



AltCtrl FW Series

AC-FW0514VP User Manual

Version: **1.0.101004**
Release Date: **2010 / 10 / 04**



Table of Contents

- 1. GETTING STARTED WITH THE AC-FW0514VP 4
- 2. SECURITY FUNCTIONAL FEATURES 5
- 3. IDENTIFY COMPONENTS..... 6
 - 3.1. FRONT PANEL 6
 - 3.2. BACK PANEL 7
 - 3.3. HARDWARE SPECIFICATION 8
 - 3.4. ENVIRONMENT CONDITIONS..... 8
- 4. CONNECT TO THE AC-FW0514VP 9
 - 4.1. SETUP AC-FW0514VP DEVICE..... 9
 - 4.2. CONFIGURE YOUR COMPUTER 10
 - 4.3. LOG IN AC-FW0514VP 19
- 5. CONFIGURATION..... 20
 - 5.1. SYSTEM 20
 - 5.1.1. System / Overview 20
 - 5.1.2. System / Time Settings..... 21
 - 5.1.3. System / Change Password 22
 - 5.1.4. System / Web Access 23
 - 5.1.5. System / Firmware Upgrade..... 24
 - 5.1.6. System / Restart Device 24
 - 5.2. NETWORK 25
 - 5.2.1. Network Config Wizard..... 25
 - 5.2.2. Network / Overview..... 28
 - 5.2.3. Network / Configuration 29
 - 5.2.4. Network / Wireless 36
 - 5.2.5. Network / Dynamic DNS 37
 - 5.3. QoS..... 38
 - 5.3.1. QoS / Overview 38
 - 5.3.2. QoS / Class 39
 - 5.3.3. QoS / IP (Classification Rule)..... 40
 - 5.4. FIREWALL 41
 - 5.4.1. Firewall / Port Forwarding..... 41
 - 5.4.2. Firewall / UPnP 42
 - 5.4.3. Firewall / IP Blacklist 42
 - 5.5. ANTI-VIRUS..... 43
 - 5.5.1. Anti-Virus / Overview 43
 - 5.5.2. Anti Virus / Signature..... 44
 - 5.5.3. Anti Virus / Configuration..... 44

5.6. WEB GUARD	46
5.6.1. Web Guard / Overview	46
5.7. URL FILTER	47
5.7.1. URL Filter / Overview	47
5.7.2. URL Filter / Configuration	48
5.8. SIGNATURE UPDATE	49
5.8.1. Signature Update / Auto Update	50
5.8.2. Signature Update / Manual Update	51
5.9. LOG AND REPORT	52
5.9.1. Logs and Report / Configuration	52
5.9.2. Logs and Report / Anti-Virus	53
5.9.3. Logs and Report / Web Guard	54
5.9.4. Logs and Report / URL Filter	55
5.9.5. Logs and Report / IP Blacklist	56
6. TROUBLE-SHOOTING	57

1. Getting Started with the AC-FW0514VP

The **AC-FW0514VP** is a useful UTM device that provides L7 security protections to the connected equipments after internet access devices. Any network equipments with standard WiFi connection, or 10/100 Mbps fast Ethernet port can connect to it, or to the switching device under its gateway coverage for protection. It is suitable to home or SMB users who has broadband internet service provided by lease line, xDSL, cable modem, or entry level of FTTX fiber optics.

AC-FW0514VP has friendly web based graphic user interface for system configuration, inspection, and management control. Without additional host CPU resource or installation process, **AC-FW0514VP** provides transparent security features such as firewall, anti-virus, Qos Bandwidth Control, malicious web drive-by download protection, and category-based URL filtering.

Features and Benefits

- ❖ The simplest and most cost effective security device.
- ❖ The simplest and most cost effective security device.
- ❖ No additional host-CPU resources consumption / No Installation needed.
- ❖ High throughput that provides rapid network Download and Access.
- ❖ Firewall, Anti-Virus, Qos Bandwidth Control ,Anti-Malicious URL, URL Protocol filterer.
- ❖ Friendly graphic user interface control, inspection report and management.
- ❖ Easy use with “**Network Config Wizard**”.
- ❖ Support PPPoE, DHCP, NAT
- ❖ Suitable for Home, SOHO and SMB users.

2. Security Functional Features

Anti-Virus

- Packet-based Virus Scanning
- Support HTTP / FTP / SMTP / POP3 / IMAP4 / TCP STREAM
- Packet-Based Decoding for Base64 / UUencode / QP
- Packet-Based Decompression for Zip / Gzip / Rar
- Detect Viruses Across in Multi-Packets

Web Guard

- Website Hijacking Prevention
- Concise URL Malicious Website Database
- Smaller Database Size
- URL Path Only and URL Host+Path Support

URL Filter

- High Speed Filtering
- Category-Based Blacklist Function
- Low Rates of Overblocking
- World's Best Site Coverage
- Comprehensive Categories

QoS Bandwidth Control

- Support QoS control for LAN IP
- Control Bandwidth of download or upload
- Config Max and Mini class for download or upload
- Config classification rules for LAN ip address

3. Identify Components

3.1. Front Panel

The LEDs indicate its operational status.



LED Description

LED	Color	Condition	Status
POWER	Green	On	Power on
		Off	Power off
WiFi	Green	On	WiFi enabled
		Blinking	Transmitting
		Off	WiFi not ready or failed
	Orange	On	Firmware updating
		Blinking	Resetting to default
WAN	Green	On	Physical link ok
		Blinking	Transmitting
		Off	Ethernet not ready or failed
LAN	Green	On	Physical link ok
		Blinking	Transmitting
		Off	Ethernet not ready or failed

3.2. Back Panel



Feature	Description
POWER	The receptacle where you plug in the power adapter
WAN	Using this port to connect your modem to AC-FW0514VP.
LAN	Using those ports to connect your PC or NB to AC-FW0514VP.
RESET	Push and hold RESET button over 5 seconds and then release to reset to factory default settings.
WiFi	Enable/disable WiFi function

Note:

Push “RESET” button can reset to factory default settings.

“RESET” button is not for “Restart Device”.

You can go to the “System / Restart Device” to reboot system, or power off and power on AC-FW0514W for “Restart Device”.

3.3. Hardware Specification

Feature	Description
Network	10/100Mbps Fast Ethernet X 5 (LAN X 4, WAN X 1) IEEE 802.11b/g/n draft
Power Supply	Switching Power Adapter Input: 100~240V ; Output: 12V / 1A Power Connector: +5V DC-in Lack
Reset	Push and hold RESET button over 5 seconds and then release to reset to factory default settings.

3.4. Environment Conditions

Feature	Description
Operating Temperature	0°C ~ 45 °C (0 °F ~ 113 °F) ambient temperature
Storage Temperature	-30 °C ~ 70 °C (-86 °F ~ 158 °F) ambient temperature
Operating Humidity	90% maximum (non-condensing)
Storage Humidity	90% maximum (non-condensing)

4. Connect to the AC-FW0514VP

4.1. Setup AC-FW0514VP device

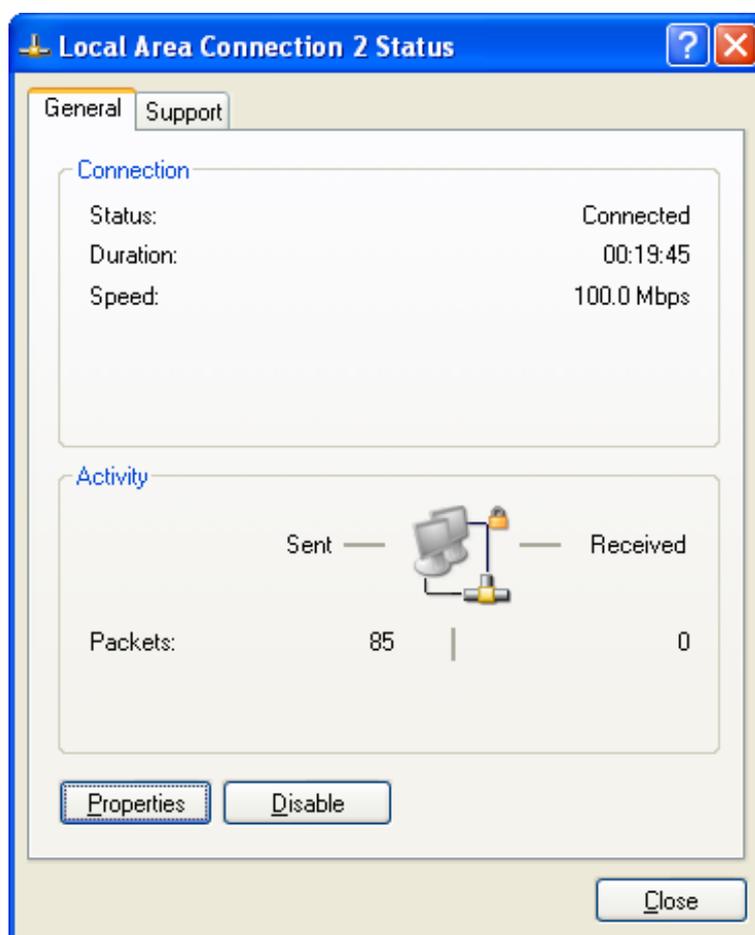
1. Power the AC-FW0514VP device by power adaptor.
2. Connect WAN to the Internet and then connect LAN to your networking devices.



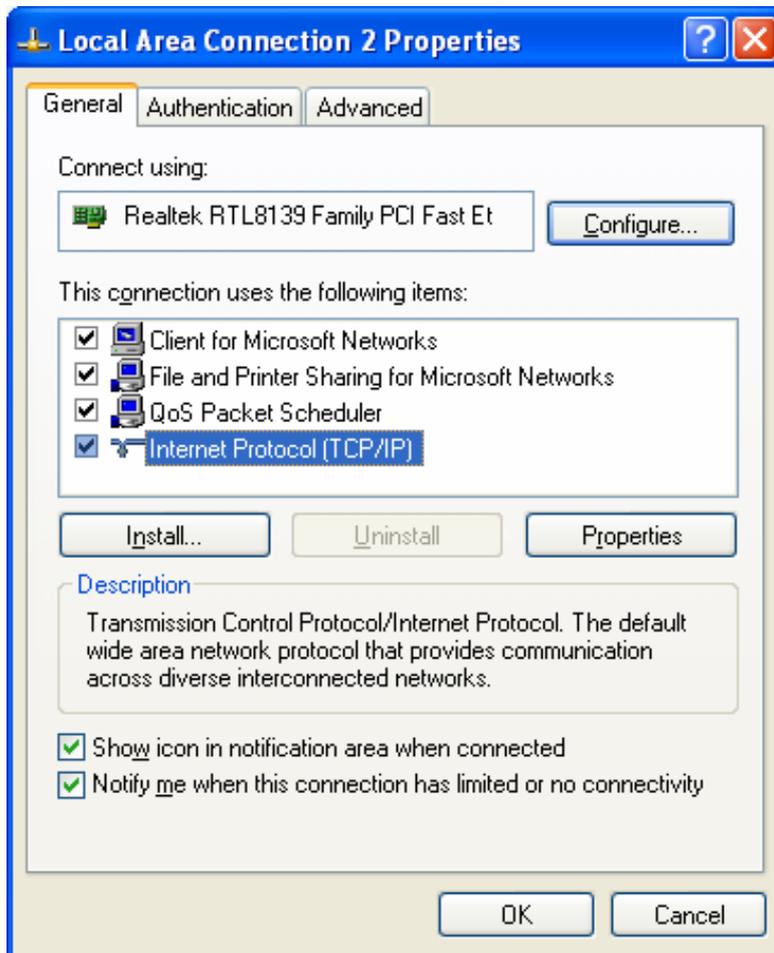
4.2. Configure your computer

❖ Windows XP configuration:

