30:FB		
Mode:	Infrastructure		
Operation Mode:	Auto		
SSID:	Default		
Domain:	FCC (1~11Ch)		
Security:	None		

Status of Wireless Networks	<p>SSID: The SSID of all found wireless AP/router will be shown here.</p> <p>Mode: If the wireless AP/router is shown as infrastructure, you have to set the camera as infrastructure mode to connect to it; If the wireless AP/router is shown as Ad-hoc, you have to set the camera as Ad-hoc mode to connect to it</p> <p>Security: The encryption of wireless AP/router will be shown here.</p> <p>Signal Strength: If the value is bigger, the signal strength is stronger.</p>
Mode	<p>Select the network type of wireless connection.</p> <p>Infrastructure: Connect the IP camera to a wireless AP/router.</p> <p>Ad-hoc: This IP camera will become a stand-alone wireless network point. Other wireless computers / devices can discover this IP camera and connect to it without the wireless access point. There is “Channel” to select only when the camera works as Ad-hoc mode.</p>
Operation Mode	<p>The default is “Auto”, it means the camera supports 802.11b+g+n. You also set it as “11g” or “11b”.</p>
SSID	<p>Input the SSID of the wireless AP/router you wish to connect.</p>
Channel	<p>This is only be showed when the user selects Ad-hoc mode in order to avoid conflict.</p> <p>If the mode is infrastructure, the channel will be set automatically the same as wireless AP/router.</p>
Security	<p>When the mode is infrastructure, it supports None, Open System, Shared Key 64bits and 128bits, WPA-PSK(TKIP/AES) and WPA2-PSK(TKIP/AES). Configure the setting consistent with the setting on the wireless router/AP that this IP camera will join the wireless network.</p>

	When the mode is Ad-hoc, it supports None, Open System, Shared Key 64bits and 128bits.
Domain	In some countries, the wireless rule might apply; please select it according to your country.

- Here is an example that shows how to connect the camera to wireless AP.

Step 1: Check the “Wireless Setting” to get into the wireless setting page and search nearby wireless AP.



Step 2: In this case, we would connect the camera to the wireless AP whose SSID is Test8888. So please input “Test8888” in the field of SSID.

Wireless Setting			
Status of Wireless Networks			
SSID	Mode	Security	Signal Strength
Test8888	Infrastructure	WPA2P SK/AES	90
ADN-4100_ENM	Infrastructure	WPA2P SK/AES	67
Wireless Setting			
MAC Address:	00:30:4F:00:30:FB		
Mode:	Infrastructure ▼		
Operation Mode:	Auto ▼		
SSID:	Test8888		
Domain:	FCC (1~11Ch) ▼		
Security:	None ▼		

Step 3: If the wireless AP has the encryption key, please input the correct password. If the wireless AP doesn't have the encryption key, please keep it as none. In this case, we set the security as WPA2-PSK, encryption as AES, and Pre-Shared Key is 11111111.

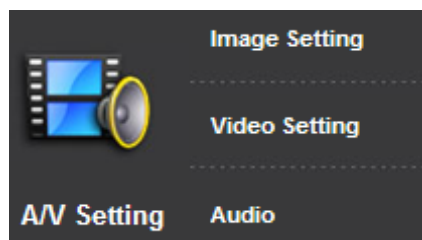
Wireless Setting	
MAC Address:	00:30:4F:00:30:FB
Mode:	Infrastructure
Operation Mode:	Auto
SSID:	Test8888
Domain:	FCC (1~11Ch)
Security:	WPA2-PSK
WPA2-PSK Setting	
Encryption	AES
Pre-Shared Key:	11111111 (ASCII format, 8~63)

Step 4: Click the "Apply" button to save change.

Step 5: Remove IP camera's Ethernet cable. IP camera will connect to the wireless AP via wireless.

Step 6: If wireless AP supports Wireless Client Table function, user is able to check the connection status via the function.

3.7 A/V Setting



3.7.1 Image Setting

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

Privacy Mask

Area 1
Area 2
Area 3
Save

Image Setting

Brightness: ▼

Contrast: ▼

Hue: ▼

Saturation: ▼

Sharpness: ▼

AGC: ▼

Shutter Time: ▼

Sense-Up: ▼

D-WDR: ▼

Anti Fog: Enable

Lens Distortion Correction: ▼

Video Orientation: Flip Mirror

Day & Night: ▼

Night to Day Lux: ▼ (about) Day to Night Lux: ▼ (about)

Current Lux: (about)

Red Gain: ▼ Blue Gain: ▼

Denoise: 3D: ▼ 2D: ▼ Default

Image adjust	Brightness, Contrast, Hue, Saturation, and Sharpness can be adjusted here.
AGC	Automatic gain control. The sensitivity of camera can be adjusted with the environmental light. Enable this function and the brighter image can be got under dim light, but the level of noise may also increase
Shutter Time	Choose as the location of your camera or fixed shutter time. The shorter the shutter time is the less light the camera receives and the image becomes darker.
Sense-Up	This function increases the sensitivity of camera to get brighter image at night. The smaller the value you select, the slower the shutter speed becomes so that the image will get brighter, and moving subjects might be blurred.
D-WDR	Digital wide dynamic range. This function enables the camera to reduce the contrast in the view to avoid the dark zones resulting from over and under exposure.
Anti Fog	Improve the image clarity on environments presenting high levels of fog or smoke.
Lens Distortion Correction	Straight the curves in the borders of the image caused by the lens angles. The available values are: OFF, 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

Video Orientation	Flip or mirror the image as per your requirement.
Day & Night / Lux setting	The camera can detect the light level of environment. Light Sensor Mode: If you choose "Light Sensor Mode", the image will be turned to black and white at night in order to keep clear. To set light sensor mode, appoint a lux standard of switching D/N here. Current lux value is provided for reference. Times Mode: Under "Times Mode" the switch time of Color / Black and white is according to the given time. Color Mode (Day): IR filter is always on. The video is colorful even it is in dark conditions. B/W Mode (Night): IR filter is always off. The video is black and white even it is in bright conditions.
Red / Blue gain	Set the values for Red / Blue gain. The available values are: -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5
Denoise	This function is able to filter the noise and blur from the image and show a clearer view. You can set the values for 2D and 3D filters.

