TRENDnet®

User's Guide

TV-IP121WN
1.01

Preface

Thank you for purchasing the TV-IP121WN, a powerful and high-quality image SecurView Wireless Day/Night Internet Camera. The infrared LEDs and light sensor enable the camera to capture images even in dark environments. The camera can be installed as a standalone system within your application environment easily and quickly, and supports remote management function so that you can access and control it using a Web browser on your computers.

This User Guide provides you with the instructions and illustrations on how to use your camera, which includes:

Chapter 1 **Introduction to Your Camera** describes the features of the camera. You will also know the components and functions of the camera.

Chapter 2 **Hardware Installation** helps you install the camera according to your application environment. You can use this camera at home, at work, at any where you want.

Chapter 3 **Accessing the Camera** lets you start using your camera without problem. The camera can be set up easily and work within your network environment instantly.

Chapter 4 **Configuring the Camera** guides you through the configuration of the camera using the web browser on your PC.

Chapter 5 **Using SecurView™ Pro** shows you the detail instructions on operating SecurView™ Pro software.

Chapter 6 **How to Access the Camera Behind a Router** provides the instruction how to setup your DDNS.

Chapter 7 **Appendix** provides the specification of the camera and some useful information for using your camera.

NOTE The illustrations and configuration values in this guide are for reference only. The actual settings depend on your practical application of the camera.

CONTENTS

PREFACE **1**
CHAPTER 1 ..... **4**
INTRODUCTION TO YOUR CAMERA **4**
1.1 CHECKING THE PACKAGE CONTENTS 4
1.2 GETTING TO KNOW YOUR CAMERA 5
1.3 FEATURES AND BENEFITS 7
1.4 SYSTEM REQUIREMENT 8
CHAPTER 2 ..... **9**
HARDWARE INSTALLATION **9**
2.1 INSTALLING THE CAMERA STAND 9
2.2 CONNECTING THE CAMERA TO LAN/WLAN 10
2.3 APPLICATIONS OF THE CAMERA 11
CHAPTER 3 ..... **12**
ACCESSING THE CAMERA **12**
3.1 USING IPSETUP 12
3.2 ACCESSING TO THE CAMERA 17
3.3 CONFIGURING THE IP ADDRESS OF THE PC 20
CHAPTER 4 ..... **21**
CONFIGURING THE CAMERA **21**
4.1 USING THE WEB CONFIGURATION 21
4.2 USING SMART WIZARD 22
4.3 BASIC SETUP 27
4.4 NETWORK SETTINGS 31
4.5 SETTING UP VIDEO & AUDIO 40
4.6 EVENT SERVER CONFIGURATION 43
4.7 MOTION DETECT 47
4.8 EVENT CONFIG 48
4.9 TOOLS 52
4.10 INFORMATION 54
CHAPTER 5 ..... **55**

SECURVIEW™ PRO SOFTWARE 55
5.1 INSTALLATION 56
5.2 USING SECURVIEW™ PRO 59
CHAPTER 6 90
HOW TO ACCESS THE CAMERA BEHIND A ROUTER 90
CHAPTER 7 96
APPENDIX 96
A.1 SPECIFICATION 96
A.2 GLOSSARY OF TERMS 98
LIMITED WARRANTY 107

CHAPTER 1

INTRODUCTION TO YOUR CAMERA

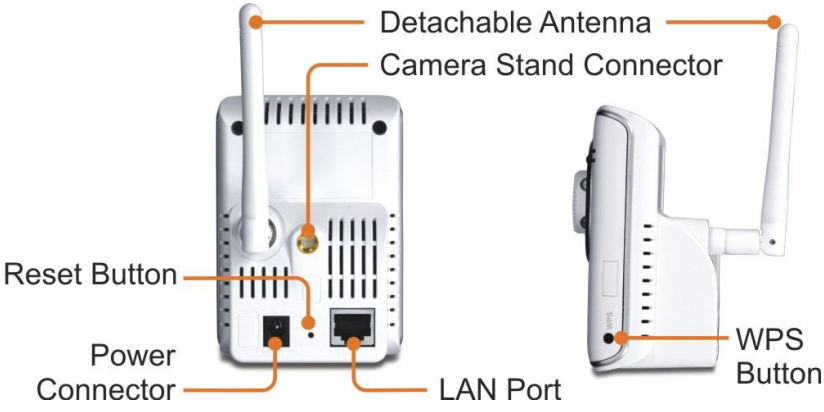
1.1 Checking the Package Contents

Check the items contained in the package carefully. You should have the following:

- TV-IP121WN
- 1 x CD-ROM (Utility & User's Guide)
- 1 x Multi-Language Quick Installation Guide
- 1 x External antenna
- 1 x 5V 2.5A power adapter
- 1 x Network cable
- 1 x Camera stand.

NOTE: If there is any packaging content missing, please contact with your local authorized dealer for replacement.

1.2 Getting to Know Your Camera



- **Built-in Microphone:** It allows the camera to receive the sound or voice

- **Infrared LEDs:** It allows your camera to capture clear images in a dark environment.
- **Lens:** Adjust the focus by rotate outside of the Lens.
- **Light Sensor:** It is used to trigger on and off the Infrared LEDs according to the environmental light level.
- **Power LED:** A steady orange light indicates the camera is powered on.
- **Link/Act LED:** A blinking green light indicates the camera's network connection correctly.
- **WPS Button:** A push button to help you to connect camera to your secured wireless network.
- **Detachable Antenna:** The detachable external antenna allows you to adjust its position to obtain the maximum signal.
- **Camera Stand Connector:** Connects the camera with the camera stand.
- **Power Connector:** Connects the AC power adapter to supply power to the camera.
- **LAN Port:** It is used to connect the network RJ-45 cable, which supports the Auto-MDIX so that the camera can detect the network speed automatically.
- **Reset Button:** Rest will be initiated when the reset button is pressed once. The power LED begins to flash.

  Factory Reset will be initiated when the reset button is pressed continuously for three seconds or when Power LED begins to light up. Release the reset button and the Power LED will begin to flash.

1.3 Features and Benefits

- **Audio Capability**
  The built-in microphone of the camera provides on-the-spot audio via the Internet, allowing you to monitor the on-site voice.

- **Day & Night Surveillance Supported**
  The six Infrared LEDs around the standard lens assembly (optional) enable the camera to capture crystal clear images in the dark environment or at night. When the Light Sensor detects the environmental light level becomes low, the camera captures the images in black & white mode using these infrared LEDs.

- **Remote Control Supported**
  By using a standard Web browser or the bundled SecurView™ Pro software application, the administrator can easily change the configuration, upgrade the firmware. The users are allowed to monitor the images and taking the snap via network.

- **Multiple Platforms Supported**
  The camera supports multiple network protocols, including TCP/IP, SMTP e-mail*, HTTP, and other Internet related protocols.

- **Multiple Applications Supported**
  Through the remote access technology, you can use the cameras to monitor various objects and places for your own purposes.
  For example, babies at home, patients in the hospital, offices and banks, and more. The camera can capture both still images and video clips, so that you can keep the archives and restore them at any time.

- **WPS (Wi-Fi Protected Setup) Supported**
  WPS is a new solution that simplifies the process of configuring Wi-Fi security settings, allowing you to establish a secure wireless network by simply pressing a button.

  Note: Support SSL with complimentary software

1.4 System Requirement

- **Networking**

  LAN: 10Base-T Ethernet or 100Base-TX Fast Ethernet, Auto-MDIX
  WLAN: Based on IEEE 802.11n technology, IEEE 802.11g/b

- **Accessing the Camera using Web Browser**

  Platform: Microsoft® Windows® 7/Vista/XP
  CPU: Intel Pentium III 800MHz or above
  RAM: 512MB
  Resolution: 800x600 or above
  User Interface: Microsoft® Internet Explorer 6.0 or above

- **Accessing the Camera using SecurView Pro**

  Platform: Microsoft® Windows® 7/Vista/XP
  Hardware Requirement:
  1 ~ 8 cameras: Intel Core 2 Duo; 2GB RAM
  9 ~ 32 cameras: Intel Core 2 Quad; 4GB RAM

NOTE: It is higher recommended that using a high performance computer to monitor multiple cameras.

CHAPTER 2

HARDWARE INSTALLATION

2.1 Installing the Camera Stand

The camera comes with a camera stand, which uses a swivel ball screw head to lock to the camera's screw hole. When the camera stand is attached, you can place the camera anywhere by mounting the camera through the three screw holes located in the base of the camera stand.

The Camera Stand

2.2 Connecting the Camera to LAN/WLAN

Use the provided Ethernet cable to connect the camera to your local area network (LAN).

When you connect the power adapter, the camera is powered on automatically. You can verify the power status from the Power LED on the front panel of the camera.

Once connected, the Link LED starts flashing green light and the camera is on standby and ready for use now.

If you use a wireless network in your application environment, you need to attach the included detachable antenna to the camera.

If your wireless network has set encryption, you can use WPS button or configure the wireless connection via a LAN connection.

NOTE: If the camera cannot connect to your wireless network, you need to install the camera in LAN and proceed with WLAN settings.

2.3 Applications of the Camera

The camera can be applied in multiple applications, including:

- Monitor local and remote places and objects via Internet or Intranet.
- Capture still images and video clips remotely.
- Upload images or send email messages with the still images attached.

The following diagram explains one of the typical applications for your camera and provides a basic example for installing the camera.

CHAPTER 3

ACCESSING THE CAMERA

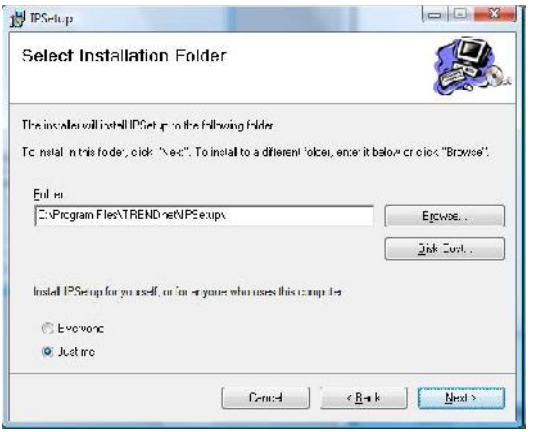
3.1 Using IPSetup

The camera comes with a convenient utility, IPSetup, which is included in the Installation CD-ROM, allowing you to search the camera on your network easily.

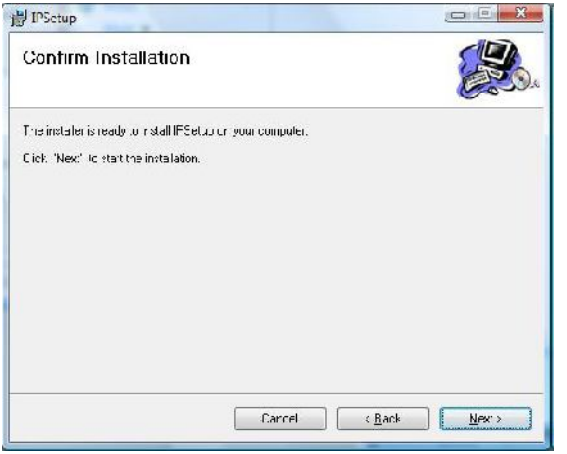
1. Insert the Installation CD-ROM into your computer's CD-ROM drive to initiate the Auto-Run program.

2. Click the **IPSetup** from the Auto-Run menu screen. Then the IPSetup Wizard will appear. Click **Next** when the **Welcome to the IPSetup Wizard** appears.

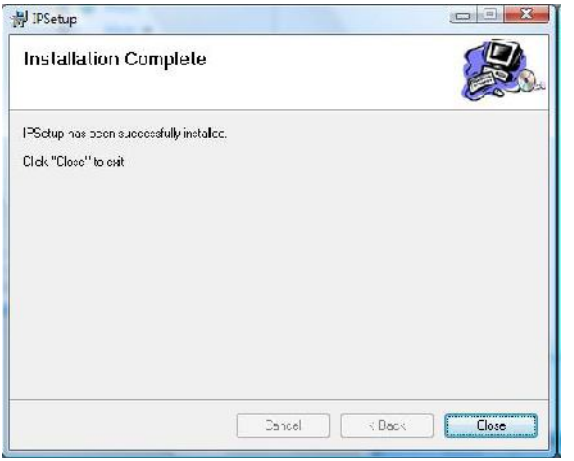
3. Click **Browse** to choose the desired destination location. By default, the destination location is C:\Program Files\TRENDnet\IPSetup. Then click **Next**.



4. Click **Next** to confirm the IPSetup software to be installed to the computer.

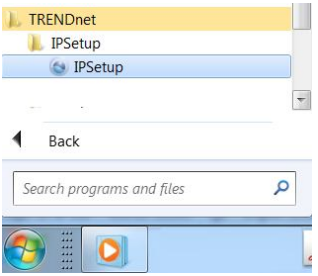


5. When the **Installation Complete** window appears, click **Close**.

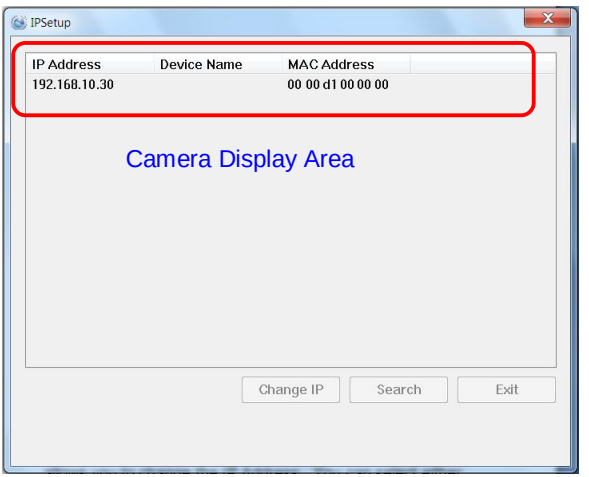


6. After installing the IPSetup utility, the application is automatically installed to your computer, and creates a folder in **Start\Program\TRENDnet\IPSetup**.

7. Click **Start**>**Programs**>**TRENDnet**>**IPSetup**, and then click **IPSetup**.



8. The IPSetup window will appear. It will search for the camera within the same network

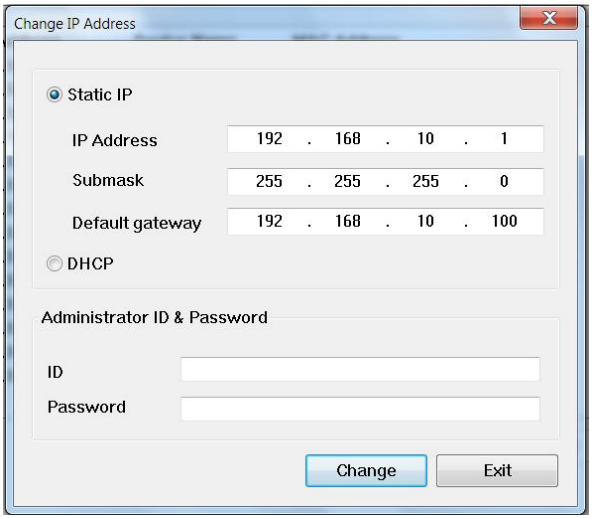


- **Camera Display Area:** By default, the IP setting on the Camera is set up DHCP. If you have DHCP server, the camera will automatic get the

IP address from DHCP server. If you do not have DHCP server on your network, it will show the default IP as 192.168.10.30.

Double click the IP address; it will link to Camera's Web Configuration page.

- **Change IP:** Click this button to bring up the following window. It allows you to change the IP Address. You can select either **Static IP** or click **DHCP**. Then, enter the Administrator ID & Password. By default the ID/Password is: **admin**. When complete, click **Change**.

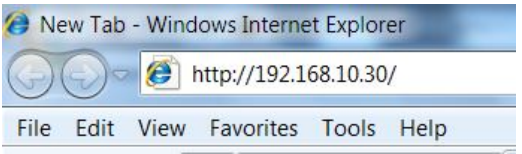


- **Search:** Click this button to search the connected camera in the same network
- **Exit:** Click this button to exit the program.

