

# User's Manual

## 3 Mega-Pixel Vandal Proof Fish-Eye IP Camera

▶ ICA-8350



---

**Copyright**

Copyright © 2013 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. (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 and have to collect such WEEE separately.

**Revision**

User's Manual for PLANET 3 Mega-Pixel Vandal Proof Fish-Eye IP Camera  
Model: ICA-8350  
Rev: 1.00 (March.2013)  
Part No. EM-ICA8350

---

## Table of Content

Chapter 1. Product Introduction.....	6
1.1. Package Contents .....	6
1.2. Product Description.....	6
1.3. Features .....	10
1.4. Product Specification .....	11
Chapter 2. Hardware Interface .....	13
2.1. Physical Description.....	13
2.1.1. Identification of ICA-8350 connector cable .....	13
2.2. Hardware Installation .....	19
2.2.1. Physical Installation .....	19
2.2.2. Network Installation.....	20
Chapter 3. Initial Utility Installation .....	22
3.1. Preparation .....	25
3.1.1. Search and View by PLANET IP Wizard II.....	25
3.2. Using UPnP of Windows XP or Vista or Win7 .....	29
Chapter 4. Installation Guide.....	29
4.1. System Requirements .....	30
4.2. Before You Begin.....	30
4.2.1. Connecting to Internet Camera.....	31
Chapter 5. Web Configuration for Live View.....	32
5.1. Live View.....	33
5.2. ActiveX Control .....	36
5.2.1. Digital Zoom .....	37
5.2.2. Snapshot.....	37
5.2.3. Record .....	38
5.2.4. Volume .....	38
5.2.5. About .....	39
Chapter 6. Network Configuration .....	40
6.1 Network setting .....	40
6.1.1. Network.....	40
6.1.2. IPv6 function .....	42
6.1.3. HTTPS .....	42
6.1.4. DDNS server.....	43
6.1.5. PPPoE .....	45
6.1.6. Streaming .....	46
6.1.7. UPnP .....	47
6.1.8. Bonjour.....	48
6.1.9. IP Filter.....	48
6.1.10. IP Notification.....	49
6.2. Adjust Camera Configuration.....	51
6.2.1. Picture .....	51
6.2.2. Privacy Mask.....	54
6.3. System .....	55
6.3.1. System .....	55

6.3.2. Date & Time .....	56
6.3.3. Maintenance .....	57
6.4. Video.....	59
6.4.1. Common .....	59
6.4.2. Overlay Image .....	60
6.4.3. Video Profile .....	62
6.4.4. ROI .....	64
6.4.5. AOI.....	65
6.5. Audio Configuration.....	66
6.6. User Privilege Access Configuration .....	67
6.7 Protocol .....	67
6.8. E-Mail Configuration.....	70
6.9. Event Detection .....	71
6.9.1 Motion Detection .....	71
6.10. Storage Configuration.....	74
6.10.1. SD Card.....	74
6.10.1. SAMBA Server .....	75
6.11. Continuous Recording .....	76
6.12. Recording List.....	77
6.12.1. Recording List.....	77
6.12.2. Continuous Recording List .....	77
6.13. Event Server Configuration .....	78
6.13.1. FTP Server.....	78
6.13.2. TCP Server .....	79
6.13.3. HTTP Server .....	80
6.13.4. SAMBA Server .....	81
6.14. Event Schedule Configuration.....	82
6.15. Record Configuration.....	86
6.16. Port Status .....	87
Chapter 7. PLANET DDNS Application .....	88
Chapter 8. Alarm I/O Connector .....	89
Chapter 9. PING IP Address.....	92
Chapter 10. Bandwidth Estimation .....	93
Chapter 11. Configure Port Forwarding Manually.....	94
Chapter 12. Power Line Frequency .....	98
Chapter 13. 3GPP .....	100
Chapter 14. Troubleshooting & Frequently Asked Questions .....	101

## Chapter 1. Product Introduction

### 1.1. Package Contents

The package should contain the followings:

- IP Camera Unit x 1
- Power Adapter x 1
- Screw package x 1
- 2 pin terminal block x 1
- User's Manual CD-ROM x 1
- Quick Installation Guide x 1

**NOTE:**

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 Internet Camera packet will cause damage and void the warranty for this product.

### 1.2. Product Description

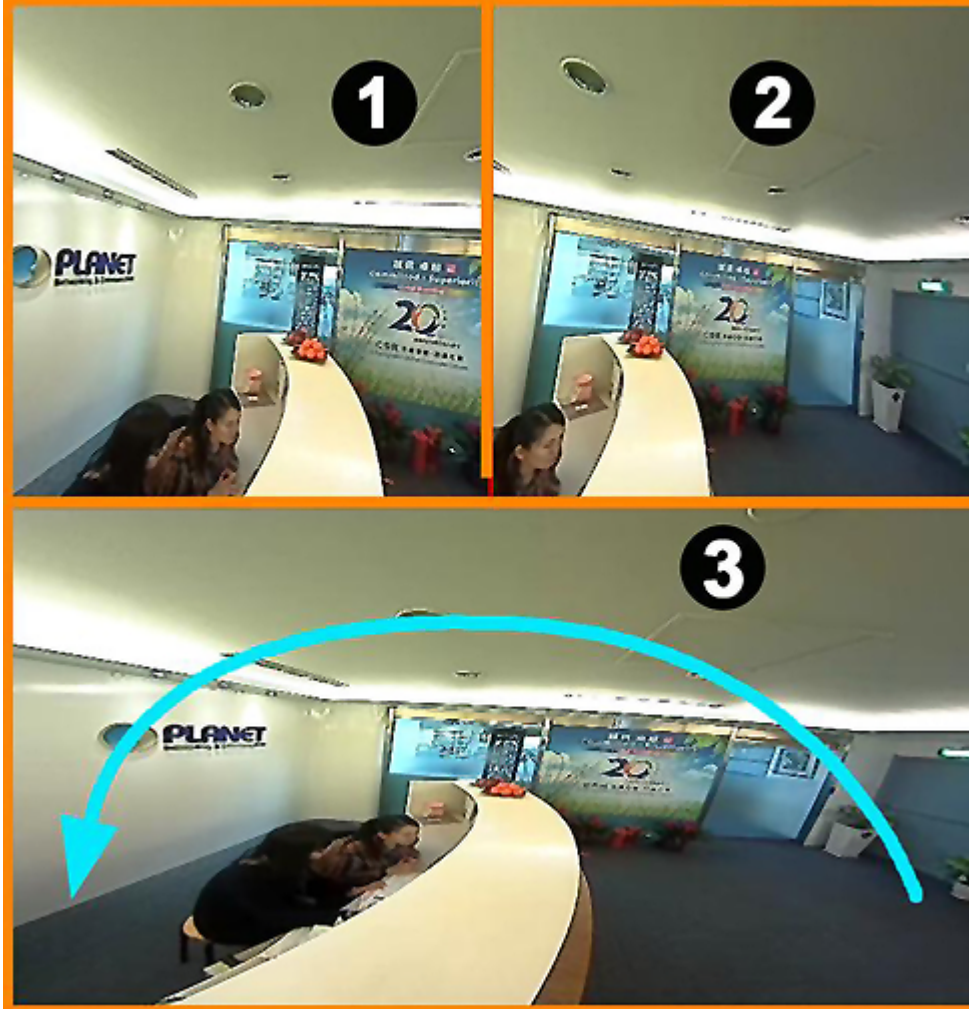
#### **Exceptional surveillance with outdoor-ready 3 Mega-Pixel Panoramic Camera**

The PLANET ICA-8350 Network Camera with 360 degree panoramic wide angle view without blind spot 180° panoramic view (wall mount) or 360° surround view (ceiling/floor/table mount). This camera supports H.264, MPEG-4, and JPEG compression formats and delivers excellent picture quality in up to 1536 x 1536 pixels at 20 frames per second (fps). Incorporating 3.4MP-resolution sensor, which is specially designed for surveillance applications, this camera provides high quality images and panorama function with quad view enables images from four different angles to display simultaneously for monitoring and recording. The IP66-rated and Vandal Proof housing protects the camera body against rain and dust and ensures operation under extreme weather conditions, which makes it an ideal solution for outdoor applications, e.g. surveillance of buildings, hospital / bank/ hotel lobby, garages, hallway, stores or offices so customers do not need to install multiple IP cameras and thus can save lots of installation and maintenance cost.



**See More of What You Value with 360° Surround View**

Furthermore, the ICA-8350 is a fisheye camera that allows you to monitor all angles of a location using just one camera and thus save lots of traditional mechanical Pan/Tilt maintenance cost. The distorted hemispherical image of the fisheye camera will be converted into the conventional rectilinear projection. Without installing any software, you can watch live view and utilize functions such as motion detection and Camera tampering through the Web interface using an IE browser. Distortion correction fixes the camera video so you can use ePTZ to zoom in, zoom out, and pan across your camera's video and survey a large area easily.

**ICA-8350: One camera - Three simultaneous views**

**Day & Night functionality**

The ICA-8350 features an automatic, removable infrared-cut filter, which enables the camera to provide color video when there is sufficient light, and black/white video in dark conditions. The camera is able to maintain clear images 24 hours a day.

**Exceptional Image quality**

Together with powerful image processing attributes like Wide Dynamic Range and 3D Digital Noise Reduction (3DNR) technology, the camera is able to filter the intense backlight surrounding a subject and remove noises from video signal. The result is that an extremely clear and exquisite picture quality can be produced even under any challenging lighting conditions.



**Camera tampering and audio detection**

Provided with three individually configurable motion detection zones, the camera can record video or trigger alarms or alerts when motion is detected in user-specified areas of the camera image. Also, the camera's built-in microphone enables it to hear what the video cannot see and to trigger the audio detection alarm when sounds like screams, glass breaking, etc., are detected.

**Advanced event management**

The ICA-8350 also supports a number of advanced features that give the camera increased flexibility and capabilities, including AV out for perform the two-way audio function, RS485 for connectivity to an optional pan/tilt enclosure which effectively adds pan/tilt functionality and inputs/outputs for connecting external devices such as door sensors and relays to activate light or close doors.

**Flexible installation and Power functionality**

The ICA-8350 incorporates Power over Ethernet supplies power to the camera via the network, eliminating the need for power cables and reducing installation costs. With other advanced features such as the Gigabit Ethernet Transmission, giving a user the utmost in bandwidth flexibility and storage efficiency. The ICA-8350 is ONVIF-compliant and therefore interoperable with other manufacturer's products. In addition, the ICA-8350 seamlessly integrates with the 64-CH central management software, providing advanced monitoring and video management features; the ICA-8350 is indisputably the top choice for reliable and high performance panoramic surveillance.

## 1.3. Features

### ➤ Camera

- High quality 3Mega-Pixel CMOS image sensor
- 360° Fish-Eye panoramic wide angle view
- 11 different 360°/180° video modes including digital PTZ function
- IP66 for outdoor application

### ➤ Video / Audio

- H.264, MPEG-4 and M-JPEG Tri-Codec
- Day/Night switch with ICR (IR-cut Filter Removable)
- 2-Way audio support with enhanced audio quality
- Max. Resolution 1536 x 1536 at 22fps

### ➤ Network and Configuration

- Equipped with Gigabit Ethernet port
- Auto MDI/MDI-X supported
- Compliant with IEEE 802.3af PoE interface for flexible deployment
- Supports IPv6 protocol in addition to the standard IP protocol version 4 (IPv4)
- RTSP / UPnP / 3GPP / HTTPS protocols selectable

### ➤ Easy Installation & Management

- ONVIF compliant
- Built-in Samba client for NAS
- 3GPP for 3G mobile remote applications
- RS-485 interface for P/T scanner control
- Digital Input / Output for integration with sensors and alarms
- Cam Viewer 3 Central management software supported

## 1.4. Product Specification

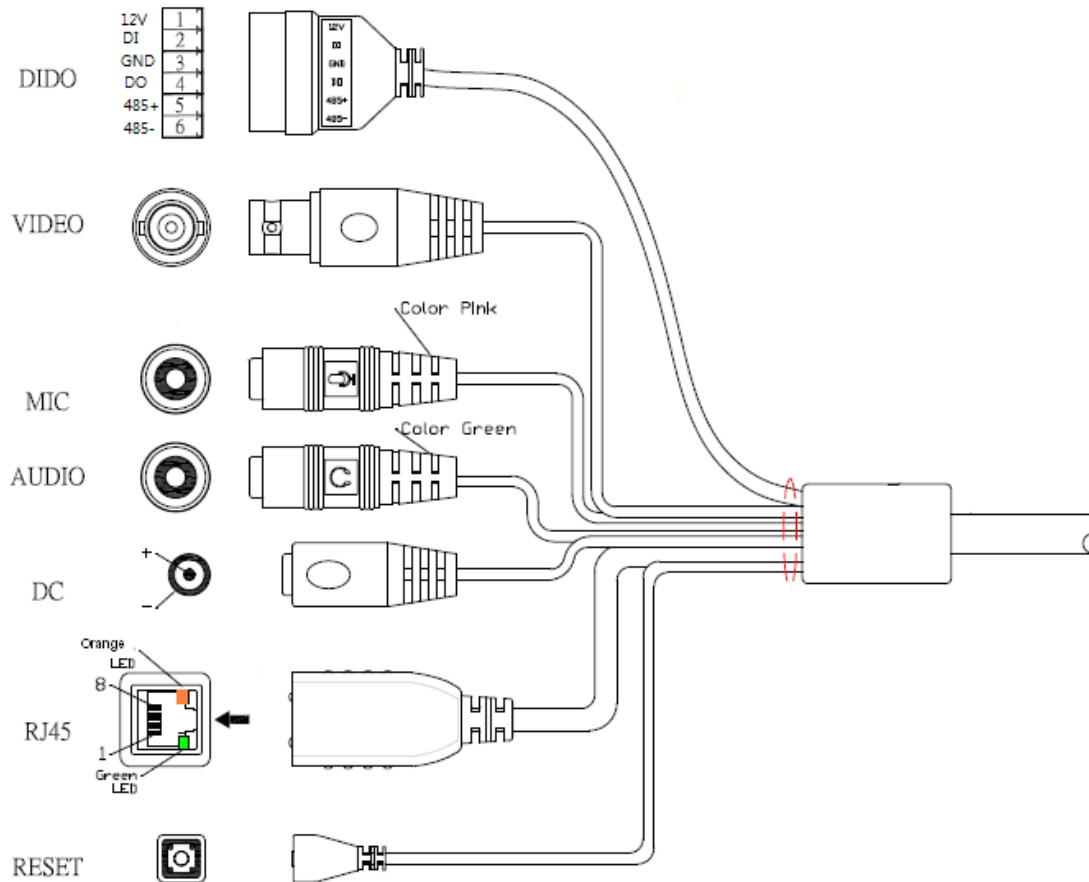
<b>Product</b>	ICA-8350 <b>3Mega-Pixel Vandal Proof Fish-Eye IP Camera</b>
<b>Camera</b>	
<b>Image Device</b>	1/2.8" 3.4Mega-Pixel progressive scan CMOS sensor
<b>Lens</b>	FOV=180 +/- 5°(D/H/V), F=2.0, f=1.25mm Mechanical IR Cut Filter Angle of view : 360 degree view angle
<b>Min Illumination</b>	0.5 Lux @ F2.0
<b>Effective Pixels</b>	1536 x 1536 pixels
<b>Video</b>	
<b>Video Encoder</b>	H.264 / M-JPEG
<b>Video Resolution</b>	H.264 1536 x 1536 / 1280 x 1280 / 768 x 768 / 384 x 384 M-JPEG 1536 x 1536 / 1280 x 1280 / 768 x 768 / 384 x 384
<b>Frame Rate</b>	Up to 22fps for all resolutions
<b>Image Setting</b>	AE, AWB 3D Noise reduction Color, brightness, sharpness, contrast Mirror/Flip 7 Privacy Masks Text, time and date overlay
<b>Streaming</b>	Simultaneously multi-profile streaming Streaming over UDP, TCP, or HTTP M-JPEG streaming over HTTP (server push) Controllable frame rate and bandwidth Constant and variable bit rate (H.264) ROI AOI
<b>Region of Interest</b>	2 windows with selectable resolution and codec max region size 640x352
<b>Rate Control</b>	CBR (Constant Bit Rate) VBR (Variable Bit Rate) EVB (Enhanced Variable Bit Rate)
<b>UI Layout</b>	<ul style="list-style-type: none"> <li>▪ 1O - One Original fish-eye view</li> <li>▪ 1P - One Panoramic view</li> <li>▪ 1R - One Regional view</li> <li>▪ 2P - Two Panoramic views</li> <li>▪ 1O3R - One Original and three Regional views</li> <li>▪ 4R - Four Regional views</li> <li>▪ 1P2R - One Panoramic and two Regional views</li> <li>▪ 1P3R - One Panoramic and three Regional views</li> <li>▪ 4R PRO - Four Regional views interactively displayed when the field of view changes in any of the views</li> </ul>
<b>Audio</b>	
<b>Audio Streaming</b>	2-Way Audio
<b>Audio Compression</b>	RTSP: G.711 64kbps, G.726 32kbps
<b>Microphone</b>	External microphone input
<b>Audio Output</b>	Adjustable audio output gain

Network and Configuration	
Network Standard	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T
Network Protocol	IPv4, IPv6, TCP/IP, UDP, HTTP, HTTPS, SMTP, FTP, NTP, DNS, DDNS, DHCP, ARP, Bonjour, UPnP, RTSP, RTP, RTCP, IGMP, PPPoE, 3GPP, ICMP, Samba
Security	Password protection, IP address filtering, HTTPS encrypted data transmission, user access log
Users	20 simultaneous unicast users
System Integration	
SDK	Open API for software integration ONVIF
Alarm Triggers	Intelligent video motion detection and external input
Alarm Events	File upload via FTP, Samba, SD card or email Notification via email, HTTP, and TCP External output activation Audio alerting output Pre and post alarm buffering
Environment	
Power Requirement	12V DC, 1A IEEE 802.3af Power over Ethernet Class 3
Power Consumption	7W max.
Operating Temperature	-20 ~ 50 Degree C
Operating Humidity	20 ~ 80% (non-condensing)
Weight (includes LENS)	817g
Dimension (W x H)	140 x 92.7 mm
Emission	CE, FCC
Connectors	10/100/1000 RJ-45 DC power jack Terminal block for 1 alarm input and 1 output RS-485 interface for pan/tilt scanners control External MIC input Audio out Composite video output (Max. resolution: D1 720 x 480 pixel) Micro SD card (Max 32GB, Class 6) Factory default reset

## Chapter 2. Hardware Interface

### 2.1. Physical Description

#### 2.1.1. Identification of ICA-8350 connector cable



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

It's for connections to 10Base-T Ethernet, 100Base-TX, or 1000Base-TX Ethernet cabling. This Ethernet port built N-Way protocol can detect or negotiate the transmission speed of the network automatically. Please use Category 5 or better cable to connect the Network Camera to an Ethernet network switch or hub.

In the LAN socket, there are two LEDs embedded:

##### **LAN LED (green color)**

This LED will be flashing while network accessing via Ethernet.

##### **Power LED (orange color)**

This LED is used to indicate whether DC power is on or not.

## **2. RS-485: Connect to a local keyboard controller.**

DI/ DO: Connect to sensor in and alarm out devices

Cable for I/O connectors:

Name	Number	Function
12VDC	1	DC 12V (50mA maximum)
DI	2	Digital signal input
GND	3	GND
DO	4	Digital signal output
485+	5	RS485 data +
485-	6	RS485 data -

## **3. Factory Default Reset**

This button is used to restore the all factory default settings. Sometimes restarting the device will make the system back to a normal state. However, if the system still got problems after restart, user can restore the factory default settings and install it again.

Restore the device:

1. While the Camera is ready and then press the button down continuously.
2. Hold the button at least 5 seconds and release it. Then the device has been restored to default settings and reboot again.

**NOTE:** Restoring the factory default setting will lose the all previous settings included IP address forever. User needs to run the IPWizard II program to search the device and configure it to let the device work properly again.

## **4. DC-in Jack**

The input power is 12VDC.

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

## **5. MIC in (audio in)**

Connect a microphone to the network camera.