3.7.2 Video Setting

Video Setting

Video System: (v)

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

TV Output Focus Bar: ON OFF

Corridor Mode: (v)

Video System	Click the drop down list to select the system type "NTSC/PAL".
TV Output	Click the drop down list to select the system type "NTSC/PAL/Auto/Off"
TV Output Focus Bar	Show the Focus Bar on TV
Corridor Mode	The function allows you to get a vertically oriented video stream from the camera. You can select "None/90 degrees/270 degrees".

Basic Mode :

Streaming 1 Setting

Basic Mode Advanced Mode

Resolution: (v)

Profile: (v)

Quality: (v)

Video Frame Rate: (v)

Video Format: (v)

RTSP Path: ex:rtsp://IP_Address/ Audio:G.711

Streaming 2 Setting

Basic Mode Advanced Mode Close

Resolution	There are 5 resolutions to choose from: 1920x1080,1280x720, 640x480, 320x240, or 176x144
-------------------	--

Profile	Profiles are different compression ways of H.264. Main profile provides better coding efficiency. Note that some devices do not support every profile. For example, iPhone4 only supports main profile.
Quality	The higher the quality is, the bigger the file size is. It might affect Internet transmitting speed if the file gets too large.
Video Frame Rate	The video refreshing rate per second. The maximum value is affected by the input resolution you choose.
Video Format	H.264 and JPEG.
RTSP Path	Set the RTSP output connecting route.

Advanced Mode:

Streaming 1 Setting

Basic Mode **Advanced Mode**

Resolution: 1920x1080

Profile: Main

Bitrate Control Mode: CBR **VBR**

Video Quantitative: 9

Video Bitrate: 4Mbps

Video Frame Rate: 30 FPS

GOP Size: 1 X FPS GOP = 30

Video Format: H.264

RTSP Path: ex:rtsp://IP_Address/ Audio:G.711

Streaming 2 Setting

Basic Mode Advanced Mode **Close**

Resolution	There are 5 resolutions to choose from: 1920x1080, 1280x720, 640x480, 320x240, or 176x144
Profile	Profiles are different compression ways of H.264. Main profile provides better coding efficiency. Note that some devices do not support every profile. For example, iPhone4 only supports main profile.
Bitrate Control Mode	There are CBR (Constant Bit Rate) and VBR (Variable Bit Rate) to use. CBR : 32Kbps~8Mbps (the higher the CBR is, the better the video quality is) VBR : 1(Low) ~10 (High) – Compression rate, the higher the compression rate is, the lower the picture quality is, and vice versa. The balance between VBR and network bandwidth will affect picture quality. Please carefully select the VBR rate to avoid picture breaking up or lagging.
Video Quantitative	The quality parameter of VBR. You can choose 1~10 compression rate. The higher the value is, the higher the image quality is.

Video Bitrate	The quality parameter of CBR. You can choose 32kbps ~ 8Mbps. The higher the value is, the higher the image quality is.
Video Frame Rate	The video refreshing rate per second. The max value is affected by the input resolution you choose.
GOP Size	It means "Group of Pictures". The higher the GOP is, the better the quality is.
Video Format	H.264, JPEG.
RTSP Path	RTSP output connecting route.

3GPP Streaming mode:

3GPP Streaming Setting

Open Close (Format=H.264)


Resolution:

Video Bitrate:

Video Frame Rate:

RTSP Path: ex:rtsp://IP_Address/v3 Audio:AMR

Resolution	There are 3 resolutions to choose from: 640x480, 320x240, or 176x144
Video Bitrate	32Kbps~1Mbps.
Video Frame Rate	The video refreshing rate per second. The maximum value is affected by the input resolution you choose.
RTSP Path	RTSP output connecting route. If the IP address of your camera is 192.168.40.150, and you key in "v3" in the column, the 3GPP path will be rtsp://192.168.40.150/v3

 The RTSP here is separated from the RTSP setting in the "IP SETTING". 3GPP Streaming can still work even you select "disabled" in the RTSP server option of IP Setting.

3.7.3 Audio Setting

The IP Camera supports 2-way audio. The user can send audio from the IP Camera by connecting external microphone to the remote PC; the user can also send audio from remote PC to IP Camera's external speaker.

(1) Audio from IP camera's external microphone to local PC: select "Enabled" to start this function. The audio compression format can be chosen from 3 options. You can also adjust the volume of

2-way audio.

Audio

IP Camera to PC

Enabled Disabled

Audio Type: G.711 (64Kbps) ▾

Adjust Volume


Mic-In: 4 (Max) ▾

Line-Out: 4 (Max) ▾

Apply

(2) Audio from local PC to IP Camera: Check “chatting” on the browsing page.

Chatting: Online Visitor : 2

 **Note** The audio will not be smooth when the SD card is recording.

3.8 Event List

Event Setting

Schedule

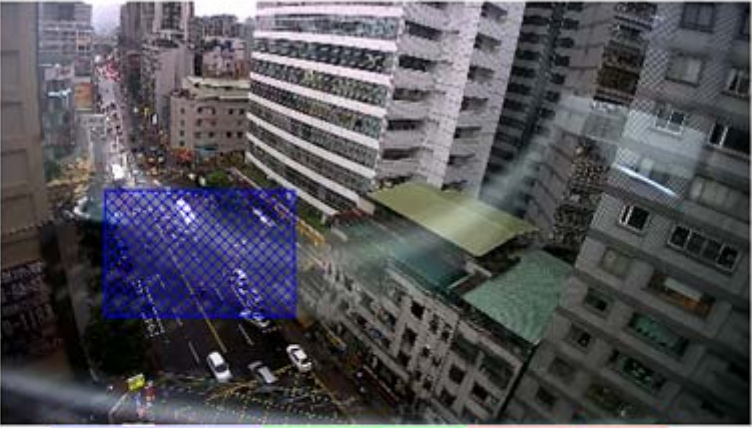
I/O Setting

Log List

Event SD Card

3.8.1 Event Setting

Motion Detection



Area Setting: Area 1 Area 2 Area 3

Sensitivity: 5 5 5

Area 1: E-mail FTP Out1 Save to SD card Samba

Area 2: E-mail FTP Out1 Save to SD card Samba

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

Subject:

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

Based on the schedule

Tampering Detection

Tampering: Enabled Disabled

E-mail FTP Out1 Save to SD card Samba

Interval: 30 sec

Record File

File Format: AVI File(with Record Time Setting)

Record Time Setting

Pre Alarm: 5 sec Post Alarm: 5 sec

Network Dis-connected

Dis-connected: Save to SD Card

Network IP Check

IP Check: Enabled Disabled

IP Address:


Interval: 30 sec

Check failed: Connection failed four times. Reboot IP Camera.