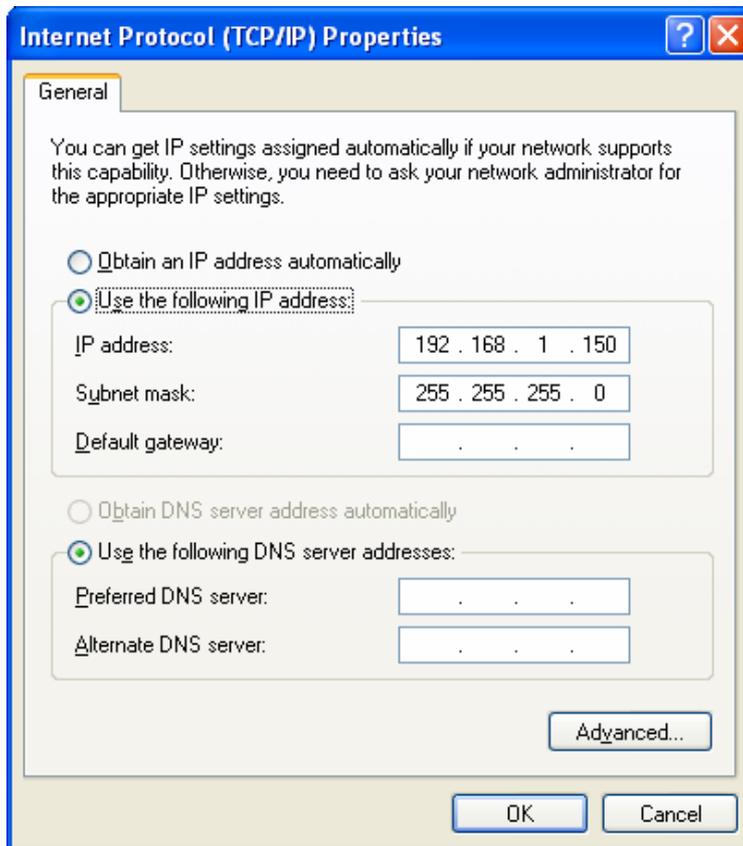
1. Click “**Start / Settings / Control Panel**” (or “**Start / Control Panel**”).
2. Click “**Network and Internet Connections**”.
3. Click “**Network Connection**”
4. Double-click “**Local Area Connection**”.



5. Click the “**Properties**” button.



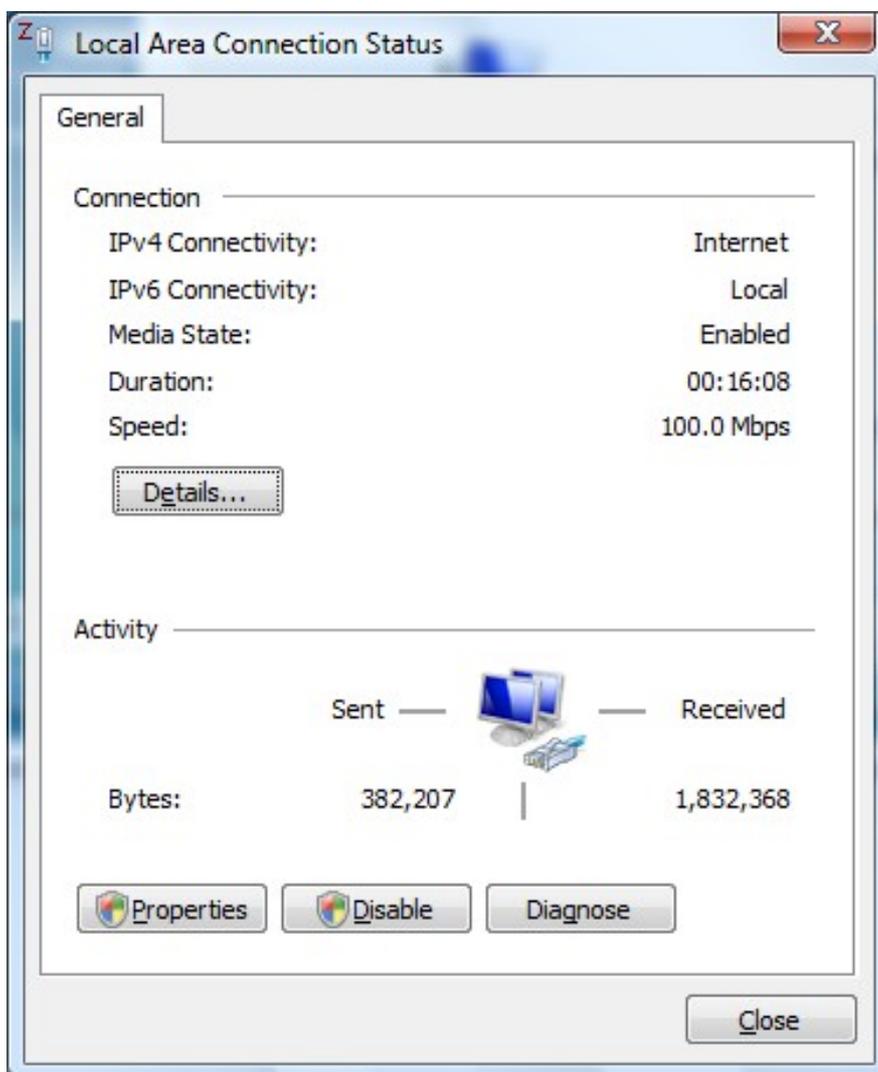
6. Ensure the box next to **“Internet Protocol (TCP / IP)”** is selected.
7. Click to highlight **“Internet Protocol (TCP / IP)”** and click the **“Properties”** button.



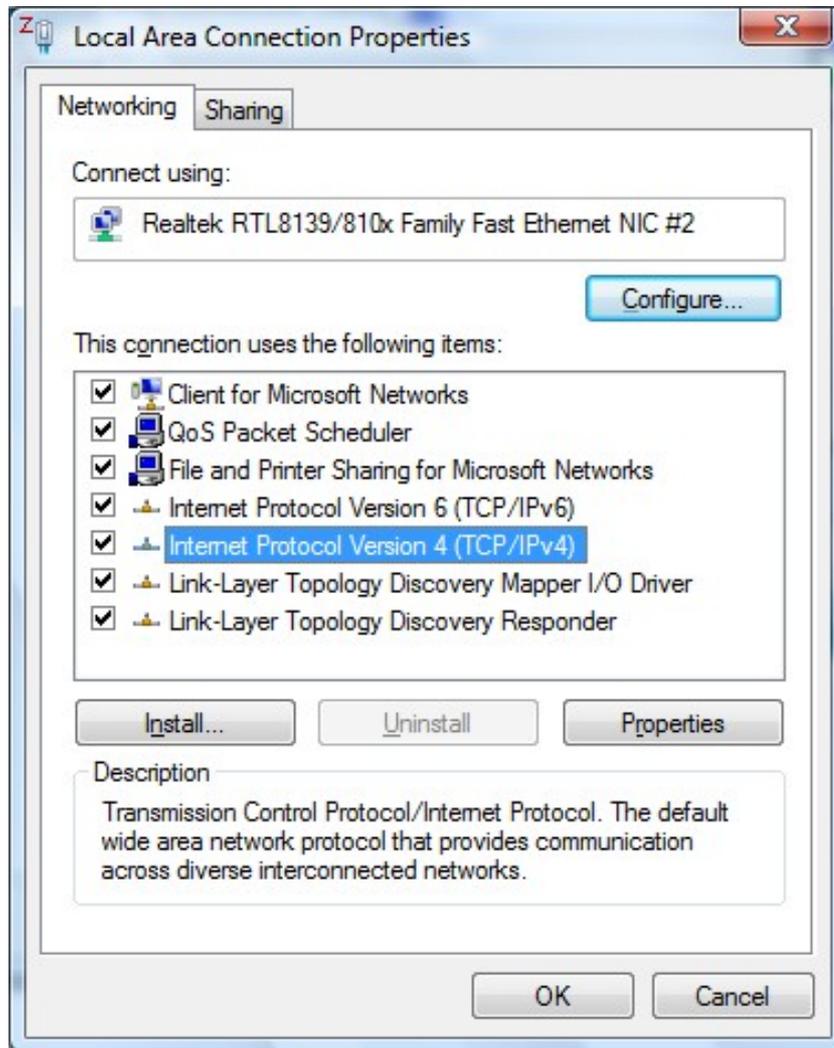
8. Select **“Use the following IP address”**, and enter IP address: **192.168.1.150***, Subnet mask: **255.255.255.0**. Click **OK** twice to exit and save your settings.
(* You can enter 192.168.1.2 ~ 192.168.1.254 as long as there is no IP conflict.)
9. You can also select **“Obtain an IP address automatically”** and click **OK** to save your settings.

❖ Windows Vista configuration:

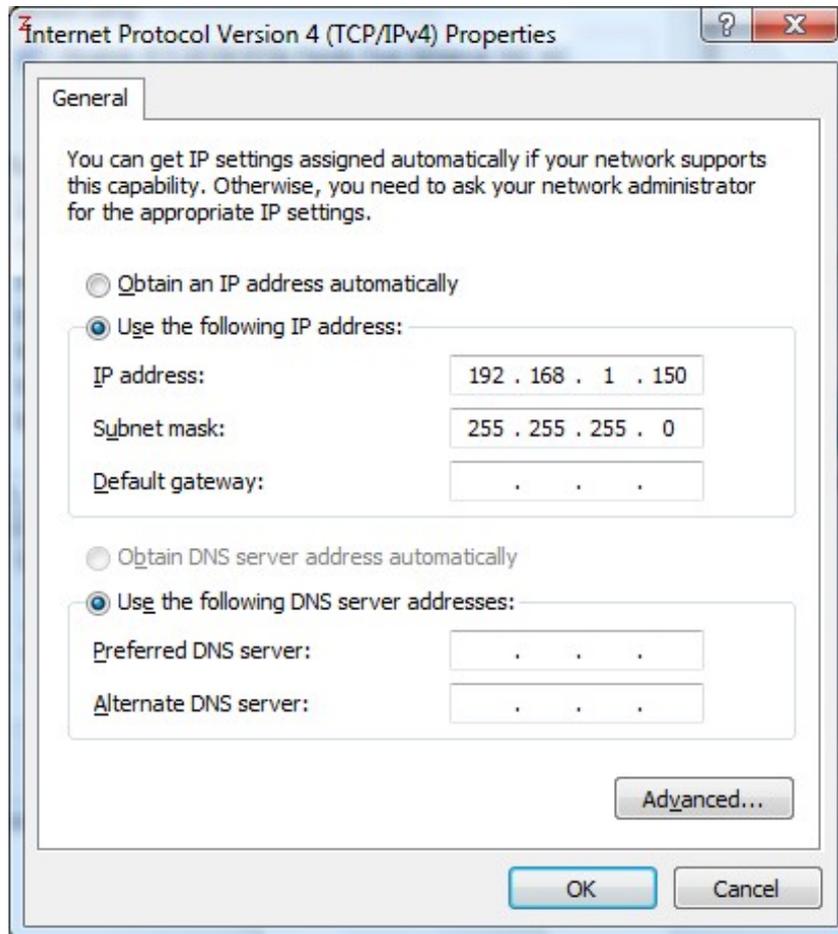
1. Click “**Start / Settings / Control Panel**” (or “**Start / Control Panel**”).
2. Click “**Network and Internet**”.
3. Click “**Network and Sharing Center**”.
4. Click “**Manage network connections**”.
5. Double-click “**Local Area Connection**”.



6. Click the “**Properties**” button.



7. Ensure the box next to “**Internet Protocol Version 4 (TCP / IPv4)**” is selected.
8. Click to highlight “**Internet Protocol Version 4 (TCP / IP v4)**” and click the “**Properties**” button.