3.2 Accessing to the Camera

Access the camera:

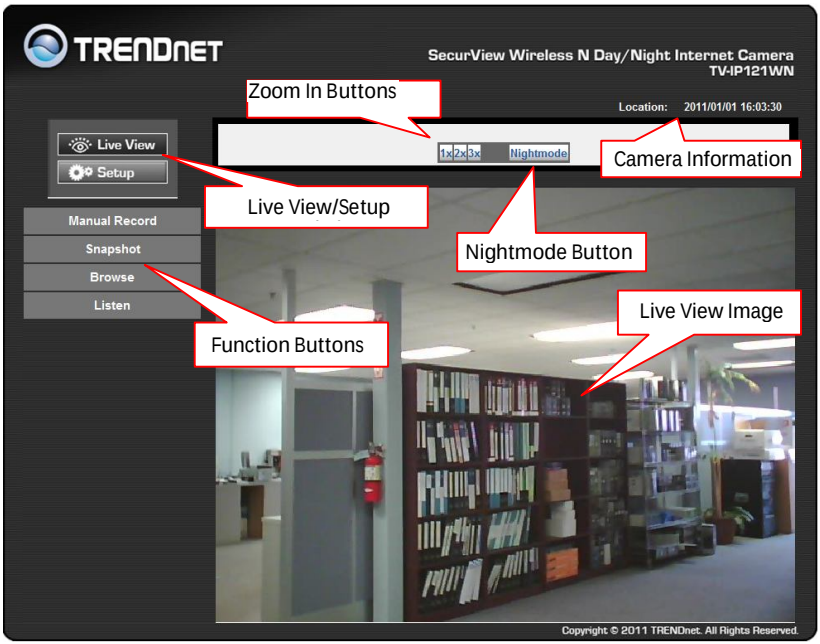
1. Open the Web browser on your computer (example showed in the User's Guide is based on the Internet Explorer).
2. Type the default IP address (192.168.10.30) or the IP address found by IPSetup in the Address bar, and then press [Enter].



3. When the login window appears, enter the default **User name** (admin) and **Password** (admin) and press **OK** to access to the main screen of the camera's Web Configuration.

NOTE: If you are initially access to the camera, you will be ask to install a new plug-in for the camera. Permission request depends on the Internet security settings of your computer. Click **Yes** to proceed.

After you login into the Web Configuration of the camera, the main page will appear as below:



The main page of the Web Configuration provides you with many useful information and functions, including:

- **Camera Information** – Display the camera's location and the current date & time. The information can be modified in the Web Configuration.
- **Live View Image** – Displays the real-time image of the connected camera.
- **Live View/Setup Switch** – Click **Setup** to configure the camera. For details, see Chapter 4.
- **Function Buttons** – Use these buttons to control the video functions.
  - **Manual Record** allows you to record and save a video clip.

- **Snapshot** allows you to capture and save a still image.
- **Browse** allows assign the destination folder to store the video clips and still images.
- **Listen** allows you receive the on-site sound and voice from the camera.

- **Zoom In Buttons** – Click the buttons to zoom in the live view image by 1x, 2x, and 3x.
- **Nightmode Button** – Click the button to enable the "nightshot mode" to deliver clearer images in the dark environment. However, this will reduce the frame rate of video setting.

NOTE: If you are using Microsoft 7/Vista platform, you may not be able to find these recorded files that are stored by **Snapshot** or **Manual Record**. You will need to disable the protected mode of Security in the IE Browser before manual record video file or taking a snapshot.

Please follow the below Steps:

1. Open IE Browser
2. Select **Tools→Internet Options**
3. Select **Security**
4. Uncheck the "**Enable Protected Mode**" then press **OK**

3.3 Configuring the IP Address of the PC

If you failed to access the camera, please check the IP address of your computer. The IP camera and computer's IP address must be in the same segment in order to communicate. Below is the procedure to change your computer's IP address.

1. On your computer, click **Start > Control Panel** to open the Control Panel window.
2. Double-click **Network Connection** to open the Network Connection window.
3. Right-click **Local Area Connection** and then click **Properties** from the shortcut menu.
4. When the Local Area Connection Properties window appears, select the **General** tab.
5. Select **Internet Protocol [TCP/IP]** and then click **Properties** to bring up the Internet Protocol [TCP/IP] Properties window.
6. To configure a fixed IP address that is within the segment of the camera, select the **Use the following IP address** option. Then, enter an IP address into the empty field. The suggested IP address is 192.168.10.x (x is 0~254 except 30), and the suggested Subnet mask is 255.255.255.0. The TV-IP121WN default IP address is 192.168.10.30.
7. When you are finished, click **OK**.

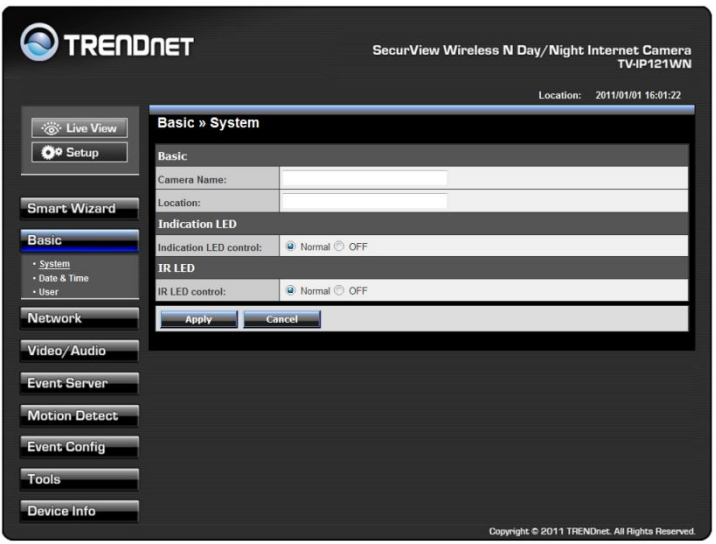
CHAPTER 4

CONFIGURING THE CAMERA

4.1 Using the Web Configuration

You can access and manage the camera through the Web browser and the provided software application SecurView™ Pro (see chapter 5 in more detail). This chapter describes the Web Configuration, and guides you through the configuration of the camera by using the web browser.

To configure the camera, click **Setup** on the main page of Web Configuration. The Web Configuration will start from the **Basic** page.

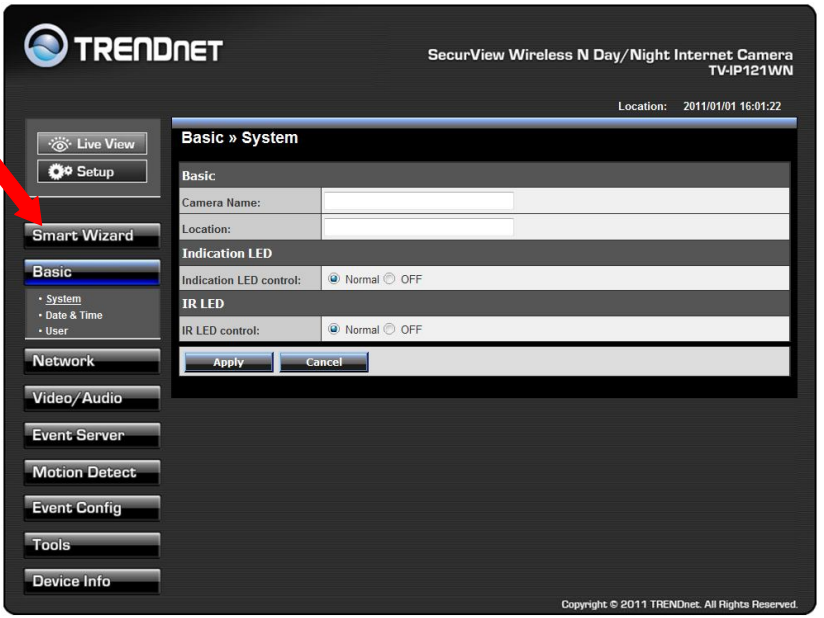


The Web Configuration contains the settings that are required for the camera in the left menu bar, including **Smart Wizard**, **Basic**, **Network**, **Video**, **Event Server**, **Motion detect**, **Event Config**, **Tools**, and **Information.**

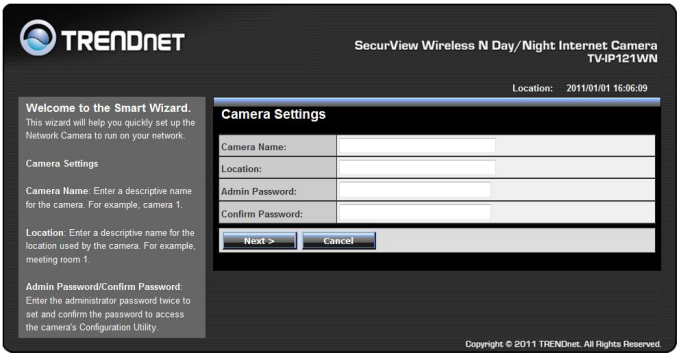
4.2 Using Smart Wizard

The camera's Smart Wizard lets you configure your camera easily and quickly. The wizard will guide you through the necessary settings with detailed instructions on each step.

To start the wizard, click **Smart Wizard** in the left menu bar.

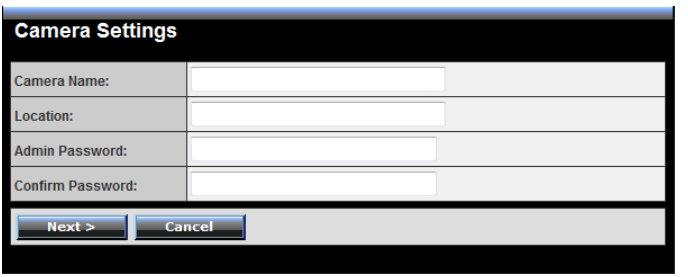


Setup Wizard main screen will pop up.



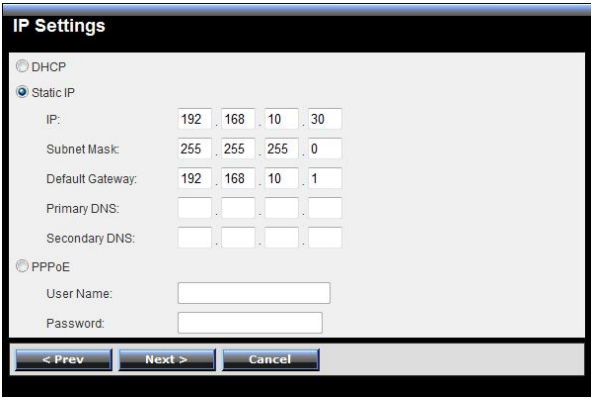
Step 1. Camera Settings

Enter **Camera name**, **Location**, new **Admin password** and enter the password again to confirm the new password, then click **NEXT**.



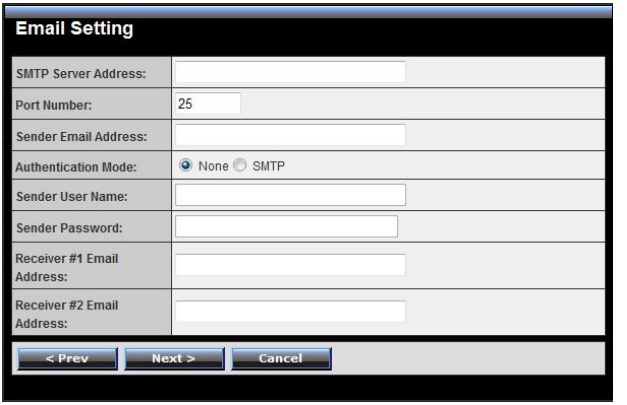
Step 2. IP Settings

Select the IP setting corresponding to your network, then click **NEXT**.



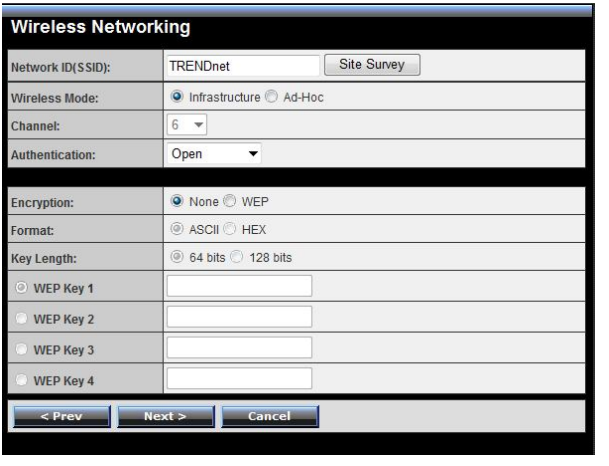
Step 3. Email Settings

Enter the required information on the Email setting, then click **NEXT**.



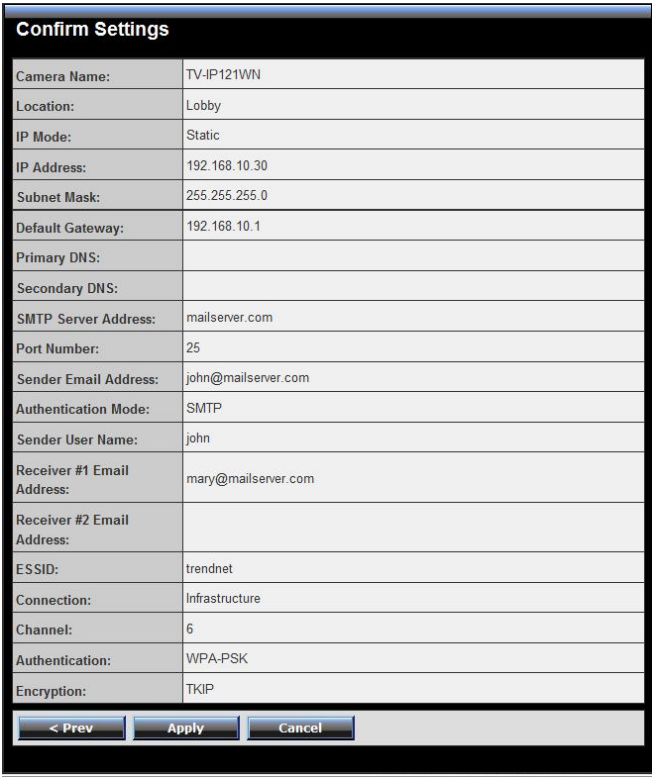
Step 4. Wireless Networking

Click Site Survey to select your wireless network's SSID, and complete all required encryption information, then click **NEXT**.



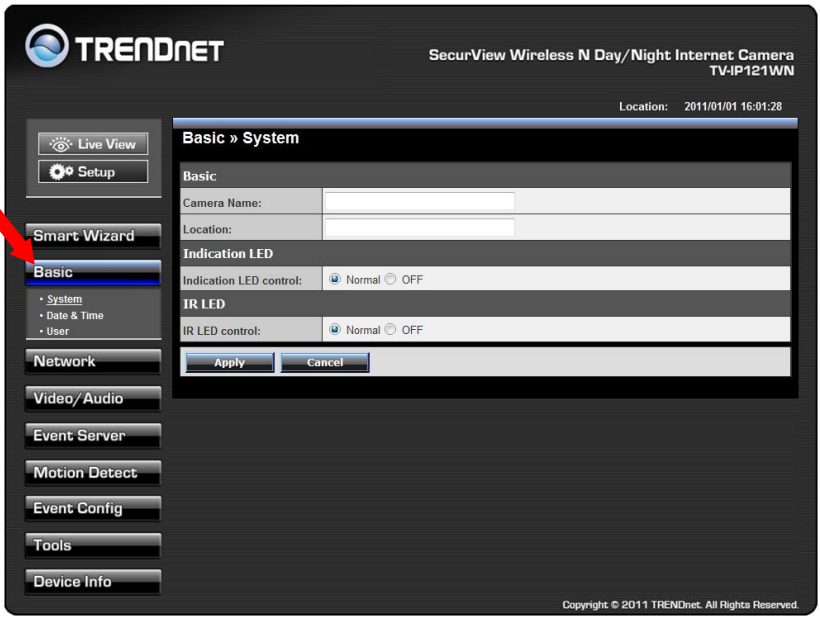
Step 5. Confirm Settings

This page shows all configuration of your camera. Click **Apply** to finish the wizard and reboot the camera. Click **Prev** to change the previous setting. Click **Cancel** to exit the Wizard without saving the setting.

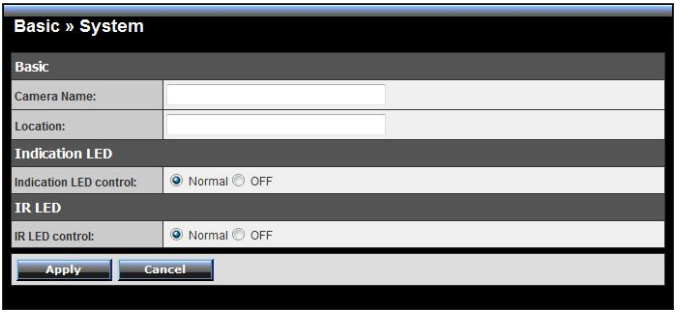


4.3 Basic Setup

The Basic menu contains three sub-menus that provide the system settings for the camera, such as the Camera Name, Location, Date & Time, and User management.