## **6. Line out (audio out)**

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

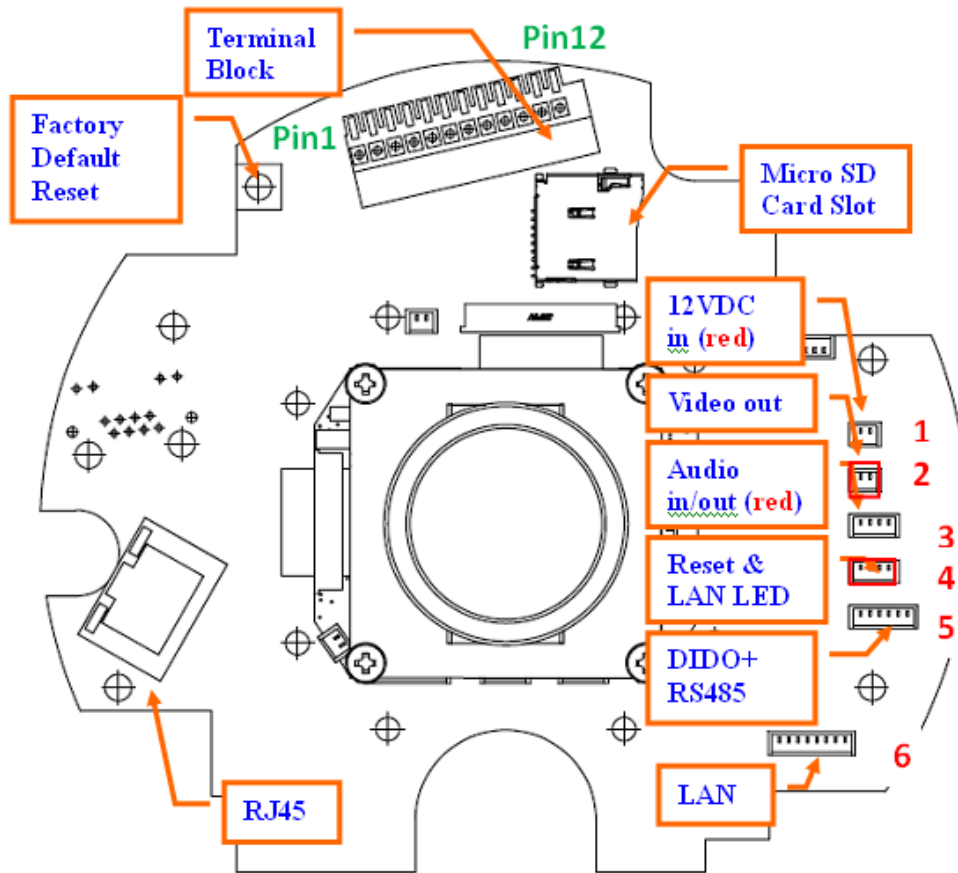
## **7. Video out (BNC connector)**

The Network Camera also provides composite video output. The video output

function is only for easy installation to check view angle and focus. The output is not a Mega-pixel resolution. Furthermore, the video output is off by default. To turn on video, please refer to Setting\Camera\Picture chapter.

## Connector board:

**NOTE:** That to cabling this camera by type of connector board, firstly, user must remove the attached “connector cable” from wafer 1~ 6 shown as below:



### 1. RJ45 LAN socket:

The LAN socket is a RJ-45 connector for connections to 10Base-T Ethernet, 100Base-TX, or 1000Base-TX Ethernet cabling. This Ethernet port built N-Way protocol can detect or negotiate the transmission speed of the network automatically. Please use Category 5 or better cable to connect the Network Camera to an Ethernet network switch or hub.

In the LAN socket, there are two LEDs embedded:

#### **LAN LED (green color)**

This LED will be flashing while network accessing via Ethernet.

#### **Power (orange color)**

This LED is used to indicate whether DC power is on or not. In addition, this LED will be flashing while the wireless accessing of the Camera.

**2. Terminal block:**

Pin definition:

Pin	Name	Function
1	12VDC in	DC 12V power input
2	MIC in-	External MIC input-
3	MIC in+	External MIC input+
4	Audio out+	
5	Audio out-	
6	Video out	Composited video output
7	12VDC out	DC 12V output (50mA maximum)
8	DI	Digital signal input
9	GND	Digital ground
10	DO	Digital signal output
11	RS485+	RS485 data +
12	RS485-	RS485 data -

**12VDC in & Power GND**

The input power is 12VDC. **Note** that supply the power to the Network Camera with the power adapter included in package.

**MIC in (audio in)**

Connect an external microphone to the camera.

**Audio out +/-**

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

**Video out**

Connect a TV monitor to the camera. User can check the focus/zoom and view angle of the camera.

**12VDC out**

The output power is 12VDC. This is used to support DI/DO devices. The output power is 12VDC/50mA maximum.

**DI/GND/DO/RS485**

Interface of Digital input/output and RS485

**3. Factory Default Reset**

This button is used to restore the all factory default settings. Sometimes restarting the device will make the system back to a normal state. However, if the system still got problems after restart, user can restore the factory default settings and configure it again.

Restore the device:

- (i) Press the button down continuously.
- (ii) Hold the button at least 5 seconds and release it. Then the device has

---

been restored to default settings and reboot again.

**Note:**

**NOTE:** Restoring the factory default setting will lose the all previous settings included IP address forever. User needs to run the IPWizard II program to search the device and configure it to let the device work properly again.

**4. Micro SD Card Slot**

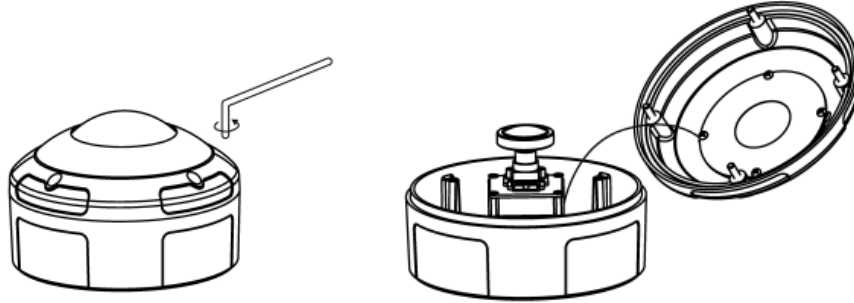
User can insert a micro SD card into this slot for recording.

**NOTE:** In case, you want to use the attached cable to connect this camera again, please check and plug the cable to wafer 1~6 properly and carefully.

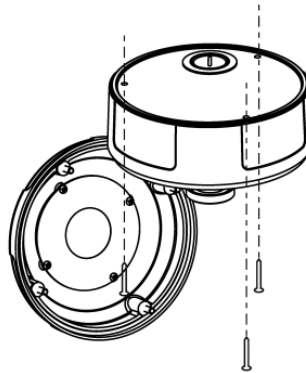
## 2.2. Hardware Installation

### 2.2.1. Physical Installation

1. Use the provided L-wrench; loosen the tamper-resistant housing cover (with screws still attached on the cover). The unit has a factory installed side conduit entry and one may adjust the cables to back conduit entry according to installation requirement.

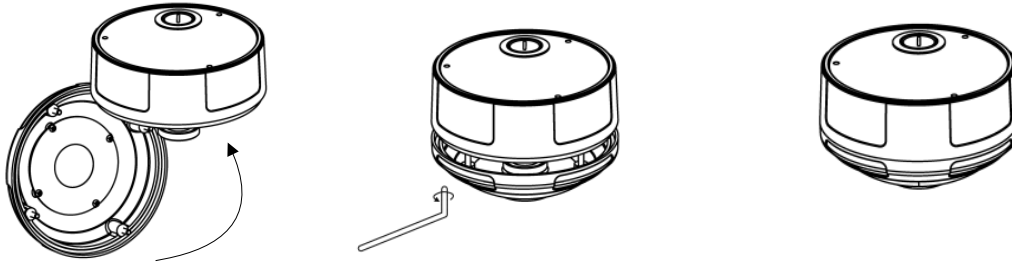


2. Set the mounting base onto the wall or ceiling and center it over the mounting hole, using the supplied three retaining screws to secure the main body.



3. Set the proper image by rotating the camera body and set the focus by turning the lens to the left or right direction. You can connect video output cable (BNC) to a TV monitor. Once the picture appeared on the monitor, and then adjusts the focus of the lens to obtain the best clear picture.

4. When the camera focus adjustment has been completed, use the provided L-wrench to fasten the tamper-resistant housing to the main body.



### 2.2.2. Network Installation

#### 1. Connect an Ethernet cable

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

**NOTE:** If there has an IEEE802.3af PoE switch in your network, you can connect the camera LAN cable to this PoE switch to obtain power. The power adapter is unnecessary when Internet camera is connected to a PoE switch.

#### 2. Attach 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. The power adapter is unnecessary when Internet camera is connected to a PoE switch. Otherwise, the product may be damaged when Internet camera is connected to a PoE switch and power adapter simultaneously.

#### 3. Attach BNC connector

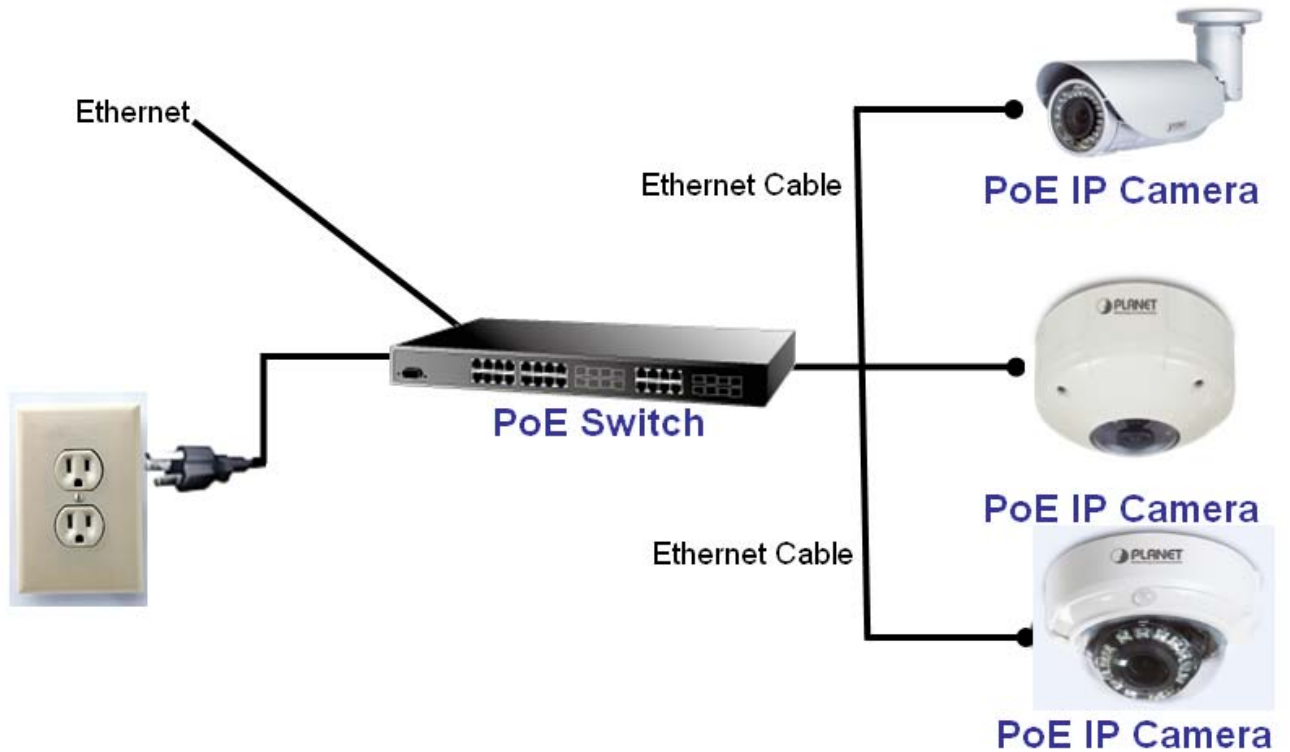
Connect the video BNC connector to a monitor set if necessary check camera viewing angle and focus.

#### 4. Attach Speaker to camera (option)

If user needs not only video stream but also audio stream, then the speaker should be attached to camera.

## 5. PoE (Power Over Ethernet)

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



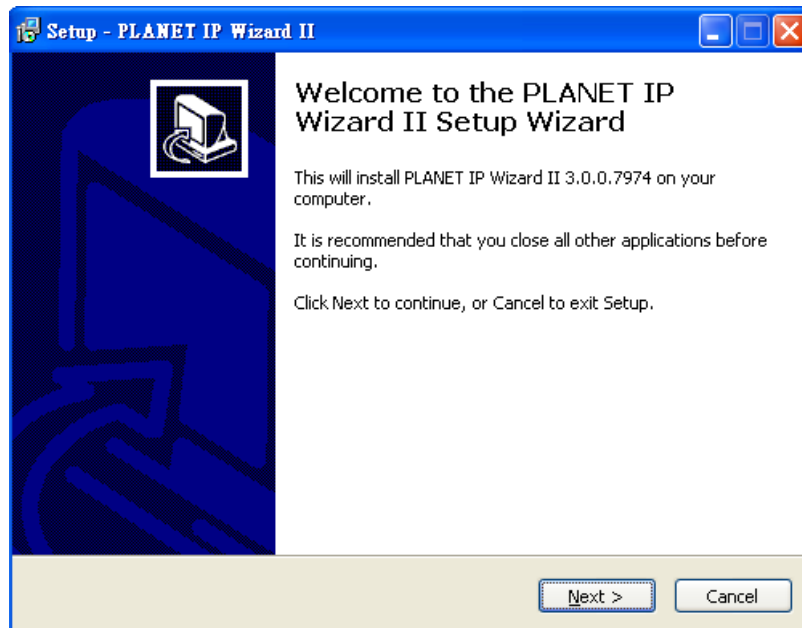
## Chapter 3. Initial Utility Installation

This chapter shows how to quick set up your IP camera. The camera is with the default settings. However to help you find the networked camera quickly the windows utility PLANET IP Wizard II can search the cameras in the network that shall help you to configure some basic setting before you started advanced management and monitoring.

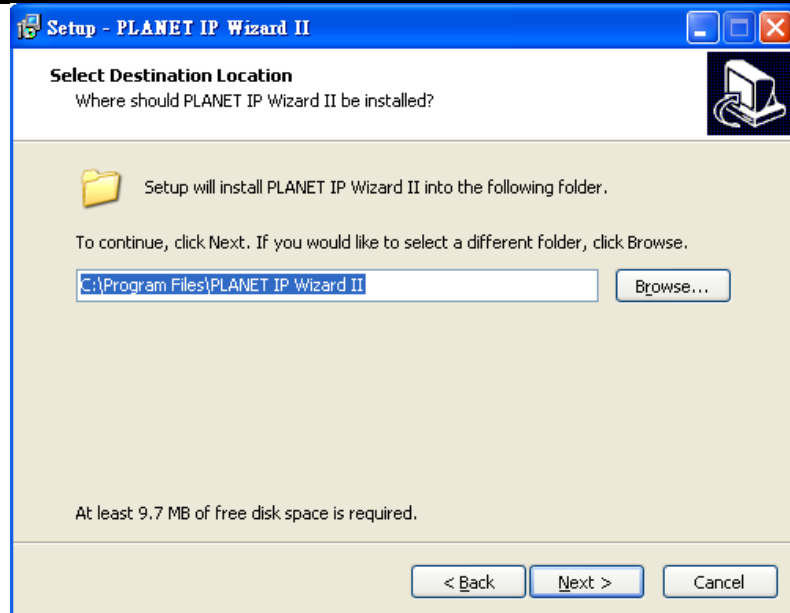
1. Insert the bundled CD into the CD-ROM drive to launch the auto-run program. Once completed, a welcome menu screen will appear.
2. Click the “IP Wizard II” hyperlink; you will see the dialog box as below.

**NOTE:** If the welcome screen does not appear, click “Start” at the taskbar. Then, select “Run” and type “D:\Utility\IPWizard II\setup.exe”, assume D is your CD-ROM drive.

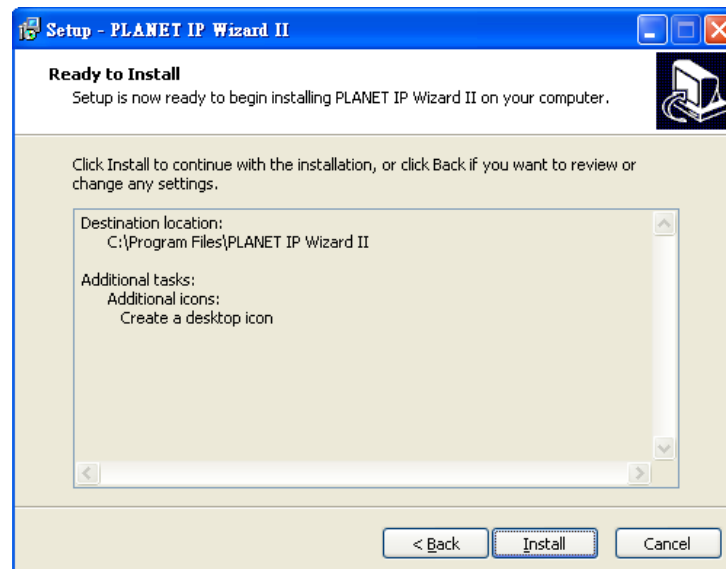
3. The “Welcome to the InstallShield Wizard for PLANET IP Wizard II” prompt will display on the screen and click “**Next**” to continue.



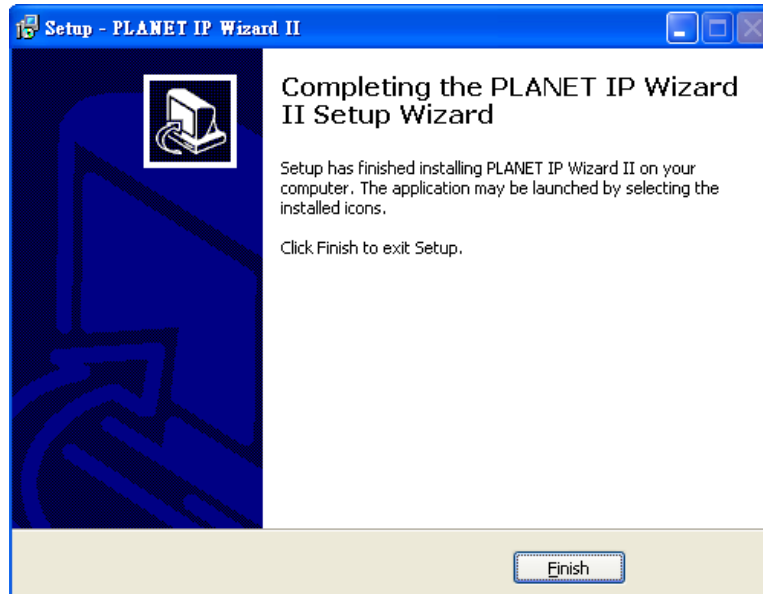
4. Please click “**Next**” to install with original settings, or you may click “**Change...**” button to modify the install folder then press “Next” to continue.



5. Please click **"Install"** to start the installation.



6. Please click **“Finish”** to complete the installation and launch program immediately.



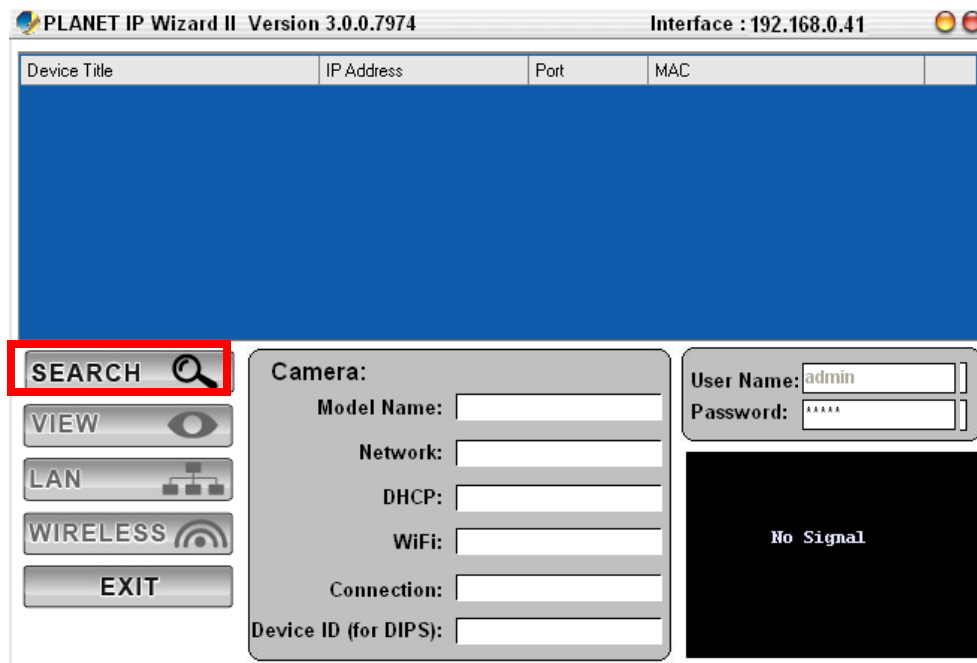
## 3.1. Preparation

When you installed the Internet Camera on a LAN environment, you may execute PLANET IP Wizard II to discover camera's IP address and set up related parameters in the camera.