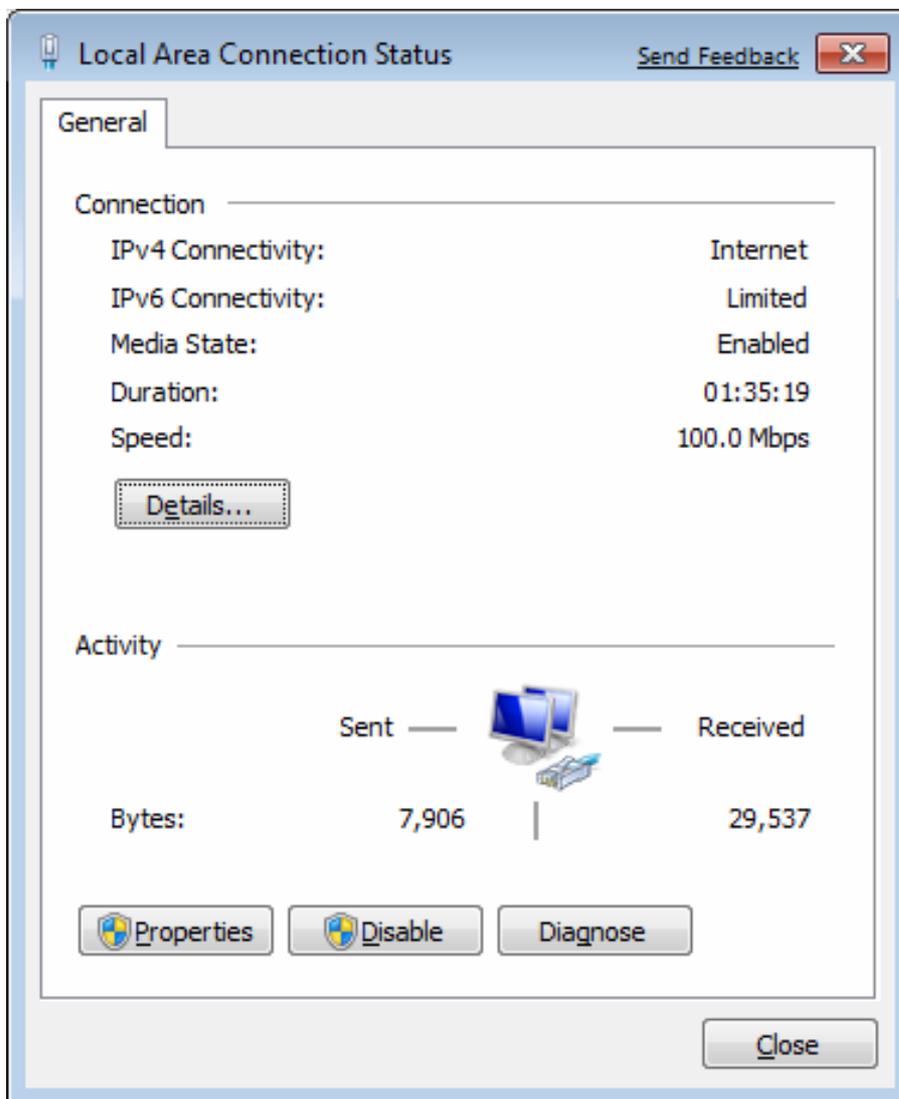


9. Select **“Use the following IP address”**, and enter IP address: **192.168.1.150***, Subnet mask: **255.255.255.0**. Click **OK** twice to exit and save your settings.
(* You can enter 192.168.1.2 ~ 192.168.1.254 as long as there is no IP confliction.)

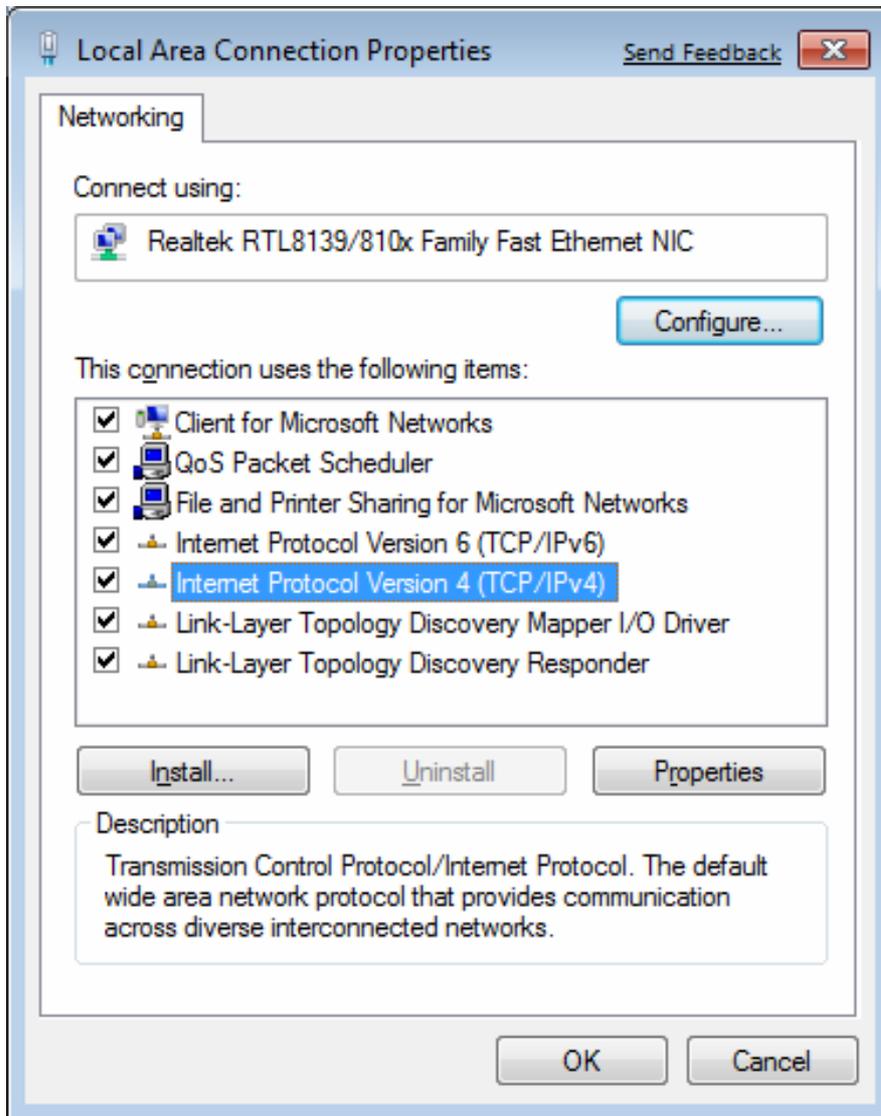
10. You can also select **“Obtain an IP address automatically”** and click **OK** to save your settings.

❖ Windows 7 configuration:

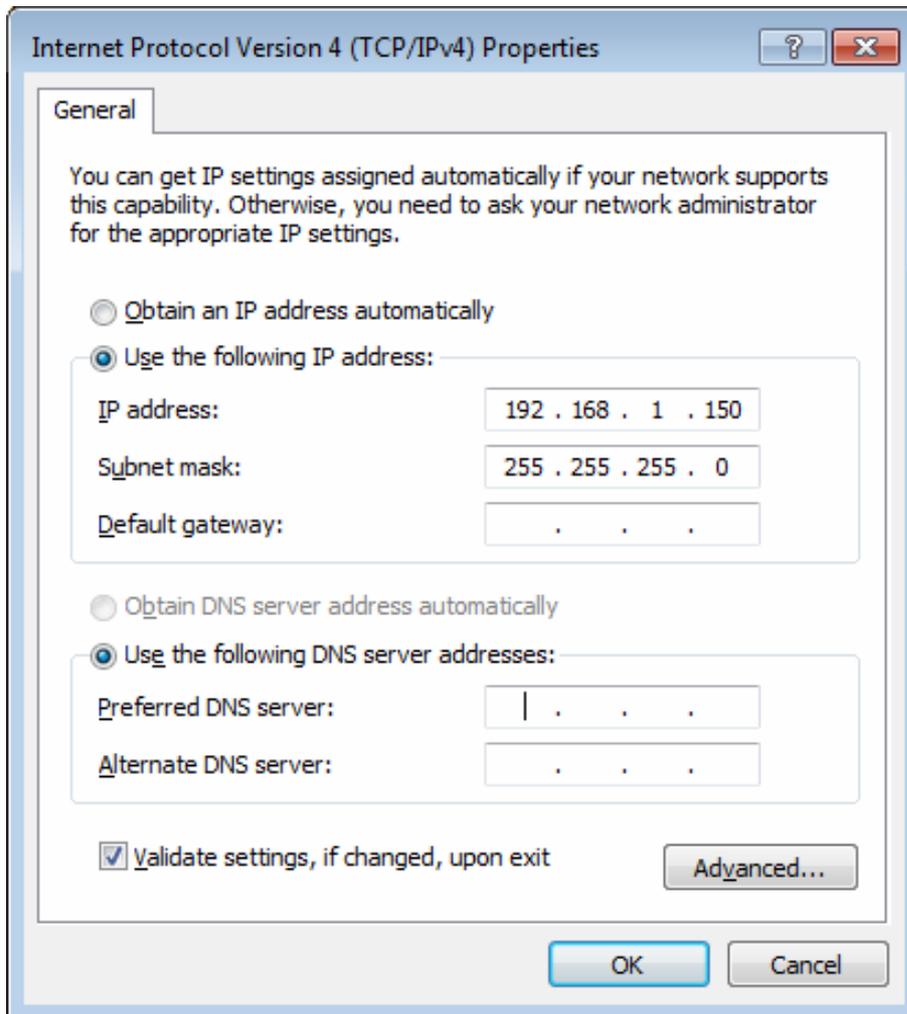
1. Click **“Start / Settings / Control Panel”** (or **“Start / Control Panel”**) .
2. Click **“Network and Internet”**.
3. Click **“Network and Sharing Center”**.
4. Click **“Change adapter settings”**.
5. Double-click **“Local Area Connection”**.



6. Click the **“Properties”** button.



7. Ensure the box next to “**Internet Protocol Version 4 (TCP / IPv4)**” is selected.
8. Click to highlight “**Internet Protocol Version 4 (TCP / IPv4)**” and click the “**Properties**” button.



9. Select **“Use the following IP address”**, and enter IP address: **192.168.1.150***, Subnet mask: **255.255.255.0**. Click **OK** twice to exit and save your settings.
(* You can enter 192.168.1.2 ~ 192.168.1.254 as long as there is no IP conflict.)
10. You can also select **“Obtain an IP address automatically”** and click **OK** to save your settings.

4.3. Log in AC-FW0514VP

This section will show you how to configure **AC-FW0514VP** by using the web-based configuration utility. Please be noted that the best supporting browsers are IE7, IE8 and Firefox 3.x. (IE6 and Firefox 2.x are not supported).

1. To access the configuration utility, open a web browser and enter:
http://192.168.1.1 (or: **192.168.1.1**)



2. Once the log in page successfully appeared, please continue to enter username and password.
For the first time, please select your language and enter default username and password.

Username: **admin**

Password: **123456**



5. Configuration

5.1. System

The system menu is where you carry out the basic setup of AC-FW0514VP. It includes time settings, change password, web access, firmware upgrade and restart device.



5.1.1. System / Overview

Overview

After you log in, go to the “**System**” and click “**Overview**” to see the system information and security service status.

System / Overview	
System Information	
Active Connection	6
Memory	61608 kB
Firmware Version	1.1.15707
Security Service Status	
Anti Virus	ON
Zip file Scan	ON
Web Guard	ON
URL Filter	OFF
Log Active	ON

5.1.2. System / Time Settings

System Time

To configure the correct time in the local zone of the internal system clock, select your time zone from the drop-down “**Select Timezone**” manual and then click “**Apply**”. Also you can tick “**Enable NTP Client**” check bottom and input the NTP Servers, or click “**Synchronize now**” button to correct system time immediately or input synchronization interval time (seconds) for auto time correction.