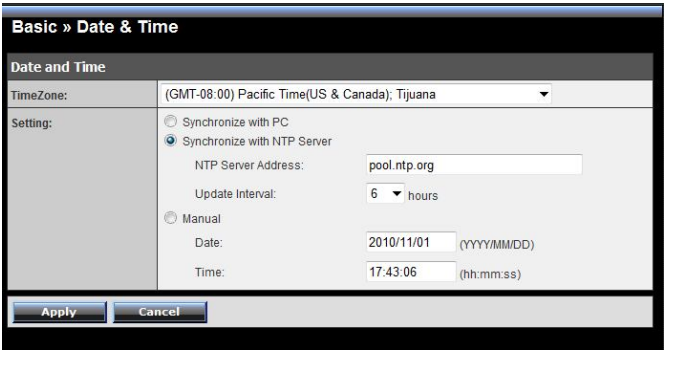
Basic >> System



- **Basic**
  - **Camera Name:** Enter a descriptive name for the camera.
  - **Location:** Enter a descriptive name for the location used by the camera.
- **Indication LED**

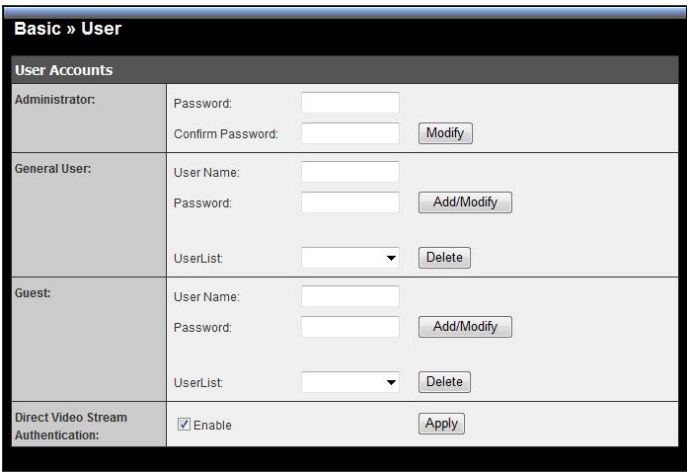
  This item allows you to set the LED illumination as desired. There are two options: **Normal** and **OFF**.

Basic >> Date & Time



- **Date & Time**
  - **TimeZone:** Select the proper time zone for the region from the pull-down menu.
  - **Synchronize with PC:** Select this option and the date & time settings of the camera will be synchronized with the connected computer.
  - **Synchronize with NTP Server:** Select this option and the time will be synchronized with the NTP Server. You need to enter the IP address of the server and select the update interval in the following two boxes.
  - **Manual:** Select this option to set the date and time manually.

Basic >> User



- **Administrator**

  To prevent unauthorized access to the camera's Web Configuration, you are strongly recommend to change the default administrator password. Type the administrator password twice to set and confirm the password.

- **General User**

- **User Name:** Enter the user's name you want to add to use the camera.
- **Password:** Enter the password for the new user.

  When you are finished, click **Add/Modify** to add the new user to the camera. To modify the user's information, select the one you want to modify from **User List** and click **Add/Modify**.
- **User List:** Display the existing users of the camera. To delete a user, select the one you want to delete and click **Delete**.

■ **Guest**
- **User Name:** Enter the guest's name you want to add to use the camera.
- **Password:** Enter the password for the new guest.
- **User List:** Display the existing guests of the camera. To delete a user, select the one you want to delete and click **Delete**.

■ **Direct Video Stream Authentication**:

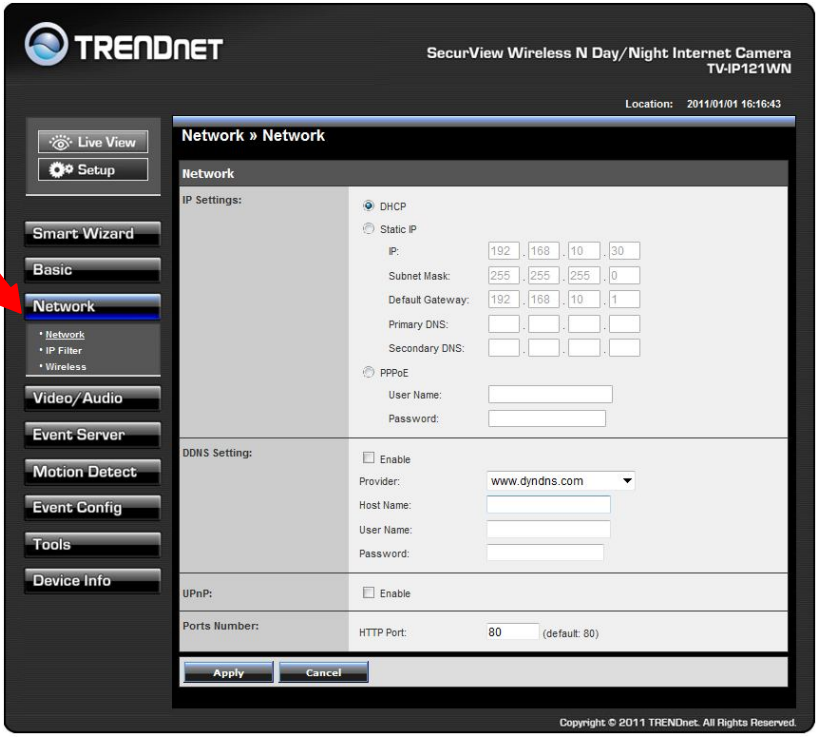
- **Enabled** = Direct link to the video stream prompts for authentication.
- **Disable** = Direct link to video does not prompt for authentication for ease of use when implementing or embedding the video stream into a custom application or webpage.

Examples of the Direct Link to video:
MJPEG Mode
http://camera_ip_address:port number/jpgview.htm

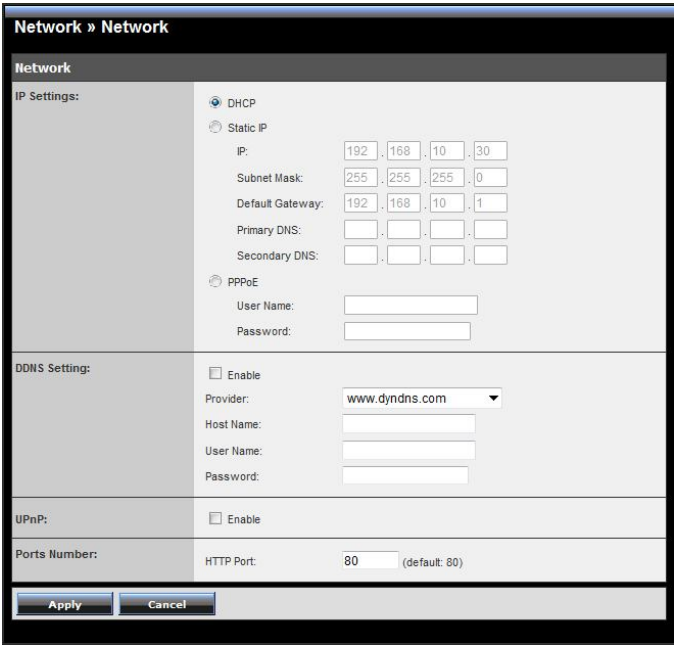
NOTE: The "General User" can access the camera and control the Function buttons of the camera's Web Configuration; the "Guest' can only view the live view image from the main page of the Web Configuration while accessing the camera. Only the "Administrator" is allowed to configure the camera through the Web Configuration.

4.4 Network Settings

The Network menu contains three sub-menus that provide the network settings for the camera, such as the IP Setting, DDNS Setting, IP Filter, and Wireless network.



Network >> Network



■ IP Setting

This item allows you to select the IP Address mode and set up the related configuration.

- **DHCP:** Select this option when your network uses the DHCP server. When the camera starts up, it will be assigned an IP address from the DHCP server automatically.
- **Static IP:** Select this option to assign the IP address for the camera directly. You can use IP Setup to obtain the related setting values.

IP	Enter the IP address of the camera. The default setting is 192.168.10.30.

Subnet Mask	Enter the Subnet Mask of the camera. The default setting is 255.255.255.0.
Default Gateway	Enter the Default Gateway of the camera. The default setting is 192.168.10.1.
Primary/ Secondary DNS	DNS (Domain Name System) translates domain names into IP addresses. Enter the Primary DNS and Secondary DNS that are provided by ISP.

- **PPPoE:** Select this option when you use a direct connection via the ADSL modem. You should have a PPPoE account from your Internet service provider. Enter the **User Name** and **Password**. The camera will get an IP Address from the ISP as starting up.

NOTE Once the camera get an IP address from the ISP as starting up, it automatically sends a notification email to you. Therefore, when you select PPPoE as your connecting type, you have to set up the email or DDNS configuration in advance.

■ **DDNS Setting**

With the Dynamic DNS feature, you can assign a fixed host and domain name to a dynamic Internet IP address. Select the **Enable** option to enable this feature. Then, select the Provider from the pull-down list and enter the required information in the **Host Name**, **User Name**, and **Password** boxes. Please note that you have to sign up for DDNS service with the service provider first (Please refer to Chapter 6 for detail information.)

■ **UPnP**

The camera supports UPnP (Universal Plug and Play), which is a set of computer network protocols that enable the device-to-device interoperability. In addition, it supports port auto mapping function so that you can access the camera if it is behind an NAT router or firewall. Select the **Enable** option to enable this feature.

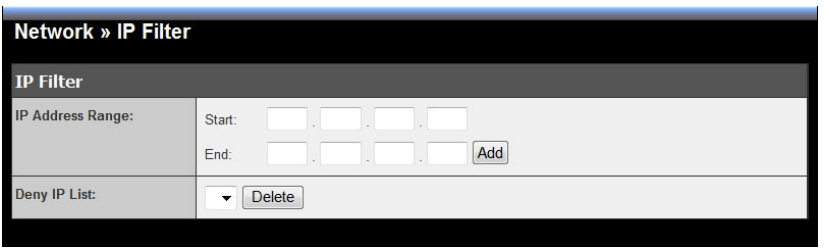
■ **Ports Number**

- **HTTP Port:** The default HTTP port is **80**.

- **RTSP Port:** Configure the transmission of streaming data within the network. The default RTSP (Real Time Streaming Protocol) port is **554**.

NOTE: If the camera is behind an NAT router of firewall, the suggested to be used is from 1024 to 65535.

Network >> IP Filter



The IP Filter setting allows the administrator of the camera to limit the users within a certain range of IP addresses to use the camera.

- **Start/End IP Address**

  Assign a range of IP addresses that are not allowed to access the camera by entering the Start IP address and End IP address. When you are finished, click **Add** to save the range setting. You can repeat the action to assign multiple ranges for the camera.

  For example, when you enter 192.168.10.50 in Start IP Address and 192.168.10.80 in End IP Address, the user whose IP address located within 192.168.10.50 ~ 192.168.10.80 will not be allowed to access the camera.

- **Deny IP List**

  The list displays the range setting(s) of IP addresses that are not allowed to access the camera. To clear the setting, select a range of IP addresses from the list and click **Delete**.

Network >> Wireless Setting

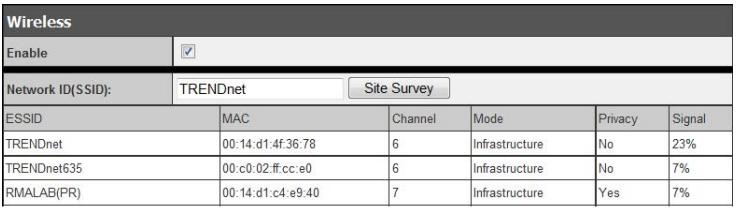
- **Wireless**

  The camera supports WLAN while you use the wireless network. Select the **Enable** option to enable this feature.

  - **Network ID (SSID}:** Keep the default setting of this option to connect the camera to any access point under the infrastructure network mode. To connect the camera to a specified access point, set a SSID for the camera to correspond with the access point's ESS-

ID. To connect the camera to an Ad-Hoc wireless workgroup, set the same wireless channel and SSID to match with the computer's configuration.

Click **Site Survey** to display the available wireless networks, so that you can easily connect to one of the listed wireless networks.



Wireless					
Enable	☑				
Network ID(SSID):	TRENDnet	Site Survey			
ESSID	MAC	Channel	Mode	Privacy	Signal
TRENDnet	00:14:d1:4f:36:78	6	Infrastructure	No	23%
TRENDnet635	00:c0:02:ff:cc:e0	6	Infrastructure	No	7%
RMALAB(PR)	00:14:d1:c4:e9:40	7	Infrastructure	Yes	7%

List of searching results

- **Wireless Mode:** Select the type of wireless communication for the camera: **Infrastructure** or **Ad-Hoc**.
- **Channel:** Select the appropriate channel from the list.
- **Authentication:** Select the authentication method to secure the camera from being used by unauthorized user: **Open**, **Shared-key**, **WPA-PSK**, and **WPA2-PSK**. The following table explains the four options:

Open	The default setting of Authentication mode, which communicates the key across the network.
Shared-key	Allow communication only with other devices with identical WEP settings.
WPA-PSK/ WPA2-PSK	WPA-PSK/WPA2-PSK is specially designed for the users who do not have access to network authentication servers. The user has to manually enter the starting password in their access point or gateway, as well as in each PC on the wireless network.

If you select **Open** or **Shared-key** as the Authentication mode, you need to complete the following settings:

Encryption: Select the **WEP** option to enable the data encryption feature to secure the camera within the wireless network.

Format: Once you enable the Encryption feature, you need to determine the encryption format by selecting **ASCII** or **HEX**. ASCII format causes each character you type to be interpreted as an eight-bit value. Hex format causes each pair of characters you type to be interpreted as an eight-bit value in hexadecimal (base 16) notation.

Key Length: Select the WEP key length you use: **64 bits** or **128 bits**.

WEP Key 1/2/3/4: Enter the WEP key(s) in the following boxes.

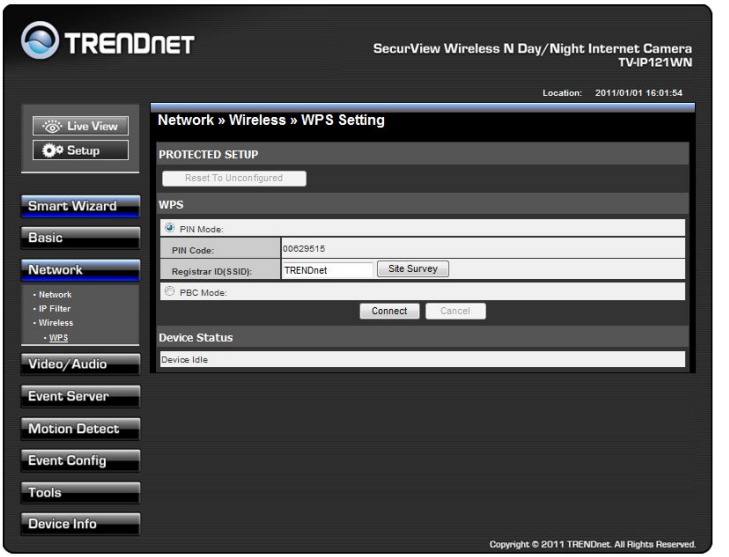
If you select **WPA-PSK** or **WPA2-PSK** as the Authentication mode, you need to complete the following settings:

Encryption: Select **TKIP** or **AES**. TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets to insure much greater security than the standard WEP security. AES (Advanced Encryption Standard) is used to ensure the highest degree of security and authenticity for digital information.

Pre-Shared Key: This is used to identify each other in the network. Enter the name in the box, and this name must match the Pre-shared key value in the remote device.

Network >> Wireless >> WPS Setting

WPS (Wi-Fi Protected Setup) sets a new standard of Wi-Fi security, providing a simplified secure network setup solution for the end users. Once the required settings have been completed, your wireless network can be protected by simply pressing the WPS button on the camera.



- **PROTECTED SETUP**

  Press the **Reset to Unconfigured** button to reset the WPS configuration of the camera.

- **WPS**

  - **PIN Mode:** The PIN (Personal Information Number) mode builds the connection by entering the PIN Code directly. Once you enter the **PIN Code** of the camera on the router (or access point) that

supports WPS, you can directly build a WPS connection between the camera and the device by simply pressing its WPS button.

- **PBC Mode:** The PBC (Push Button Configuration) mode builds the connection by scanning the devices in the wireless network. Once you press the camera's WPS button, it starts to scan the WPS devices in the wireless network, and then you can build the WPS connection by clicking the **Connect** button.