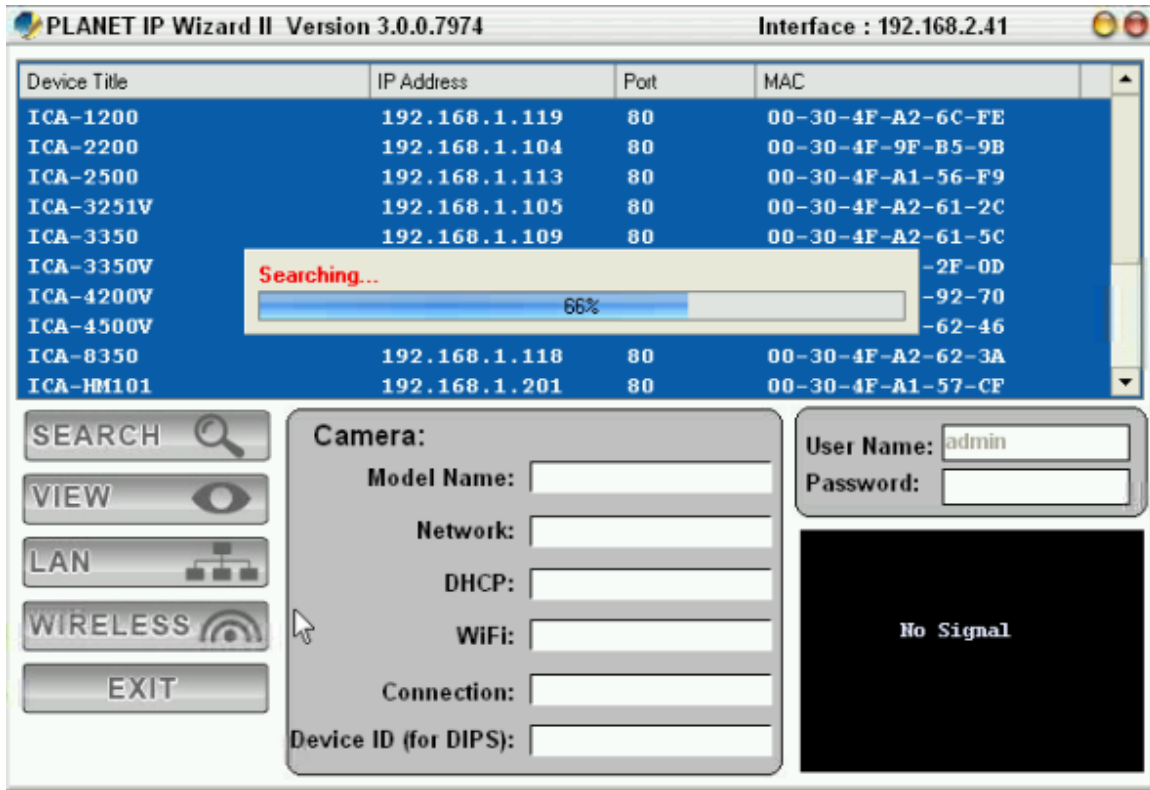
### 3.1.1. Search and View by PLANET IP Wizard II

When you installed the Internet Camera on a LAN environment, you have two easy ways to search your cameras by PLANET IP Wizard II or UPnP discovery. Here is the way to execute PLANET IP Wizard II to discover camera's IP address and set up related parameter in a camera.

#### ✓ Search



When launch the Planet IP Wizard II, a searching windows will pop up. Planet IP Wizard II is starting to search Internet Cameras on the LAN. The existed devices will be listed as below.





### ✓ View


If Planet IP Wizard II finds Internet Camera, View button will be available. Please select the camera you want to view and click the View button. Then you could see the Video from camera directly. Furthermore you could double click the left button of mouse to link to the Internet Camera by browser.


PLANET IP Wizard II Version 3.0.0.7974 Interface : 192.168.0.41

Device Title	IP Address	Port	MAC
ICA-8350	192.168.0.20	80	00-30-4F-A2-62-3A

SEARCH 

**VIEW** 

LAN 

WIRELESS 

EXIT

**Camera:**

Model Name: ICA-8350

Network: Wired

DHCP: OFF


WiFi: Ethernet Only

Connection: Not Connected

Device ID (for DIPS): N/A

User Name: admin


Password: \*\*\*\*\*





In case you want to change the IP related parameters of wired interface, please select the Internet Camera you want to configure and click the LAN button. Relative settings will be carried out as below.


PLANET IP Wizard II Version 3.0.0.7974 Interface : 192.168.0.41

Device Title	IP Address	Port	MAC
ICA-8350	192.168.0.20	80	00-30-4F-A2-62-3A

SEARCH 

VIEW 

**LAN** 

WIRELESS 

EXIT

**LAN:**

Network: ☒ Static IP ☐ DHCP IP

IP Address: 192.168.0.20

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

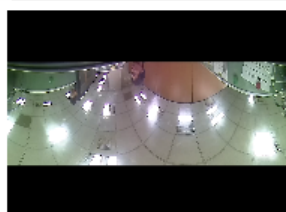
DNS1: 168.95.1.1

DNS2: 168.95.1.2


<< >>

User Name: admin

Password: \*\*\*\*\*





In case, you do not want to change username and/or password, then just click “**Submit**” button to perform your setting accordingly. Click “<<” button will go back to previous page.  
If you like to change username and/or password of the device, just click the check button. Then, the related fields will show up as below.





Interface : 192.168.0.41

Device Title	IP Address	Port	MAC
ICA-8350	192.168.0.20	80	00-30-4F-A2-62-3A

SEARCH 

VIEW 

LAN 

WIRELESS 

EXIT

User:


☐ Change Password

<<

Submit

User Name:

Password:



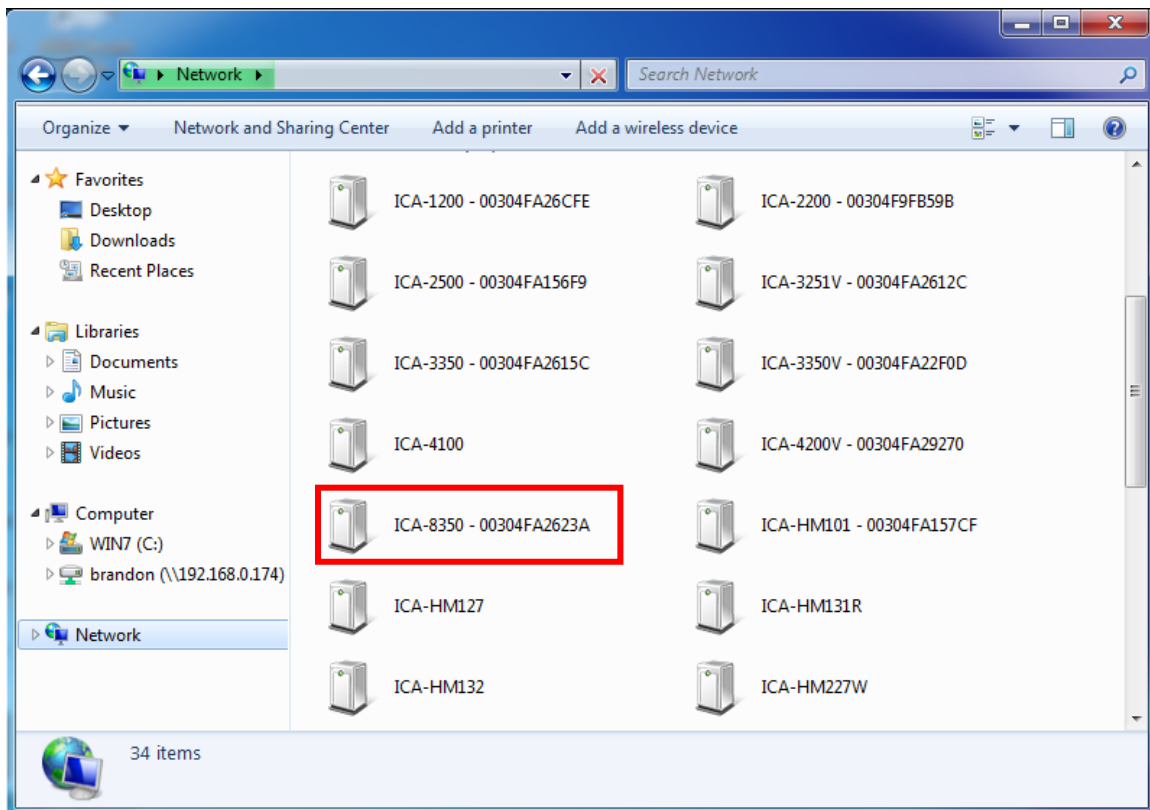
After keying in new username and password, click “**Submit**” button to perform your setting accordingly. Click “<<” button will go back to previous page.

### 3.2. Using UPnP of Windows XP or Vista or Win7

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.

**NOTE:** Please notice that MS Windows 2000 does not support UPnP feature.

To discover your device, go to your Computer and click Network.



Click the targeted Device. Then Internet Explorer will connect to this IP Camera automatically.

## Chapter 4. Installation Guide

### 4.1. System Requirements

The Internet Camera can be monitoring on all of Windows operating system that suggest with system requirement below in order to got better video performance.

Network Interface	10/100MBase-TX Ethernet
Monitoring System	Recommended for Internet Explorer 9.0 or later
System Hardware	<ul style="list-style-type: none"><li>· CPU: Intel® Core™ i5 Processor or faster</li><li>· Memory Size : 2GB or more</li><li>· VGA card resolution : 1920 x 1080 or higher</li><li>· VGA card memory : 1GB or above</li></ul>

**NOTE:** Please notice that MS Windows 2000 does not support UPnP feature.

1. The listed information is minimum system requirements only. Actual requirement will vary depending on the nature of your environment.
2. The ICA-8350 series can be managed by PLANET IP Wizard II if you want to configure more detail information and settings of PLANET IP Wizard II software please refer to the CD-ROM folder "D:\Utility\IPWizardII\setup.exe", assume D is your CD-ROM drive.

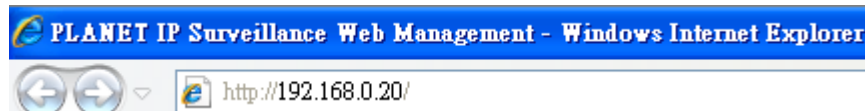
### 4.2. Before You Begin

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

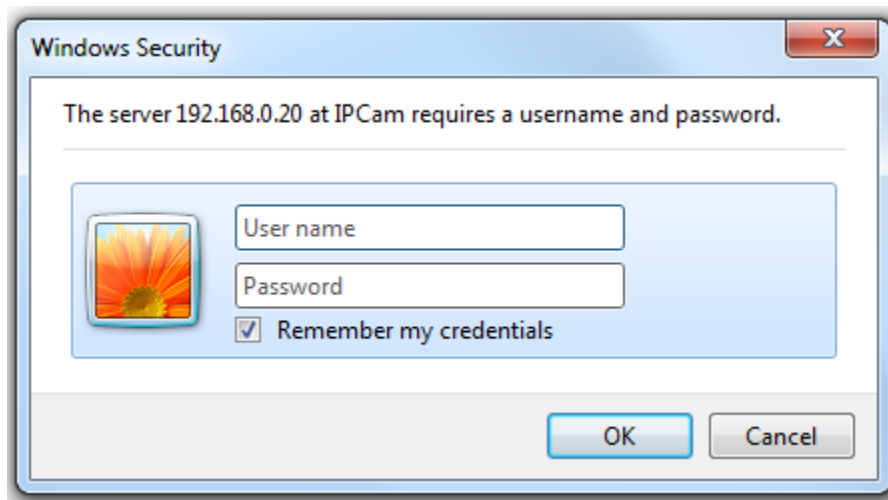
#### 4.2.1. Connecting to Internet Camera

- Use the following procedure to establish a connection from your PC to the Internet Camera.
- 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/>"

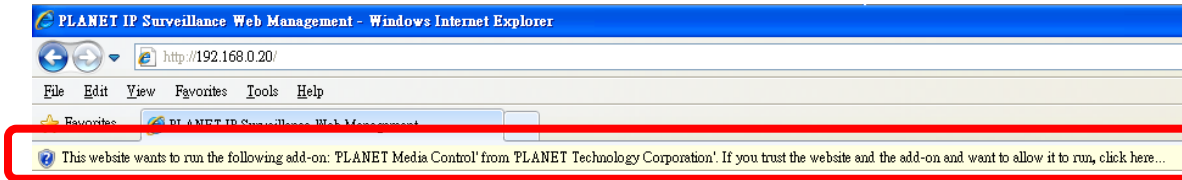


The login window of Internet Camera will appear,  
Default login **username/password** is: **admin / admin**

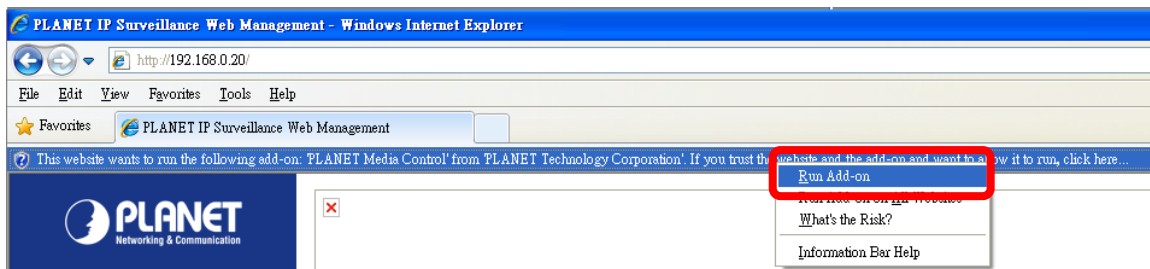


**NOTE:** If the User name and Password have been changed with PLANET IP Wizard II, please enter the new User name and Password here.

After logged on, you should see the following messages at the top of Internet Explorer:



Click on the message, and click **Run Add-on**



When you see this message, click **Run** to install required ActiveX control



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

You should be able to see the images captured from the Internet Camera in the web page now. For advanced functions, please refer to instructions given in follows chapters.

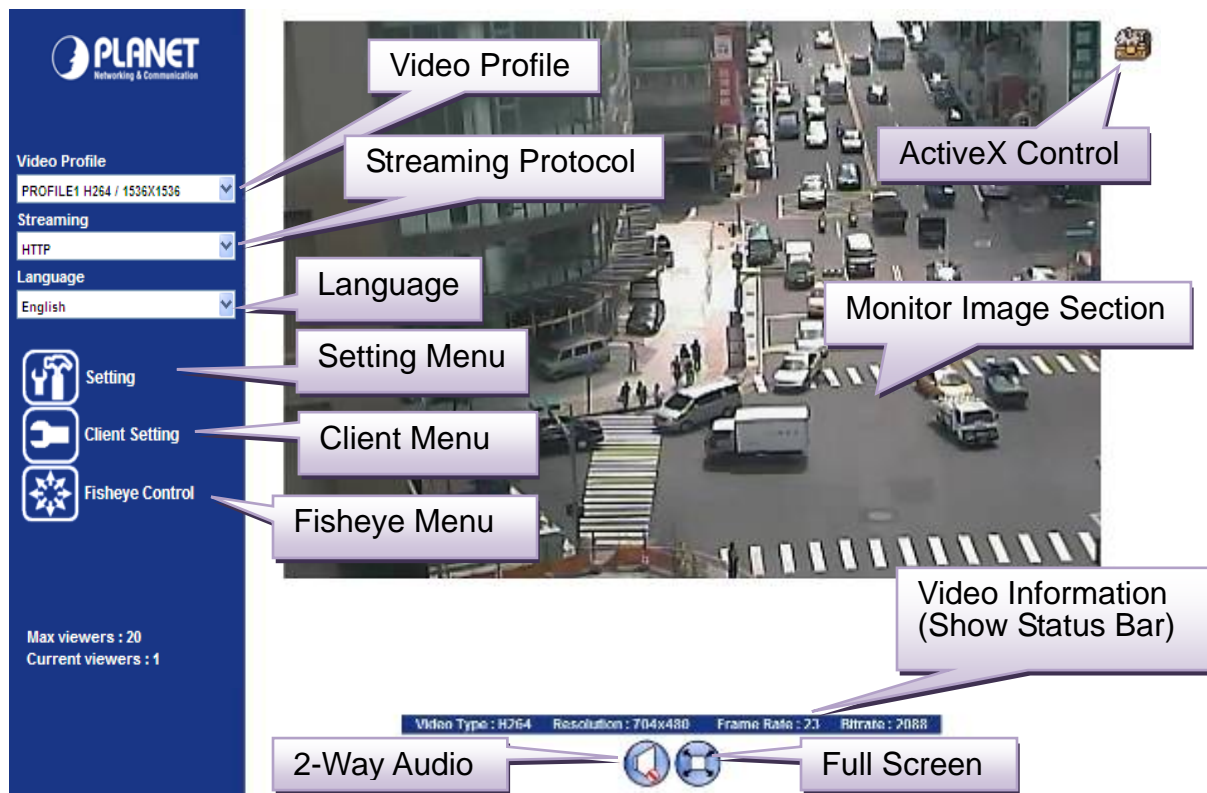
**NOTE:** If you log in the camera as an ordinary user, setting function will be not available. If you log in the camera as the administrator, you can perform all the settings provided within the device.

## Chapter 5.Web

# Configuration for Live View

## 5.1. Live View

Start-up screen will be as follow no matter an ordinary users or an administrator.



### Monitor Image Section

The image shot by the camera is shown here. The date and time are displayed at the top of the window.

### Video Profile

The camera support multi-profile for three compressions H264, MPEG-4 and M-JPEG simultaneously. User can chose the proper and/or preferred profile here.

### Full Screen

Click this button to display the image in full-screen mode (uses every available space to display the image captured by this camera).

### 2-Way Audio

The Internet Camera supports 2-way audio function. User can chose to enable or disable this function by toggling the icon below



: Disable audio uploading function.



: Enable audio uploading function.

### ActiveX Control

The plug-in ActiveX control supports a lot of functions by clicking the left mouse button. Note that this feature only supports on the ActiveX control within Microsoft® Internet Explorer.

### Setting Menu

This function is detail setting for the camera that only available for user logged into camera as administrator.

Item	Action
Network	Configure Network settings such as IPv6, ONVIF, DHCP, DDNS, 3GPP, PPPoE and UPnP.
Camera	Adjust camera parameters.
System	Configure system information, date & time, maintenance, and view system log file.
Video	Configure bit rate and frame rate of video profiles.
Audio	Configure audio parameters.
User	Setup user name, password and login privilege.
Protocol	Setup ONVIF and SNMP configuration.
E-Mail	Setup E-Mail configuration.
Object Detection	Setup Object detection.
Storage	Status and configuration of SD card and Samba server.
Continuous Recording	Files list inside the SD Card and Samba server.
Recording List	Files list inside the SD Card.
Event Server	Setup FTP/TCP/HTTP/Samba server for event
Event Schedule	Configure the schedule while event triggered.

### Streaming Protocol

User can select proper streaming protocol according to networking environment.

### Language

The device could provide multiple languages to meet customer's requirement.

**Client Setting:** Click this button to display the client extra control panel for 2-way Audio and Full Screen.

**Fisheye control:** **Position:**  
Choose the properly position depend on this camera installed.  
There are three options: Ceiling, Wall, and Desktop.

**Display Mode:**  
Choose the display mode depend on this camera installed.

Where:

**1O** - One Original fisheye view.

**1P** - One Panoramic view

**1R** - One Regional view

**2P** - Two Panoramic views

**1O3R** - One Original and three Regional views

**4R** - Four Regional views

**4R PRO** - Four Regional views interactively displayed when the field of view changes in any of the views

**1P2R** - One Panoramic and two Regional views

**1P3R** - One Panoramic and three Regional views



**Window:**  
Choose a window to activate PTZ function if the Display Mode supported.

**Camera direction:**

Control camera up/down/left/right and home position.

**Speed:**

Choose the speed of Pan and Tilt.

**Zoom:**

Press **WIDE** to zoom out, and press **TELE** to zoom in.

**Preset:**

Add/Update/Delete the preset positions or Go to one of these positions.

**Video  
Information**

Display video information including video format, resolution, frame rate and bit rate.

## 5.2. ActiveX Control

The plug-in ActiveX control supports a lot of functions by clicking the left mouse button. Note that this feature only supports on the ActiveX control within Microsoft® Internet Explorer.

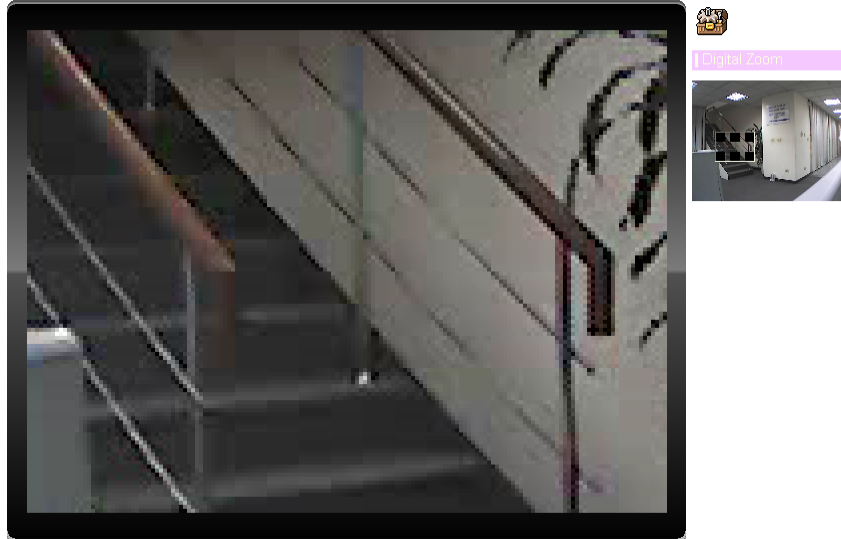
On the ActiveX control icon, click the Left Mouse Button, then a menu pop-up. This menu provides features that are unique to the ActiveX control. These features include:

- Digital Zoom,
- Snapshot,
- Record,
- Volume,
- About



### 5.2.1. Digital Zoom

Click **Digital Zoom** to activate this function as above. User can drag or scale the box over the video to adjust zoom ratio and position.