You can **untick** “**Enable NTP Client**” check bottom then setup date and time manually and click “**Apply**”.

System / Time Settings

Time Settings

Select Timezone: (GMT+07:00) Bangkok, Hanoi, Jakarta

Enable NTP Client

NTP Server 1: pool.ntp.org Port: 123

NTP Server 2: europe.pool.ntp.org Port: 123

NTP Server 3: north-america.pool.ntp.org Port: 123

NTP Server 4: asia.pool.ntp.org Port: 123

Synchronization Interval: 3600 (Seconds)

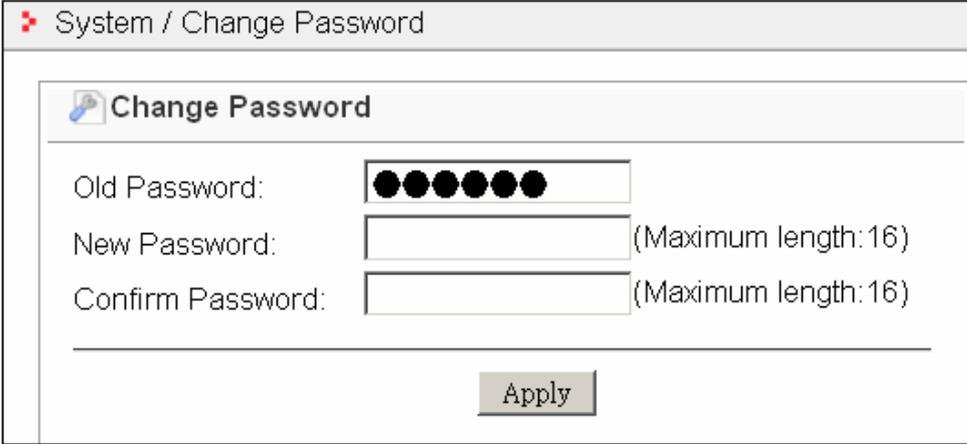
Setup Date & Time Manually: 2000 / 01 / 02 (Year/Month/Day)

04 : 15 : 26 (Hours:Minutes:Seconds)

5.1.3. System / Change Password

Change Password

It is highly recommended you change the default password. Enter a new password and confirm by entering the new password again. And then click “**Apply**” to change.



System / Change Password

Change Password

Old Password:

New Password: (Maximum length: 16)

Confirm Password: (Maximum length: 16)

Apply

5.1.4. System / Web Access

Web Access

LAN / WAN web access means that you can connect to web GUI via LAN / WAN IP address. We provide both HTTPS and HTTP web access, and you can change HTTPS port or HTTP port by entering a new port, and then click “**Apply**” to change.

WAN port web access is disabled by default settings for security reason. You can select “**Enable WAN Web Access**” and then click “**Apply**” to enable WAN web access.

System / Web Access

Web Access

LAN IP : 192.168.1.1

LAN Web Access: HTTPS & HTTP

HTTPS Port: 443

HTTP Port: 80

WAN IP : 192.168.2.1

Enable WAN Web Access: HTTPS & HTTP

HTTPS Port: 443

HTTP Port: 80

Apply

Note:

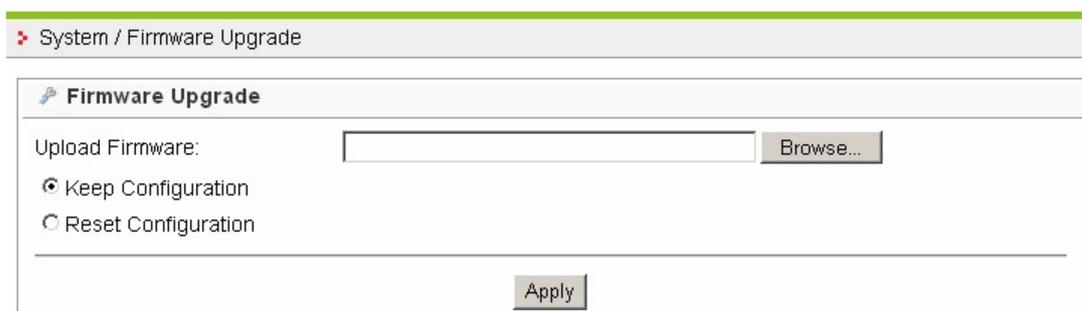
You can access “Bridge IP” or “Management IP” from internal(LAN) or external(WAN) when you choose “Bridge” mode. “Web Access” page will not be showed when you choose “Bridge” mode.

5.1.5. System / Firmware Upgrade

Firmware Upgrade

Upgrade the firmware of AC-FW0514VP when a new version of firmware releases.

When you got the new firmware file, assign it at this page, then click **“Apply”** to complete the firmware upgrade.



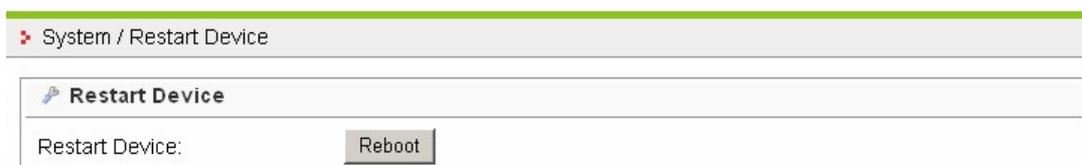
The screenshot shows a web interface for 'System / Firmware Upgrade'. It features a section titled 'Firmware Upgrade' with an 'Upload Firmware:' label, a text input field, and a 'Browse...' button. Below this are two radio button options: 'Keep Configuration' (selected) and 'Reset Configuration'. At the bottom of the section is an 'Apply' button.

Note: The orange LED **“WiFi”** lights on and the message **“System is upgrading firmware, please don’t power off or reboot now.”** shows during the upgrading process. **DO NOT power off or prevent power cut-off during the process of firmware upgrade, it may cause the system breakdown and can not be recovered to normal operating condition.**

5.1.6. System / Restart Device

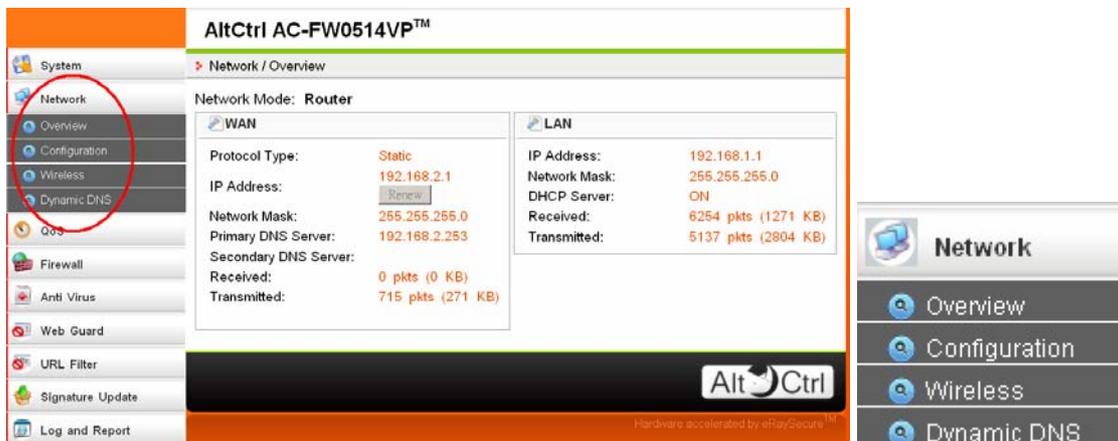
Reboot System

Click to the **“System”** menu and then goes to **“Restart Device”** icon. In this screen, click **“Reboot”** button to reboot your system.



The screenshot shows a web interface for 'System / Restart Device'. It features a section titled 'Restart Device' with a 'Restart Device:' label and a 'Reboot' button.

5.2. Network

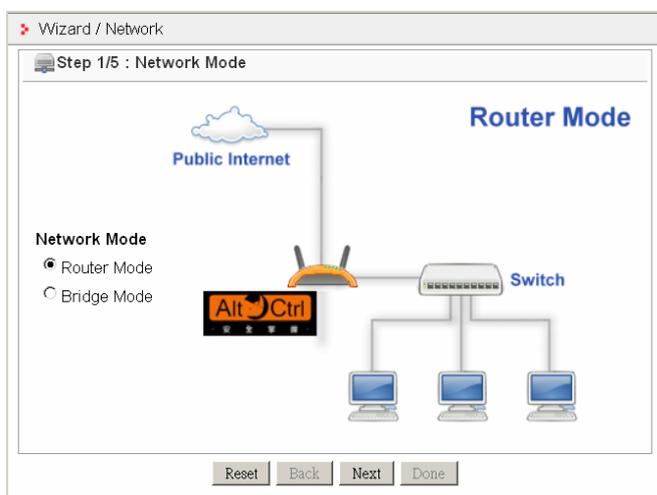


Default Network Settings:

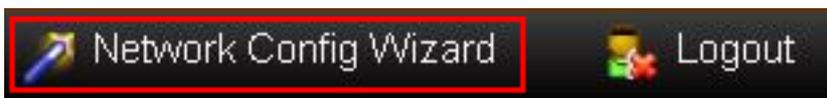
- Network Mode : Router Mode
- WAN IP : DHCP
- LAN IP : 192.168.1.1 (Enable DHCP Server)

5.2.1. Network Config Wizard

When you log in AC-FW0514VP ,the browser will popup “Network Config Wizard”.

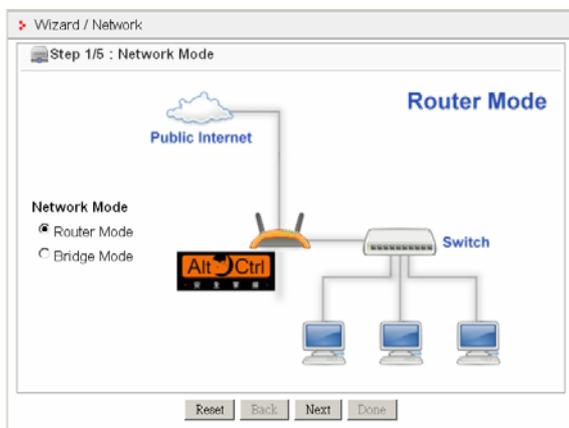


Or you can click the " Network Config Wizard" manually on the top to start Wizard.

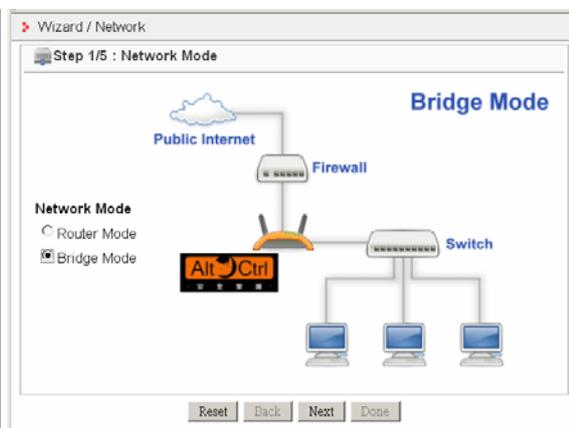


1. Step 1/5 : Choose “Network Mode”.

You can choose “**Router Mode**” or “**Bridge Mode**”.