■ **Device Status**

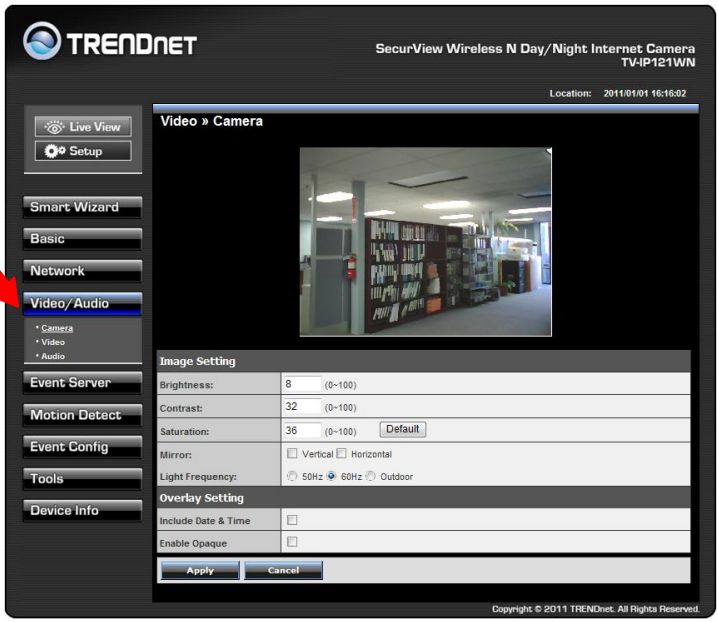
Display the WPS configuration of the camera.

TIP The Power LED indicates the WPS connection status by:

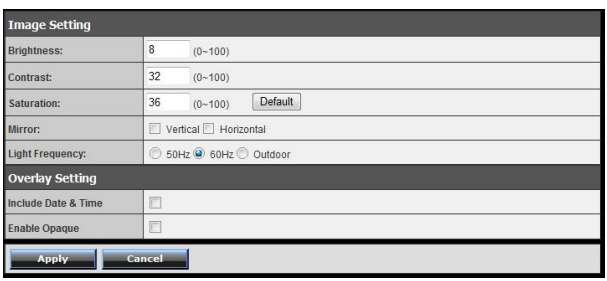
- blinking 3 times when the connection is built successfully.
- repeatting 3 times of short-short-long blink when the connection is failed.

4.5 Setting up Video & Audio

The Video & Audio menu contains three sub-menus that provide the video and audio settings for the camera.



Video & Audio >> Camera

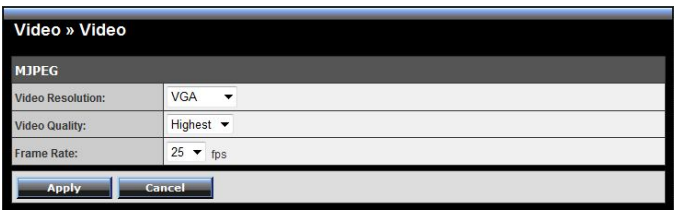


- **Image Setting**
  - **Brightness:** Adjust the brightness level from 0 ~ 100.
  - **Contrast:** Adjust the contrast level from 0 ~ 100.
  - **Saturation:** Adjust the colors level from 0 ~ 100.

    Click **Default** to restore the default settings of the three options above.
  - **Mirror:** Select the **Horizontal** option to mirror the image horizontally. Select the **Vertical** option to mirror the image vertically.
  - **Light Frequency:** Select the proper frequency according to the camera's location: **50Hz**, **60Hz**, or **Outdoor**.

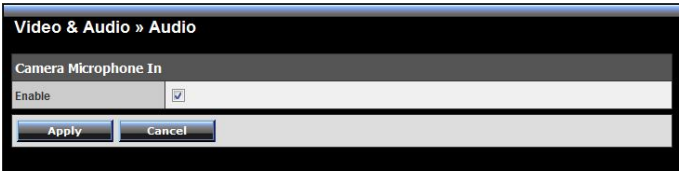
- **Overlay Setting**
  - **Includes Date & Time:** Select this option to display the date & time stamp on the live view image.
  - **Enable Opaque:** Select this option to set a black background to the displayed date & time stamp.

Video & Audio >> Video



- **MJPEG**
  - **Video Resolution:** Select the desired video resolution from the three formats: **VGA**, **QVGA** and **QQVGA**. The higher setting (VGA) obtains better video quality while it uses more resource within your network.
  - **Video Quality:** Select the desired image quality from five levels: **Lowest**, **Low**, **Medium**, **High**, and **Highest**.
  - **Frame Rate:** Select **Auto** or a proper setting depending on your network status.

Video & Audio >> Audio

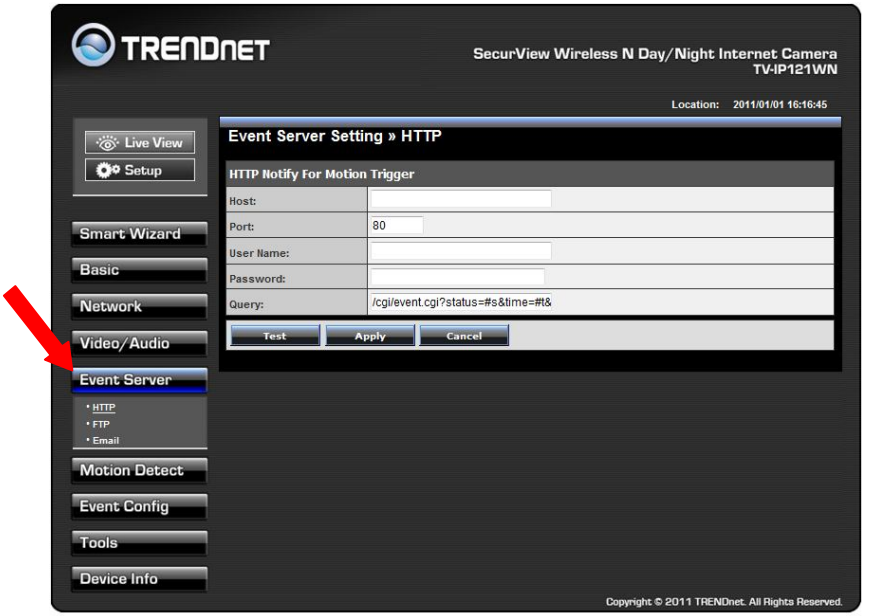


- **Camera Microphone In**

  Select the **Enable** option to enable the camera's audio function, so that you can receive the on-site sound and voice from the camera

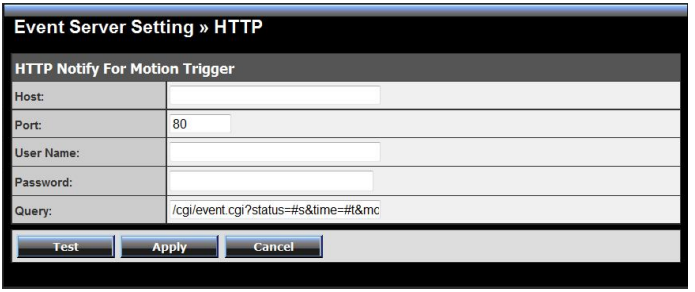
4.6 Event Server Configuration

The Event Server menu contains two sub-menus that allow you send notification to NVR server or upload images to FTP, and send emails that include still images.



When you complete the required settings on HTTP Notify for Motion Trigger, or FTP, or Email, click **Test** to test the related configuration is correct or not. Once the camera connects to the server successfully, click **Apply**.

Event Server Setting>> HTTP



- **HTTP Notify For Motion Trigger**

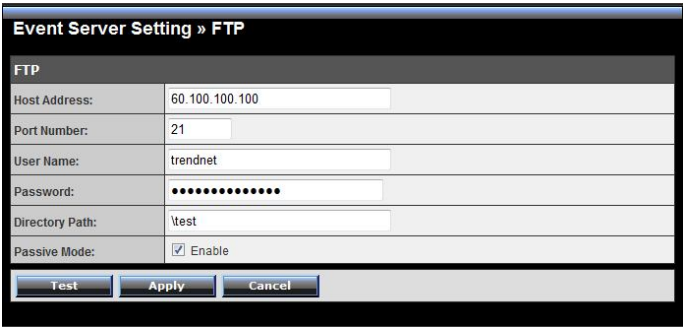
  Send the query parameter via an HTTP notification when an event is triggered.

  - Host: Enter the IP of the HTTP server
  - Port: Enter the Port number of the HTTP server
  - User Name: Enter the username of the HTTP server
  - Password: Enter the password of the HTTP server
  - Query: Enter the query parameter for the request if necessary

Example:

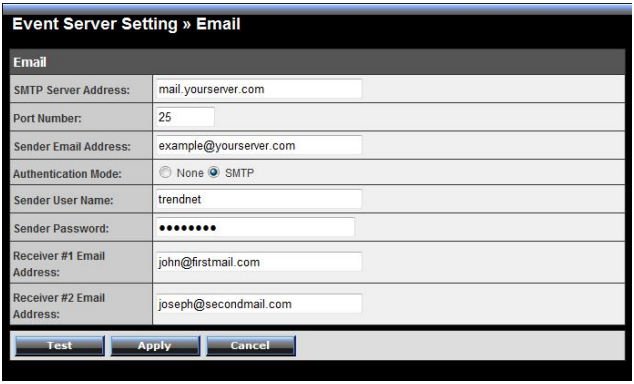
Host: 192.168.10.1
Port: 80
Query: xxx.cgi?name1=value1&name2=value2
Example: cgi/event.cgi?status=#s&time=#t&model=modelname
Result:
http://192.168.10.1:80/cgi/event.cgi?status=#s&time=#t&model=modelname

Event Server Setting>> FTP



- **FTP**
  - **Host Address:** Enter the IP address of the target FTP server.
  - **Port Number:** Enter the port number used for the FTP server.
  - **User Name:** Enter the user name to login into the FTP server.
  - **Password:** Enter the password to login into the FTP server.
  - **Directory Path:** Enter the destination folder for uploading the images. For example, \test.
  - **Passive Mode:** Select the **Enable** option to enable passive mode.

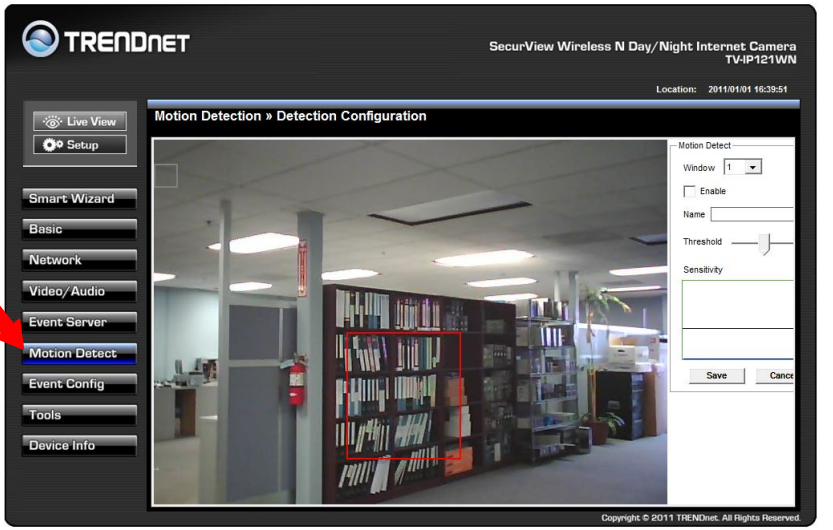
Event Server Setting >> Email



- **Email**
  - **SMTP Server Address:** Enter the mail server address.
  - **Sender Email Address:** Enter the email address of the user who will send the email.
  - **Authentication Mode:** Select **None** to disable the authentication feature, or select **SMTP** and then enter the **User Name** and **Password** according to the mail server configuration.
  - **Sender User Name:** Enter the user name to login the mail server.
  - **Sender Password:** Enter the password to login the mail server.
  - **Receiver #1 Email Address:** Enter the first email address of the user who will receive the email.
  - **Receiver #2 Email Address:** Enter the second email address of the user who will receive the email.

4.7 Motion Detect

The Motion Detect menu contains the command and option that allow you to enable and set up the motion detection feature of the camera. The camera provides two detecting areas.



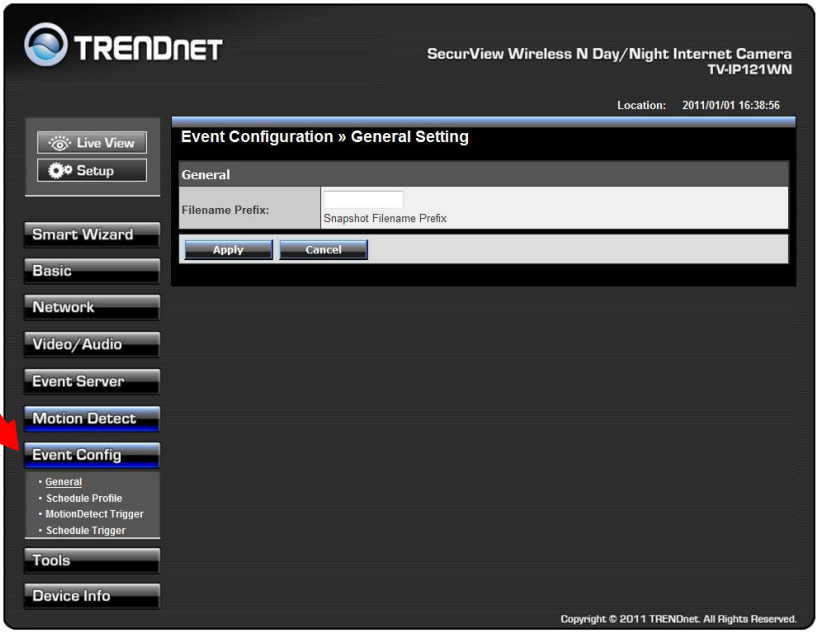
To enable the detecting area, select **Window 1** or **2** from the pull-down list, and then select **Enable**. When the detecting area is enabled, you can use the mouse to move the detecting area and change the area coverage.

- **Name:** Assign a name to the detecting area.
- **Threshold:** Move the slide bar to adjust the level for detecting motion to record video.

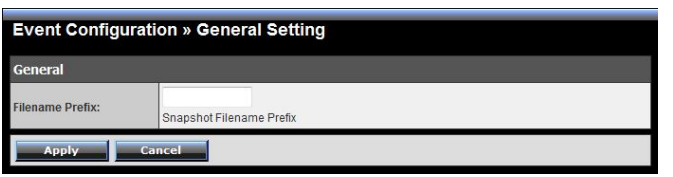
-

4.8 Event Config

The Event Config menu contains four sub-menus that provide the commands to configure event profiles.

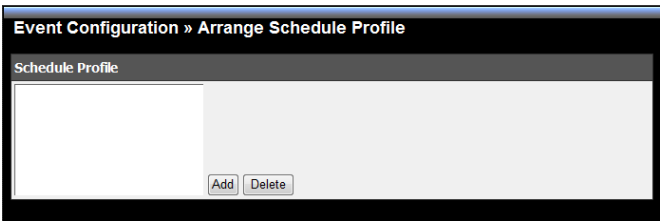


Event Configuration >> General Setting



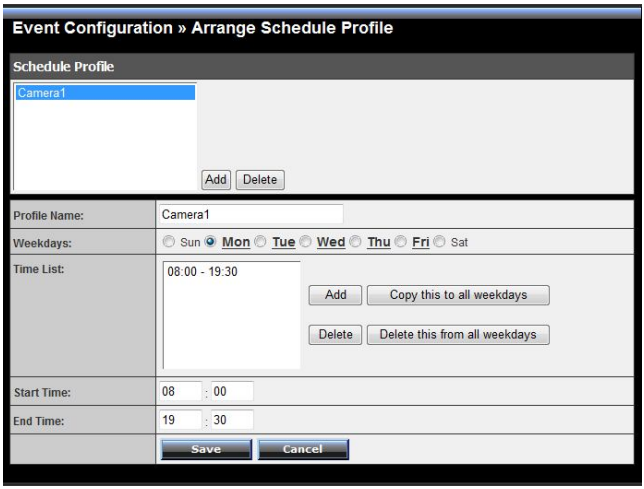
- **Snapshot/Recording Subfolder:** You can assign a given sub-folder for captured file. Otherwise, leave this option blank to use the default setting.

Event Configuration >> Arrange Schedule Profile



This sub-menu displays the scheduled profile(s). To customize the profile, click **Add** and then enter a descriptive name for the profile in the prompt dialog window.

After entering the profile name, click **OK** and the profile is added to the Schedule Profiles list. To delete the profile, select the profile in the list and click **Delete**.