### 5.2.2. Snapshot

Click **Snapshot** to activate this function. Press **Snapshot** button to take a picture. The image file is saved as JPEG format into your local PC. Select **Browser**, the pop-up window to select the save path and file name prefix, select **OK** to continue.

If you like to retrieve the saved image, select the file to display the saved image by using any one of graph editing tools.



### 5.2.3. Record

Click **Record** to activate this function. Press **Record** button to start recording. The video file is saved as ASF format into your local PC. While you want to stop it, press **Stop** to stop recording. Select **Browser**, the pop-up window to select the save path and file name prefix, select **OK** to continue.

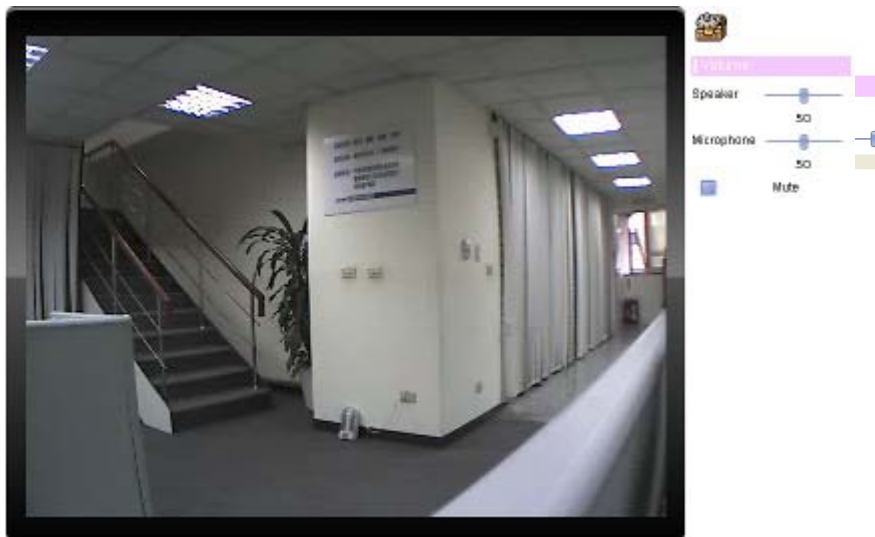
After stop recording, list the files, this file is named as Video\_yyyymmddhhmmss.asf

The ASF files can be display by the standard Windows Media Player, but it needs the DixectX 9.0 or later version to be installed.



### 5.2.4. Volume

Click Volume to activate this function. These have two control bars for speaker and microphone volume. Scroll this control bar to adjust the audio attribute. Check the volume mute will mute the speaker output.



### 5.2.5. About

Click **About** to show the ActiveX information

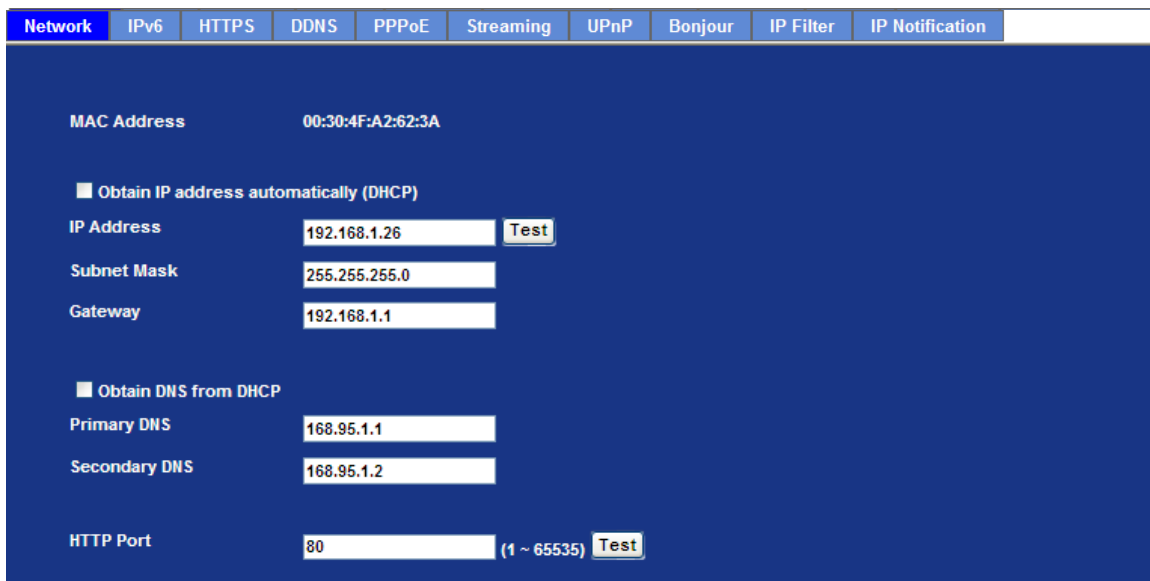


## Chapter 6. Network Configuration

### 6.1 Network setting

#### 6.1.1. Network

This section provides the menu of connecting the device through Ethernet cable.



<b>MAC address</b>	Display the Ethernet MAC address of the device. Note that user cannot change it.
<b>Obtain an IP address automatically (DHCP)</b>	<p>Enable this checked box when a DHCP server is installed on the network to issue IP address assignment. With this setting, the IP address is assigned automatically. If this device cannot get an IP address within limited tries, the device will assign a default IP address for 192.168.0.20.</p> <p>If you do not select “Obtain an IP address automatically”, then you need to enter these network parameters by yourself.</p>
<b>IP Address</b>	This address is a unique numbers that identifies a computer or device on the WAN or LAN. These numbers are usually shown in groups separated by periods, for example: 192.168.0.200

<b>Subnet Mask</b>	Subnets allow network traffic between hosts to be separated based on the network's configuration. In IP networking, traffic takes the form of packets. IP subnets advance network security and performance to some level by organizing hosts into logical groups. Subnet masks contain four bytes and usually appear in the same "dotted decimal" data. For example, a very common subnet mask in its binary demonstration 11111111 11111111 11111111 00000000 will usually be shown in the corresponding, more readable form as 255.255.255.0.
<b>Gateway</b>	A gateway is a piece of software or hardware that passes information between networks. You'll see this term most often when you either log in to an Internet site or when you're transient email between different servers.
<b>Obtain DNS from DHCP</b>	Enable this checked box when a DHCP server is installed on the network and provide DNS service.
<b>Primary DNS</b>	When you send email or position a browser to an Internet domain such as xxxxx.com, the domain name system translates the names into IP addresses. The term refers to two things: the conventions for naming hosts and the way the names are control across the Internet.
<b>Secondary DNS</b>	The same function as DNS1. It is option not necessary
<b>HTTP Port</b>	<p>The device supports two HTTP ports. The first one is default port 80 and this port is fixed. This port is very useful for Intranet usage. The second HTTP port is changeable. Users could assign the second port number of http protocol, and the WAN users should follow the port number to login. If the http port is not assigned as 80, users have to add the port number in back of IP address. For example: <a href="http://192.168.0.20:8080">http://192.168.0.20:8080</a>.</p> <p>Therefore, the user can access the device by either <a href="http://xx.xx.xx.xx/">http://xx.xx.xx.xx/</a>, or <a href="http://xx.xx.xx.xx:xxxx/">http://xx.xx.xx.xx:xxxx/</a> to access the device.</p> <p>If multiple devices are installed on the LAN and also required to be accessed from the WAN, then the <b>HTTP Port</b> can be assigned as the virtual server port mapping to support multiple devices.</p>

**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.

When the configuration is finish, please click “**OK**” to save and enable the setting.

### 6.1.2. IPv6 function

Internet Protocol version 6 (IPv6) is called the “IP Next Generation” (IPng), which is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. It is backward compatible and thus expected to slowly replace IPv4, with the two existing side by side for many years.

Network	<b>IPv6</b>	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
---------	-------------	-------	------	-------	-----------	------	---------	-----------	-----------------

IPv6 ☒ Disable ☐ Enable

**IPv6**

To enable or disable the IPv6 function here.

### 6.1.3. HTTPS

HTTPS: Stands for Hypertext Transfer Protocol Secure

HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for sensitive transactions in corporate information systems. The main idea of HTTPS is to create a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.

Network	IPv6	<b>HTTPS</b>	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
---------	------	--------------	------	-------	-----------	------	---------	-----------	-----------------

HTTPS ☐ Disable ☒ Enable

Port  (1 ~ 65535)

**HTTPS** To enable or disable the HTTPS service here. Note that the HTTPS function of this device is not only encrypted the web content but also audio/video data.

**Port** Choose the HTTPS port. The default value is 443.

## 6.1.4. DDNS server

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 easy 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 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, 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](http://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.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<p>DDNS <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>Server Name <input type="text" value="PLANET DDNS"/></p> <p>DDNS Host <input type="text" value=""/> .planetddns.com (6 ~ 16 Digits )</p> <p>User Name <input type="text" value=""/> (6~16 Digits)</p> <p>Password <input type="text" value=""/> (6~16 Digits)</p> <p>Internet Status Connected (210.61.134.92)</p>									

**DDNS** To enable or disable the DDNS service here.

**Server name** Choose the built-in DDNS server.

**DDNS Host** The domain name is applied of this device.

**User Name** The user name is used to log into DDNS.

**Password** The password is used to log into DDNS.

This model adds Planet easy DDNS that when this function enable will occur hostname with PLANET DDNS and end six of MAC automatically. User don't go to web of [www.planetddns.com](http://www.planetddns.com) apply new account.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<p>DDNS <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>Server Name <input type="text" value="PLANET Easy DDNS"/></p> <p>DDNS Host <input type="text" value="pla2623a.planetddns.com"/></p> <p>Internet Status Connected (210.61.134.92)</p>									

## 6.1.5. PPPoE

PPPoE: Stands for Point to Point Protocol over Ethernet

A standard builds on Ethernet and Point-to-Point network protocol. It allows Internet Camera 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 setup on a LAN environment to program the PPPoE information first, and then connect to the xDSL modem. Power on again, then the device will dial on to the ISP connect to the WAN through the xDSL modem.

The procedures are

- Connect to a LAN by DHCP or Fixed IP
- Access the device, enter **Setting → Network → PPPoE** as below

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<div> <div>PPPoE</div> <div> <input checked="" type="radio"/> Disable           <input type="radio"/> Enable         </div> </div> <div> <div>User Name</div> <div> <input type="text"/> <div>(&lt; 65 Digits)</div> </div> </div> <div> <div>Password</div> <div> <input type="password"/> <div>(&lt; 65 Digits)</div> </div> </div> <div> <div>IP Address</div> <div> <input type="text"/> <div>(readonly)</div> </div> </div> <div> <div>Subnet Mask</div> <div> <input type="text"/> <div>(readonly)</div> </div> </div> <div> <div>Gateway</div> <div> <input type="text"/> <div>(readonly)</div> </div> </div> <div> <div>Status</div> <div> <input type="text"/> <div>(readonly)</div> </div> </div>									

<b>PPPoE</b>	To enable or disable the PPPoE service here.
--------------	--

<b>User Name</b>	Type the user name for the PPPoE service which is provided by ISP.
------------------	--

<b>Password</b>	Type the password for the PPPoE service which is provided by ISP.
-----------------	---

<b>IP Address / Subnet Mask / Gateway</b>	Shows the IP information got from PPPoE server site.
---	--

<b>Status</b>	Shows the Status of PPPoE connection.
---------------	---------------------------------------

## 6.1.6. Streaming

RTSP is a streaming control protocol, and a starting point for negotiating transports such as RTP, multicast and Unicast, and for negotiating codecs. RTSP can be considered a "remote control" for controlling the media stream delivered by a media server. RTSP servers typically use RTP as the protocol for the actual transport of audio/video data.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<div> <div>RTSP Port</div> <div> <input type="text" value="554"/> <span>(554 ~ 65535)</span> <input type="button" value="Test"/> </div> </div> <div> <div>RTP Port</div> <div> <input type="text" value="50000"/> <span>~</span> <input type="text" value="50999"/> <span>(1024 ~ 65535)</span> </div> </div>									

**RTSP Port** Choose the RTSP port. The RTSP protocol allows a connecting client to start a video stream. Enter the RTSP port number to use. The default value is 554.

**RTP Port** Specify the range of transmission port number of video stream. The default range is 50000 to 50999. User can specify a number between 1024 and 65535.

**NOTE**

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

The camera must be set as Multi-profile mode, not Mega-pixel mode. Otherwise this device cannot serve 3GPP stream.

To use the 3GPP function, it strongly recommends installing the Networked Device with a public and fixed IP address without any firewall protection.

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, Quicktime or Realplayer currently)
2. Use the following URL to access: `rtsp://host/mpeg4/media.3gp`  
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 phone.

## 6.1.7. UPnP

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 Internet Camera. If your operating system is UPnP enabled, the device will automatically be detected and a new icon will be added to "My Network Places." If you do not want to use the UPnP functionality, it can be disabled

In addition, this device also provides UPnP IGD function for NAT traversal easily. Use NAT traversal when your device is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router will be forwarded to the device.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<p><b>UPnP</b> <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p><b>Friendly Name</b> <input type="text" value="ICA-8350 - 00304FA2623A"/> (readonly)</p> <p><b>UPnP NAT Traversal</b> <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p><b>Port Range</b> <input type="text" value="32768"/> ~ <input type="text" value="65535"/> (1 ~ 65535)</p> <p><b>External IP Address</b> <input type="text" value="AddPortMapping(32768, 32768, 192.168.1.118) failed with"/> (readonly)</p>									

<b>UPnP</b>	To enable or disable the UPnP service here.
<b>Friendly Name</b>	Shows the friendly name of this device here.
<b>UPnP NAT Traversal</b>	When enabled, the device will attempt to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the NAT router first.
<b>Port Range</b>	The port range will open in NAT router.
<b>External IP address</b>	Show the IP address and port for WAN access through Internet. If NAT traversal is configured successfully, user can use this IP address and port to access this device.

## 6.1.8. Bonjour

The Bonjour service allows IP camera can be discovered with Apple Safari browser applied, once the option enable the IP camera will be show the Friendly Name in the Bonjour bookmarks menu of Safari browser.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<p><b>Bonjour</b> <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p><b>Friendly Name</b> <input type="text" value="ICA-8350 - 00304FA2623A"/> (readonly)</p>									

**Bonjour** To enable or disable the Bonjour service here.

**Friendly Name** Shows the friendly name of this device here.

## 6.1.9. IP Filter

You can enter different user's IP address which are allowing enter or denying by the device.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<p><b>IP Filter</b> <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p><b>IP Filter Policy</b> <input type="radio"/> Deny <input checked="" type="radio"/> Allow</p> <p><input type="button" value="Save"/></p> <div> <div></div> <div> <p><b>Filter IP List</b></p> <p><b>Filter IP</b> <input type="text"/></p> <p><input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="DeleteAll"/></p> </div> </div>									

**IP Filter** To enable or disable the IP filter function here.

**IP Filter Policy** Choose the filter policy where is denying or allowing.

## 6.1.10. IP Notification

In case the IP address is changed, system is able to send out an email to alert someone if the function is enabled.

Network	IPv6	HTTPS	DDNS	PPPoE	Streaming	UPnP	Bonjour	IP Filter	IP Notification
<p>SMTP Notification(email) <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>Send To <input type="text"/> (&lt; 129 Digits)</p> <p>Subject <input type="text" value="IP notification"/> (&lt; 65 Digits)</p> <p>TCP Notification <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>TCP Server <input type="text"/> (&lt; 65 Digits)</p> <p>TCP Port <input type="text"/> (1 ~ 65535)</p> <p>Message <input type="text"/> (&lt; 65 Digits)</p> <p>HTTP Notification <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>URL <input type="text" value="http://"/> (&lt; 61 Digits)</p> <p>HTTP Login Name <input type="text"/> (&lt; 22 Digits)</p> <p>HTTP Login Password <input type="text"/> (&lt; 22 Digits)</p> <p>Proxy Address <input type="text"/> (&lt; 129 Digits)</p> <p>Proxy Port <input type="text"/> (1 ~ 65535)</p> <p>Proxy Login Name <input type="text"/> (&lt; 22 Digits)</p>									

### SMTP Notification (e-mail)

If enable this function, then the “**Send to**” and “**Subject**” field need to be filled.

#### Send To

Type the receiver’s e-mail address. This address is used for reply mail.

#### Subject

Type the subject/title of the E-mail.

#### TCP Notification

If enable this function, then the “**TCP Server**”, “**TCP Port**”, and “**Message**” fields need to be filled.

#### TCP Server

Type the server name or the IP address of the TCP server.

#### TCP Port

Set port number of TCP server.

#### Message

The message will be sent to FTP server.

#### HTTP Notification

If enable this function, then the fields below need to be filled.

#### URL

Type the server name or the IP address of the HTTP server

<b>HTTP Login name</b>	Type the user name for the HTTP server.
<b>HTTP Login Password</b>	Type the password for the HTTP server.
<b>Proxy Address</b>	Type the server name or the IP address of the HTTP Proxy.
<b>Proxy Port</b>	Set port number of Proxy.
<b>Proxy Login name</b>	Type the user name for the HTTP Proxy.
<b>Proxy Login Password</b>	Type the password for the HTTP Proxy.
<b>Custom parameter</b>	User can set specific parameters to HTTP server.
<b>Message</b>	The message will be sent to HTTP server.

## 6.2. Adjust Camera Configuration

Use this menu to set the function of the camera of Internet Camera

### 6.2.1. Picture

PicturePrivacy MaskPreset Setting

White Balance

Auto

Exposure Control

Auto Exposure

Power Frequency

☐ 50Hz
 ☒ 60Hz

Exposure Value

50

(0 ~ 100)

Color Level

50

(0 ~ 100)

Hue

50

(0 ~ 100)

Brightness

50

(0 ~ 100)

Contrast

50

(0 ~ 100)

Sharpness

50

(0 ~ 100)

Local video output

☒ Disable
 ☐ Enable

ICR

Auto

Current Value 2720

Refresh



#### White Balance

Auto: will adjust the white balance automatically.

Hold: will hold the white balance.

#### Exposure Control

Auto Exposure: will adjust the image sensor exposure automatically.

Hold Exposure: will hold the exposure setting.

Manual Exposure: User can configure sensor exposure to fixed setting.

Outdoor: In case this camera is installed in outdoor, then shall enable this option.

Otherwise, disable it. The feature can improve auto-exposure performance under strong sunlight.

#### Power Frequency

Frequency of power line: 50 or 60Hz.

<b>Exposure Value</b>	<p>Exposure value is AE target value. This value is to adjust the integration, analog gain and digital gain to achieve the target brightness value (Exposure Value).</p> <p>This value is dependent to "Auto Exposure" only</p>
<b>Color Level</b>	Large value will be colorful.
<b>Hue</b>	Change the value will result to color tuning.
<b>Brightness</b>	Large value will brighten camera.
<b>Contrast</b>	Large value will contrast camera heavily.
<b>Sharpness</b>	Large value will sharpen camera.
<b>Local video output</b>	<p>Enable or disable video signal of BNC connector. It's very useful to check view angle or focus during camera installation. However, disable this function will save power a lot. Suggest to disabling it after camera installed well.</p>
<b>ICR</b>	<p>Use built-in photo sensor or manual to control ICR.</p> <p>In case user selects manual mode, there are 4 modes: Night (On), Day (Off), Auto or Schedule to control built-in IR LEDs. This function is very useful under low illumination environment even 0 Lux.</p> <p>In case the Auto mode is selected, user needs to specify 3 parameters in advance:</p> <p>Night Mode Threshold (0~10000): this value set the threshold to turn on IR LED. It should be lower or equal to Day Mode Threshold.</p> <p>Day Mode Threshold (0~10000): this value set the threshold to turn off IR LED. It should be higher or equal to Night Mode Threshold.</p> <p>Delay Time: The delay time between LED ON/OFF switching.</p> <p>Note: that Current Value is the current luminance from the captured video. It's a useful reference to set LED ON/OFF Threshold.</p>
<b>3D De-Noise</b>	<p>This function can remove or lower unwanted noise and preserve fine details and edges as possible.</p>

**WDR**

This function is to provide clear images even under back light circumstances. The higher “Strength” level will adjust contrast compensation stronger.


**Default Settings**

Restore to factory image settings.

### 6.2.2. Privacy Mask

Use this page to specify privacy mask window 1 to window 7 and set the name and gray level for selected window.

Picture
Privacy Mask
Preset Setting



Add
Delete

Name

Level  

0 (Black)

Save

#### Add and Delete

To add or delete the privacy mask windows, user can specify up to 7 windows to mask the video captured by this device. By dragging mouse on the image, you can change the position and size of the selected window accordingly.

#### Name

Name of the specified privacy window

#### Level

To define the gray level of mask block. The smaller value will be darker.

**NOTE:** This function is not recommended for camera with ePTZ actions.

## 6.2.3 Preset Setting

This page provides the edit tool to modify or delete the “Preset Setting” item by item.