Save to SD card

(When IP check failed, first step will save to SD card, continuing other saving storage)

Motion Detection	IP camera allows 3-area motion detection. When motion is triggered, it can send the video to some specific mail addresses, transmit the video to remote ftp server and SAMBA, and trigger the relay. To set up the motion area, click "Area Setting" and use mouse to drag and draw the area. The same operation is done for areas 2 and 3. If you select "save to
-------------------------	--

	SD card", the video or snapshot will be saved to Micro SD card.
Interval	For example, if you select "10 sec" here, once the motion is detected and action is triggered, it cannot be triggered again within 10 seconds.
Based on the schedule	When the option box is ticked, only during the selected schedule time the motion detection is enabled. That is, for example, the 11th hour of Monday has not been colored in the schedule table, then no action will be triggered even the camera detects motion during 11:00~12:00 on Monday.
Tampering Detection	When the camera view is covered, moved, hit by strong light, or out of focus, the tampering detection will be triggered, and send snapshot or video to mail/FTP/Samba/SD card, or trigger the external alarm.
Record File Setting	IP camera allows 3 different types of recording file to change its record size. When motion/alarm is triggered, there are 3 different types of recording modes: (1) AVI File (With Record File Setting) (2) JPEG Files (With Record Time Setting), only streaming 1 with JPEG compression format. (3) JPEG File (Single File with Interval Setting)
Record Time Setting	<p>Pre Alarm allows users to check what causes the trigger. Post Alarm will start to record when the trigger happens.</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">  <p>Note</p> <p>Pre/Post Alarm record time is based on record time setting and IP cam built-in RAM memory. Limited by IP cam built-in RAM memory, when information is too much or video quality is set too high, it will cause recording frame to drop or decrease on post alarm recording time.</p> </div>
Network Disconnected	To avoid video loss, the camera will start to save the video to local SD card when it detects no network connection. The video recording will continuously be saved onto SD card and divided into every 10 minutes a file until the network is reconnected successfully. The oldest file will be deleted if the capacity of SD card is full.
Network IP check	Key-in the target IP address and interval. The camera checks once in a while according to the setting interval time if it can link to the target IP address. If connection fails, the camera starts to save the video to SD card

3.8.2 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: Second(s) [1..50000]

File Name:

Restart IP Camera Automatically

Restart

[Apply](#)


Schedule	After completing the schedule setup, the camera data will be recorded according to the scheduled setup.
Snapshot	After enabling the snapshot function, user can select the storage position of snapshot file, the interval time of snapshot and the reserved file name of snapshot.
Interval	The interval between two snapshots.
File Name	After enabling the snapshot function, user can select the storage position of snapshot file, the interval time of snapshot and the reserved file name of snapshot.
Restart IP Camera Automatically	The device will reboot automatically according to the dropdown list. Please make sure the Time setting is correct when this function is enable.

3.8.3 I/O Setting

The ICA-W3250V supports 1 input/1 output. When input is triggered, it can send the video to some specific mail addresses, transmit the video to remote ftp server, and trigger the relay and SAMBA.

I/O Setting	
Input Setting	
Input 1 Sensor:	<input type="text" value="N.O"/>
Input 1 Action:	<input type="checkbox"/> E-mail <input type="checkbox"/> FTP <input type="checkbox"/> Out1 <input type="checkbox"/> Save to SD card <input type="checkbox"/> Samba
Subject:	<input type="text" value="GPIO In Detected!"/>
Interval:	<input type="text" value="10 sec"/>
<input type="checkbox"/> Based on the <u>schedule</u>	
Output Setting	
Mode Setting:	<input checked="" type="radio"/> OnOff Switch <input type="radio"/> Time Switch
Interval:	<input type="text" value="10 sec"/>

Alarm Input Setting	The GPIO I/O port input activates related action when I/O input is triggered.
Interval	For example, if you select "10 sec" here, once the motion is detected and action is triggered, it cannot be triggered again within 10 seconds.
Based on the schedule	When the option box is ticked, only during the selected scheduled time the I/O is enabled. That is, for example, the 11th hour of Monday has not been colored in the scheduled table, then no action will be triggered even the camera detects input signal during 11:00~12:00 on Monday.
GPIO Output Setting	The GPIO I/O port output activates On/Off Switch, Slide Switch or Pan/Tilt Module for use with relay box.
On Off Switch	The camera triggers the external device and lasts for 10 seconds. You can turn off the alarm manually by clicking "off" on the right bottom of the live video page.
Time Switch	The camera triggers the external device and lasts for certain of time according to the interval setting, and the user is not allowed to break off the alarm manually.

 Note	Please connect to propriety relay box to reduce the risk of electric shock & damaged.
--	---

3.8.4 Log List

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.

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

3.8.5 SD card

Playback


Please insert a micro SD card before power on the camera. Make sure to push the micro SD card into the slot completely.