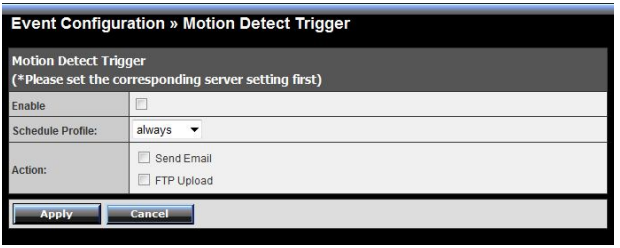
- **Profile Name:** Display the profile name that you select in the Schedule Profiles list.

- **Weekdays:** Select the weekday(s) that you want to separately assign in the schedule profile. The weekday that has been assigned will be displayed with green color.

- **Time List:** Display the time period that you have assigned within the selected weekday. To assign the same time period to every weekday, click **Add this to all weekdays**; click **Delete this from all weekdays** to remove the selected time period from every weekday. Click Delete to remove the selected time period.

- **Start/End Time:** Enter the start and end time and then click **Add** to assign a time period within in the selected weekday.

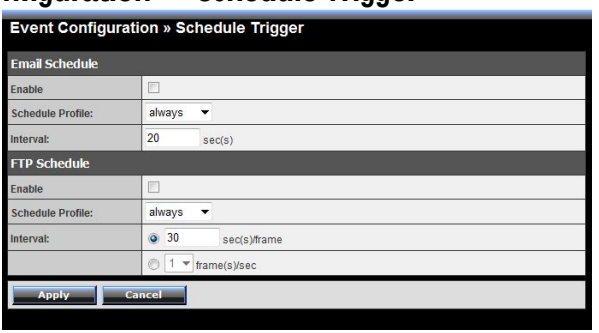
Event Configuration >> Motion Detect Trigger



Select the **Enable** option to enable the trigger function of the camera, so that you can send captured images within the detecting area to the FTP server, or email receiver. You have to configure corresponding settings, such as FTP server and email server, to enable this feature.

- **Schedule Profile:** Select a schedule profile from the pull-down list.
- **Action:** Select the destination that the captured images will be sent to: **Send Email**, or **FTP Upload**.

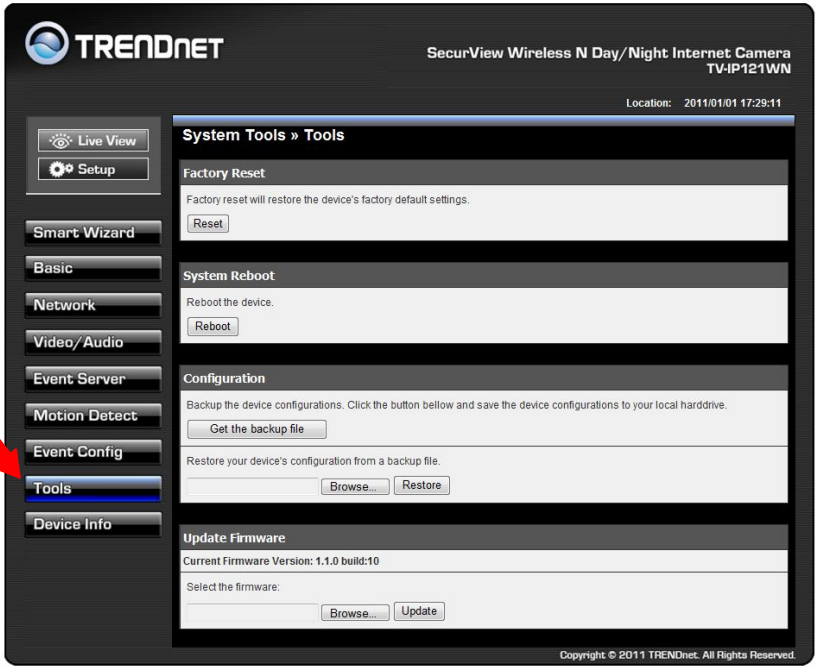
Event Configuration >> Schedule Trigger



You can separately configure the schedule for trigger function of the camera by **Email**, or **FTP**. Select the **Enable** option on each item, and then select a **Schedule Profile** from the pull-down list and set the **Interval** time.

4.9 Tools

The Tools menu provides the commands that allow you to restart or reset the camera. You can also backup and restore your configuration, and upgrade the firmware for the camera.



- **Factory Reset**

  Click **Reset** to restore all factory default settings for the camera.

- **System Reboot**

  Click **Reboot** to restart the camera just like turning the device off and on. The camera configuration will be retained after rebooting.

- **Configuration**

  You can save your camera configuration as a backup file on your computer. Whenever you want to resume the original settings, you can restore them by retrieving the backup file.

  - **Backup:** Click **Get the backup file** to save the current configuration of the camera.
  - **Restore:** Click **Browse** to locate the backup file and then click **Restore**.

- **Update Firmware**

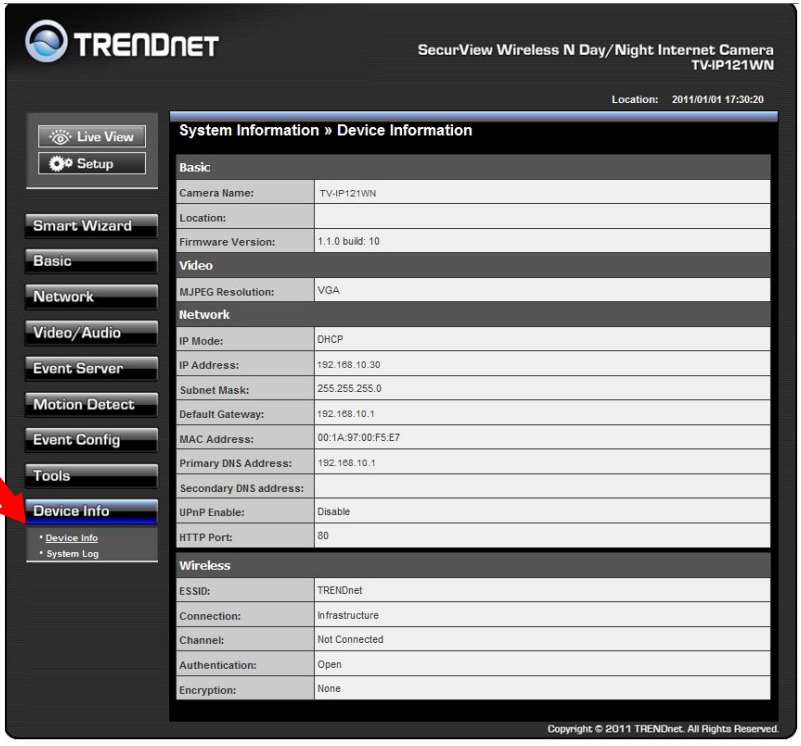
  This item displays the current firmware version. You can upgrade the firmware for your camera once you obtained a latest version of firmware.

  - **Select the firmware:** Click **Browse** to locate the backup file and then click **Update**.

    WARNING:
    Firmware upgrade failure may permanently damage the unit and cause it to malfunction. Do not interrupt the firmware upgrade process by disconnecting it from the network or unplugging its power from the power outlet once the firmware upgrade process has begun. Never perform a firmware upgrade over wireless connections or via remote access connections.

4.10 Information

The Information menu displays the current configuration and events log of the camera.



- **Device Info**

  Display the Basic, Video, Network, and Wireless settings of the camera.

- **System Log**

  The Logs table displays the events log recorded by the system.

CHAPTER 5

SECURVIEW™ PRO SOFTWARE

This chapter describes detailed instructions on using SecurView Pro, a customized software application with a user-friendly interface that allows you to access your cameras. The Software can monitor and record up to 36 cameras. It also let you change some basic settings of the camera, such as schedule profiles and motion detecting areas. The SecurView Pro also supports audio or Pan/Tilt function.

It is recommended to use a high performance computer if you want to connect multiple cameras simultaneously.

- **Platform:** Microsoft® Windows® 7/Vista/XP
- **Hard Disk:** 80GB or above
- **Resolution:** 1024x768 or above
- **Hardware Requirement**
  1 ~ 8 cameras: Intel Core 2 Duo; 2GB RAM
  9 ~ 32 cameras: Intel Core 2 Quad; 4GB RAM

* For Windows Vista users: please go to **User Accounts and Family Safety** > **User Accounts** > **Turn User Account Control on or off**, then uncheck the checkbox of "**Use User Account Control (UAC) to help protect your computer**". Restart your computer to validate the setting. For additional information of User Account Control, please go to http://www.microsoft.com/windows/products/windowsvista/features/details/useraccountcontrol.mspx

* For Windows 7 users, please go to **Control Panel** > **User Accounts** > **Change User Account Control Setting** to lower your notify setting. For additional information of User Account Control, please go to http://windows.microsoft.com/en-us/windows7/products/features/user-account-control

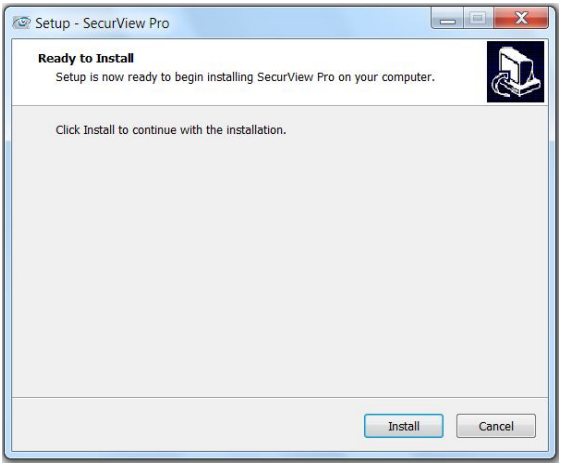
5.1 Installation

1. Insert the Installation CD-ROM into your computer's CD-ROM drive to initiate the Auto-Run program.
2. Click the **SecurView Pro** from the Auto-Run menu screen.

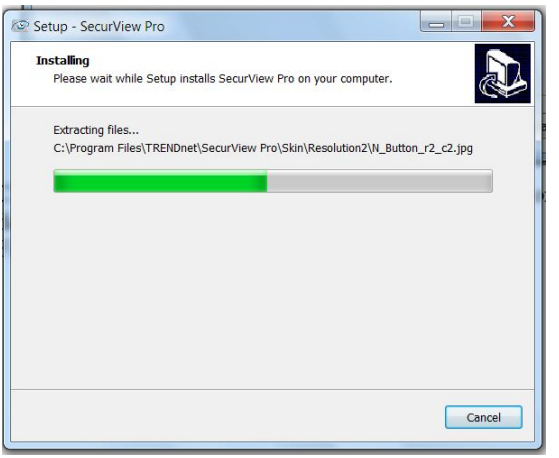
NOTE: To use SecurView Pro, you must have Microsoft .NET Framework 2.0 installed in the computer. The setup wizard will detect it and, if the program is not installed yet, it will ask you to install it during the process of installing SecurView™ Pro.

NOTE: Microsoft Windows Installer 3.0 or above is a required component to install SecurView Pro. For more information of the required component during installation, please visit the Microsoft support Website.

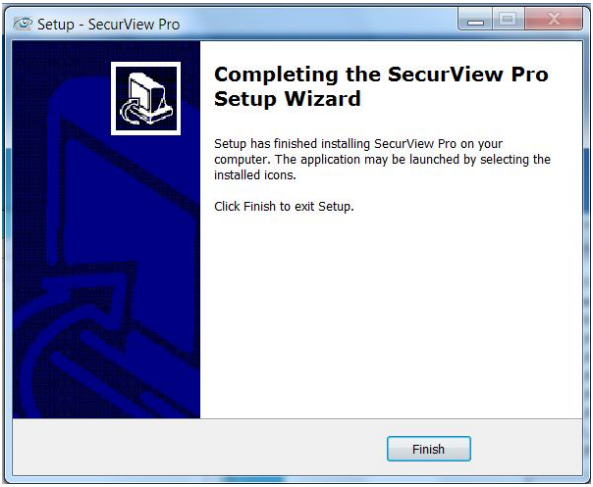
3. Then **SecurView Pro** Setup Wizard will appear. Click "***Install***".



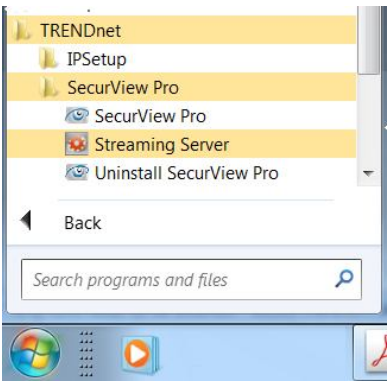
4. Wait until the program finish the installation. By default, the destination location is C:\Program Files\TRENDnet\SecurView Pro.



5. Click "***Finish***" to finish the installation.



6. After installing the SecurView Pro, the application is automatically installed to your computer, and creates a folder in " ***Start \Program\TRENDnet\SecurView Pro*** ".



5.2 Using SecurView™ Pro

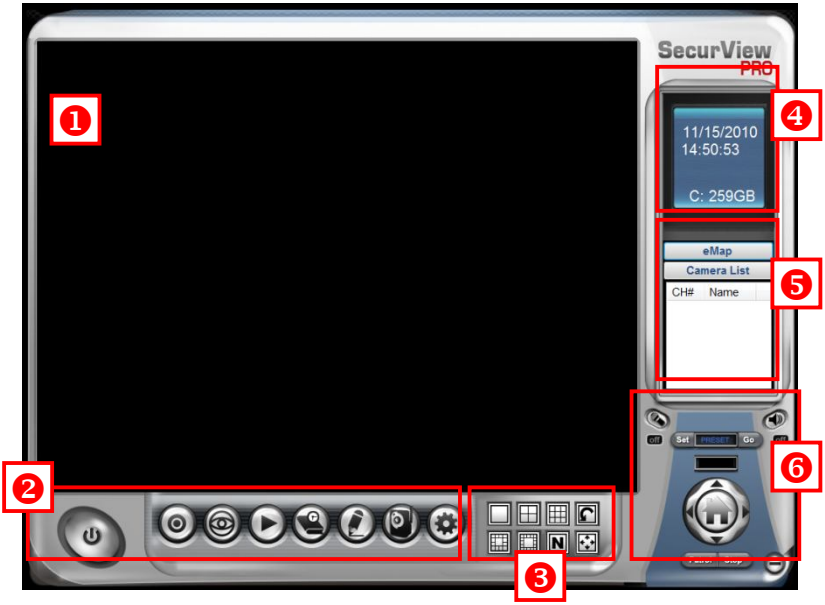
5.2.1 Launch the Program

To start SecurView Pro, click **Start > All Programs > TRENDnet >SecurView Pro > SecurView Pro**. You can also start the program by double-click the SecurView Pro icon on your desktop.

On the login window, enter the **User name/Password** and click **OK** to login. The default **User name/Password is admin/admin**. If you wish to save the login information, please select **Auto Login**.

5.2.2 Main Window and Features

When you start and login to SecurView Pro, the Main window will display as below:



The Main window provides you with the information on operating the system, as well as the control panel such as the Quick Launch buttons, and so on.

NOTE For best result, it is higher recommended to configure resolution setting to 1024 x 768 or higher; otherwise, it cannot be displayed on the screen when launching the program.

❶ **Live View Window** displays the live video of the connected camera(s).

❷ **Quick Launch Buttons** are located below the Live View Window, providing you with the following quick-launch functions:

Button	Function
	Logout : To log out the SecurView Pro program **Close:** To close the SecurView Pro program
	Restore Recording Type: Restore all recording type to current camera's setting **All Continuous Recording:** Continuous recording on all cameras **Stop All Recording:** Stop recording on all cameras
	View Setting: To configure eMap settings **eMap View:** To view current maps **Camera Status:** Display cameras status
	Playback: Playback recorded files
	Schedule: Display Schedule Configuration window
	Event Server: Setup a SMTP server **Address Book:** Add/Remove email address for event notification **Event Trigger**: Setup event trigger configuration
	Device Setting : Set up the camera **Recording Setting**: Set up the recording path
	Account information: Setup administrator password **Version**: Display software version **System Setting:** Software settings

❸ **Camera View Mode** buttons in this area allow you to switch the camera view mode.

Buttons	Functions
	Display the connected camera(s) in a single camera view mode.
	Display the connected camera(s) in a quad view mode.
	Display the connected camera(s) in a 3 x 3 grid view mode.
	Display the connected camera(s) in a 13-camera view mode using a split window. The first camera is displayed as the major view.
	Display the connected camera(s) in a 17-camera view mode using a split window. The first camera is displayed as the major view.
	Display the connected camera(s) in a N x N grid view mode, supporting up to 36 cameras.
	Display the live view of the selected camera in full screen mode. Click ESC on the keyboard to return to Main window.
	Automatically switch the live view of each connected cameras in single camera view mode by 30 seconds*. Click once to start and click again to stop. * The auto-switch time is set as 30 seconds by default, which can be changed by clicking the → **System Setting** and then change the value from the pull-down list of the **Auto Switch time interval** option.