Picture
Privacy Mask
**Preset Setting**

Preset Number	Preset Name	Home Position

Preset List

Preset Number

Preset Name

Home Position
☐ Enable
☒ Disable

Modify
Delete

## 6.3. System

Use this menu to perform the principal settings of Internet Camera.

### 6.3.1. System

System
Date & Time
Maintenance

Device Title
(0 ~ 30 Digits)

Software Version
6.M.2.10388

Network LED
☒ Enable
☐ Disable

Power LED
☒ Enable
☐ Disable

Log

```

Feb  5 04:57:04 ICA-8350 user.debug rtsp-svr: client request: 'OPTIONS' 'rtsp://192.168
Feb  5 04:57:09 ICA-8350 user.err syslog: nvram_commit! (1821)
Feb  5 04:57:10 ICA-8350 user.debug rtsp-svr: client request: 'OPTIONS' 'rtsp://192.168
Feb  5 04:57:16 ICA-8350 user.err syslog: nvram_commit! (1822)
Feb  5 04:57:24 ICA-8350 user.err syslog: nvram_commit! (1823)
Feb  5 04:57:32 ICA-8350 user.err syslog: nvram_commit! (1824)
Feb  5 04:57:34 ICA-8350 user.debug rtsp-svr: client request: 'OPTIONS' 'rtsp://192.168
Feb  5 04:57:39 ICA-8350 user.err syslog: nvram_commit! (1825)
Feb  5 04:57:40 ICA-8350 user.debug rtsp-svr: client request: 'OPTIONS' 'rtsp://192.168
Feb  5 04:57:46 ICA-8350 user.err syslog: nvram_commit! (1826)
Feb  5 04:57:53 ICA-8350 user.err syslog: nvram_commit! (1827)
Feb  5 04:58:00 ICA-8350 user.err syslog: nvram_commit! (1828)
Feb  5 04:58:04 ICA-8350 user.debug rtsp-svr: client request: 'OPTIONS' 'rtsp://192.168

```

<b>Device title</b>	You can enter the name of this unit here. It's very useful to identify the specific device from multiple units.
<b>Software version</b>	This information shows the software version in the device.
<b>Network LED</b>	Switch the LED light of this Internet Camera on or off, that Network LEDs will stop working; in case you don't want other people know the camera is transferring data.
<b>Power LED</b>	Switch the LED light of this Internet Camera on or off.
<b>Log</b>	User can check the system log information of the device, including the Main Info, Appended Info, Operator IP, and so on ...
<b>Reload</b>	Click this button; user can refresh the log information of the device.

### 6.3.2. Date & Time

User can setup the time setting of Internet Camera, make it synchronized with PC or remote NTP server. Also, you may select the correct time zone of your country.

System
Date & Time
Maintenance

Server Date & Time

2013-1-07 10:53:43

PC Time

2013-1-7 10:53:40

Adjust

☐ Synchronize with PC
☐ Manual setting : Date : 2013 Jan 07 Time : 10 : 53 : 28
☒ Synchronize with NTP

NTP Server

time.stdtime.gov.tw Test

NTP Sync. Interval

24 hour

Timezone

GMT (Dublin, Lisbon, London, Reykjavik)

Daylight Saving

☒ Disable
☐ Enable

Daylight Saving StartTime

Jan 01 00 : 00 : 00

Daylight Saving StopTime

Jan 01 00 : 00 : 00

Daylight Saving Offset

+ 01 : 00 : 00

<b>Server Date &amp; Time</b>	Displays the date and time of the device
<b>PC Time</b>	Displays the date and time of the connected PC

<b>Adjust</b>	<b>Synchronize with PC:</b>	Click this option to enable time synchronization with PC time
	<b>Manual setting:</b>	Click this option to set time and date manually
	<b>Synchronize with NTP:</b>	Click this option if you want to synchronize the device's date and time with those of time server called NTP server (Network Time Protocol)
<b>NTP server name</b>	Type the host name or IP address or domain name of the NTP server.	
<b>NTP sync. Interval</b>	Select an interval between 1 and 23 hours at which you want to adjust the device's time referring to NTP server	
<b>Time zone</b>	Set the time difference from Greenwich Mean Time in the area where the device is installed.	
<b>Daylight saving</b>	Check this item to enable daylight saving adjustment.	
<b>Daylight Saving Start Time</b>	Sets up the date and time of daylight saving start time.	
<b>Daylight Saving Stop Time</b>	Sets up the date and time of daylight saving stop time.	
<b>Daylight Saving Offset</b>	Sets up the date of daylight saving offset.	

### 6.3.3. Maintenance

System	Date & Time	Maintenance
Default Settings (Including Network Setting)		Factory Default Settings
Default Settings (Excluding Network Setting)		Default Settings
Backup Setting	Backup Setting	
Restore Setting	<input type="text"/>	Browse... Restore Setting Reset
Firmware Upgrade	<input type="text"/>	Browse... Firmware Upgrade Reset
System Restart	Restart	

<b>Default Settings (Include the network setting)</b>	Recall the device hard factory default settings. Note that click this button will reset all device's parameters to the factory settings (including the IP address).
<b>Default Settings (Except the network setting)</b>	The unit is restarted and most current settings are reset to factory default values. This action will not reset the network setting.
<b>Backup Setting</b>	To take a backup of all of the parameters, click this button. If necessary, it will then be possible to return to the previous settings, if settings are changed and there is unexpected behavior.
<b>Restore Setting</b>	Click the " <b>Browse</b> " button to locate the saved backup file and then click the "Restore Setting" button. The settings will be restored to the previous configuration.

<b>Firmware upgrade</b>	<p>The device supports new firmware upgrade.</p> <ol style="list-style-type: none"> <li>1. Close all other application programs which are not necessary for firmware update.</li> <li>2. Make sure that only you access this device at this moment</li> <li>3. Disable Motion Detection function.</li> <li>4. Select "<b>Firmware name</b>"</li> <li>5. Select the Firmware binary file.</li> </ol> <p><i>Note :</i></p> <p><i>That it must make sure that the Firmware only applies to this device, once update, it will be burned into FLASH ROM of system.</i></p> <ol style="list-style-type: none"> <li>6. Once the firmware file was selected, select "<b>Upgrade</b>".</li> <li>7. The upgrade progress information will be displayed on the screen.</li> <li>8. A message will be shown while the firmware upgraded. Once the upgrading process completed, the device will reboot the system automatically.</li> <li>9. Please wait for 80 seconds, and then you can use PLANET IP Wizard II to search the device again.</li> </ol>
-------------------------	---

### Warning!!!

**The download firmware procedure cannot be interrupted. If the power and/or network connection are broken during the download procedure, it might possibly cause serious damage to the device.**

**Please be aware that you should not turn off the power during updating the firmware and wait for finish message.**

**Furthermore, do not try to upgrade new firmware if it's not necessary.**

<b>System Restart</b>	The device is restarted without changing any of the settings.
-----------------------	---

## 6.4. Video

This page provide user configure OSD, overlay, profile, ROI and AOI.

### 6.4.1. Common

Common	Overlay Image	Video Profile	ROI	AOI
<b>Text Overlay Setting</b>				
Font Color		797979	Set Color	Default Color
Background Color		101010	Set Color	Default Color
Transparency		0 (opacity)	▼	
<input type="checkbox"/> Include Date				
<input checked="" type="radio"/> Predefined		YYYY-MM-DD ▼		
<input type="radio"/> Own		%Y-%m-%d (0 ~ 12 Digits)		
<input type="checkbox"/> Include Time				
<input checked="" type="radio"/> Predefined		24h ▼		
<input type="radio"/> Own		%H:%M:%S (0 ~ 12 Digits)		
<input type="checkbox"/> Include Text				
		(0 ~ 20 Digits)		

#### Text Overlay Setting

There are some important information can be embedded into image, including date, time, and/or text.

## 6.4.2. Overlay Image

User can upload bitmap file to the camera and overlay the picture on streaming video and set its attributes.

Common
Overlay Image
Video Profile
ROI
AOI

Upload Own Image
☐ Include overlay image
Image Overlay Setting

Browse...
Upload File
Reset

Coordinates
X  Y

File
<No overlay image>

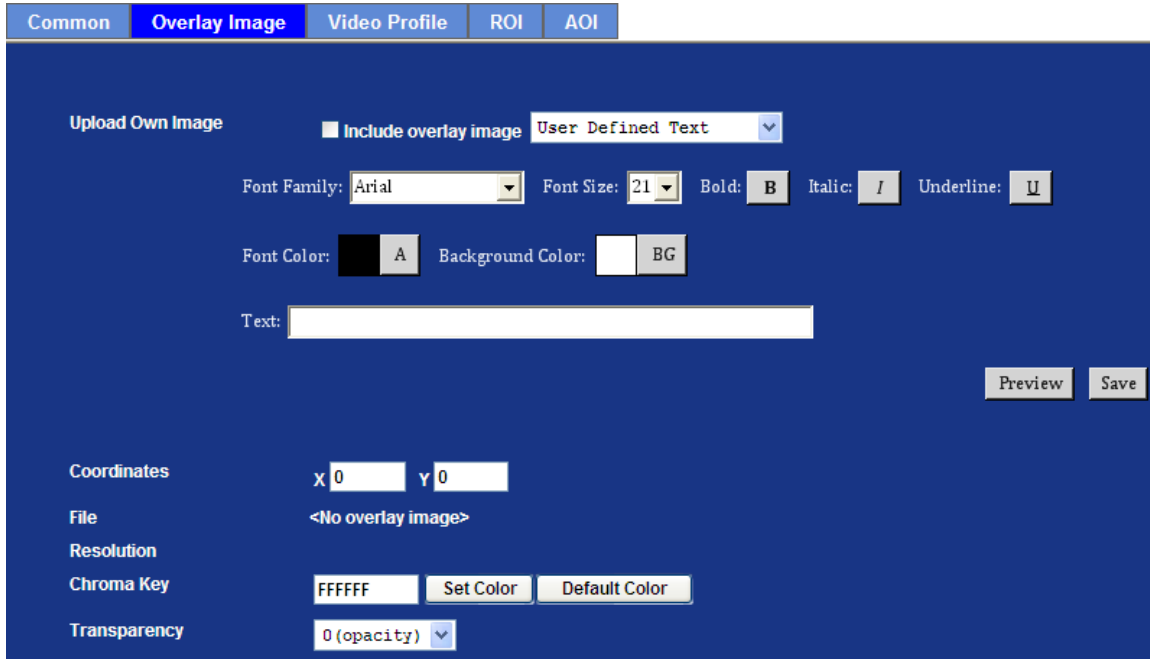
Resolution

Chroma Key
Set Color
Default Color

Transparency

<b>Upload own image</b>	Currently, user can download bitmap file only to camera.
<b>Image Overlay Setting</b>	Check this item to enable image overlay. Otherwise, the uploaded bitmap will not be overlaid on video.
<b>Coordinates</b>	Set position of image on the video.
<b>File</b>	Information of the uploaded bitmap file.
<b>Resolution</b>	Size information of the uploaded bitmap file
<b>Chroma Key (Background Color)</b>	Define the Chroma key of the uploaded bitmap file. Then user can set transparency of the bitmap
<b>Transparency</b>	Lower value will lower transparent. Value 0 means opacity

User can select “Image Overlay Setting” mode and overlay a text string onto camera image.



**Upload own image** The font style can be chosen in this page. Once the font type settled, click “Save” button to upload text to image.

**Coordinates** Set position of image on the video.

**File** Information of the uploaded bitmap file.

**Resolution** Size information of the uploaded bitmap file

**Chroma Key (Background Color)** Define the Chroma key of the uploaded bitmap file. Then user can set transparency of the bitmap

**Transparency** Lower value will lower transparent. Value 0 means opacity

### 6.4.3. Video Profile

User can modify the detail parameter for each video profiles in this page.

Common	Overlay Image	Video Profile	ROI	AOI					
Name	Video Type	Resolution	Rate Control	Quality	Bitrate	Max Frame Rate	GOP Control	ROI	Multicast
Profile1	h264/Baseline	1536x1536	EVBR	75	-	22	22	no	no
Profile2	mjpeg	1536x1536	VBR	75	-	7	1	no	no
Profile3	h264/Baseline	1280x1280	EVBR	70	-	22	22	no	no
Profile4	mjpeg	1280x1280	VBR	90	-	7	1	no	no
Profile5	h264/Baseline	768x768	EVBR	70	-	22	22	no	no
Profile6	mjpeg	768x768	VBR	90	-	7	1	no	no
Profile7	h264/Baseline	384x384	EVBR	70	-	22	22	no	no
Profile8	mjpeg	384x384	VBR	90	-	22	1	no	no

Name	Profile1
Video Type	h264 Baseline
Resolution	1536x1536
ROI	<input checked="" type="radio"/> Yes <input type="radio"/> No
Rate Control	EVBR Quality 75 Max Bitrate 6144 K bps 384 ~ 6144
Max Frame Rate	22
GOP Control	22
Multicast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Multicast Video	IP Address 239.198.97.181 Port 0 (0 means auto, 1024 ~ 65534)
Multicast Audio	IP Address 239.198.97.181 Port 0 (0 means auto, 1024 ~ 65534)

**Name** To assign a name to the selected profile.

**Video Type** Video codec of the selected profile.

**Resolution** Resolution of the selected profile.

**ROI** Assign the selected profile as a ROI stream or not. (Only available for the profiles with max resolution)

**Rate Control** Defines the rate control method of this profile. There are four options: Constant Bit Rate (CBR), Variable Bit Rate (VBR), and Enhanced Variable Bit Rate (EVBR).

For CBR, the video bit rate is between low to high bandwidth based on different resolutions. User can set the desired bit rate to match the limitation of bandwidth.

For VBR, user should choose the quality level to set the video quality rather than bit rate. The quality level is between 1 and 100. The higher value can reach the better quality but of course will consume

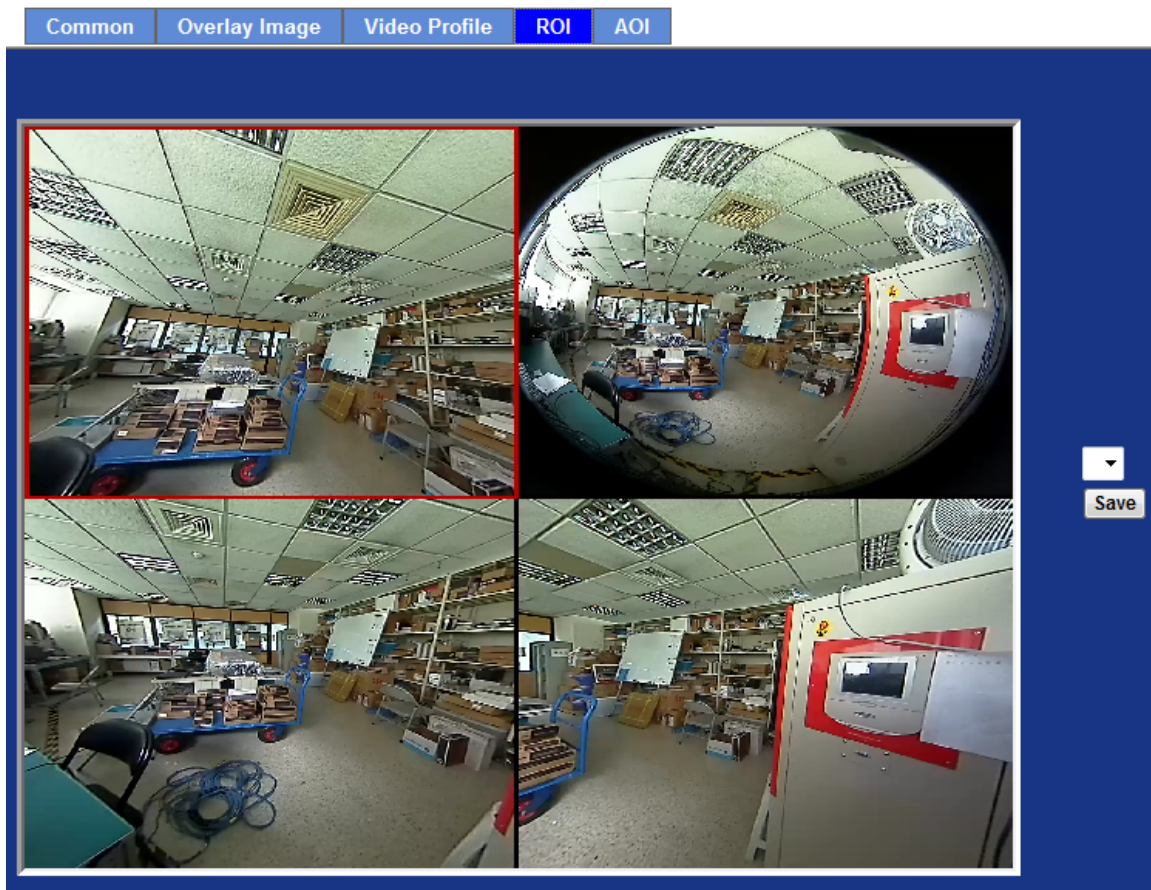
	<p>higher bandwidth.</p> <p>For EVBR, the video bitrates is based on normal VBR mode. However, the target bitrates can be increased to max target bitrates while lots of motion in video. The max target bitrates will keep a pre-defined time period and then back to normal VBR mode.</p>
<b>Max Frame Rate</b>	Defines the targeted frame rate of this profile. For example, set the frame rate to 15 fps, then the image will be updated for 15 frames per second. User can set the desired max frame rate versus video quality under the limited bandwidth.
<b>GOP Control</b>	Defines the Intra/Inter-frame (I/P) ratio of this profile. For example, set the GOP to 30, then the video stream will have one Intra-frame every 30 frames.
<b>Multicast</b>	Enable or disable the multicast function.
<b>Multicast Video</b>	IP address and port for multicast video streaming of the selected profile.
<b>Multicast Audio</b>	IP address and port for multicast audio streaming of the selected profile
<b>Time to live</b>	Time to live (TTL) is a mechanism that limits the lifespan of data in a computer or network. Once the prescribed event count or timespan has elapsed, data is discarded. TTL prevents a data packet from circulating indefinitely.
<b>Always Enable Multicast</b>	Multicast streaming is always enabled or by request

### **Warning!!!**

**To enable the multicast streaming, you shall make sure your Intranet does support multicast function. Otherwise, your Intranet may fall into network storm seriously.**

#### 6.4.4. ROI

ROI means Region of Interest. Use this page to specify location of ROI windows. Only the maximum resolution profiles can be defined as ROI. In this model, only profile 1 and 2 can use ROI.

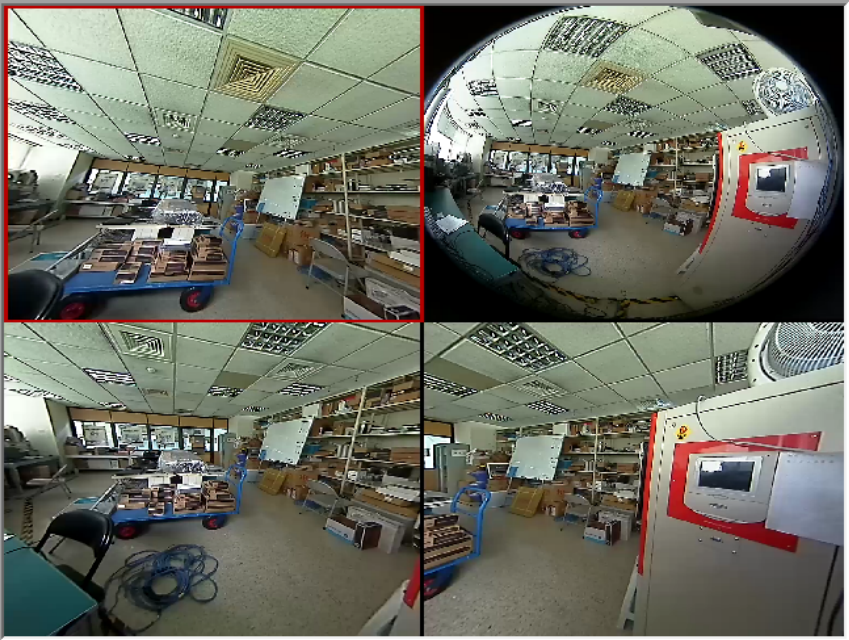


**NOTE:** This function is not recommended for camera with ePTZ actions

### 6.4.5. AOI

AOI means Area of Interest. Use this page to specify location and size of AOI windows. Only the profiles with H.264 codec and VBR rate control can support AOI function. It enables a non-uniform distribution of the image quality between a selected region (the AOI) and the rest of the image (background).

Common
Overlay Image
Video Profile
ROI
AOI



Name

Level  
10

Only profile with H.264 codec and VBR rate control supports AOI

#### Add and Del

To add or delete the AOI windows. User can specify up to 2 AOI windows to change the video quality in specified areas. By dragging mouse on the image, you can change the position and size of the selected AOI window accordingly

#### Name

Name of the specified AOI window.

#### Level

Adjust the video quality of specified AOI window. The higher value will be better video quality.