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

Playback

20121019 20121023 20121024

SD Card: << 856M / 969M >>



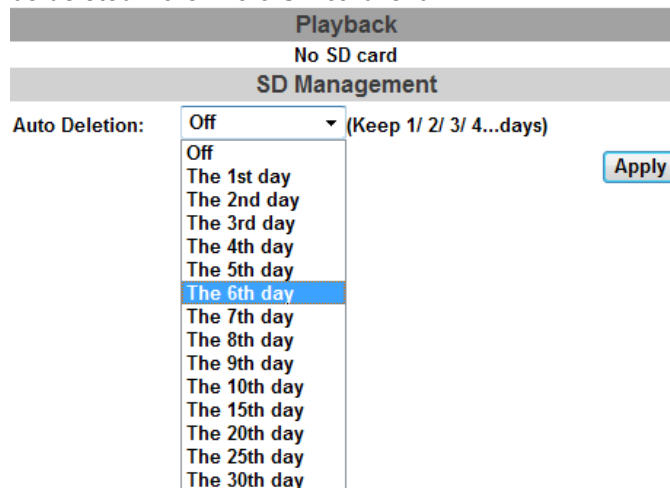
2012/10/23 Del			
Time	Video	Event Type	
11:55:48	115548m.avi	Motion Detection	<input type="checkbox"/>
12:22:16	122216m.avi	Motion Detection	<input type="checkbox"/>
12:23:01	122301m.avi	Motion Detection	<input type="checkbox"/>
12:24:06	122406m.avi	Motion Detection	<input type="checkbox"/>
12:25:04	122504m.avi	Motion Detection	<input type="checkbox"/>

Files link daily.

SD Management

Choosing "The 1st day" means the recording file will be kept for one day. For example, it is five o'clock now. Choose "The 1st day". The files will be kept from five o'clock yesterday to five o'clock today.

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



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

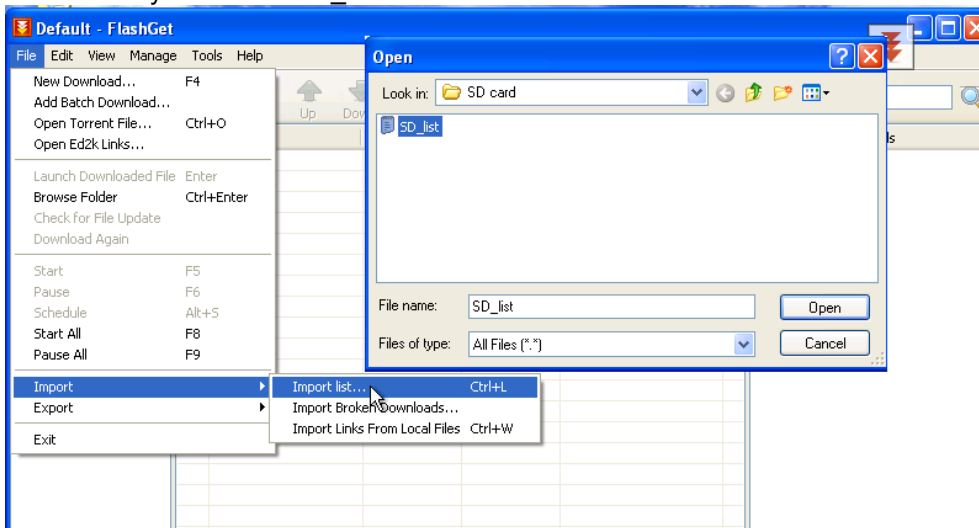
Copy to PC

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

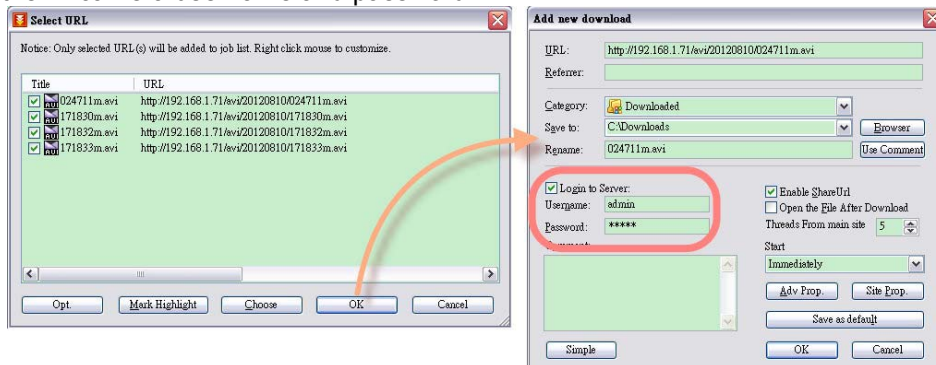
To use FlashGet for downloading the image and video data from the micro SD card, please follow the steps:



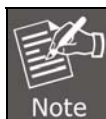
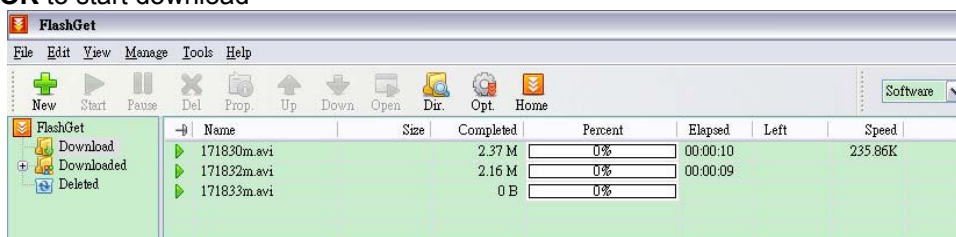
Open FlashGet, select "File" → "Import" → "Import list", and find the link list file you just saved. The file name may be called "SD_list".



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.



Click **OK** to start download

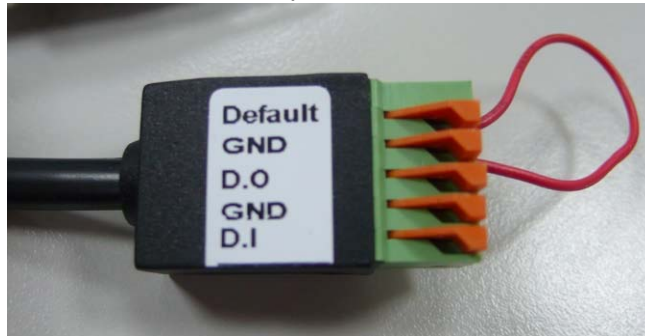


FlashGet is free software that can be downloaded from FlashGet official website. The example above is based on FlashGet ver.1.9.6.1073.