❹ **System Information** displays the system information, including the date and time, and the available storage space of the system.

❺ **Live View Status** provides the status of live view mode, including **Camera List** and **eMap**.

- **Camera List** displays the status of the connected cameras. If multiple cameras are connected, you can switch to the live view of each camera by simply selecting the camera from the list.
- **eMap** allows you to select the desired camera to the view from the map easily. Please note that you have to set up the eMap for monitoring in advance.

❻ **Camera Control Buttons** provides the control buttons that allow you to control the selected camera.

Buttons	Functions
	Talk On/Off. Click to enable/disable the speaker function of the connected camera. This option is available only in single camera view mode.
	Listen On/Off. Click to enable/disable the microphone function of the connected camera. This option is available only in single camera view mode.
	For Pan/Tilt cameras, use this control panel to set the preset positions (up to 8 positions). Use Navigation buttons to adjust camera position, and then select the position number (1~8) from the Set button. To move to the preset position, simply select the position number (1~8) from the Go button.
	Navigation Buttons (Left/Right/Up/Down/Home). If the connected camera has pan/tilt functions, the Navigation buttons allow you to move the camera lens position. Clicking the Home (center) button will move the camera lens to the assigned home position.
	The **Patrol/Stop** buttons are used to enable/disable the patrol function of the camera. Click **Patrol** to start patrolling through the preset positions once. Click **Stop** to stop patrolling.

5.2.3 Manage the Cameras

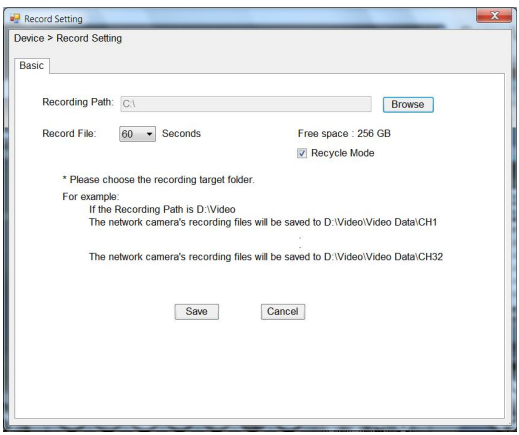
Before adding the cameras, please setup the recording setting first.

■ Configure Recording Settings

1. Click the button and then select **Record Setting**.

2. Default path is C:\, click **Browse** and select the desire directory then click **Save** to complete the configuration.

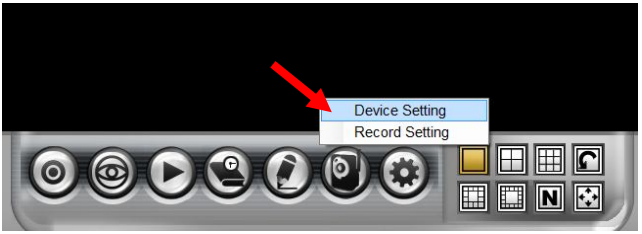
To change the time interval for recording, select time from the pull-down menu.



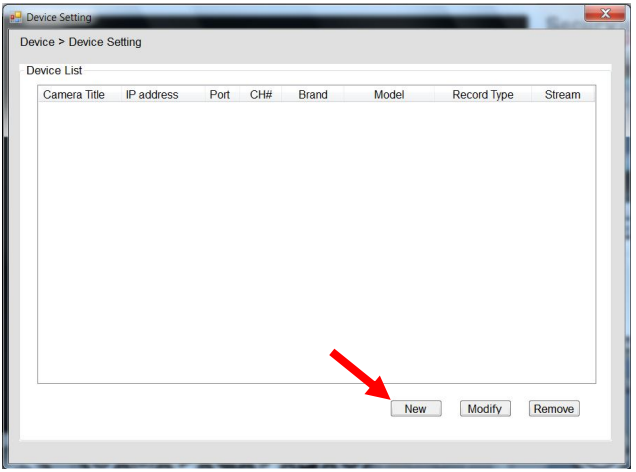
NOTE: The system will automatically delete the oldest files (10%) when the size of recorded files is up to 90% of the storage space.

Add a Camera

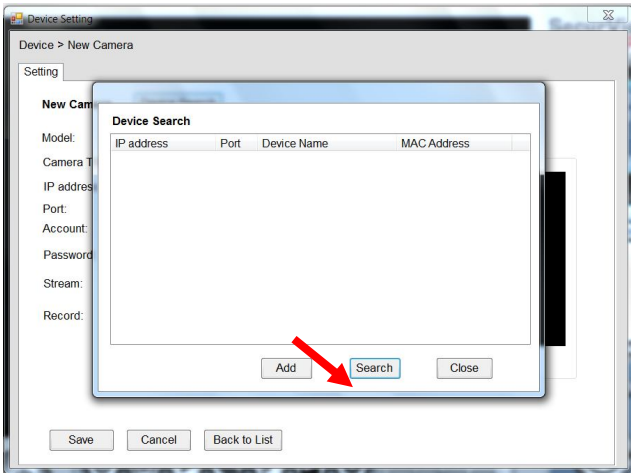
1. Click the button and select **Device Setting** to display the Device Setting window.



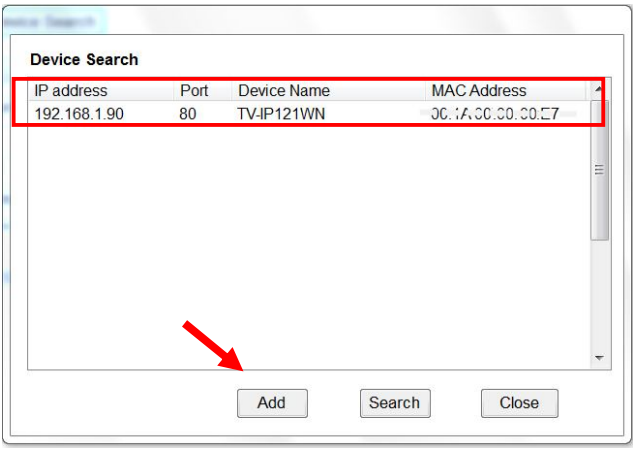
2. Click **New**.



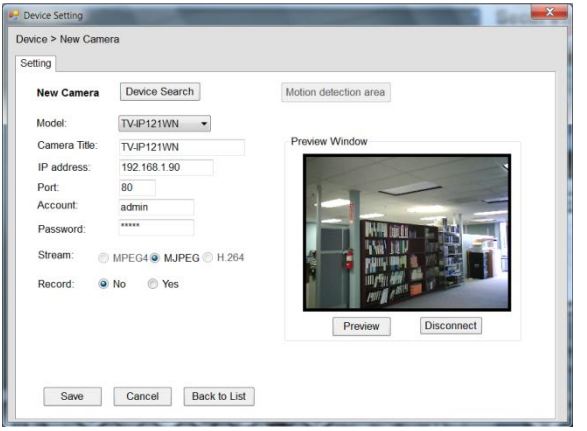
3. Click on **Search**, all cameras that's connected to your network would appear.



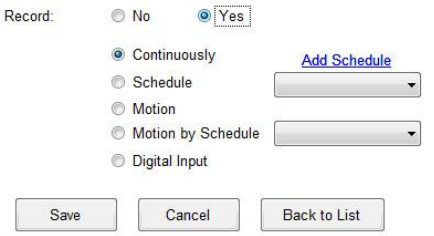
4. Select the camera you would like to add and then click **Add**.



5. The information of the camera will display on the screen. It will auto detect the IP address/port number and display the stream type of the camera. Please type in the correct user name and password, then select **Preview** to view live image.



6. To setup recording style, select **Yes** on **Record** option. These four recording types will appear. Select one of the recording type, configure it then click **Save**.

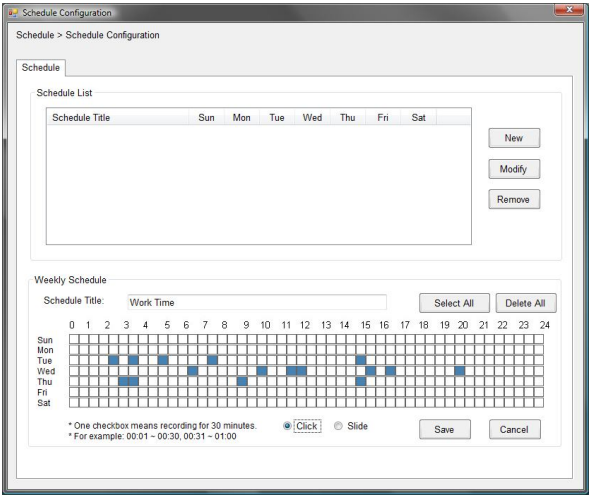


Continuously:
Record the stream video continuously

Schedule:

Records stream video by schedule. You can setup the schedule by click **Add Schedule** here.

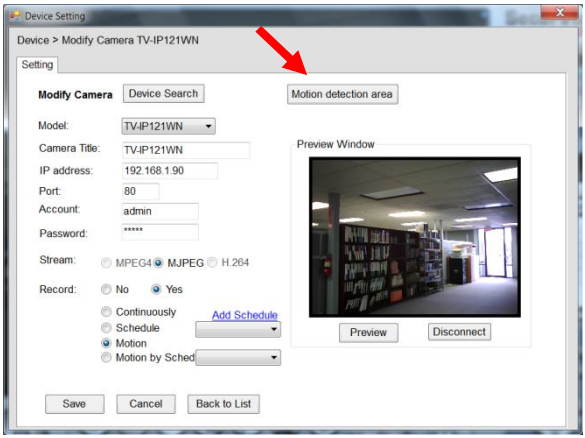
Click on **New** to create a new schedule and select the time to record. Click on Save when finish.



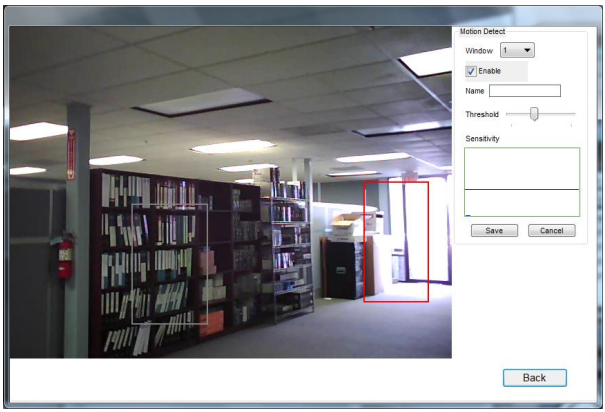
Motion:

Record video by Motion Detection. Motion detection recording required to setup a motion detection area. If you are adding a new camera, you must save the camera information first before setup the motion detection area.

To use motion detection record, please enable the detection areas first. Click on **Motion detection area** to setup



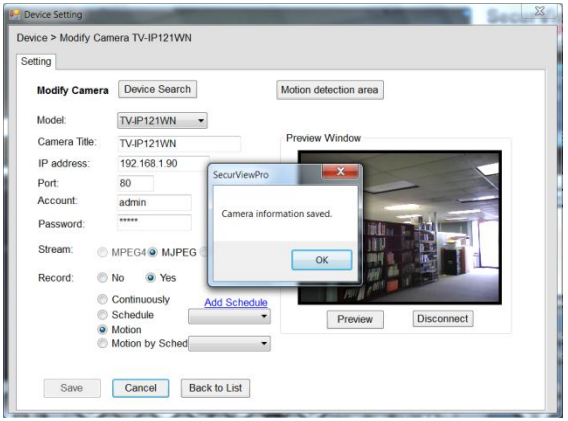
Enable motion detection windows, set up the senstivity and click on **Save**.



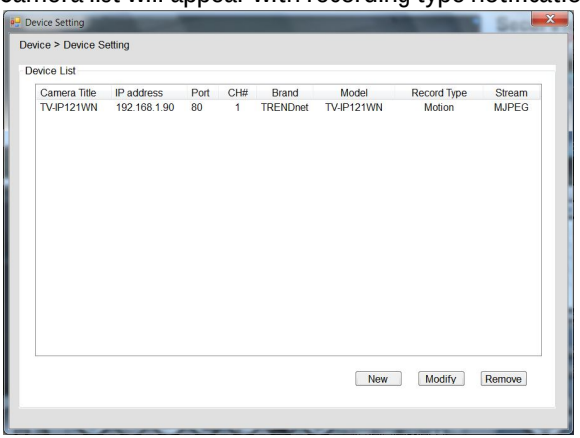
Motion by Schedule:
same requirement as Motion & Schedule recording.
Digital Input:

Recording triggered when there I/O port is triggered.

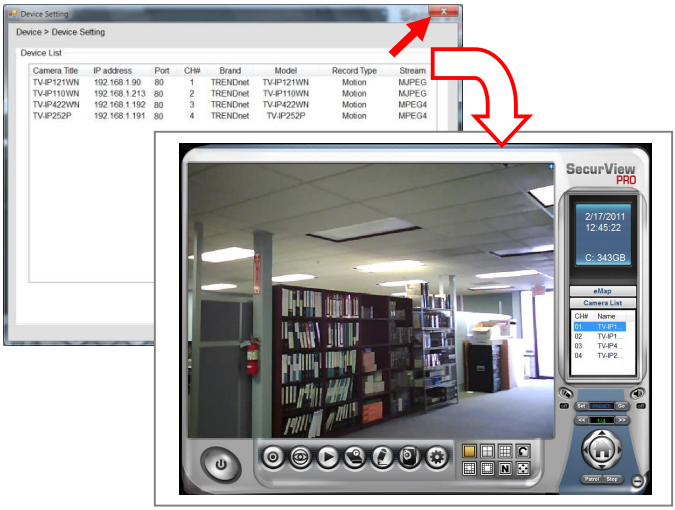
After all recording methods are configured, click **Save** to apply the settings.



7. Camera list will appear with recording type notification.



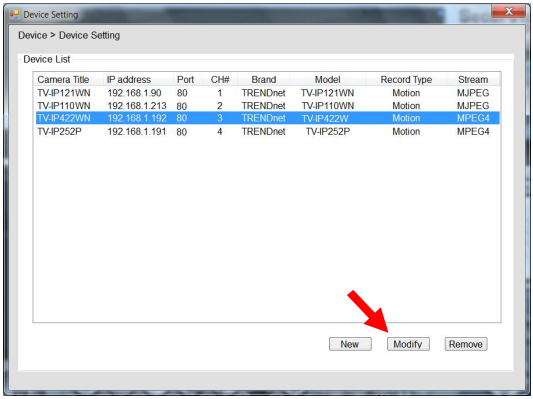
8. Once you added all the cameras, click the close button “x” on the **Device Setting** windows to return to the main windows. The cameras will display here.



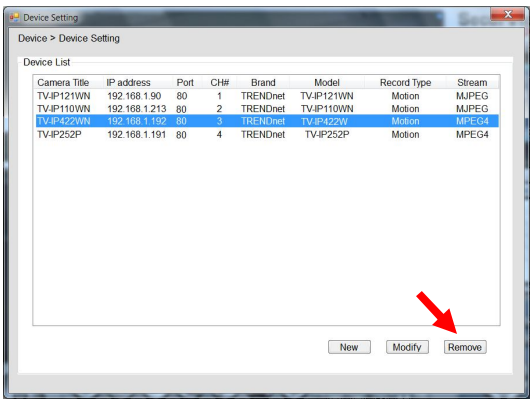
NOTE Divx/Xvid codec is required for viewing the image of camera. If the image cannot be displayed in the Live View/Preview window normally, click the following path to download and install the required component: http://download.divx.com/divx/DivXInstaller.exe

■ Edit / Delete a Camera

1. **To edit a camera:** From the Device Setting window, highlight the camera you would like to edit then click on **Modify** button.



2. **To delete a camera:** select the desired one and then click **Remove**. Click **Yes** to confirm.



View Camera Image

Since you have added camera(s) to the system, the image of the selected camera(s) will be displayed on the Live View Window automatically. You can view a maximum of 36 cameras simultaneously. Additionally, you can select one-camera or other view mode to display the video from the Camera View Mode buttons.