Router Mode

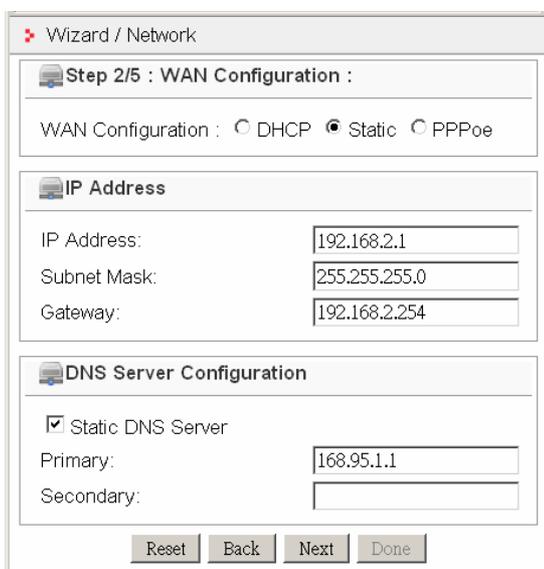


Bridge Mode

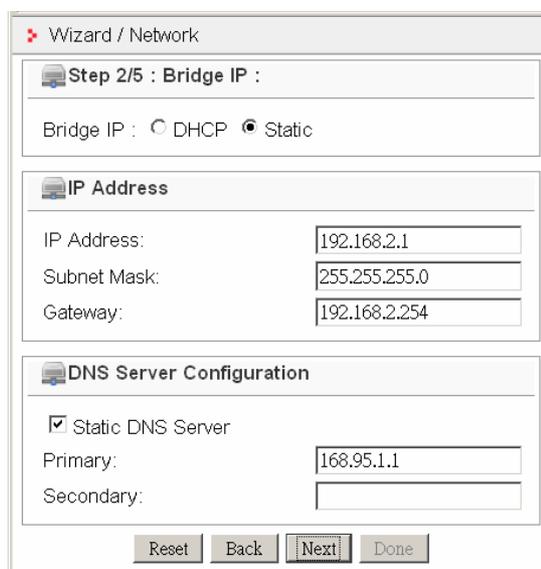
2. Step 2/5 : WAN/Bridge IP Configuration :

In “**Router Mode**”, you can select “**DHCP**”, “**Static**” or “**PPPoE**” for the **WAN IP**.

In “**Bridge Mode**”, you can select “**DHCP**” or “**Static**” for the **Bridge IP**.



Router Mode

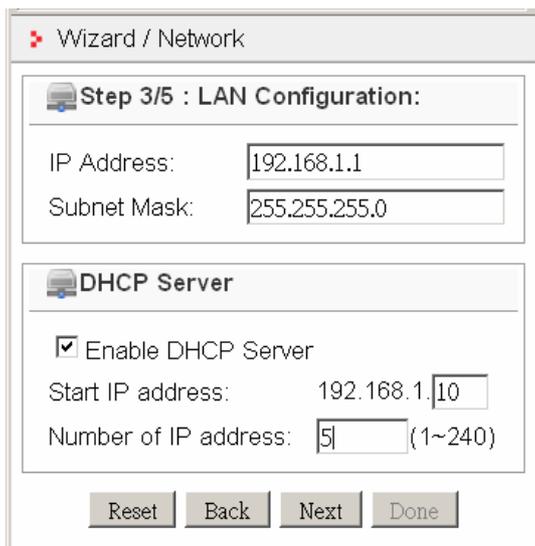


Bridge Mode

3. Step 3/5 : LAN/Management IP Configuration:

In "Router Mode", you can "Enable DHCP Server" for the LAN.

In "Bridge Mode", you can access AC-FW0514VP with "Management IP" even in the "DHCP" client for the WAN.



Wizard / Network

Step 3/5 : LAN Configuration:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server

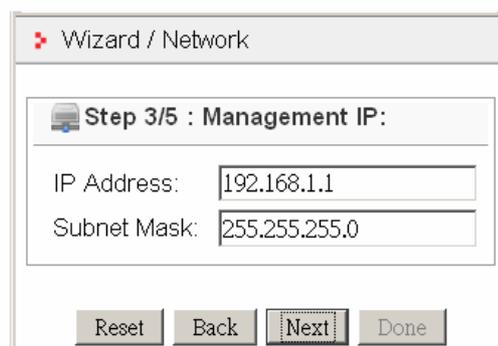
Enable DHCP Server

Start IP address: 192.168.1.10

Number of IP address: 5 (1~240)

Reset Back Next Done

Router Mode



Wizard / Network

Step 3/5 : Management IP:

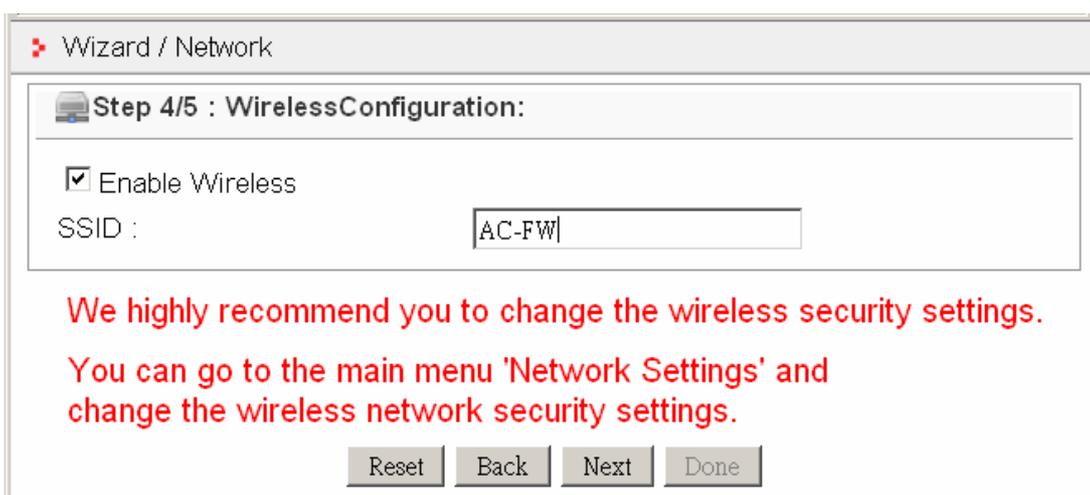
IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Reset Back Next Done

Bridge Mode

4. Step 4/5 : Wireless Configuration:



Wizard / Network

Step 4/5 : WirelessConfiguration:

Enable Wireless

SSID : AC-FW

We highly recommend you to change the wireless security settings.

You can go to the main menu 'Network Settings' and change the wireless network security settings.

Reset Back Next Done

5. Step 5/5 : Summery

Wizard / Network

Step 5/5 : Summery

Network Mode: Router Mode

WAN

WAN IP Setting: Static

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.2.254

Static DNS Server: Yes

Primary: 168.95.1.1

Secondary:

LAN

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Enable DHCP Server: Yes

Start IP address: 192.168.1.10

Number of IP address: 5

Enable Wireless: Yes

Wireless SSID: AC-FW

Reset Back Next Done

Router Mode

Wizard / Network

Step 5/5 : Summery

Network Mode: Bridge Mode

Bridge Mode IP

WAN IP Setting: Static

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.2.254

Static DNS Server: Yes

Primary: 168.95.1.1

Secondary:

Management IP

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Enable Wireless: Yes

Wireless SSID: AC-FW

Reset Back Next Done

Bridge Mode

5.2.2. Network / Overview

Overview shows the current connecting status.

Network / Overview

Network Mode: Router

<p>WAN</p> <p>Protocol Type: Static</p> <p>IP Address: 192.168.2.1 <input type="button" value="Renew"/></p> <p>Network Mask: 255.255.255.0</p> <p>Primary DNS Server: 192.168.2.253</p> <p>Secondary DNS Server:</p> <p>Received: 0 pkts (0 KB)</p> <p>Transmitted: 715 pkts (271 KB)</p>		<p>LAN</p> <p>IP Address: 192.168.1.1</p> <p>Network Mask: 255.255.255.0</p> <p>DHCP Server: ON</p> <p>Received: 6254 pkts (1271 KB)</p> <p>Transmitted: 5137 pkts (2804 KB)</p>	
--	--	---	--

5.2.3. Network / Configuration

Network Mode:

Click configuration and select your Network Mode.
You can choose “**Bridge**” mode or “**Router**” mode.
Default setting is “**Router**” mode.

Network / Configuration

Network Mode: Router

WAN Configuration LAN Configuration

WAN IP Setting: DHCP

 **DNS Server Configuration**

Static DNS Server

Primary:

Secondary:

Apply

* Router Mode :

WAN Configuration (Router Mode)

Select “**DHCP**” client to be assigned an IP address automatically by DHCP server and then click “**Apply**” to validate the setting.

❖ Network / Configuration

Network Mode: Router ▾

WAN Configuration LAN Configuration

WAN IP Setting: DHCP ▾

 **DNS Server Configuration**

Static DNS Server

Primary:

Secondary:

Apply

Or, select “**Static**” to input your own static IP that was provided by network administrator or by ISP. You may have to fill in subnet mask and gateway in this case.

Then click “**Apply**” to validate the setting.

✚ Network / Configuration

Network Mode: Router

WAN Configuration LAN Configuration

WAN IP Setting: Static

IP Address

IP address:	192.168.2.1
Subnet Mask:	255.255.255.0
Gateway:	192.168.2.254

DNS Server Configuration

Static DNS Server

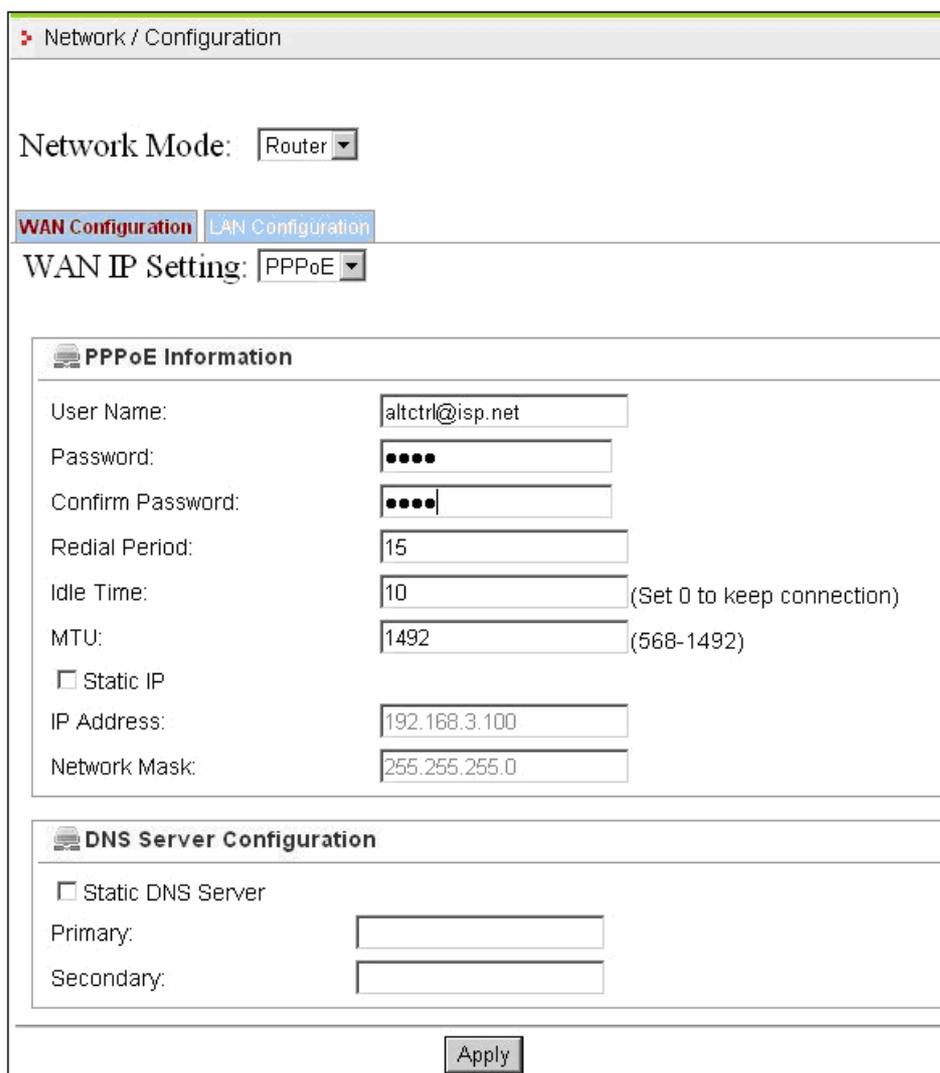
Primary:	192.168.2.253
Secondary:	

Apply

Or, select “**PPPoE**” to access WAN IP by entering PPPoE information.