Appendix A. Factory Default

To recover the default IP address and password, please follow the steps:

- Remove the power and Ethernet cable.
- Take an electronic wire, plug one side of the wire into "Default" and the other side into "GND" on the terminal block as the picture is shown below.



- Connect power to the camera again. It takes around 30 seconds to boot the camera.
- Remove the wire and plug in the Ethernet cable after the camera finishes booting.
- Re-login the camera using the default IP (<http://192.168.0.20>) where both user name and password are **admin**.

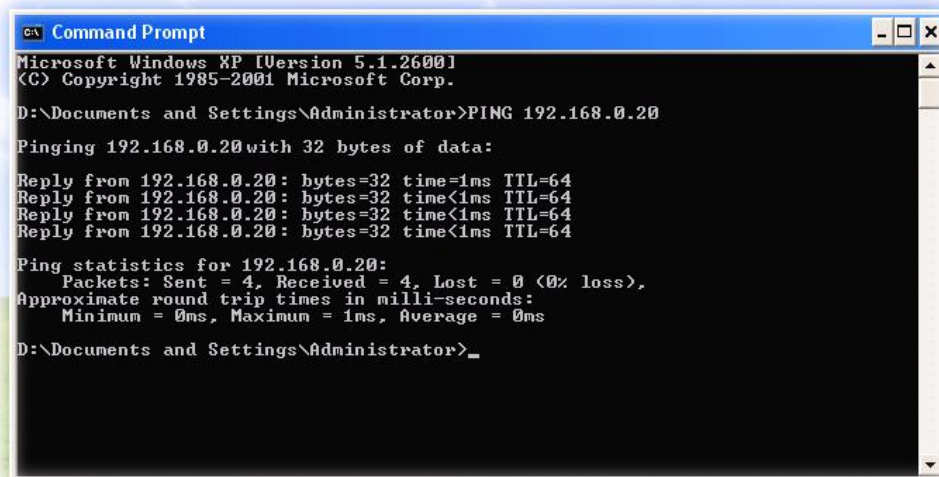
Appendix B. Ping IP Address

The ping (stands for Packet Internet Groper) command is used to detect whether a specific IP address is accessible by sending a packet to the specific address and waiting for a reply. It's also a very useful tool to confirm whether or not Internet camera is installed or if the IP address conflicts with any other device over the network.

If you want to make sure the IP address of Internet camera, utilize the ping command as follows:

- Start a DOS window.
- Type ping x.x.x.x, where x.x.x.x is the IP address of the internet camera.

The replies, as illustrated below, will provide an explanation to the problem.



```
C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\Administrator>PING 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Reply from 192.168.0.20: bytes=32 time=1ms TTL=64
Reply from 192.168.0.20: bytes=32 time<1ms TTL=64
Reply from 192.168.0.20: bytes=32 time<1ms TTL=64
Reply from 192.168.0.20: bytes=32 time<1ms TTL=64

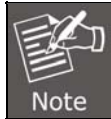
Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

D:\Documents and Settings\Administrator>_
```

If you want to detect any other device that conflicts with the IP address of internet camera, you also can utilize the ping command but you must disconnect the internet camera from the network first.

Appendix C. 3GPP Access

To use the 3GPP function, in addition to the previous section, you might need more information or configuration to make this function works.



To use the 3GPP function, it is strongly recommended to install the Networked Device with a public and fixed IP address without any firewall protection.

RTSP Port:

Port 554 is the default for RTSP service. However, sometimes, some service providers change this port number for some reasons. If so, user needs to change this port accordingly.

Dialing procedure:

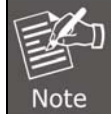
1. Choose a verified player (PacketVideo or Realplayer)
2. Use the following default URL to access:

rtsp://IP-Address/3g

Where *host* is the host name or IP address of the camera.

Compatible 3G mobile phone:

Please contact your dealer to get the approved list of compatible 3G phones.



Besides IP camera and 3G mobile phone, you will also need to make sure the ISP and company have provided the 3GPP service to you.