**NOTE:** This function is not recommended for camera with ePTZ actions

## 6.5. Audio Configuration

**Setting**

Audio

☐ Disable
 ☒ Enable

Audio Type

Audio Mode

☒ Simplex
 ☐ Full duplex

Input Gain

Output Gain

<b>Audio</b>	To enable or disable audio function.
<b>Audio type</b>	To select G711 or G726 for <i>audio</i> coding.
<b>Audio Mode</b>	To select Simplex or Full duplex (2-way audio) mode.
<b>Input Gain</b>	To adjust gain of input audio.
<b>Output Gain</b>	To adjust gain of output audio.

## 6.6. User Privilege Access Configuration

Use this menu to set the user names and password of the Administrator and up to 10 users, and access right of each user.

Setting

Viewer Login

☒ Anonymous
☐ Only users in database
Save

User Name	Access Right
admin	administrator

User List

User Name

(1 ~ 20 Digits)

Password

(0 ~ 20 Digits)

Verify Password

(0 ~ 20 Digits)

Access Right

☐ Administrator
☒ Viewer

Add
Modify
Delete

### Viewer Login

Select "Anonymous" to allow any one viewing the video once connected. Otherwise, only users in database can view the video after login.

### Access Right

Administrator can access every function in this device. However, Viewers only can view the video and access limited function.

### Add, Modify, and Delete of Users account

Manage the user's account of viewer user.

## 6.7 Protocol

Use this menu to select enable or disable ONVIF, also setup SNMP configuration.

### ONVIF

ONVIF
SNMP

ONVIF

☐ Disable
☒ Enable

☒ V1.0
☐ V1.01/V1.02/V2.0/V2.1/V2.2

ONVIF is a global and open industry forum with the goal to facilitate the development and use of a global open standard for the interface of physical IP-based security products. Or in other words, to create a standard for how IP products within video surveillance and other physical security areas can communicate with each other.

#### ONVIF

To enable or disable the ONVIF interface here.

#### Version

Currently, the V1.0 or V1.01/1.02/V2.0/V2.1.1 is available.

### SNMP

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

#### ONVIF

#### SNMP

SNMP v1	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SNMP v2c	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Read community	<input type="text" value="public"/> (< 33 Digits)
Write community	<input type="text" value="write"/> (< 33 Digits)
Traps	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Trap address	<input type="text" value="192.168.1.41"/> (< 257 Digits)
Trap community	<input type="text" value="1234"/> (< 33 Digits)
Available traps	<input checked="" type="checkbox"/> Cold start <input type="checkbox"/> Warm start <input type="checkbox"/> Link up <input type="checkbox"/> Authentication failed

#### SNMP v1

To enable or disable the SNMP v1 function here.

#### SNMP v2c

To enable or disable the SNMP v2c function here.

#### Read community

#### Write community

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.

<b>Traps</b>	Trap is a mechanism that allows the managed device to send messages to manager instead of waiting passively for polling from the manager.
<b>Trap address</b>	The IP address of SNMP traps station.
<b>Trap community</b>	Trap Community means the community that can receive the trap message.
<b>Available traps</b>	The camera reboots by web restart or power cycle.
<b>Cold start</b>	
<b>Available traps</b>	Modify SNMP setting when camera online.
<b>Warm start</b>	
<b>Available traps</b>	The camera connected network.
<b>Link up</b>	
<b>Available traps</b>	When content of read community is wrong, MIB browser connecting to camera will appear trap message.
<b>Authentication failed</b>	

## 6.8. E-Mail Configuration

You may setup SMTP mail parameters for further operation of Event Schedule. That's, if users want to send the alarm message out, it will need to configure parameters here and also add at least one event schedule to enable event triggering.

Setting

SMTP Server	mail.planet.com.tw (< 129 Digits)	Test
SMTP Port	25 (1 ~ 65535)	
SSL	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
SMTP Authentication	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Authentication User Name	admin (< 65 Digits)	
Authentication Password	***** (< 22 Digits)	
E-mail From	admin@planet.com.tw (< 129 Digits)	
E-mail To	support@planet.com.tw (< 129 Digits)	
E-mail Subject	message (< 65 Digits)	

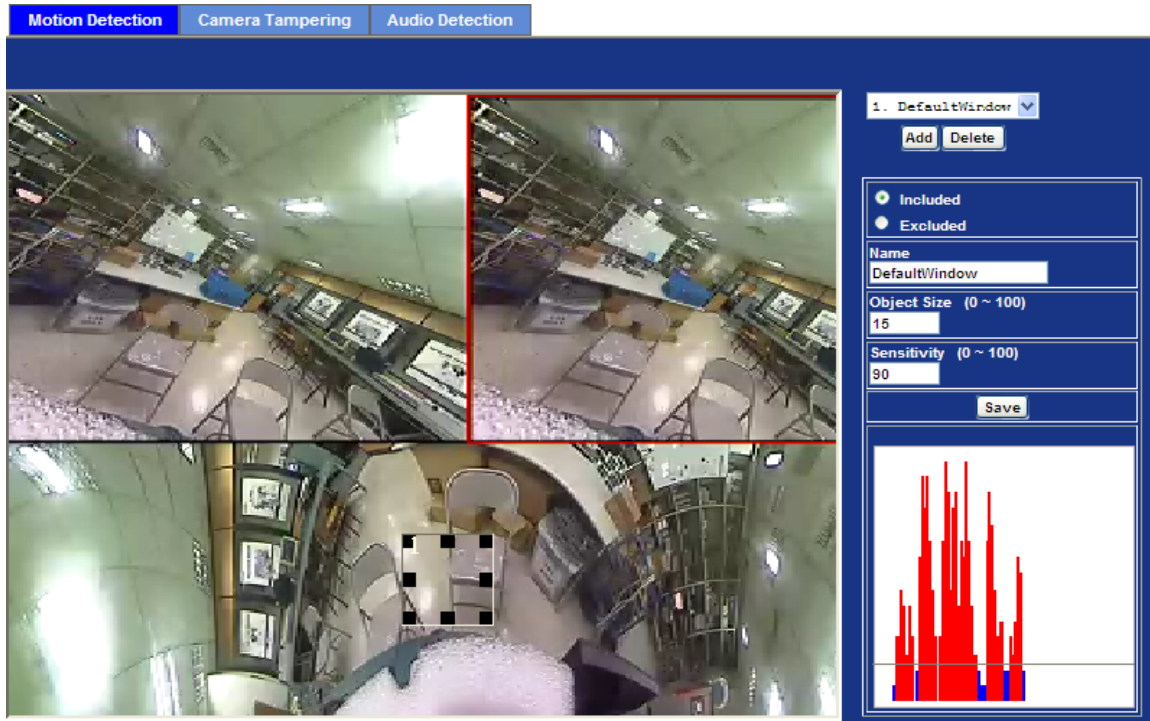
<b>SMTP Server</b>	Type the SMTP server name or the IP address of the SMTP server.
<b>Test</b>	Send a test mail to mail server to check this account is available or not.
<b>SMTP Port</b>	Set port number of SMTP service.
<b>SSL</b>	Enable SSL function or not.
<b>SMTP Authentication</b>	<p>Select the authentication required when you send an e-mail.</p> <p><b>Disable:</b> If no authentication is required when an e-mail is send.</p> <p><b>Enable:</b> If authentication is required when an e-mail is sent.</p>
<b>Authentication User Name</b>	Type the user name for the SMTP server if Authentication is Enable.
<b>Authentication Password</b>	Type the password for the SMTP server if Authentication is Enable.
<b>E-mail From</b>	Type the sender's E-mail address. This address is used for reply e-mails.
<b>E-mail To</b>	Type the receiver's e-mail address.
<b>E-mail Subject</b>	Type the subject/title of the e-mail.

## 6.9. Event Detection

This device supports 3 types of event detection: Motion detection, Camera tampering, and Audio detection.

### 6.9.1 Motion Detection

Use this menu to specify motion detection window 1 to window 10 and set the conditions for detection while observing a captured image.



#### Add and Delete

To add or delete the motion windows. User can specify up to 4 Included and/or Excluded windows to monitor the video captured by this device. By dragging mouse on the image, you can change the position and size of the selected motion window accordingly.

#### Included or Excluded Window

These windows can be specified as Included or Excluded type.

##### Included:

Windows target specific areas within the whole video image

##### Excluded:

Windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

#### Name

Name of the specified motion window.

#### Object Size

Defines the object size of motion detection. The higher object size will only larger objects trigger motion detection. The lower object size will

even small objects trigger motion detection too. Generally speaking, the smaller size will be easier to trigger event.

<b>Sensitivity</b>	Defines the sensitivity value of motion detection. The higher value will be more sensitivity.
<b>NOTE:</b>	<b>This function is not recommended for camera with ePTZ actions</b>

### 6.9.2. Camera Tampering

Camera tampering detection is a new intelligent functionality that further strengthens the benefit of Network Camera. When the camera is moved, partially obscured, severely defocused, covered or sprayed, an event can be triggered to send notifications, upload images/files to remote server or email...

Motion Detection
Camera Tampering
Audio Detection

Minimum duration
10 Seconds

<b>Minimum duration</b>	Define the minimum triggered duration by camera tampering detection. The triggered duration less than target value will be ignored to filter false alarms.
<b>NOTE:</b>	<b>This function is not recommended for camera with ePTZ actions</b>

### 6.9.3. Audio Detection

Audio detection alarm can be used as a complement to motion detection. Since audio detection can react to events in areas too dark for the video motion detection functionality to work properly. In addition, it can be used to detect activity in areas outside of the camera's view.

Motion Detection
Camera Tampering
**Audio Detection**

Audio Alarm Level  50 (0 ~ 100)

**Audio Alarm Level**

Define the threshold value of audio detection.

## 6.10. Storage Configuration

This page shows the status of attached SD card and Samba server. You may setup related parameters to manage the attached SD card or Samba server also.

### 6.10.1. SD Card

SD Card

SAMBA Server

Disk ID

SD\_DISK

Mount

Unmount

Status

Free space

57% - 1126844KB

Reload

Format

Total size

1966080 KB

Status

OK

Full

No

Readonly

No

☐ Enable automatic disk cleanup

Remove recordings older than:

7

day(s)

Remove oldest recordings when disk is:

95

% full

☐ Lock disk

#### Enable automatic disk cleanup

Delete old recorded files while the conditions are reached as below.

#### Remove recordings order than

Delete old files by days.

#### Remove oldest recordings when disk is

Delete old files by left capacity.

#### Lock disk

Lock the SD card. Once SD card is locked, all files can't be deleted.

### 6.10.1. SAMBA Server

This page shows the status of SAMBA server. You may setup related parameters to manage the remote SAMBA server.

SD Card
SAMBA Server

Host	192.168.0.201	(1 ~ 63 Digits)
Share	share	(1 ~ 63 Digits)
User Name	test	(< 63 Digits)
Password	*****	(< 63 Digits)
Status	Online	
Total size	13.34 GB	
Free space	59% - 7.88 GB	
SAMBA Server	<input type="button" value="Unmount"/>	

<b>Host</b>	Type the SAMBA server domain name or the IP address of the SMTP server.
<b>Share</b>	Type the share folder of remote SAMBA server which the camera will upload files to this space.
<b>User name</b>	Type the user name for the remote SAMBA server
<b>Password</b>	Type the password for the remote SAMBA server.

## 6.11. Continuous Recording

The camera can continuously record video stream into files and save them to attached SD card or remote SAMBA server.

Continuous Recording

Continuous Recording

Record File Type

Disk

Path

☒ Disable
 ☐ Enable

Profile1 h264 / 1536x1536

AVI

☐ SD Card
 ☒ SAMBA Server

PLANET-00304FA2623A

( For example: Folder1/Folder2/Folder3 ) ( 1 ~ 63 Digits )

Restart

(Restarting will delete the current recording.)

Oldest recordings will be removed if the disk is 90% full and free space is smaller than 1GB.

<b>Continuous Recording</b>	Enable or disable this function.
<b>Record File Type</b>	Choose a video profile to record.
<b>Disk</b>	Save recorded files to SD card or remote SAMBA server.
<b>Path</b>	Define the folder path for the recorded files.
<b>Restart</b>	Be careful, click this button will delete all continuous files recorded in SD card or remote SAMBA server.

## 6.12. Recording List

### 6.12.1. Recording List

This page only shows the event recording files which stored in SD card. User may play or delete the selected file.

Recording List
Continuous Recording List

Date	File	Trigger by	Size
20120329	20120326_113301.avi	motion00occur	2004 KB
20120330	20120326_115716.avi	motion00occur	2068 KB
20120326	20120326_115732.avi	motion00occur	2081 KB
	20120326_115740.avi	motion00occur	2067 KB
	20120326_115749.avi	motion00occur	2093 KB
	20120326_115755.avi	motion00occur	2059 KB
	20120326_115932.avi	motion00occur	2057 KB
	20120326_115943.avi	motion00occur	2056 KB
	20120326_115951.avi	motion00occur	2090 KB
	20120326_121234.avi	motion00occur	2074 KB
	20120326_121329.avi	motion00occur	2067 KB
	20120326_121411.avi	motion00occur	2056 KB

Reload
Play Remove

### 6.12.2. Continuous Recording List

This page only shows the continuous recording files which stored in SD card or remote SAMBA server. User may play or delete the selected file.

Recording List
Continuous Recording List

Disk: SAMBA Server  
Path: PLANET-00304FA2623A

Date	File	Trigger by	Size
20120326	20120326_113156.avi	continuous	15506 KB
	20120326_113656.avi	continuous	17931 KB
	20120326_114156.avi	continuous	19834 KB
	20120326_114657.avi	continuous	19608 KB
	20120326_115157.avi	continuous	19150 KB
	20120326_115659.avi	continuous	50094 KB
	20120326_120200.avi	continuous	20253 KB
	20120326_120701.avi	continuous	19704 KB
	20120326_121201.avi	continuous	27162 KB

Reload
Play Remove

## 6.13. Event Server Configuration

### 6.13.1. FTP Server

You may setup FTP parameters for further operation of Event Schedule. That's, if users want to send the alarm message to an FTP server, it will need to configure parameters here and also add at least one event schedule to enable event triggering as SMTP.

FTP Server
TCP Server
HTTP Server
SAMBA Server

Name	FTP Server	FTP Port	FTP Path
FTP	192.168.0.174	21	/anthony/test

Name	FTP	(< 22 Digits)
FTP Server	192.168.0.174	(< 65 Digits) <input type="button" value="Test"/>
FTP Login Name	admin	(< 22 Digits)
FTP Login Password	*****	(< 22 Digits)
FTP Port	21	(1 ~ 65535)
FTP Path	/admin/test	(< 65 Digits)
FTP Passive Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	

**Name** User can specify multiple FTP paths as wish. Therefore, user needs to specify a name for each FTP setting.

**FTP Server** Type the server name or the IP address of the FTP server.

**Test** Check the FTP server whether this account is available or not.

**FTP Login name** Type the user name for the FTP server.

**FTP Login Password** Type the password for the FTP server.

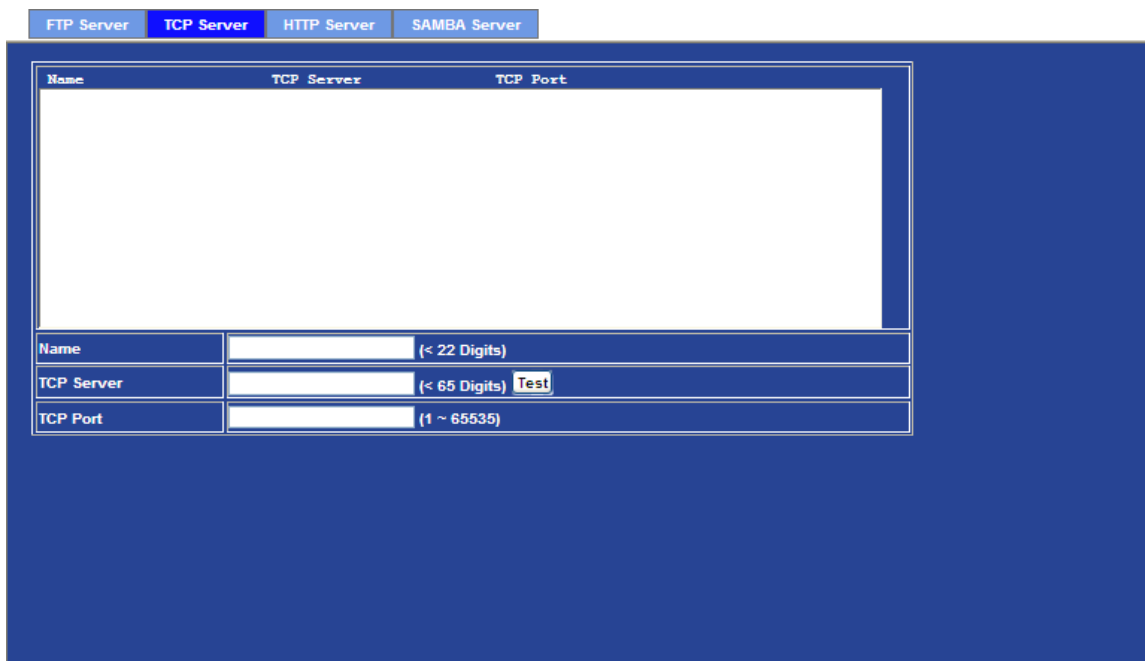
**FTP Port** Set port number of FTP service.

**FTP Path** Set working directory path of FTP server.

**FTP Passive Mode** Select passive or active mode connecting to FTP server.

### 6.13.2. TCP Server

In addition to send video file to FTP server, the device also can send event message to specified TCP server.



Name	TCP Server	TCP Port

Name  (< 22 Digits)  
 TCP Server  (< 65 Digits)   
 TCP Port  (1 ~ 65535)

**Name** User can specify multiple TCP servers as wish. Therefore, user needs to specify a name for each TCP server setting.

**TCP Server** Type the server name or the IP address of the TCP server.

**TCP Port** Set port number of TCP server.

### 6.13.3. HTTP Server

The device also can send event message to specified HTTP server.



<b>Name</b>	User can specify multiple HTTP servers as wish. Therefore, user needs to specify a name for each HTTP server setting.
<b>URL</b>	Type the server name or the IP address of the HTTP server.
<b>Test</b>	Check the HTTP server whether it is available or not.
<b>HTTP Login name</b>	Type the user name for the HTTP server.
<b>HTTP Login Password</b>	Type the password for the HTTP server.
<b>Proxy Address</b>	Type the server name or the IP address of the HTTP Proxy.
<b>Proxy Login name</b>	Type the user name for the HTTP Proxy.
<b>Proxy Login Password</b>	Type the password for the HTTP Proxy.
<b>Proxy Port</b>	Set port number of Proxy.

#### 6.13.4. SAMBA Server

The device also can send video stream to specified SAMBA server. Most of the time, the SAMBA server will be another PC or NAS server.

FTP Server
TCP Server
HTTP Server
**SAMBA Server**

Name	SAMBA Server	SAMBA Path
samba	192.168.0.201	share

Name	samba	(< 22 Digits)
SAMBA Server	192.168.0.201	(< 65 Digits) <b>Test</b>
SAMBA Login Name	test	(< 22 Digits)
SAMBA Login Password	*****	(< 22 Digits)
SAMBA Path	share	(< 65 Digits)

<b>Name</b>	User can specify multiple HTTP servers as wish. Therefore, user needs to specify a name for each HTTP server setting.
<b>SAMBA Server</b>	Type the server name or the IP address of the SAMBA server.
<b>Test</b>	Check the SAMBA server whether this account is available or not.
<b>SAMBA Login name</b>	Type the user name for the SAMBA server.
<b>SAMBA Login Password</b>	Type the password for the SAMBA server.
<b>SAMBA Path</b>	Set working directory path of SAMBA server.

## 6.14. Event Schedule Configuration

This menu is used to specify the schedule of Event or Schedule Trigger and activate the some actions provided by this device. Where the Schedule Trigger will be activated by user-define interval without event happened.