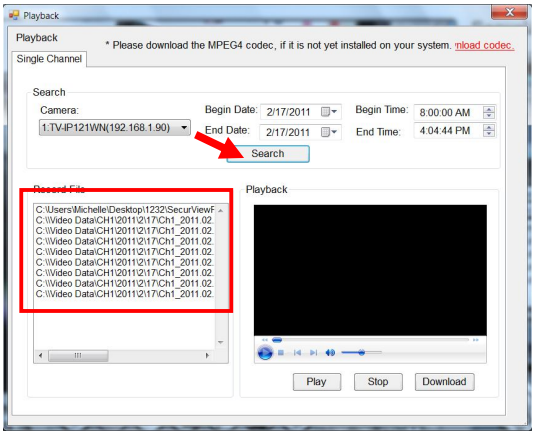
For example, if you use only one camera, select single camera view mode ( ), and the Live View Window will display the view as below. You can select the other modes according to your need.

The **Information icon** ( ) on the top-right corner of the window provides you with the options to connect/disconnect the camera, select a camera to be displayed in the window, capture a still image of the camera live video, or switch to eMap mode. Click the Information icon to pop up the shortcut menu and select the desired option.

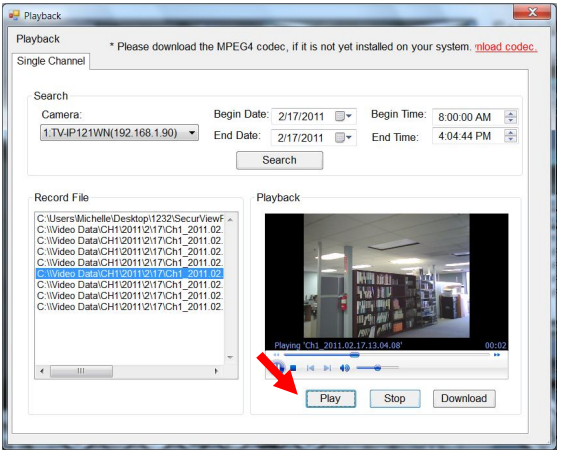
■ Playback the Recorded Files

1. Click the button to display the Playback window.

2. On the **Playback** window, select the camera and setup the begin/end date and begin/end time, then click **Search**. The search result will be displayed in the **Record File list**.



3. To playback the video clip, select the desired file and click **Play**.



5.2.4 eMap Setup & Camera Status

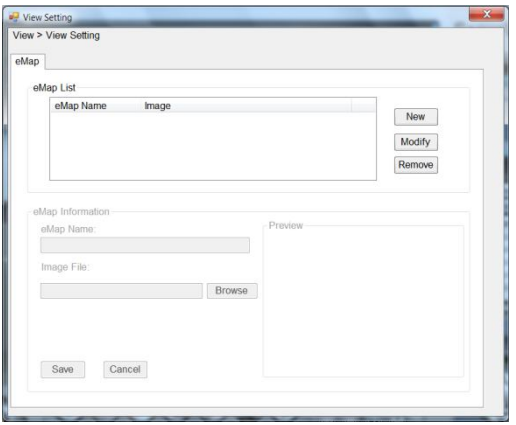
■ Manage eMap

Click the button and select **View Setting** to manage eMap.

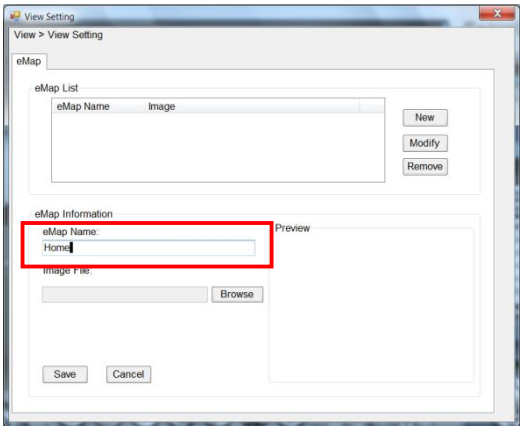
eMap refers to the geography and device scope in the SecurView Pro, which visually presents the devices in your security system. It uses a background of the area (e.g. a picture or a map) as the interface for monitoring.

To add an eMap

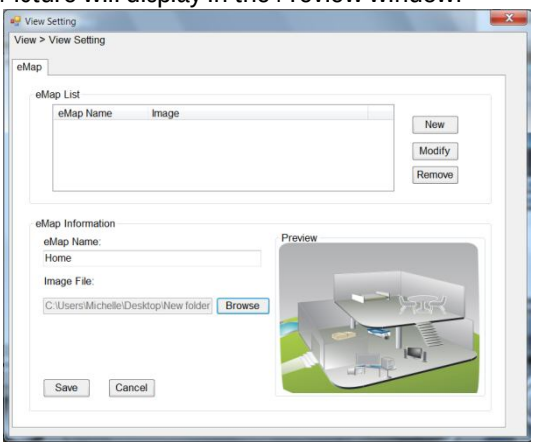
1. On the View Setting window, click **New**.



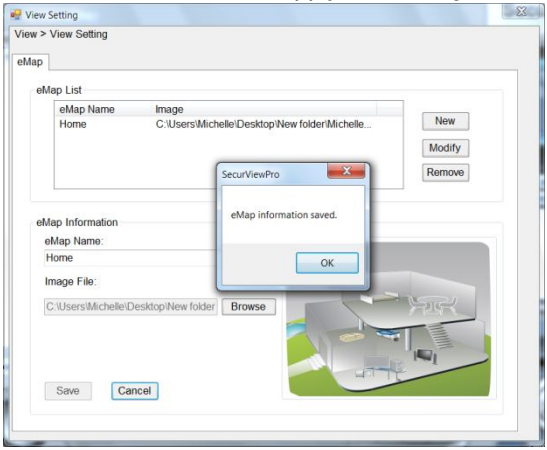
2. Enter an **eMap** name.



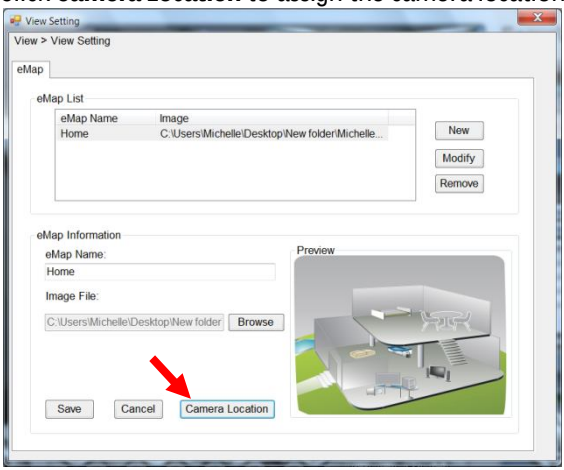
3. Click **Browse** to select a **Picture File** from your computer. Picture will display in the Preview window.



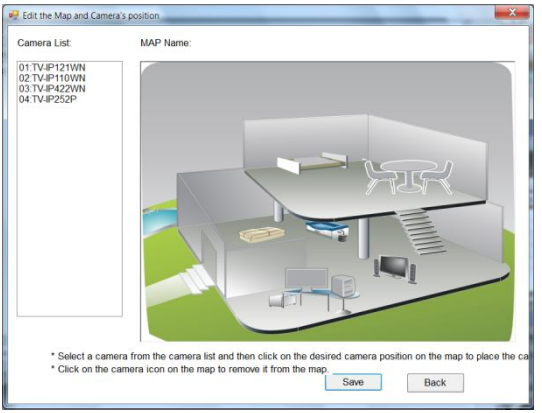
4. Click **Save** and click **OK** to apply the settings.



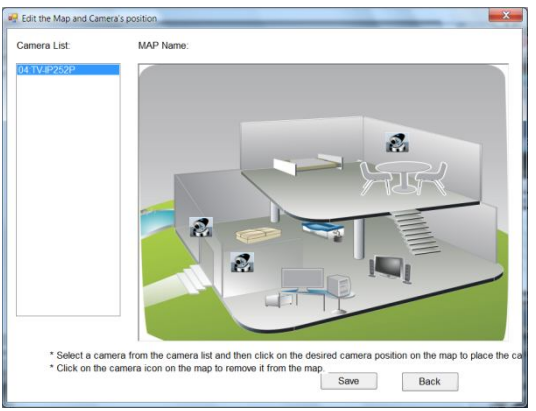
5. Click **Camera Location** to assign the camera location.



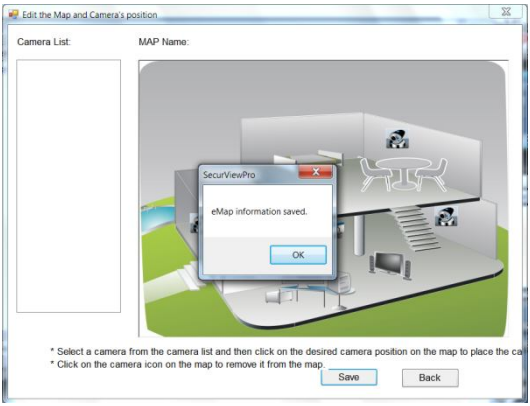
6. The following screen appears.



7. Select the camera from the list and then click the position on the map. The camera icon will be displayed on map.



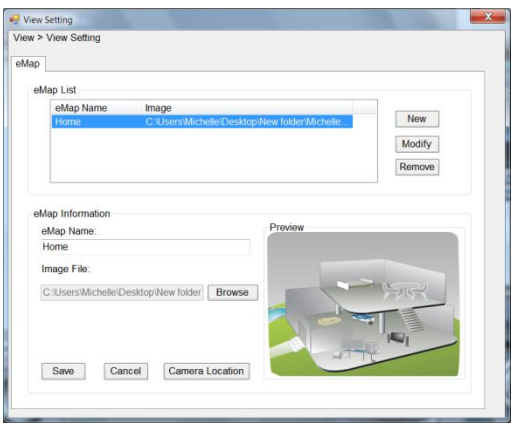
8. Click **Save** when complete.



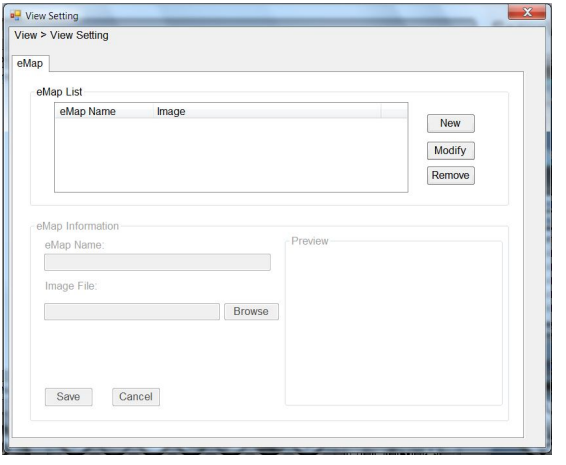
To modify/remove an eMap

1. **To edit the eMap:** In the eMap List, select the map name from eMap list, and click **Modify**.

   The map's information will display on the preview windows. After changes the setting information, click **Save** to save the setting.

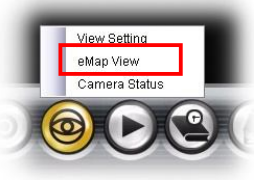


2. **To delete the eMap:** In the eMap List, select the desired one and click **Remove**. The selected map will be removed from the list.



■ View eMap

a. Click the button and select **eMap View**.



b. Select the map from the eMap Name list.

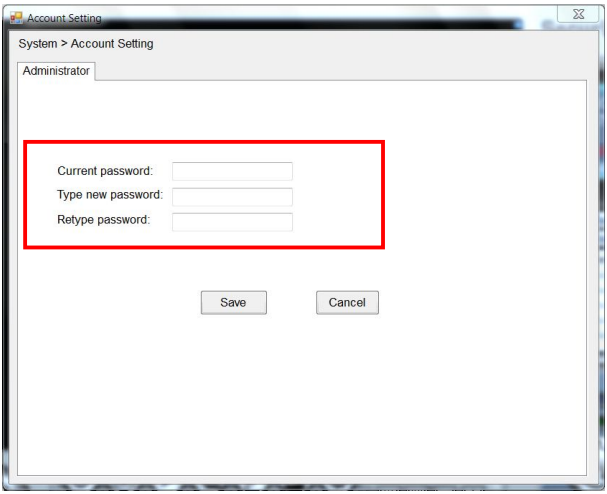
■ **Camera Status** Click the camera icon , the camera Live Monitor window will display live image on that camera.

5.2.5 System Info

■ Account

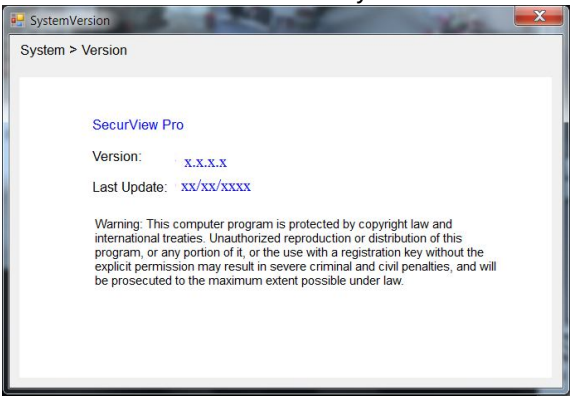
Click the **System** button and select **Account** to change the administrator password of the system.

Enter the **Current password**, and then enter the new password twice (in the **Type new password** and **Retype password** boxes). Then click **Save**.



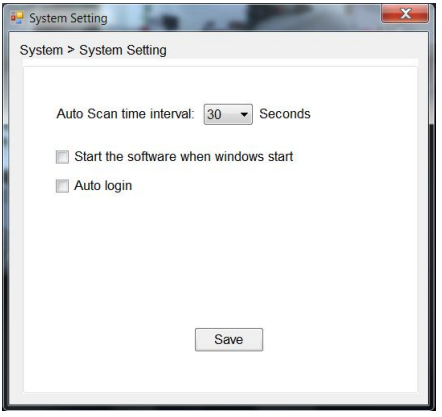
■ Version

Click the **System** button and select **Version** to view the current firmware version of the system.



■ System Setting

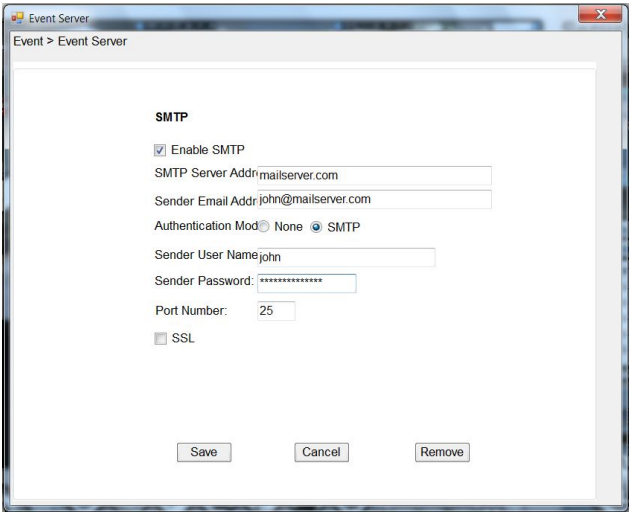
Click the **System** button and select **System Setting**. **Auto Scan** period can be set from 30 seconds to 100 seconds.



5.2.6 Event Settings

■ Setting up Event Server

Click the button and select **Event Server** to configure the SMTP settings for email notification use.



Select the **Enable SMTP** option and configure the following information correctly to start the email feature.

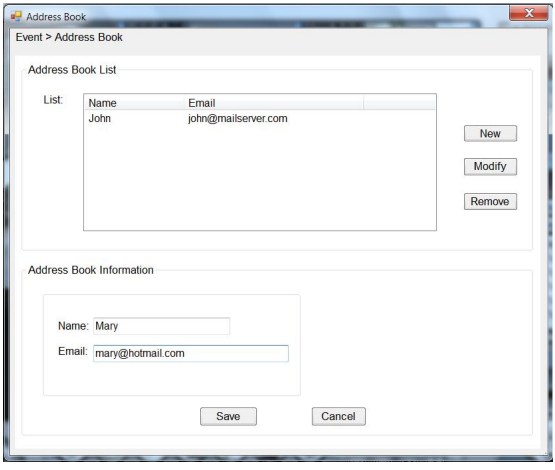
- **SMTP Server Address:** Enter the mail server address. For example, mymail.com or smtp.gmail.com or smtp.live.com
- **Sender Email Address:** Enter the email address of the user who will send the email. For example, John@mailserver.com.
- **Authentication Mode:** Select **None** or **SMTP** according to the mail server configuration.
- **Sender User Name:** Enter the user name to login the mail server.
- **Sender Password:** Enter the password to login the mail server.
- **Port Number:** Enter the port number used for the email server.
- **SSL:** If the mail server requires an encrypted connection, you should check the **SSL** option. For example, gmail users, please select this option.