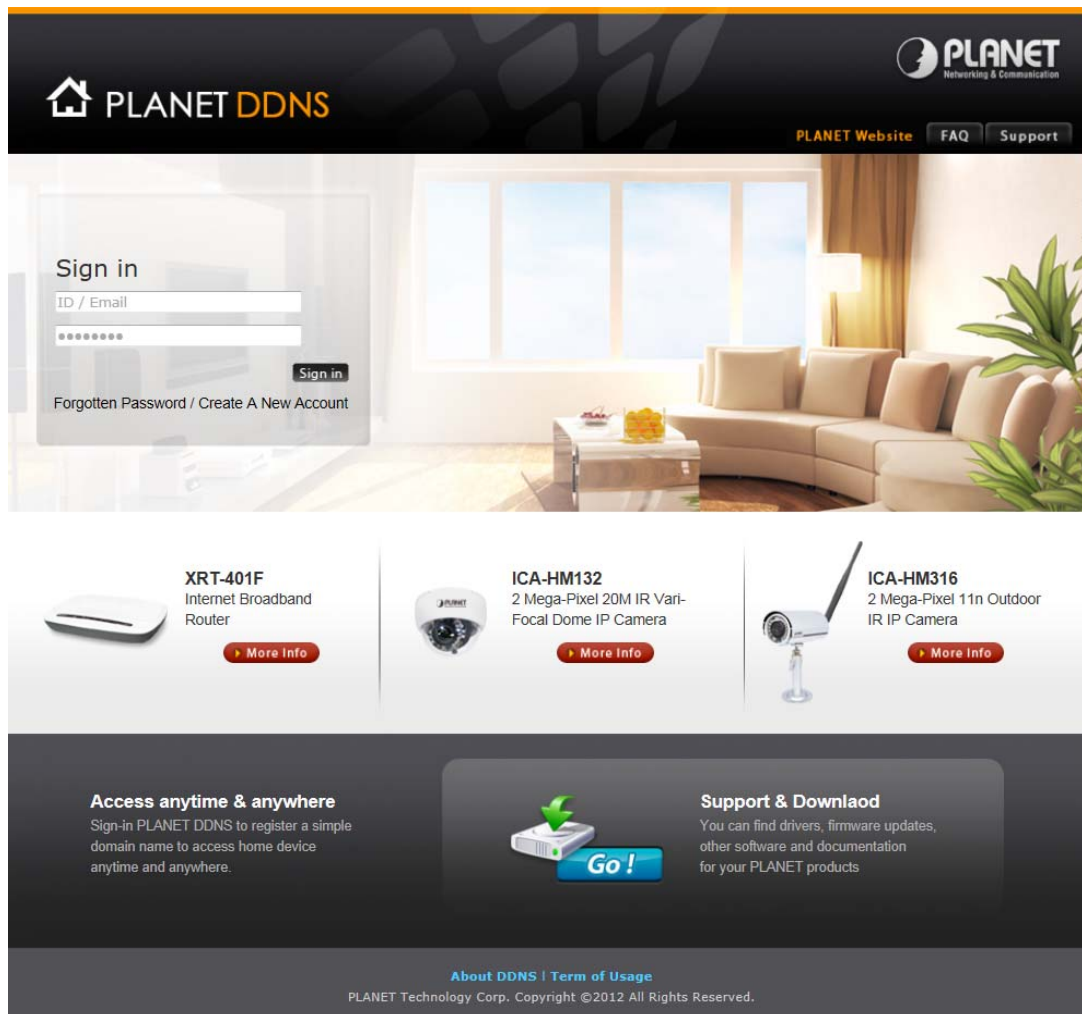
Appendix D. Planet DDNS Application

Configuring PLANET DDNS steps:

Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example: Register an account at <http://planetddns.com>

Step 2: Enable DDNS option through accessing web page of the camera.

Step 3: Input all DDNS settings.



The screenshot shows the PLANET DDNS website. At the top, there is a navigation bar with the PLANET logo and links for 'PLANET Website', 'FAQ', and 'Support'. Below the navigation bar is a large banner image of a modern living room. On the left side of the banner, there is a 'Sign in' form with fields for 'ID / Email' and a password field, and a 'Sign in' button. Below the form are links for 'Forgotten Password / Create A New Account'. Below the banner, there are three product cards: 1. XRT-401F Internet Broadband Router with a 'More Info' button. 2. ICA-HM132 2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera with a 'More Info' button. 3. ICA-HM316 2 Mega-Pixel 11n Outdoor IR IP Camera with a 'More Info' button. At the bottom, there are two sections: 'Access anytime & anywhere' with a description and a 'Go!' button, and 'Support & Download' with a description. The footer contains the text 'About DDNS | Term of Usage' and 'PLANET Technology Corp. Copyright ©2012 All Rights Reserved.'

Appendix E. Configuring Port Forwarding Manually

The device can be used with a router. If the device wants to be accessed from the WAN, its IP address needs to be set up as a fixed IP address. The port forwarding or Virtual Server function of router also needs to be set up. This device supports UPnP traversal function. Therefore, user could use this feature to configure port forwarding of NAT router first. However, if user needs to configure port forwarding manually, please follow the steps below:

Manually installing the device with a router on your network is an easy 3–step procedure as follows:

1. Assign a local/fixed IP address to your device
2. Access the Router with your Web browser
3. Open/Configure Virtual Server Ports of your Router

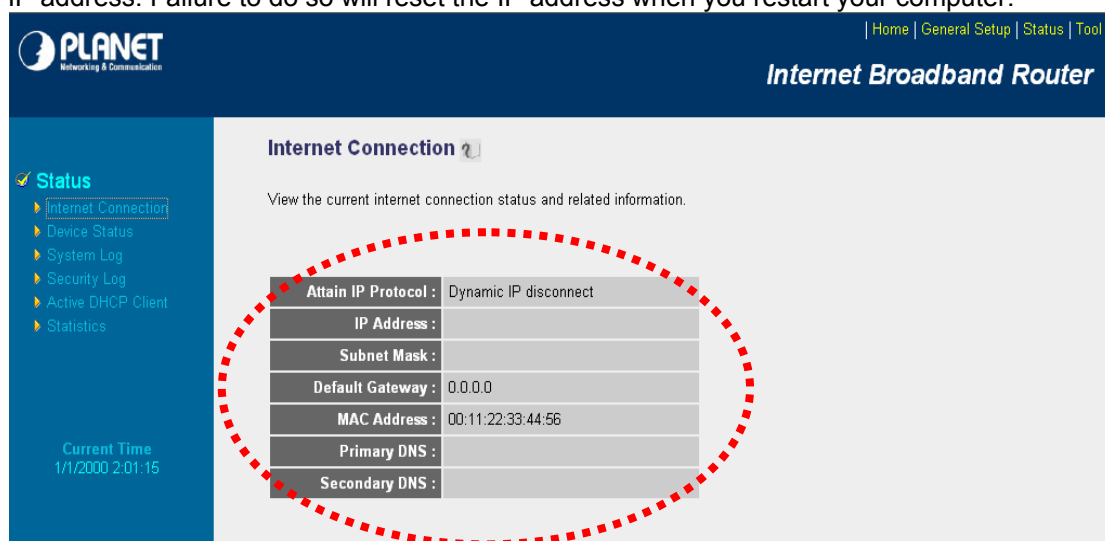
1. Assign a local/fixed IP address to your device

The device must be assigned a local and fixed IP Address that allows it to be recognized by the router. Manually setup the device with a fixed IP address, for example, *192.168.0.100*.

2. Access the Router with your Web browser

The following steps generally apply to any router that you have on your network. PLANET WNRT-620 is used as an example to clarify the configuration process. Configure the initial settings of the router by following the steps outlined in the router's **Quick Installation Guide**.