User Name	PPPoE user information
Password	PPPoE password
Confirm Password	Confirm user password
Redial Period (secs)	Re-connection time period if failed
Idle Time (mins)	Auto disconnecting if network idle for some time
MTU	Maximum Transmission Unit is the size (in bytes) of the largest protocol data unit.

In PPPoE, users can enter static IP address and network mask information if applicable.



The screenshot shows a web-based configuration interface for a network device. The main menu is 'Network / Configuration'. Under 'Network Mode', 'Router' is selected. The 'WAN Configuration' tab is active, and 'WAN IP Setting' is set to 'PPPoE'. The 'PPPoE Information' section contains the following fields:

- User Name: altctrl@isp.net
- Password: [masked with dots]
- Confirm Password: [masked with dots]
- Redial Period: 15
- Idle Time: 10 (Set 0 to keep connection)
- MTU: 1492 (568-1492)
- Static IP
- IP Address: 192.168.3.100
- Network Mask: 255.255.255.0

The 'DNS Server Configuration' section is also visible, with the following fields:

- Static DNS Server
- Primary: [empty field]
- Secondary: [empty field]

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

Click “**Apply**” to validate the setting.

LAN Configuration (Router Mode)

To change the default LAN setting, setup your IP address and subnet mask then click “**Apply**”.

AC-FW0514VP can function as a DHCP server in Router mode. Please tick “**Enable DHCP Server**” check bottom and input the Start IP address and the number of DHCP client range from 1 to 240.

WAN Configuration LAN Configuration

Local Network
IP Address:
Subnet Mask:

DHCP Server
 Enable DHCP Server
Start IP address: 192.168.1.
Number of IP address: (1~240)
Domain:

*** Bridge Mode:**

Bridge IP (Bridge Mode):

Select “**DHCP**” client to be assigned an IP address by DHCP server. Or select “**Static**” to input effective static IP provided by network administrator or by ISP. You may have to fill in subnet mask and gateway in this case. Click “**Apply**” to activate the setting.

✚ Network / Configuration

Network Mode: Bridge

Bridge IP

Management IP

WAN IP Setting: Static

IP Address

IP address:	192.168.2.1
Subnet Mask:	255.255.255.0
Gateway:	192.168.2.254

DNS Server Configuration

Static DNS Server

Primary:	192.168.2.253
Secondary:	

Apply

Management IP (Bridge Mode):

If you choose “**Bridge**” mode and select “**DHCP**” client to be assigned an IP address by DHCP server, you do not know what IP address that AC-FW0514VP get. So you can assign another “**Management IP**” on AC-FW0514VP. You can access it with “**Management IP**”.

To change the default “**Management IP**” settings like IP address, subnet mask then click “**Apply**”.

✚ Network / Configuration

Network Mode:

 **Local Network**

IP Address:

Subnet Mask:

 **DHCP Server**

Enable DHCP Server

Start IP address:

Number of IP address: (1~240)

Domain:

5.2.4. Network / Wireless

Wireless communication is supported by 802.11b / g / n draft.

Enable Wireless

Enable / Disable Wireless function to display the setting.

Network Mode

This identifies the networking standards available to your network.

SSID

SSID is a 32-character alphanumeric key uniquely identifying a wireless LAN.

Hide SSID

Enable this Hide SSID feature to improve the security of your WLAN.

Frequency

Choose you wireless radio channel or *auto Channel* by default.

Security Mode

We provide WEP / WPAPSK / WPA2PSK Encryption Protocols. WPAPSK / WPA2PSK is more secure than WEP.

WPA Algorithm

WPA Algorithm is the encryption algorithm of Security mode.

You can choose TKIP / AES / TKIP+AES encryption algorithm.

WEP / WPA Key

The WEP / WPA key is used for authentication.

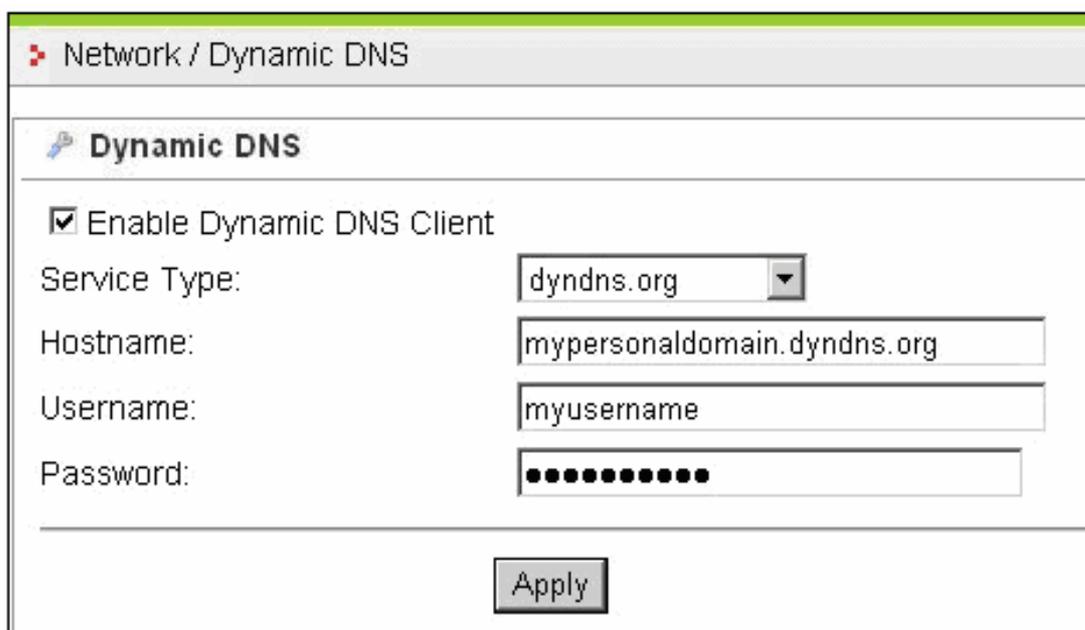
Click “**Apply**” to activate the wireless settings.

The screenshot shows the 'Network / Wireless' configuration page. At the top, there is a tab labeled 'Network / Wireless'. Below it, the 'Wireless' section is active. The 'Enable Wireless' checkbox is checked. The 'Network Mode' is set to '802.11 B/G/N mixed mode'. The 'SSID' is 'Default_SSID' with a note '1~32 characters'. The 'Hide SSID' is set to 'Disable'. The 'Frequency' is set to 'Auto Channel'. The 'Security Mode' is set to 'WEP'. The 'WEP Key' is represented by a series of dots, with a note '5 or 13 ascii characters / 10 or 26 hex numbers'. There is a 'Show Password' checkbox which is unchecked. At the bottom right of the configuration area, there is an 'Apply' button.

5.2.5. Network / Dynamic DNS

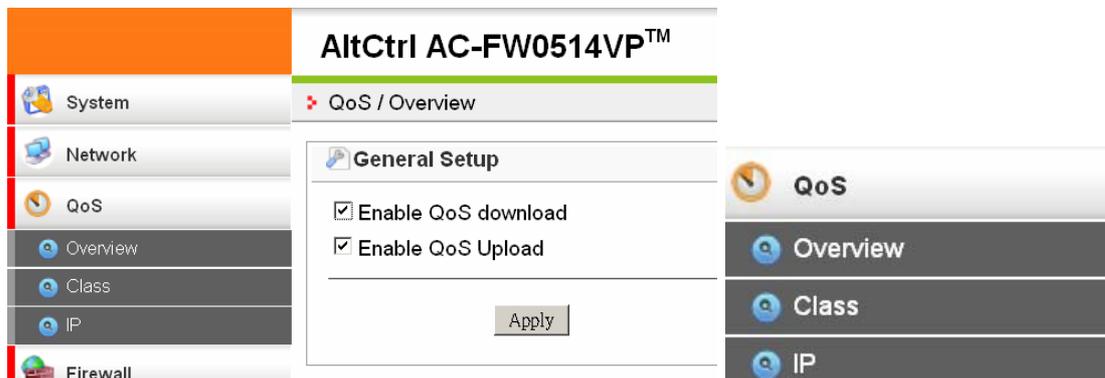
Dynamic DNS is a domain name service allowing aliasing of dynamic IP addresses to static hostnames.

If you have registered with a DDNS service provider, select the **“Enabled Dynamic DNS Client”** check box, and fill out hostname / username / password provided by DDNS service provider.



The screenshot shows a configuration window titled "Network / Dynamic DNS". Inside, there is a section for "Dynamic DNS" with a key icon. The "Enable Dynamic DNS Client" checkbox is checked. Below it, there are four input fields: "Service Type" (a dropdown menu showing "dyndns.org"), "Hostname" (text box with "mypersonaldomain.dyndns.org"), "Username" (text box with "myusername"), and "Password" (password field with 10 dots). An "Apply" button is located at the bottom center of the window.

5.3. QoS

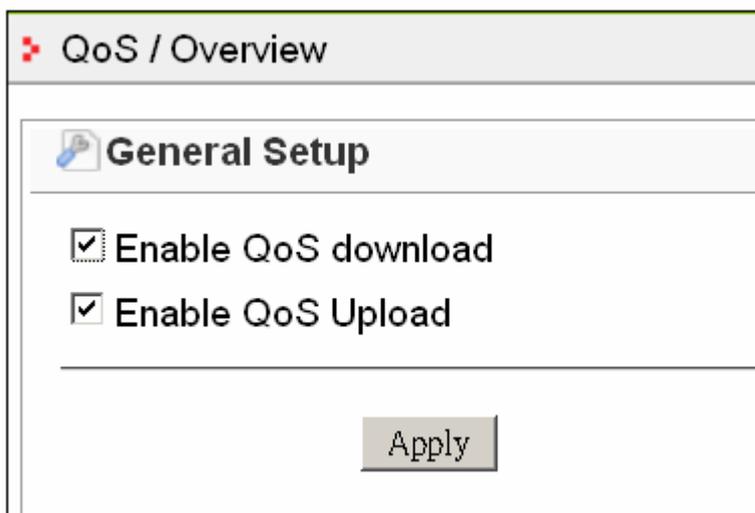


5.3.1. QoS / Overview

This page displays the overview of QoS function, please select the required function and click “**Apply**”.

Enable QoS download: Enable QoS download control function.
The default setting is OFF.

Enable QoS Upload: Enable QoS Upload control function.
The default setting is OFF.



5.3.2. QoS / Class

“**QoS Class**” can help you to set Max and Min Download / Upload Bandwidth Class.

Input the “**Class Name**”, “**Bandwidth Min**” and “**Bandwidth Max**” information and click “**Add**” to add Class List entry. Click “**Edit**” to change the selected Class Values and click “**Save**”. Click “**Remove**” to delete the selected Class.

The maximum Class is 5 Classes.