Setting	Record	Port Status
Name	<input type="text"/>	
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Type	<input checked="" type="radio"/> Event Trigger <input type="radio"/> Schedule Trigger, Interval <input type="text" value="60"/> ( Seconds)	
Enable Time	<input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Start from <input type="text" value="0"/> : <input type="text" value="0"/> , Duration <input type="text" value="24"/> : <input type="text" value="0"/> ((max 168:00 hours) )	
Trigger by	<input type="checkbox"/> Sensor <input type="text" value="Change to active"/> <input type="checkbox"/> Motion Area <input type="text" value="DefaultWindow"/> <input type="checkbox"/> Camera Tampering <input type="checkbox"/> Audio Detection <input type="text" value="Over Alarm Level"/>	
Record File Prefix	<input type="text"/> (0 ~ 48 Digits)	
Action	<input type="checkbox"/> Voice Alert, Duration <input type="text" value="5"/> ( 0~86400 Seconds ) <input type="checkbox"/> Alarm Out, Duration <input type="text" value="5"/> ( 0~86400 Seconds ) <input type="checkbox"/> Send FTP <input type="text" value=""/> <input type="checkbox"/> Send TCP <input type="text" value=""/> <input type="checkbox"/> Send HTTP <input type="text" value=""/> <input type="checkbox"/> Send E-Mail <input type="checkbox"/> Send SD <input type="checkbox"/> Send Samba <input type="text" value=""/> <input type="checkbox"/> ICR <input type="text" value="0"/> ( 0~86400 Seconds )	

**Name** Name of the Event or Schedule.

**Enable** Enable or disable this Event or Schedule.

**Type** Schedule start with Event trigger or Schedule trigger.

**Enable Time** Define the feasible time slot.

**Trigger by** Select the triggered sources with event trigger.

**Record File Prefix** Define the prefix of recorded filename

**Action** Define the actions once event triggered.

### Example1.

Send file to FTP server by motion triggered always:

**Step 1** Select event trigger

**Step 2** Enable time: start from 00:00 to 24:00 every day

**Step 3** Trigger by: Motion Area (Added in Object Detection page)

**Step 4** Action: Send FTP (Add in Event Server -> FTP Server page)

Setting		Record	Port Status
Name	Enable	Type	Weekday
Sent To FTP	yes	Event	1111111
Start	Duration	Trigger by Prefix	Action
0:0	24:0	x,M0,x,x	FTP
<div> <div>Name</div> <div>Sent To FTP</div> </div>			
<div> <div>Enable</div> <div> <input checked="" type="radio"/> Yes           <input type="radio"/> No         </div> </div>			
<div> <div>Type</div> <div> <input checked="" type="radio"/> Event Trigger           <input type="radio"/> Schedule Trigger, Interval <input type="text" value="60"/> ( Seconds )         </div> </div>			
<div> <div>Enable Time</div> <div> <input checked="" type="checkbox"/> Sun           <input checked="" type="checkbox"/> Mon           <input checked="" type="checkbox"/> Tue           <input checked="" type="checkbox"/> Wed           <input checked="" type="checkbox"/> Thu           <input checked="" type="checkbox"/> Fri           <input checked="" type="checkbox"/> Sat         </div> </div>			
<div> <div>Start from</div> <div> <input type="text" value="0"/> : <input type="text" value="0"/> , Duration <input type="text" value="24"/> : <input type="text" value="0"/> ((max 168:00 hours )         </div> </div>			
<div> <div>Trigger by</div> <div> <input type="checkbox"/> Sensor <input type="text" value="Change to active"/> </div> </div>			
<div> <div> <input checked="" type="checkbox"/> Motion Area <input type="text" value="DefaultWindow"/> </div> </div>			
<div> <div> <input type="checkbox"/> Camera Tampering         </div> </div>			
<div> <div> <input type="checkbox"/> Audio Detection <input type="text" value="Over Alarm Level"/> </div> </div>			
<div> <div>Record File Prefix</div> <div> <input type="text" value=""/> (0 ~ 48 Digits)         </div> </div>			
<div> <div> <input type="checkbox"/> Voice Alert, Duration <input type="text" value=""/> ( 0~86400 Seconds )         </div> </div>			
<div> <div> <input type="checkbox"/> Alarm Out, Duration <input type="text" value=""/> ( 0~86400 Seconds )         </div> </div>			
<div> <div> <input checked="" type="checkbox"/> Send FTP <input type="text" value="FTP"/> </div> </div>			
<div> <div> <input type="checkbox"/> Send TCP <input type="text" value=""/> </div> </div>			
<div> <div> <input type="checkbox"/> Send HTTP <input type="text" value=""/> </div> </div>			

### Example2.

Send file to E-Mail server by motion triggered from Friday 18:00 to Saturday 06:00

**Step 1** Select event trigger.

**Step 2** Enable time: start from Friday 18:00 and keep work in 12 hours, so it will stop on Saturday 06:00.

**Step 3** Trigger by: Motion Area (Added in Object Detection page)

**Step 4** Action: Send e-mail (Add in E-Mail page)

- i. To email address: You need to input the receiver email address.
- ii. Subject: You could specify the email subject.
- iii. Message: You could specify the email content.

Setting		Record	Port Status
Name	Enable	Type	Weekday
Sent To E-mail	yes	Event	0000010
Start	Duration	Trigger by Prefix	Action
18:0	12:0	x,M0,x,x	SMTP
<div> <div>Name</div> <div>Sent To E-mail</div> </div>			
<div> <div>Enable</div> <div> <input checked="" type="radio"/> Yes           <input type="radio"/> No         </div> </div>			
<div> <div>Type</div> <div> <input checked="" type="radio"/> Event Trigger           <input type="radio"/> Schedule Trigger, Interval <input type="text" value="60"/> ( Seconds )         </div> </div>			
<div> <div>Enable Time</div> <div> <input type="checkbox"/> Sun           <input type="checkbox"/> Mon           <input type="checkbox"/> Tue           <input type="checkbox"/> Wed           <input type="checkbox"/> Thu           <input checked="" type="checkbox"/> Fri           <input type="checkbox"/> Sat         </div> </div>			
<div> <div>Start from</div> <div>18</div> <div>:</div> <div>0</div> <div>, Duration</div> <div>12</div> <div>:</div> <div>0</div> <div>((max 168:00 hours))</div> </div>			
<div> <div>Trigger by</div> <div> <input type="checkbox"/> Sensor <input type="text" value="Change to active"/> </div> </div>			
<div> <input checked="" type="checkbox"/> Motion Area <input type="text" value="DefaultWindow"/> </div>			
<div> <input type="checkbox"/> Camera Tampering         </div>			
<div> <input type="checkbox"/> Audio Detection <input type="text" value="Over Alarm Level"/> </div>			
<div> <div>Record File Prefix</div> <div><input type="text" value=""/></div> <div>(0 ~ 48 Digits)</div> </div>			
<div> <input type="checkbox"/> Voice Alert, Duration <input type="text" value=""/> ( 0~86400 Seconds )         </div>			
<div> <input type="checkbox"/> Alarm Out, Duration <input type="text" value=""/> ( 0~86400 Seconds )         </div>			
<div> <input type="checkbox"/> Send FTP <input type="text" value=""/> </div>			
<div> <input type="checkbox"/> Send TCP <input type="text" value=""/> </div>			
<div> <input type="checkbox"/> Send HTTP <input type="text" value=""/> </div>			
<div> <input checked="" type="checkbox"/> Send E-Mail         </div>			

### Example3.

Enable Voice Alert every 10-minute during 18:00 to 24:00 from Monday to Friday.

**Step 1** Type: Select schedule trigger and interval is 10-minute.

**Step 2** Enable Time: Select Monday to Friday, and set start time from 18:00 and keep work in 6 hours.

**Step 3** Trigger by: You do not need to choose it, because this will be triggered every minute.

**Step 4** Action: Voice Alert.

Setting		Record	Port Status					
Name	Enable	Type	Weekday	Start	Duration	Trigger by	Prefix	Action
Trigger_Voice_alert	yes	Schedule	0111110	18:0	6:0	x,M0,x,x		VOICE
Name	Trigger_Voice_alert							
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No							
Type	<input type="radio"/> Event Trigger <input checked="" type="radio"/> Schedule Trigger, Interval <input type="text" value="600"/> ( Seconds )							
Enable Time	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat Start from <input type="text" value="18"/> : <input type="text" value="0"/> , Duration <input type="text" value="6"/> : <input type="text" value="0"/> ((max 168:00 hours ) )							
Trigger by	<input type="checkbox"/> Sensor <input type="text" value="Change to active"/> <input checked="" type="checkbox"/> Motion Area <input type="text" value="DefaultWindow"/> <input type="checkbox"/> Camera Tampering <input type="checkbox"/> Audio Detection <input type="text" value="Over Alarm Level"/>							
Record File Prefix	<input type="text"/> (0 ~ 48 Digits)							
Action	<input checked="" type="checkbox"/> Voice Alert, Duration <input type="text" value="10"/> ( 0~86400 Seconds ) <input type="checkbox"/> Alarm Out, Duration <input type="text"/> ( 0~86400 Seconds ) <input type="checkbox"/> Send FTP <input type="text"/> <input type="checkbox"/> Send TCP <input type="text"/> <input type="checkbox"/> Send HTTP <input type="text"/>							

## 6.15. Record Configuration

User can choose the type of record file for event or schedule application.

Setting	Record	Port Status
Record File Type	Profile1 h264 / 1536x1536	
Record File Prefix		
Pre Trigger Duration	5	(0 ~ 20 Seconds)
Best Effort Duration	30	(1 ~ 60 Seconds)
Max File Size	3072	(256 ~ 3072 Bytes)

**Record File Type** Choose AVI or JPEG file format for record file.

**Record File Prefix** Define the prefix of recorded filename.

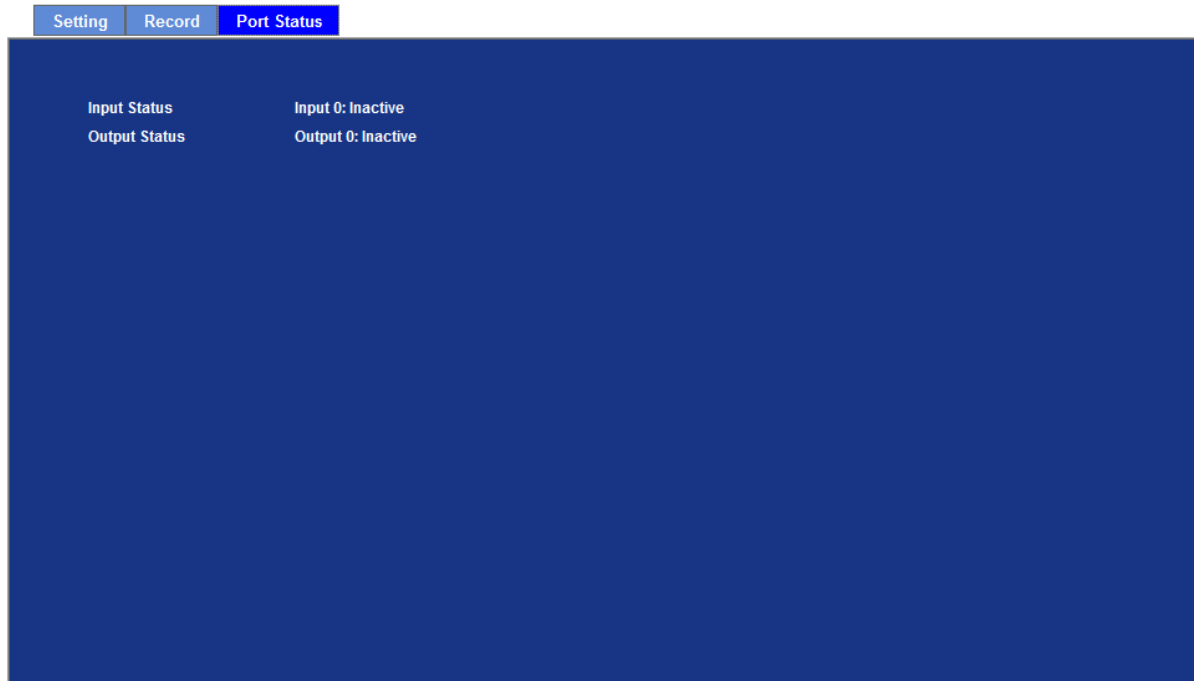
**Pre-Trigger Duration** Define the maximum duration of pre-alarm.

**Best Effort Duration** Define the best effort duration of post-alarm.

**Max File Size** Define the maximum buffer size of record file.

## 6.16. Port Status

User can check the status of digital input and output (DIDO).



<b>Input Status</b>	Show either inactive or active.
---------------------	---------------------------------

<b>Output Status</b>	Show either inactive or active.
----------------------	---------------------------------

## Chapter 7. PLANET DDNS

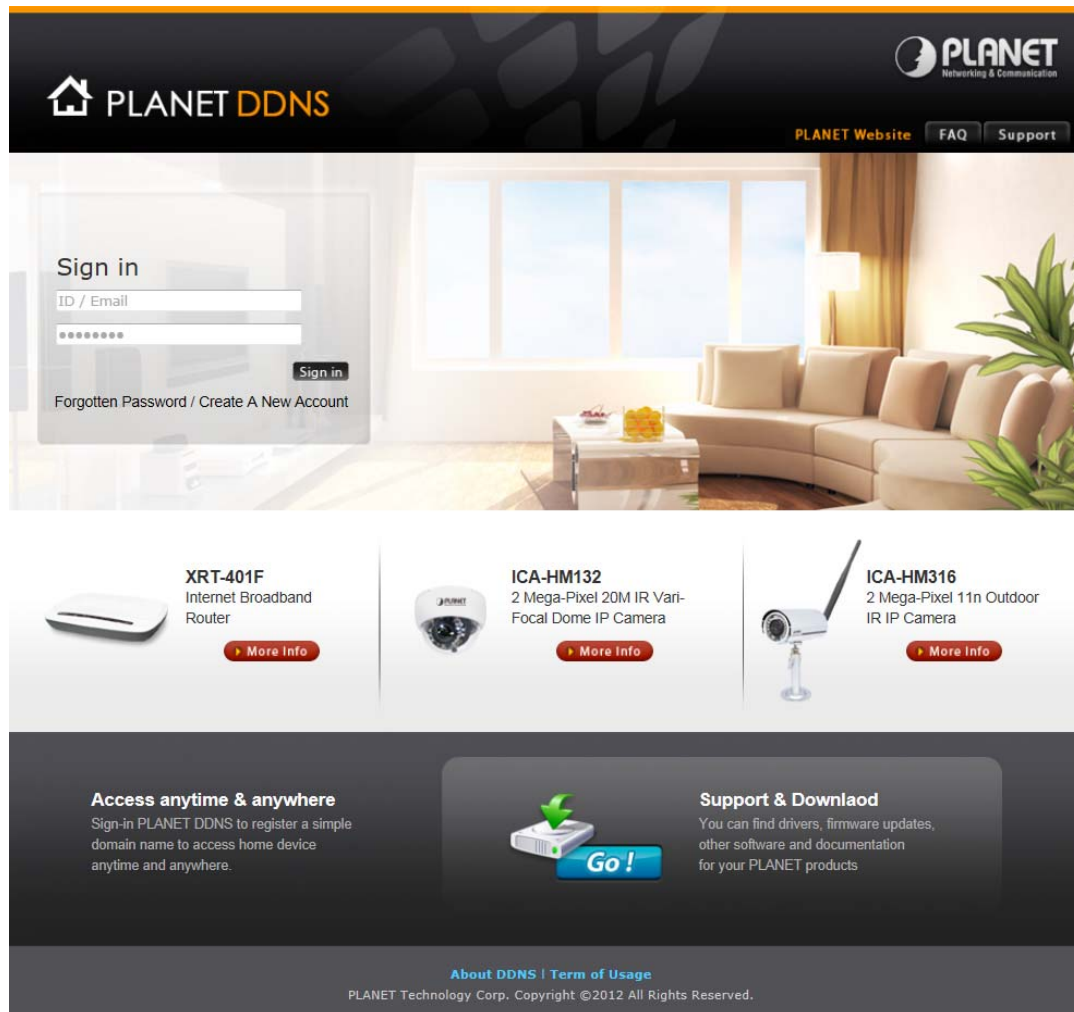
### Application

#### 1. Configure PLANET DDNS steps:

**Step 1** Enable DDNS option through accessing web page of IP Camera.

**Step 2** Select on DDNS server provide, and register an account if you do not use yet.

Let's take dyndns.org as an example. Register an account in <http://planetddns.com>



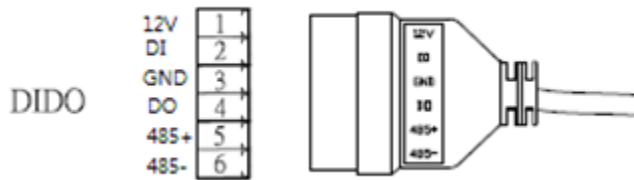
The screenshot shows the PLANET DDNS website. At the top, there's a navigation bar with the PLANET logo, a home icon, and links for 'PLANET Website', 'FAQ', and 'Support'. Below the navigation bar is a large banner image of a modern living room. On the left side of the banner, there's a 'Sign in' form with fields for 'ID / Email' and a password field, a 'Sign in' button, and links for 'Forgotten Password' and 'Create A New Account'. Below the banner, there are three product cards: 'XRT-401F Internet Broadband Router', 'ICA-HM132 2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera', and 'ICA-HM316 2 Mega-Pixel 11in Outdoor IR IP Camera'. Each card has a 'More Info' button. At the bottom, there's a dark grey section with two columns. The left column is titled 'Access anytime & anywhere' and describes the benefit of registering a simple domain name. The right column is titled 'Support & Download' and describes the availability of drivers, firmware updates, and documentation. A 'Go!' button is positioned between the two columns. At the very bottom, there's a footer with links for 'About DDNS' and 'Term of Usage', and a copyright notice for PLANET Technology Corp. ©2012 All Rights Reserved.

## Chapter 8. Alarm I/O

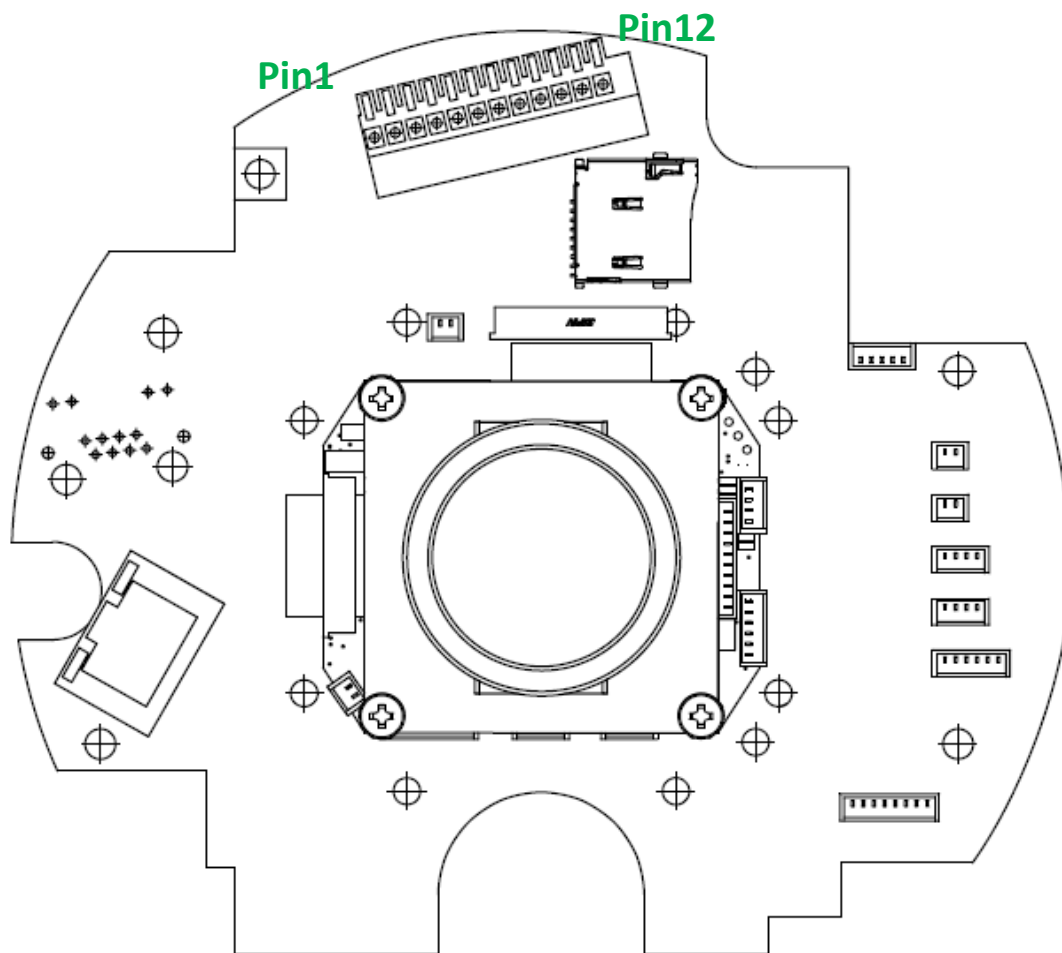
### Connector

Some features of the Camera can be activated by an external sensor that senses physical changes in the area device is monitoring. These changes can include intrusion detection or certain physical change in the monitored area. For examples, the external sensor can be a door switch or an infrared motion detector. These devices are customer provided, and are available from dealers who carry surveillance and security products. Electrically, they must be able to provide a momentary contact closure.

This device provides a general I/O terminal block with one digital input and one output for device control. Pin 2 and 3 can be connected to an external sensor. The input voltage will be monitored from the initial state 'LOW'. If the external sensor need 12VDC power, then it can connect to Pin1 (50mA maximum). The Alarm Output of pin 3 and 4 can be used to turn on or off the external device. The pin5 and 6 are connected to RS485 interface.