If you have cable or DSL service, you will most likely have a dynamically assigned WAN IP address. 'Dynamic' means that your router's WAN IP address can change from time to time depending on your ISP. A dynamic WAN IP address identifies your router on the public network and allows it to access the Internet. To find out what your router's WAN IP address is, go to the **Status** screen on your router and locate the WAN information for your router. As shown on the following page the WAN IP address will be listed. This will be the address that you will need to type in your web browser to view your camera over the Internet. Be sure to uncheck the **Reset IP address at next boot** button at the top of the screen after modifying the IP address. Failure to do so will reset the IP address when you restart your computer.



The screenshot shows the PLANET web interface for an Internet Broadband Router. The page title is "Internet Connection" and it provides information about the current internet connection status. A table lists the following details:

Attain IP Protocol :	Dynamic IP disconnect
IP Address :	
Subnet Mask :	
Default Gateway :	0.0.0.0
MAC Address :	00:11:22:33:44:56
Primary DNS :	
Secondary DNS :	

The IP Address field is circled in red in the original image, indicating where the WAN IP address is listed.

Your WAN IP Address will be listed here.

3. Open/set Virtual Server Ports to enable remote image viewing


The firewall security features built into the router and most routers prevent users from

accessing the video from the device over the Internet. The router connects to the Internet over a series of numbered ports. The ports normally used by the device are blocked from access over the Internet. Therefore, these ports need to be made accessible over the Internet. This is accomplished using the **Virtual Server** function on the router. The Virtual Server ports used by the camera must be opened through the router for remote access to your camera.


Follow these steps to configure your router's Virtual Server settings

- Click **Enabled**.
- Enter a unique name for each entry.
- Select **Both** under **Protocol Type (TCP and UDP)**
- Enter your camera's local IP address (e.g., **192.168.0.100**, for example) in the **Private IP** field.
- If you are using the default camera port settings, enter **80** into the **Public** and **Private Port** section and click **Add**.

A checkmark appearing before the entry name will indicate that the ports are enabled.



Note Some ISPs block access to port 80. Be sure to check with your ISP so that you can open the appropriate ports accordingly. If your ISP does not pass traffic on port 80, you will need to change the port the camera uses from 80 to something else, such as 8080. Not all routers are the same, so refer to your user manual for specific instructions on how to open ports.


Home | General Setup | Status | Tool

Internet Broadband Router

Virtual Server ?

You can configure the Broadband router as a Virtual Server so that remote users accessing services such as the Web or FTP at your local site via Public IP Addresses can be automatically redirected to local servers configured with Private IP Addresses. In other words, depending on the requested service (TCP/UDP) port number, the Broadband router redirects the external service request to the appropriate internal server (located at one of your LAN's Private IP Address).

Enable Virtual Server

Private IP	Private Port	Type	Public Port	WAN Port	Comment
<input type="text"/>	<input type="text"/>	Both	<input type="text"/>	WAN1	<input type="text"/>

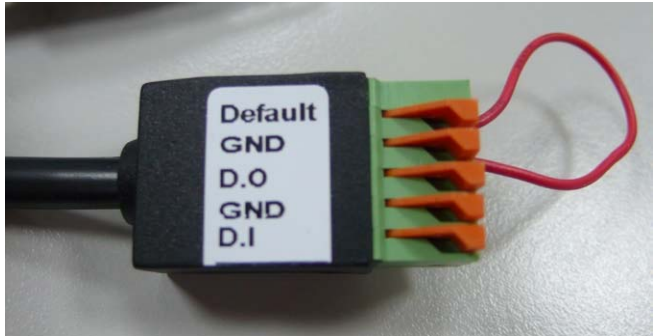
Current Virtual Server Table:

Private IP	Private Port	Type	Public Port	WAN Port	Comment	Select
192.168.0.100	80	TCP+UDP	80	WAN1	ICA-HM230	<input type="checkbox"/>

Enter valid ports in the **Virtual Server** section of your router. Please make sure to check the box on this line to enable settings. Then the device can be accessed from WAN by the router's WAN IP address.

By now, you have finished your entire PC configuration for this device.

Appendix F. Troubleshooting & Frequently Asked Questions

Features	
The video and audio codec is adopted in the device.	<p>The device utilizes H.264 and M-JPEG triple compression to provide high-quality images where H.264 is standards for video compression and M-JPEG is a standard for image compression.</p> <p>The audio codec is defined as AMR for 3GPP and G.711 for RTSP streaming.</p>
The maximum number of users that accesses the device simultaneously.	The maximum number of users is limited to 10. However, it also depends on the total bandwidth accessed to this device from clients.
Installing this device	
The network cabling is required for the device.	The device uses Category 5 UTP cable allowing 10 and/or 100 BASE-T networking.
The device will be installed and work if a firewall exists on the network.	If a firewall exists on the network, port 80 is open for ordinary data communication. The HTTP port and RTSP port need to be opened on the firewall or NAT router.
The username and password for the first time or after factory default reset	<p>Username = admin and Password = admin.</p> <p>Note that it's all case sensitivity.</p>
Forgot the username and password	<p>Follow the steps below:</p> <ol style="list-style-type: none"> 1. Remove the power and Ethernet cable. 2. Take an electronic wire, plug one side of the wire into "Default" and the other side into "GND" on the terminal block as the picture is shown below.  <ol style="list-style-type: none"> 3. Connect power to the camera again. It takes around 30 seconds to boot the camera. 4. Remove the wire and plug in the Ethernet cable after the camera finishes booting. 5. Re-login the camera by the default IP (http://192.168.0.20) and the user name and password are admin.
Forgot the IP address of the device.	Check IP address of device by using the PLANET Smart Discovery Lite program or by UPnP discovery or set the device to default by