When completed, click **Save** and then select **OK**. The system will automatically start the Event Service.

TIP The status of Event Service is indicated by the icon in the system bar.

Sending Notification to the User

Click the button and select **Address Book** to assign the user to the Address Book of the camera. The user will receive a real-time notification from the system while triggering out.



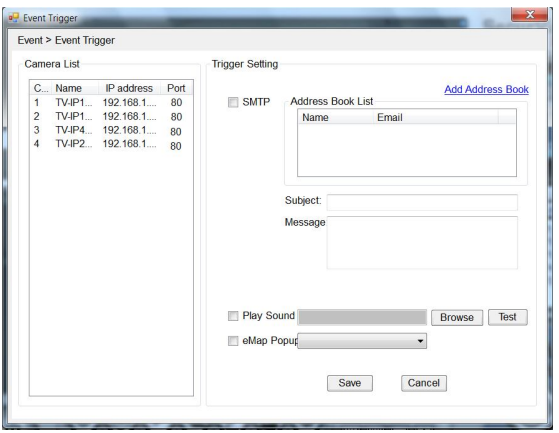
1. On the Address Book window, click **New**.
2. In the Address Book Information field, enter the **Name** and **Email** of the user.
3. When completed, click **Save**. The user will be displayed in the Address Book List.

4. **To edit the user:** In the Address Book List, select the desired user and click **Modify**. The user's information will be displayed, where you can change the user's information and then click **Save** when completed.

5. **To delete the user:** In the Address Book List, select the desired user and click **Remove**. The selected user will be removed from the list.

■ Configuring Event Trigger

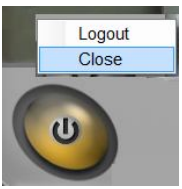
Click the button and select **Event Trigger** to configure the trigger out function of the camera.



1. On the Event Trigger window, select the desired camera from the Camera List.
2. Do one of the following:
   - **SMTP:** Select this option and enter the Subject and Message, the system will send an email message to the selected user(s) in the Address Book List.
   - **Play Sound:** Select this option select a sound file from the computer, so that the system will alarm by the sound while triggering out.
   - **eMap Popup:** Select this option and select the eMap profile from the pull-down menu. The camera view of the eMap will be displayed while triggering out.

5.2.7 Close Program

When you have finished operating, click the button and select **Logout** to logout the system or **Close** to exit the program.



CHAPTER 6

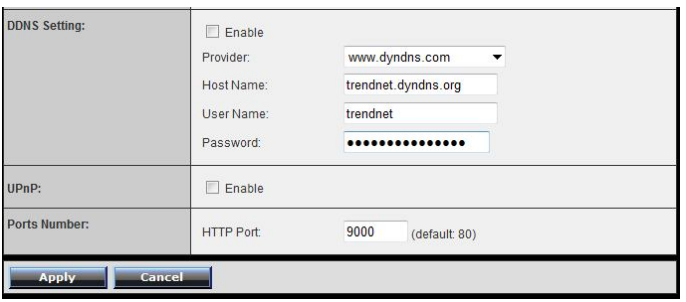
How to access the camera behind a Router

You can either setup the Dynamic DNS connection via camera itself or your home router. An account from any of the listed DDNS providers is required prior to this operation.

Configure DDNS on your Camera

1. Go to Camera's **DDNS Setting** page, click **Enable** to activate the feature. Then select a DDNS provider from the list.

2. Enter your DDNS's the Host Name, User Name and Password.

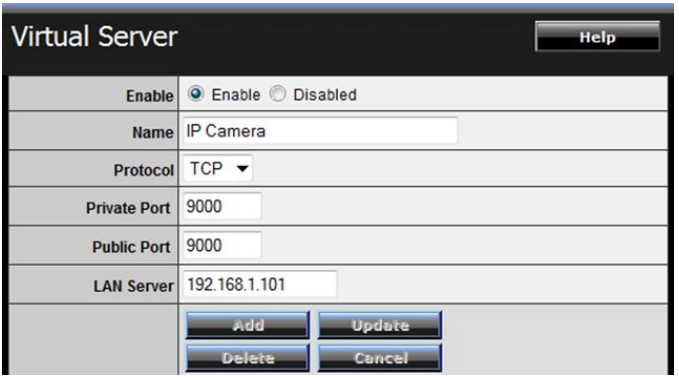


3. In the **Port Number** section, assign an HTTP port of the camera. The default HTTP Port on the camera is 80. The example shows above is using port number 9000.

4. Open another web browser and go to your Router's Web Configuration page. (In the example, TRENDnet's TEW-651BR Wireless N router is used)

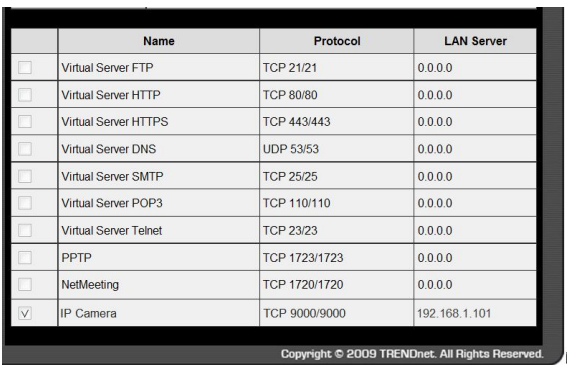
5. Go to **Virtual Server*** section and create a new entry.
Enable: Click **Enable**
Name: Enter the application name (eg. CameraName)
Protocol: Select **TCP**

Private Port: The HTTP port that you assign on your Camera.
Public Port: The port used on remote side to access to your Camera.
LAN Server: The local IP address of your Camera.



Then click **Add** to add the application.

* Please refer to your router's user's manual for detail **Virtual Server** setting. Some router might use **Port Forwarding** or **Special applications** for this function. The setup steps should be very similar.

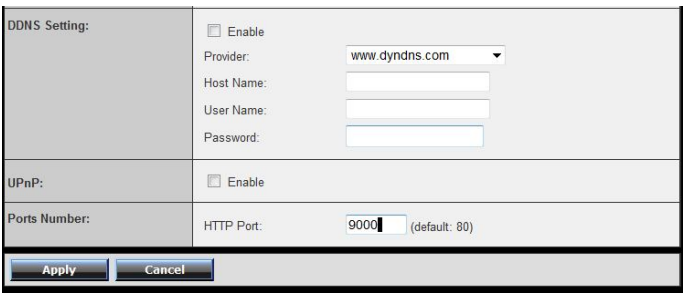


6. Open another web browser and enter your DDNS domain and camera's port number.
http://yourDomainName:PortNumber

7. Camera's login page will appear.

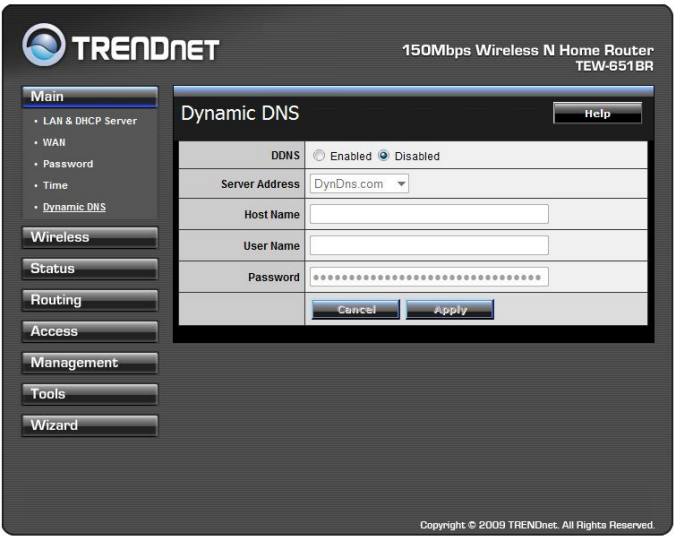
Configure DDNS on your router

1. Go to Camera's **DDNS → Ports Number** section, assign a HTTP port for your camera and click **Apply**.

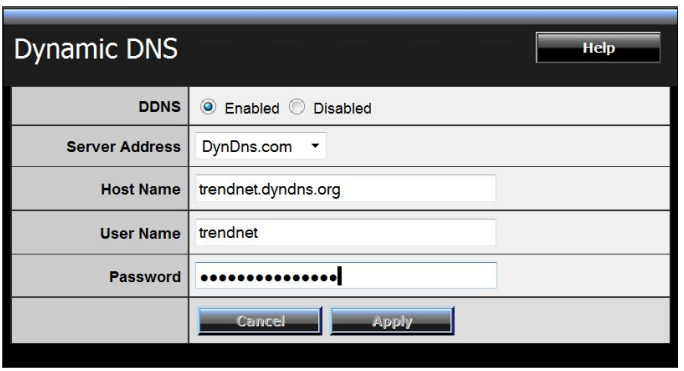


2. Login to your router's web configuration page.

3. Find the **Dynamic DNS** configuration section.



4. Enable DDNS, fill out the following information and then click **Apply**.



5. Go to **Virtual Server*** section and create a new entry.
   Enable: Click **Enable**
   Name: Enter the application name (eg. Camera Name)
   Protocol: Select **TCP**
   Private Port: The HTTP port that you assign on your Camera.
   Public Port: The port used on remote side to access to your Camera.
   LAN Server: The local IP address of your Camera.

   Click **Add** to add the application.

   * Please refer to your router's user's manual for detail **Virtual Server** setting. Some router might use **Port Forwarding** or **Special applications** for this function. The setup steps should be very similar.

6. Open another web browser and enter your DDNS domain and camera's port number.
   http://yourDomainName:PortNumber

7. The camera login page will appear.

CHAPTER 7

APPENDIX

A.1 Specification

- **Image Sensor**

Sensor	1/4” color CMOS
Resolution	640x480

- **Video**

Compression	MJPEG
Video resolution	VGA/QVGA/QQVGA; up to 30fps

- **System Hardware**

Processor	ARM9 base
RAM	32MB SDRAM
ROM	4MB NOR Flash
Power	DC 5V

- **Communication**

LAN	10/100Mbps Fast Ethernet, auto-sensed, Auto-MDIX
WLAN	Based on IEEE 802.11n technology, IEEE 802.11g/b
Protocol support	TCP/IP, UDP, ICMP, DHCP, NTP, DNS, DDNS, SMTP, FTP, PPPoE, UPnP

- **User Interface**

LAN	One RJ-45 port
Antenna	One external antenna

Reset	One Reset button
LEDs	Power LED (amber); Link LED (green)

- **Audio**

Input	Built-in MIC
Codec	PCM

- **Software**

OS Support	Windows 7/Vista/XP
Browser	Internet Explorer 6.0 or above
Software	SecurView Pro for playback/recording/ configuration features

- **Operating Environment**

Temperature	- Operation: 0°C ~ 45°C
	- Storage: -15°C ~ 60°C
Humidity	Max. 85% non-condensing

- **EMI**

FCC Class B, CE Class B

A.2 Glossary of Terms

NUMBERS

10BASE-T 10BASE-T is Ethernet over UTP Category III, IV, or V unshielded twisted-pair media.

100BASE-TX The two-pair twisted-media implementation of 100BASE-T is called 100BASE-TX.

A

ADPCM Adaptive Differential Pulse Code Modulation, a new technology improved from PCM, which encodes analog sounds to digital form.

AMR AMR (Adaptive Multi-Rate) is an audio data compression scheme optimized for speech coding, which is adopted as the standard speech codec by 3GPP.

Applet Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer form that the applet was sent.

ASCII American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters.

ARP Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address.

AVI Audio Video Interleave, it is a Windows platform audio and video file type, a common format for small movies and videos.

B

BOOTP Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address.

C

Communication Communication has four components: sender, receiver, message, and medium. In networks, devices and application

tasks and processes communicate messages to each other over media. They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium.

Connection In networking, two devices establish a connection to communicate with each other.

D

DHCP Developed by Microsoft, DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. It also supports a mix of static and dynamic IP addresses. This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address. DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one.

DNS Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name *www.network_camera.com* might translate to *192.167.222.8*.

E

Enterprise network An enterprise network consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and operates the company's mission-critical applications.

Ethernet The most popular LAN communication technology. There are a variety of types of Ethernet, including 10Mbps (traditional Ethernet), 100Mbps (Fast Ethernet), and 1,000Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology.

F

Fast Ethernet Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media.

Firewall Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

G

Gateway A gateway links computers that use different data formats together.

Group Groups consist of several user machines that have similar characteristics such as being in the same department.

H

HEX Short for hexadecimal refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

I

Intranet This is a private network, inside an organization or company that uses the same software you will find on the public Internet. The only difference is that an Intranet is used for internal usage only.

Internet The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP). The Internet provides different ways to access private and public information worldwide.

Internet address To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP addresses

IP Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the *packet*) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules. In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks.

IP address IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example 80.80.80.69 is an IP address. When you "call" that number, using any connection methods, you get connected to the computer that "owns" that IP address.

ISP ISP (Internet Service Provider) is a company that maintains a network that is linked to the Internet by way of a dedicated communication line. An ISP offers the use of its dedicated communication lines to companies or individuals who can't afford the high monthly cost for a direct connection.

J

JAVA Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for

creating applets and applications for the Internet, Intranet and other complex, distributed network.

L

LAN Local Area Network a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings.

M

MJPEG MJPEG (Motion JPEG) composes a moving image by storing each frame of a moving picture sequence in JPEG compression, and then decompressing and displaying each frame at rapid speed to show the moving picture.

MPEG4 MPEG4 is designed to enable transmission and reception of high-quality audio and video over the Internet and next-generation mobile telephones.

N

NAT Network Address Translator generally applied by a router that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network. NAT solves the problem. When devices within your network request information from the Internet, the requests are forwarded to the Internet under the router's IP address. NAT distributes the responses to the proper IP addresses within your network.

Network A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of network are:

LAN – (local area network): Computers are in close distance to one another. They are usually in the same office space, room,

or building.

WAN – (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves.

NWay Protocol A network protocol that can automatically negotiate the highest possible transmission speed between two devices.

P

PCM PCM (Pulse Code Modulation) is a technique for converting analog audio signals into digital form for transmission.

PING Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used to troubleshoot Internet connections.

PPPoE Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection.

Protocol Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions. Some protocols are responsible for formatting and presenting and presenting data that will be transferred from file server memory to the file server's net work adapter Others are responsible for filtering information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). Protocols that dictate the format of data for transferors the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD), implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP),a part of the

Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol.

R

RJ-45 RJ-45 connector is used for Ethernet cable connections.

Router A router is the network software or hardware entity charged with routing packets between networks.

RTP RTP (Real-time Transport Protocol) is a data transfer protocol defined to deliver **live media** to the clients at the same time, which defines the transmission of video and audio files in real time for Internet applications.

RTSP RTSP (Real-time Streaming Protocol) is the standard used to transmit **stored media** to the client(s) at the same time, which provides client controls for random access to the content stream.

S

Server It is a simple computer that provides resources, such as files or other information.

SIP SIP (Session Initiated Protocol) is a standard protocol that delivers the real-time communication for Voice over IP (VoIP), which establishes sessions for features such as audio and video conferencing.

SMTP The Simple Mail Transfer Protocol is used for Internet mail.

SNMP Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices.

Station In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations.

Subnet mask In TCP/IP, the bits used to create the subnet are called the subnet mask.

T

(TCP/IP) Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of various transmission methods. It was developed y the Department of Defense to connect different computer types and led to the development of the Internet.

Transceiver A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports.

U

UDP The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite

User Name The USERNAME is the unique name assigned to each person who has access to the LAN.

Utility It is a program that performs a specific task.

UTP Unshielded twisted-pair. UTP is a form of cable used by all access methods. It consists of several pairs of wires enclosed in an unshielded sheath.

W

WAN Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques.

WEP WEP is widely used as the basic security protocol in Wi-Fi networks, which secures data transmissions using 64-bit or 128-bit encryption.

Windows Windows is a graphical user interface for workstations that use DOS.

WPA	WPA (Wi-Fi Protected Access) is used to improve the security of Wi-Fi networks, replacing the current WEP standard. It uses its own encryption, Temporal Key Integrity Protocol (TKIP), to secure data during transmission.
WPA2	Wi-Fi Protected Access 2, the latest security specification that provides greater data protection and network access control for Wi-Fi networks. WPA2 uses the government-grade AES encryption algorithm and IEEE 802.1X-based authentication, which are required to secure large corporate networks.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TV-IP121WN – 3 Years Limited Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is

required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT

OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to http://www.trendnet.com/gpl or http://www.trendnet.com Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at http://www.trendnet.com/register

Copyright ©2011. All Rights Reserved. TRENDnet.