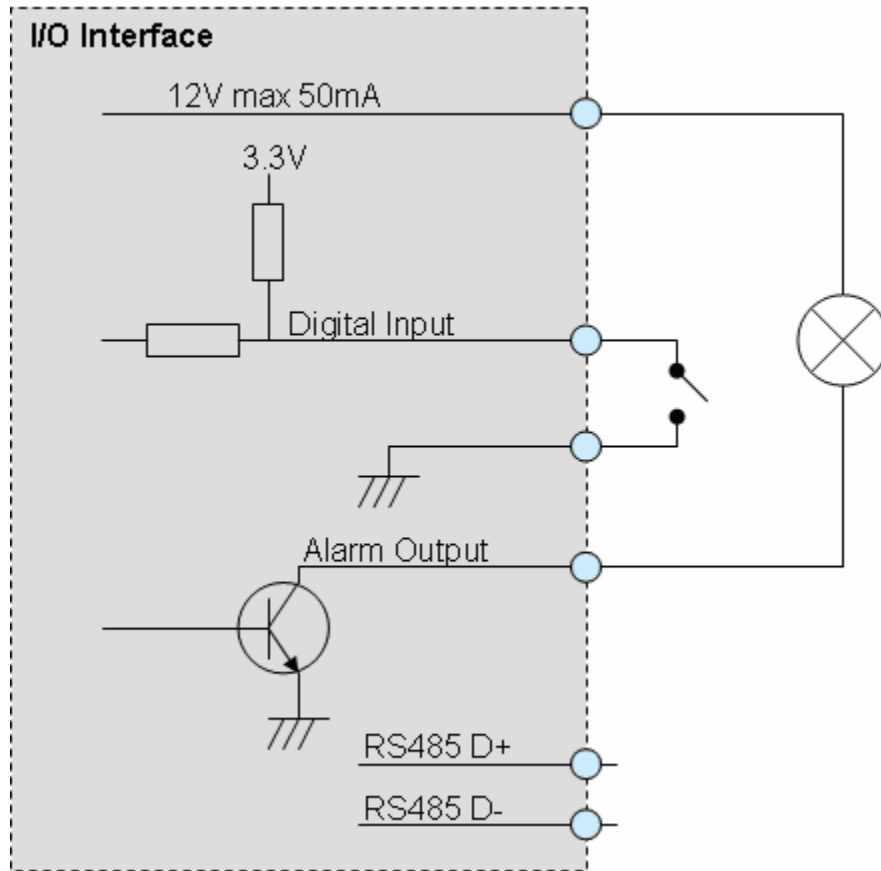
Pin	Function
1	12VDC power supply (50mA maximum)
2	Digital Input
3	GND
4	Alarm Output
5	RS485 data +
6	RS485 data -



Pin	Name	Function
1	12VDC in	DC 12V power input
2	Power GND	Power ground
3	MIC in	External MIC input
4	Audio out+	
5	Audio out-	
6	Video out	Composited video output
7	12VDC out	DC 12V output (50mA maximum)
8	DI	Digital signal input
9	GND	Digital ground
10	DO	Digital signal output
11	RS485+	RS485 data +
12	RS485-	RS485 data -

User can refer to the schematic below to make a proper connection between I/O connector and external sensor and output device.

### Explanation of External I/O Circuit Diagram:



### CAUTION!

- THE LOW VOLTAGE/CURRENT CIRCUITS AND HIGH VOLTAGE/CURRENT CIRCUITS ARE IN THE NETWORK CAMERA CIRCUIT. THE QUALIFIED ELECTRICIAN SHOULD DO THE WIRING NOT BY YOURSELF. INCORRECT WIRING COULD DAMAGE NETWORK CAMERA. YOU COULD RECEIVE THE FATAL ELECTRIC SHOCK.
- THE EXTERNAL I/O IS NOT CAPABLE OF CONNECTING DIRECTLY TO DEVICES THAT REQUIRE LARGE AMOUNTS OF CURRENT. IN SOME CASES, A CUSTOM INTERFACE CIRCUIT (CUSTOMER PROVIDED) MAY HAVE TO BE USED. SERIOUS DAMAGE TO NETWORK CAMERA MAY RESULT IF A DEVICE IS CONNECTED TO THE EXTERNAL I/O THAT EXCEEDS ITS ELECTRICAL CAPABILITY.

## Chapter 9.PING IP

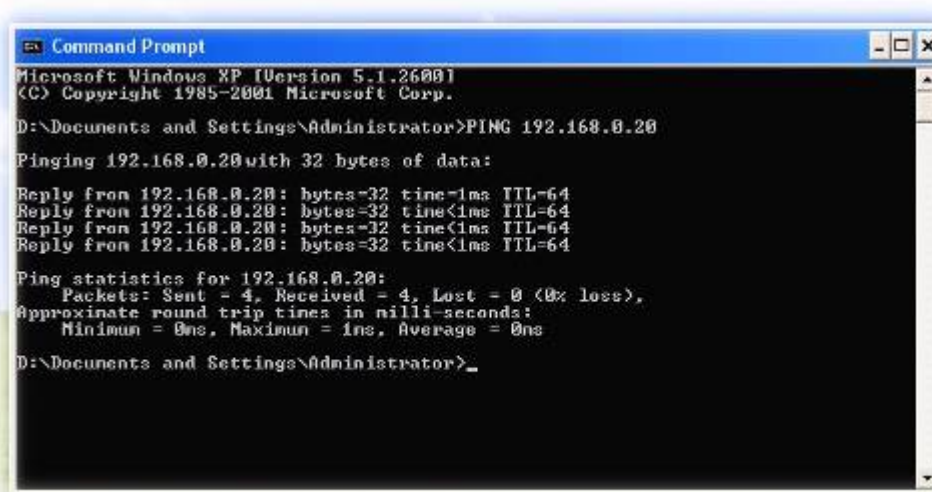
### Address

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 the device installed or if the IP address conflicts with any other devices over the network.

If you want to make sure the IP address of the device, utilize the PING command as follows:

- Launch a Command Prompt.
- Type ping x.x.x.x, where x.x.x.x is the IP address of the device. For example,  
ping 192.168.0.20

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



```
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 devices conflicts with the IP address of Network Camera, also can utilize the PING command but you must disconnect the Camera from the network first.

## Chapter 10. Bandwidth

### Estimation

The frame rate of video transmitted from the device depends on connection bandwidth between client and server, video resolution, codec type, and quality setting of server. Here is a guideline to help you roughly estimate the bandwidth requirements for your device.

The required bandwidth depends on content of video source. The slow motion video will produce smaller bit rate generally and fast motion will produce higher bit rate vice versa. Actual results generated by the device may be varying.

Image Resolution	Average range of data sizes for JPEG mode	Average bit rate for MPEG4 mode	Average bit rate for H.264 mode
384 x 384	10 ~ 30k byte per frame	256kbps~768kbps @ 22fps	192kbps~512kbps @ 22fps
768 x 768	25 ~ 60K byte per frame	-	384kbps~1536kbps @ 22fps
1280 x 1280	200 ~ 500k byte per frame	-	1536kbps~10000kbps @ 22fps
1536 x 1536	300 ~ 750k byte per frame	-	2048kbps~12000kbps @ 22fps

**NOTE:** Audio streaming also takes bandwidth around 32kbps. Some xDSL/Cable modem upload speeds could not even reach up to 128 kbps. Thus, you may not be able to receive good quality video while also streaming audio on a 128 kbps or lower connection. Even though the upload speed is more than 128kbps, for optimal video performance, disabling audio streaming will get better video performance.

## Chapter 11. Configure 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 setup as fixed IP address, also the port forwarding or Virtual Server function of router needs to be setup. 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 as below:

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

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

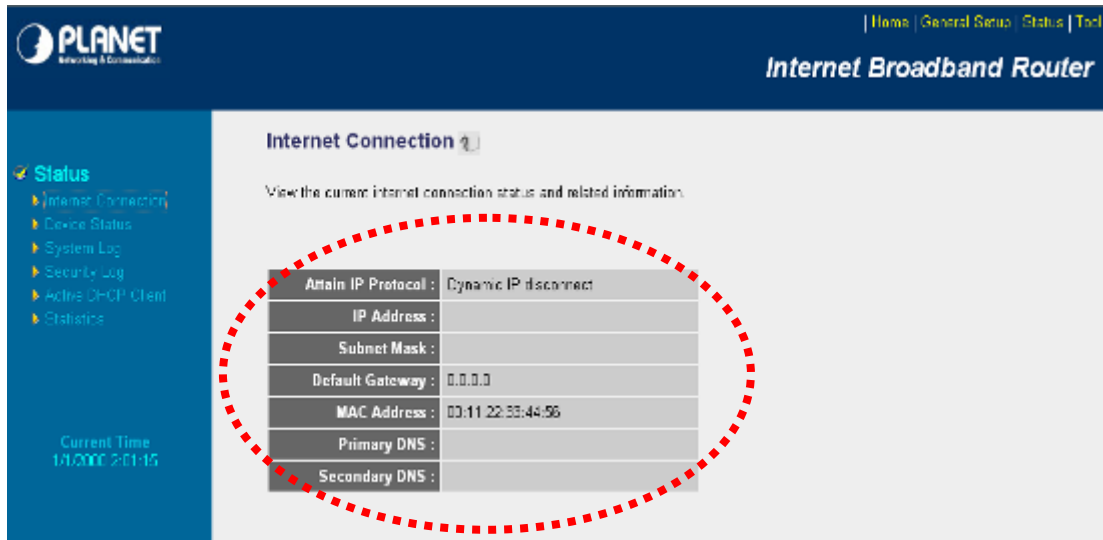
#### 1. Assign a local/fixed IP address to your device

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. The 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.



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.

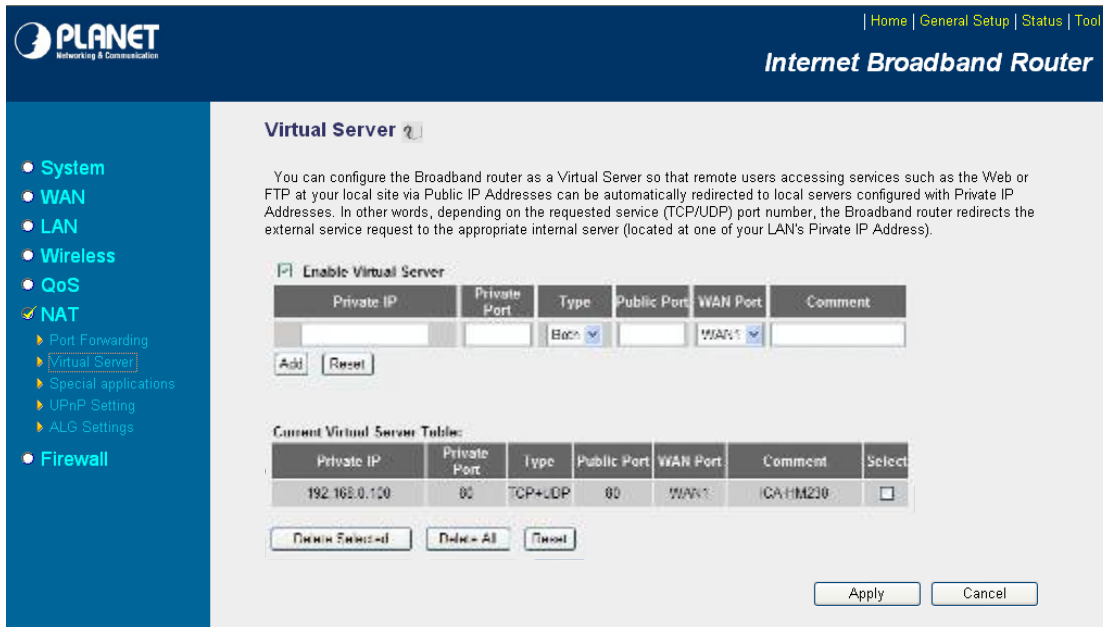
Follow these steps to configure your router's Virtual Server settings

- 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, click **Add**.

A check mark 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.



**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
		Both		WAN1	

Add Reset

Current Virtual Server Tables:

Private IP	Private Port	Type	Public Port	WAN Port	Comment	Select
192.168.0.100	80	TCP+UDP	80	WAN1	ICA-HM210	<input type="checkbox"/>

Delete Forward Delete All Delete

Apply Cancel

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 access from WAN by the router's WAN IP Address.

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

## Chapter 12.Power Line

### Frequency

COUNTRY	VOLTAGE	FREQUENCY	COMMENTS
Argentina	220V	50 Hz	*Neutral and line wires are reversed from that used in Australia and elsewhere.
Australia	230V*	50 Hz	*Outlets typically controlled by adjacent switch. Though <i>nominal</i> voltage has been officially changed to 230V, 240V is within tolerances and commonly found.
Austria	230V	50 Hz	
Brazil	110/220V*	60 Hz	*127V found in states of Bahia, Paran?(including Curitiba), Rio de Janeiro, S 綫 Paulo and Minas Gerais (though 220V may be found in some hotels). Other areas are 220V only, with the exception of Fortaleza (240V).
Canada	120V	60 Hz	
China, People's Republic of	220V	50 Hz	
Finland	230V	50 Hz	
France	230V	50 Hz	
Germany	230V	50 Hz	
Hong Kong	220V*	50 Hz	
India	230V	50 Hz	
Italy	230V	50 Hz	
Japan	100V	50/60 Hz*	*Eastern Japan 50 Hz (Tokyo, Kawasaki, Sapporo, Yokohoma, and Sendai); Western Japan 60 Hz (Osaka, Kyoto, Nagoya, Hiroshima)
Malaysia	240V	50 Hz	
Netherlands	230V	50 Hz	
Portugal	230V	50 Hz	
Spain	230V	50 Hz	
Sweden	230V	50 Hz	
Switzerland	230V	50 Hz	
Taiwan	110V	60 Hz	
Thailand	220V	50 Hz	

United Kingdom	230V*	50 Hz	*Outlets typically controlled by adjacent switch. Though <i>nominal</i> voltage has been officially changed to 230V, 240V is within tolerances and commonly found.
United States of America	120V	60 Hz	

## Chapter 13. 3GPP

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

**Note:** that to use the 3GPP function, it strongly recommends 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 currently)
2. Use the following URL to access:

**<rtsp://host/mpeg4/media.3gp>**

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 phone.

## Chapter 14. Troubleshooting & Frequently Asked

### Questions

Question	Answer or Resolution
<b>Features</b>	
The video and audio codec is adopted in the device.	The device utilizes H.264, MPEG4 and JPEG triple compression to providing high quality images. Where H.264 and MPEG4 are standards for video compression and JPEG is a standard for image compression. The audio codec is defined as G.711/G.726 for RTSP streaming.
The maximum number of users accesses the device simultaneously.	The maximum number of users is limited to 20. However, it also depends on the total bandwidth accessed to this device from clients. The maximum data throughput of the device is around 100~200Mbps for UDP mode and 50Mbps for HTTP mode. Therefore, the actual number of connected clients is varying by streaming mode, settings of resolution, codec type, frame rate and bandwidth. Obviously, the performance of the each connected client will slow down when many users are logged on.
The device can be used outdoors or not.	The device is weatherproof.
<b>Install this device</b>	
Status LED does not light up.	<ul style="list-style-type: none"> <li>• Check and confirm that the DC power adaptor, included in packaged, is used. Secure the power connector and re-power it on again.</li> <li>• If the problem is not solved, the device might be faulty. Contact your dealer for further help.</li> </ul>
The network cabling is required for the device.	The device uses Category 5 or better UTP cable allowing 10 Base-T, 100 Base-TX, or 1000 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	Username = <b>admin</b> and Password = <b>admin</b> . Note that it's all case sensitivity.
Forgot the username and password	Follow the steps below. <ol style="list-style-type: none"> <li>1. Restore the factory default setting by pressing and holding down more than 5 seconds on the device.</li> <li>2. Reconfigure the device.</li> </ol>
Forgot the IP address of	Check IP address of device by using the PLANET IPWizard II

the device.	program or by UPnP discovery.
PLANET IPWizard II program cannot find the device.	<ul style="list-style-type: none"> <li>• Re-power the device if cannot find the unit within 1 minutes.</li> <li>• Do not connect device over a router. IPWizard II program cannot detect device over a router.</li> <li>• If IP address is not assigned to the PC which running IPWizard II program, then IPWizard II program cannot find device. Make sure that IP address is assigned to the PC properly.</li> <li>• Antivirus software on the PC might interfere with the setup program. Disable the firewall of the antivirus software during setting up this device.</li> <li>• Check the firewall setting of your PC or Notebook.</li> </ul>
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 IPWizard II program fails to save the network parameters.	<ul style="list-style-type: none"> <li>• Network may have trouble. Confirm the parameters and connections of the device.</li> </ul>
<b>UPnP NAT Traversal</b>	
Cannot work with NAT router	<ul style="list-style-type: none"> <li>• Maybe NAT router does not support UPnP function. Please check user's manual of router and turn on UPnP function.</li> <li>• Maybe UPnP function of NAT router is not compatible to the IP camera. Please contact your dealer to get the approval routers list.</li> </ul>
Some IP cameras are working but others are failed	<ul style="list-style-type: none"> <li>• Maybe too many IP cameras have been installed on the LAN, and then 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.</li> </ul>
<b>Access this device</b>	
Cannot access the login page and other web pages of the Network Camera from Internet Explorer	<ul style="list-style-type: none"> <li>• 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.</li> <li>• May be due to 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.</li> <li>• Make sure the Internet connection and setting is ok.</li> <li>• Make sure enter the IP address of Internet Explorer is correct. If the Network Camera has a dynamic address, it may have changed since you last checked it.</li> <li>• Network congestion may prevent the web page appearing quickly. Wait for a while.</li> </ul> <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"> <li>• Make sure the http port used by the Network Camera,</li> </ul>

	<p>default=80, is forward to the Network Camera's private IP address.</p> <ul style="list-style-type: none"> <li>• The port number assigned in your Network Camera might not be available via Internet. Check your ISP for available port.</li> <li>• The proxy server may prevent you from connecting directly to the Network Camera, set up not to use the proxy server.</li> <li>• Confirm that Default Gateway address is correct.</li> <li>• The router needs Port Forwarding feature. Refer to your router's manual for details.</li> <li>• Packet Filtering of the router may prohibit access from an external network. Refer to your router's manual for details.</li> <li>• Access the Network Camera from the Internet with the global IP address of the router and port number of Network Camera.</li> <li>• 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.</li> <li>• When you use DDNS, you need to set Default Gateway and DNS server address.</li> <li>• If it's not working after above procedure, reset Network Camera to default setting and installed it again.</li> <li>• If the problem is not solved, the Network Camera might be faulty. Contact your dealer for further help.</li> </ul>
Image or video does not appear in the main page.	<ul style="list-style-type: none"> <li>• The first time the PC connects to Network Camera, a pop-up <b>Security Warning window</b> will appear to download ActiveX Controls. When using Windows XP, or Vista, log on with an appropriate account that is authorized to install applications.</li> <li>• Network congestion may prevent the Image screen from appearing quickly. You may choose lower resolution to reduce the required bandwidth.</li> </ul>
Check the device's ActiveX is installed on your computer	<p>Go to C:\Windows\Downloaded Program Files and check to see if there is an entry for the file "<b>IPCamera Control</b>". 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>
Internet Explorer displays the following message: "Your current security settings prohibit downloading ActiveX controls".	<p>Setup the IE security settings or configure the individual settings to allow downloading and scripting of ActiveX controls.</p>
The device work locally but not externally.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Make sure that the device isn't conflicting with any other web</li> </ul>

	<p>server running on your LAN.</p> <ul style="list-style-type: none"> <li>• Check the configuration of the router settings allow the device to be accessed outside your local LAN.</li> <li>• Check the bandwidth of Internet connection. If the Internet bandwidth is lower than target bit rate, the video streaming will not work correctly.</li> </ul>
The unreadable characters are displayed.	Use the operating system of the selected language. Set the 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"> <li>• 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.</li> <li>• Check the bandwidth of Internet connection. If the Internet bandwidth is lower than target bit rate, the video streaming will not work correctly.</li> <li>• Ethernet switching hub can smooth the frame rate.</li> </ul>
Blank screen or very slow video when audio is enabled.	<ul style="list-style-type: none"> <li>• Your connection to the device does not have enough bandwidth to support a higher frame rate for the streamed image size. Try reducing the video streaming size to 384 x 384 and/or disabling audio.</li> <li>• Audio will consume 32 kbps. Disable audio to improve video. Your Internet connection may not have enough bandwidth to support streaming audio from the device.</li> </ul>
Image Transfer on e-mail or FTP does not work.	<ul style="list-style-type: none"> <li>• Default Gateway and DNS server address should be set up correctly.</li> <li>• If FTP does not work properly, ask your ISP or network administrator about the transferring mode of FTP server.</li> </ul>
<b>Video quality of the device</b>	
The focus on the Camera is bad.	<ul style="list-style-type: none"> <li>• The lens is dirty or dust is attached. Fingerprints, dust, stain, etc. on the lens can degrade the image quality.</li> </ul>
The color of the image is poor or strange.	<ul style="list-style-type: none"> <li>• Adjust White Balance.</li> <li>• To insure 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.</li> <li>• 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.</li> </ul>
Image flickers.	<ul style="list-style-type: none"> <li>• Wrong power line frequency makes images flicker. Make sure the 50 or 60Hz format of your device.</li> <li>• If the object is dark, the image will flicker. Make the condition around the Camera brighter.</li> </ul>
Noisy images occur.	The video images might be noisy if the device is located in a very low light environment. Make the condition around the camera brighter.
<b>Miscellaneous</b>	
Cannot play the recorded ASF file	Have installed Microsoft's DirectX 9.0 or later and use the Windows Media Player 11.0 or later to play the AVI filed recorded by the Device.