	Reset button.
PLANET Smart Discovery Lite program cannot find the device.	<ul style="list-style-type: none"> ● Re-power the device if cannot find the unit within 1 minute. ● Do not connect device over a router. PLANET Smart Discovery Lite program cannot detect device over a router. ● If IP address is not assigned to the PC that runs PLANET Smart Discovery Lite program, then PLANET Smart Discovery Lite program cannot find device. Make sure that IP address is assigned to the PC properly. ● Antivirus software on the PC might interfere with the setup program. Disable the firewall of the antivirus software during setting up this device. ● Check the firewall setting of your PC or Notebook.
Internet Explorer does not seem to work well with the device	Make sure that your Internet Explorer is version 6.0 or later. If you are experiencing problems, try upgrading to the latest version of Microsoft's Internet Explorer from the Microsoft webpage.
PLANET Smart Discovery Lite program fails to save the network parameters.	Network may have trouble. Confirm the parameters and connections of the device.
UPnP NAT Traversal	
Cannot work with NAT router	Maybe NAT router does not support UPnP function. Please check user's manual of router and turn on UPnP function.
Some IP cameras are working while others failed	Maybe too many IP cameras have been installed on the LAN, and thus NAT router is out of resource to support more cameras. You could turn off and on NAT router to clear out of date information inside router.
Accessing this device	
Cannot access the login page and other web pages of the Network Camera from Internet Explorer	<ul style="list-style-type: none"> ● Maybe the IP address of the Network Camera is already being used by another device or computer. To confirm this possible problem, disconnect the Network Camera from the network first, and then run the ping utility to check it out. ● Maybe it's the network cable. Try correcting your network cable and configuration. Test the network interface by connecting a local computer to the Network Camera via a crossover cable. ● Make sure the Internet connection and setting are OK. ● Make sure the IP address of Internet Explorer you entered is correct. If the Network Camera has had a dynamic address, it may have changed since you last checked it. ● Network congestion may prevent the web page from appearing quickly. Wait for a while. <p>The IP address and Subnet Mask of the PC and Network Camera must be in the same class of the private IP address on the LAN.</p> <ul style="list-style-type: none"> ● Make sure the http port used by the Network Camera, default=80, is forwarded to the Network Camera's private IP address. ● The port number assigned in your Network Camera might not be available via Internet. Check your ISP for available port.

	<ul style="list-style-type: none"> ● The proxy server may prevent you from connecting directly to the Network Camera. You are advised not to use the proxy server. ● Confirm that Default Gateway address is correct. ● The router needs Port Forwarding feature. Refer to your router's manual for details. ● Packet Filtering of the router may prohibit access from an external network. Refer to your router's manual for details. ● Access the Network Camera from the Internet with the global IP address of the router and port number of Network Camera. ● Some routers reject the global IP address to access the Network Camera on the same LAN. Access with the private IP address and correct port number of Network Camera. ● When you use DDNS, you need to set Default Gateway and DNS server address. ● If it's not working after following the above procedure, reset Network Camera to default setting and install it again.
<p>Image or video does not appear on the main page.</p>	<ul style="list-style-type: none"> ● The first time the PC connects to Network Camera, a pop-up Security Warning window will appear to download ActiveX Controls. When using Windows XP, or Vista, log on with an appropriate account that is authorized to install applications. ● Network congestion may prevent the Image screen from appearing quickly. You may choose lower resolution to reduce the required bandwidth.
<p>How to check whether the device's ActiveX is installed on your computer</p>	<p>Go to C:\Windows\Downloaded Program Files and check to see if there is an entry for the file "Web Watch2 Control". The status column should show "Installed". If the file is not listed, make sure your Security Settings in Internet Explorer are configured properly and then try reloading the device's home page. Most likely, the ActiveX control did not download and install correctly. Check your Internet Explorer security settings and then close and restart Internet Explorer. Try to browse and log in again.</p>
<p>Internet Explorer displays the following message: "Your current security settings prohibit downloading of ActiveX controls".</p>	<p>Set up the IE security settings or configure the individual settings to allow downloading and scripting of ActiveX controls.</p>
<p>The device works locally but not externally.</p>	<ul style="list-style-type: none"> ● Might be caused from the firewall protection. Check the Internet firewall with your system or network administrator. The firewall may need to have some settings changed in order for the device to be accessible outside your LAN. ● Make sure that the device isn't conflicting with any other web server running on your LAN. ● Check the configuration of the router settings to allow the device to be accessed outside your local LAN. ● Check the bandwidth of Internet connection. If the Internet bandwidth is lower than target bit rate, the video streaming will not work correctly.
<p>The unreadable characters are</p>	<p>Use the operating system of the selected language. Set the</p>

displayed.	Encoding or the Character Set of the selected language on the Internet Explorer.
Frame rate is slower than the setting.	<ul style="list-style-type: none"> ● The traffic of the network and the object of the image affect the frame rate. The network congestion causes frame rate slower than the setting. ● Check the bandwidth of Internet connection. If the Internet bandwidth is lower than target bit rate, the video streaming will not work correctly. ● Ethernet switching hub can smooth the frame rate.
Image Transfer on e-mail or FTP does not work.	<ul style="list-style-type: none"> ● Default Gateway and DNS server address should be set up correctly. ● If FTP does not work properly, ask your ISP or network administrator about the transferring mode of FTP server.
Video quality of the device	
The focus on the Camera is bad.	The lens is dirty or dust is attached. Fingerprints, dust, stain, etc. on the lens can degrade the image quality.
The color of the image is poor or strange.	<ul style="list-style-type: none"> ● Adjust White Balance. ● To ensure the images you are viewing are the best they can be, set the Display property setting (color quality) to 16bit at least and 24 bit or higher if possible within your computer. ● The configuration on the device image display is incorrect. You need to adjust the image related parameters such as brightness, contrast, hue and sharpness properly.
Image flickers.	<ul style="list-style-type: none"> ● If the object is dark, the image will flicker. Make the condition around the Camera brighter.

Appendix G. Micro SD Card Compatibility

The following is the Micro SD Card recommended:

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
	SDHC	class10	4GB
	SDHC	class10	8GB
	SDHC	class10	16GB
	SDHC	class10	32GB
SanDisk	SDHC	class4	4GB
	SDHC	class4	8GB
	SDHC	class4	16GB
	SDHC	class4	32GB