QoS / Class

QoS Download | QoS Upload

Class

Add Download class

Class Name: DL2
 Bandwidth Mini: 500 kbit/s
 Bandwidth Max: 800 kbit/s

Class list Maximum Number: 5

#	Class Name	Bandwidth Mini	Bandwidth Max	Edit	Remove
0	Default	Zero	Maximum		
1	DL1	100kbit/s	800kbit/s	Edit	Remove
2	DL2	500kbit/s	800kbit/s	Edit	Remove

Class list Maximum Number: 5

#	Class Name	Bandwidth Mini	Bandwidth Max	Edit	Remove
0	Default	Zero	Maximum		
1	DL1	100kbit/s	800kbit/s	Edit	Remove
2	DL2	500 kbit/s	800 kbit/s	Save	Remove

QoS / Class

QoS Download | **QoS Upload**

Class

Add Upload class

Class Name: UL2
 Bandwidth Mini: 300 kbit/s
 Bandwidth Max: 800 kbit/s

Class list Maximum Number: 5

#	Class Name	Bandwidth Mini	Bandwidth Max	Edit	Remove
0	Default	Zero	Maximum		
1	UL1	200kbit/s	400kbit/s	Edit	Remove
2	UL2	300kbit/s	800kbit/s	Edit	Remove

Class list Maximum Number: 5

#	Class Name	Bandwidth Mini	Bandwidth Max	Edit	Remove
0	Default	Zero	Maximum		
1	UL1	200 kbit/s	400 kbit/s	Save	Remove
2	UL2	300kbit/s	800kbit/s	Edit	Remove

5.3.3. QoS / IP (Classification Rule)

“**QoS IP (Classification Rule)**” can help you to set the QoS Download / Upload Bandwidth Classification Rule for certain IP Address.

Choose “**Download Service Class**” or “**Upload Service Class**” and input “**IP**” information, then click “**Add**” to add Classification Rule List entry. You can click “**Up**” or “**Down**” to change thr the selected rule priority. Click “**Remove**” to delete the selected Rule.

The maximum Classification Rule is 10 Rules for each Download and Upload.

QoS / IP

Classification Rule

Add Classification Rule

Download Service Class DL1 ▾

Upload Service Class UP1 ▾

IP 192.168.1.100 Add

Download Maximum Number: 10

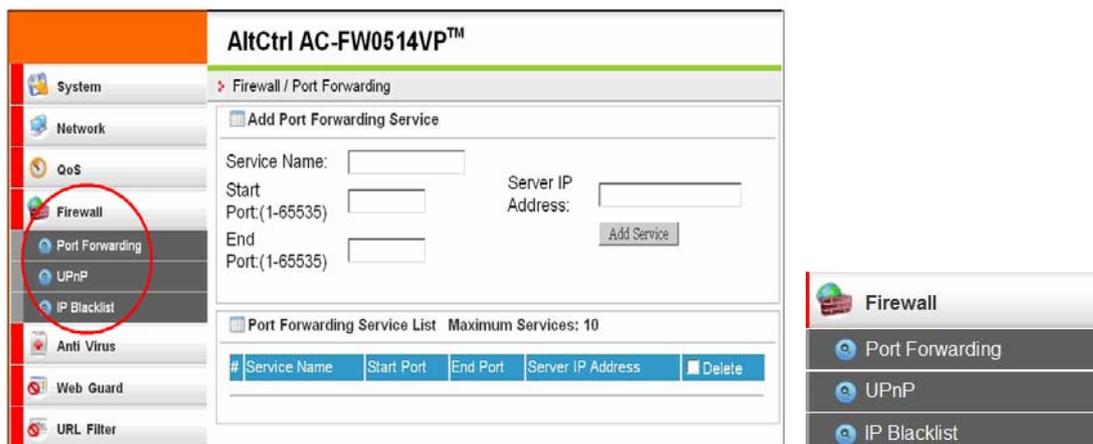
#	IP	Class	Priority	Remove
1	192.168.1.100	DL1	Up Down	Remove

Upload Maximum Number: 10

#	IP	Class	Priority	Remove
1	192.168.1.100	UP1	Up Down	Remove

5.4. Firewall

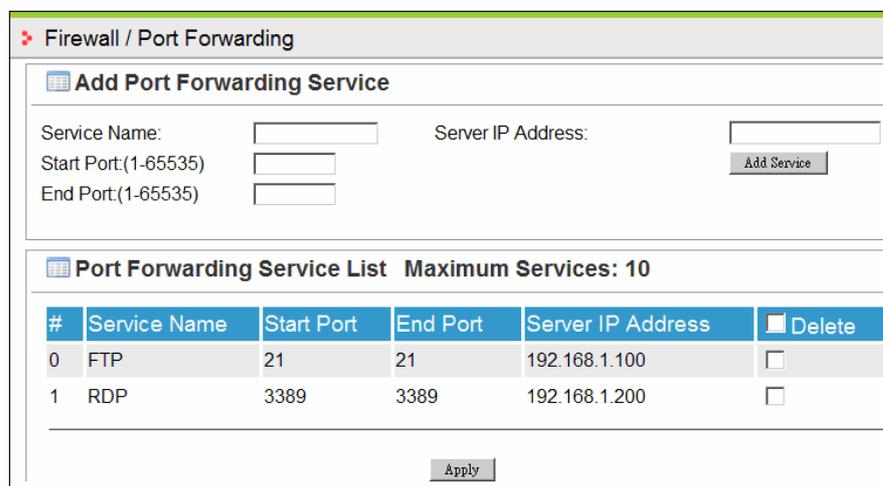
The firewall category provides three kinds of function, port forwarding, UPnP, and IP Blacklist.



5.4.1. Firewall / Port Forwarding

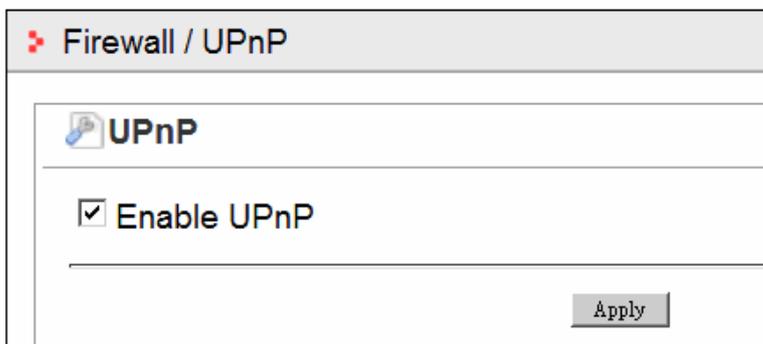
“**Port Forwarding**” can help you to access those servers which are behind the LAN port of AC-FW0514VP. But the function is only enabled automatically when the network is set as “**Router**” mode.

Input the port forwarding information and click “**Add Service**” to add Port Forwarding Service List entry. Click “**Delete**” to delete the selected services. The maximum port forwarding is 10 services.



5.4.2. Firewall / UPnP

UPnP can do automatically NAT traversal, enumerate existing port mappings, and adding and removing port mappings automatically. The function is enabled automatically when the network is set as “**Router**” mode.



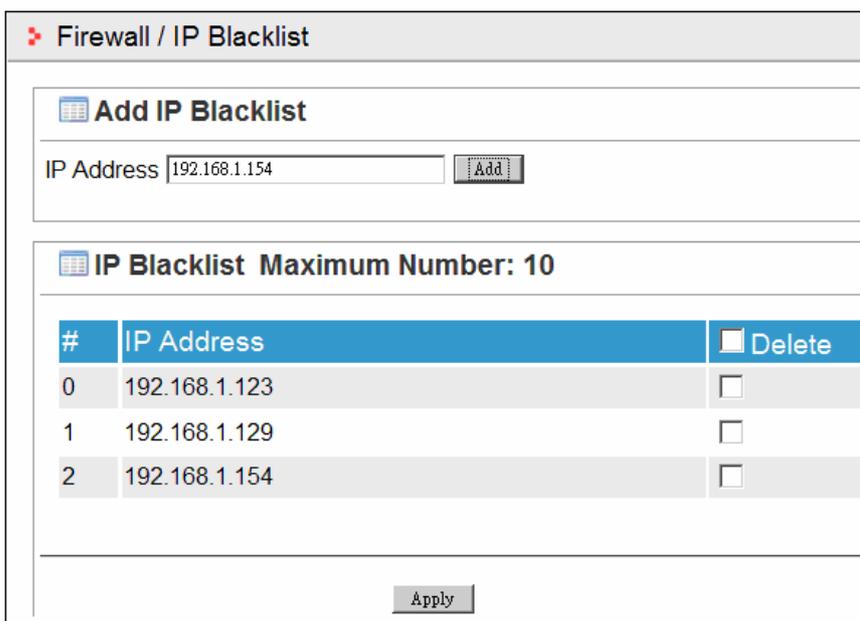
The screenshot shows a configuration window titled "Firewall / UPnP". Inside, there is a sub-section for "UPnP" with a checked checkbox labeled "Enable UPnP". An "Apply" button is located at the bottom right of the window.

5.4.3. Firewall / IP Blacklist

IP Blacklist can help you to deny access of some IP address.

Input IP address and click “**Add**” will add IP blacklist list entry. Tick Delete to delete the service.

The maximum number of blocked is 10 IP's.



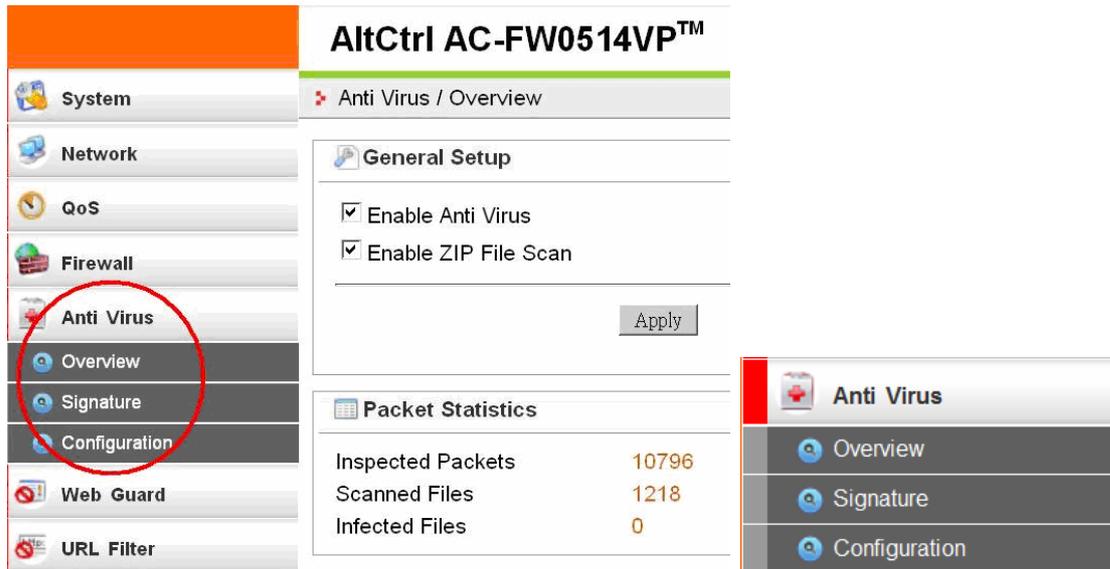
The screenshot shows a configuration window titled "Firewall / IP Blacklist". It features an "Add IP Blacklist" section with an input field for "IP Address" containing "192.168.1.154" and an "Add" button. Below this is a section titled "IP Blacklist Maximum Number: 10" containing a table with three columns: "#", "IP Address", and "Delete".

#	IP Address	Delete
0	192.168.1.123	<input type="checkbox"/>
1	192.168.1.129	<input type="checkbox"/>
2	192.168.1.154	<input type="checkbox"/>

An "Apply" button is located at the bottom of the window.

5.5. Anti-Virus

With virus protection, the Anti-Virus screen lets you to setup your category of virus and check the infected severity.



5.5.1. Anti-Virus / Overview

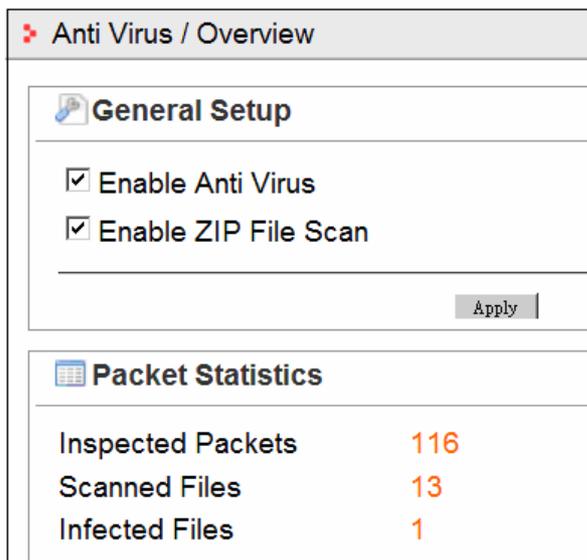
This page displays the overview of the Anti-Virus function, please select the required function and click “**Apply**”.

Enable Anti-Virus: Enable Anti-Virus function.

The default setting is ON.

Enable ZIP File Scan: Enable ZIP file (ZIP / RAR / GZ) scan function.

The default setting is ON.



5.5.2. Anti Virus / Signature

You can check AV signature list here.

Anti Virus / Signature				
Signature				
1/131 Next >>>				
ID	Name	Category	Outbreak	Severity
2053	EICAR-Test-File	Virus	N	Low
5000001	W32.W.Allaple	Virus	Y	High
5000005	Troj.GameThief.W32.Magania	Virus	Y	High
5000008	Troj.Spy.W32.VBStat	Spy	Y	High
5000014	W32.W.Runfer	Virus	Y	High
5000015	AdWare.W32.Agent	Virus	Y	High
5000016	W32.W.Bagle	Virus	Y	High
5000017	W32.W.Otwycal	Virus	Y	High

5.5.3. Anti Virus / Configuration

Setup the action of Anti Virus, which includes Log and Destroy file.

Log: Virus detection and record log in the system; you can check the log list at the **Log and Report / Anti Virus** page. The default setting is ON.

Destroy File: Enable or disable the infected file destroy function. If this function is on, the infected files by viruses will be destroyed when AC-FW0514VP detects them. If this function is OFF, then the destroy file function will not be administered.

The default setting is ON.

Click **“Restore”** to change the settings to factory default values.

Anti Virus / Configuration

Action Configuration

Protocol	Action	
	Log	Destroy Virus
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IMAP4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TCP STREAM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Category	Action	
	Log	Destroy Virus
Spy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virus	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Outbreak	Action	
	Log	Destroy Virus
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity	Action	
	Log	Destroy Virus
High	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Restore Anti Virus to factory defaults

Restore Anti Virus to factory defaults

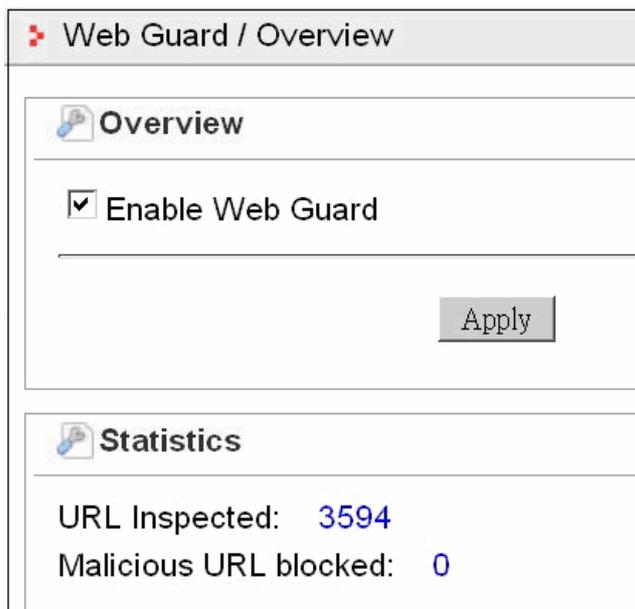
5.6. Web Guard

This screen lets you to enable Web Guard and overview the number of URL inspected and malicious URL blocked.



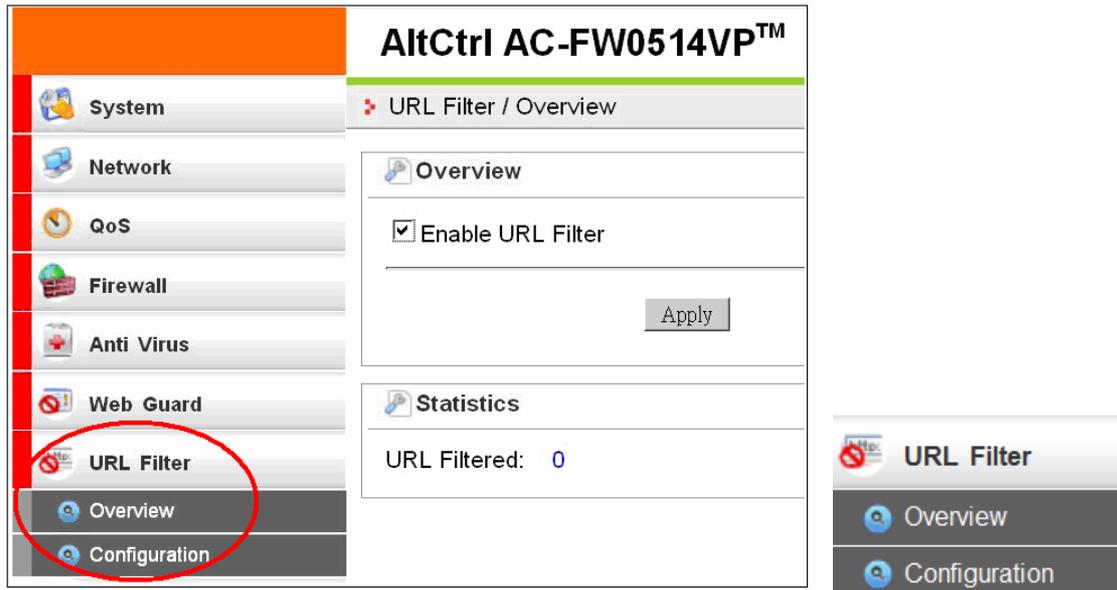
5.6.1. Web Guard / Overview

Enable or disable Web Guard and click “**Apply**”.



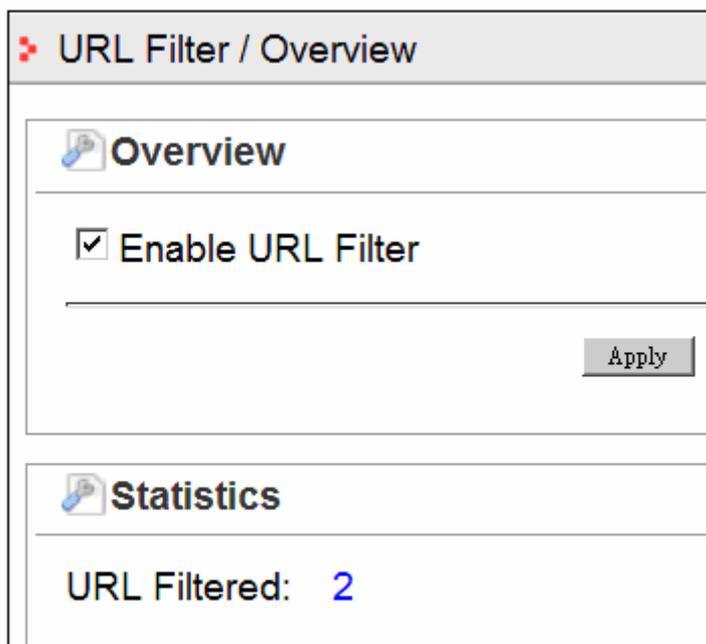
5.7. URL Filter

This screen lets you to enable URL Filter function and configure the rules of web control.



5.7.1. URL Filter / Overview

Enable or Disable URL Filter and click “**Apply**”.



5.7.2. URL Filter / Configuration

Enable or disable the categories to be blocked. You can select or deselect multiple categories and click **“Apply”** to change the configuration.

Click **“Select All”** will enable all categories. Click **“Unselect All”** will disable all categories.

✖ URL Filter / Configuration

 **Blocked Categories**

<input type="checkbox"/> Adult Content	<input type="checkbox"/> News
<input type="checkbox"/> Job Search	<input type="checkbox"/> Gambling
<input type="checkbox"/> Travel_Tourism	<input type="checkbox"/> Shopping
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Chatrooms
<input type="checkbox"/> Dating Sites	<input type="checkbox"/> Game Sites
<input type="checkbox"/> Investment Sites	<input type="checkbox"/> E_Banking
<input type="checkbox"/> Crime_Terrorism	<input type="checkbox"/> Personal_Beliefs_Cults
<input type="checkbox"/> Politics	<input type="checkbox"/> Sports
<input type="checkbox"/> www_Email_Sites	<input type="checkbox"/> Violence_Undesirable
<input type="checkbox"/> Malicious	<input type="checkbox"/> Search Sites
<input type="checkbox"/> Health Sites	<input type="checkbox"/> Clubs and Societies
<input type="checkbox"/> Music Downloads	<input type="checkbox"/> Business Oriented
<input type="checkbox"/> Government Blocking List	<input type="checkbox"/> Educational
<input type="checkbox"/> Advertising	<input type="checkbox"/> Drugs_Alcohol
<input type="checkbox"/> Computing_IT	<input type="checkbox"/> Swimsuit_Lingerie_Models
<input type="checkbox"/> Spam	<input type="checkbox"/> Virus

5.8. Signature Update

AltCtrl AC-FW0514VP™

- System
- Network
- QoS
- Firewall
- Anti Virus
- Web Guard
- URL Filter
- Signature Update
- Auto Update
- Manual Update
- Log and Report

Signature Update / Auto Update

Status

Auto Update Enabled Disable

Details

Last update check 2010/07/27 11:16

Update

Signature Version

AntiVirus	20100726-01	
Web Guard	20100726-01	

Network

Update Server http://acuptw1.altctrl.com.tw/aus/?q=kms/auth

Check Period 6 hours Apply

HTTP Proxy Disable Enable

Apply

Signature Update

Auto Update

Manual Update

49

5.8.1. Signature Update / Auto Update

This page shows auto update information.

Click **“Enable / Disable”** to Enable / Disable the Auto Updates.
 Click **“Update”** to update signature automatically and view the signature update status.

Select the **“Check Period”** stroll for the auto update signature time period, and click **“Apply”** to validate the setting.

Select the **“Enable”** radio button to and input the proxy server to text field then click **“Apply”** to enable HTTP Proxy setting.

 Signature Update / Auto Update

 Status

Auto Update	Enabled	<input type="button" value="Disable"/>
--------------------	----------------	--

 Details

Last update check	2000/01/01 11:16	<input type="button" value="Update"/>
Signature Version	AntiVirus	20100903-00
	Web Guard	20100903-00

 Network

Update Server	http://acuptw1.altctrl.com.tw/aus/?q=kms/auth	
Check Period	<input type="text" value="6 hours"/> <input type="button" value="Apply"/>	
HTTP Proxy	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input style="width: 200px;" type="text"/> <input type="button" value="Apply"/>

 License

Serial Number	
----------------------	--

5.8.2. Signature Update / Manual Update

Besides auto update method, AC-FW0514VP also supports manually signature update. By assigning and browsing local signature file and then click “**Apply**”, you can update new signature by yourself.

Signature Update / Manual Update

 **Upload Signature**

Signature File:

 **Details**

Signature Version

AntiVirus	20100507-01
Web Guard	20100507-01

5.9. Log and Report

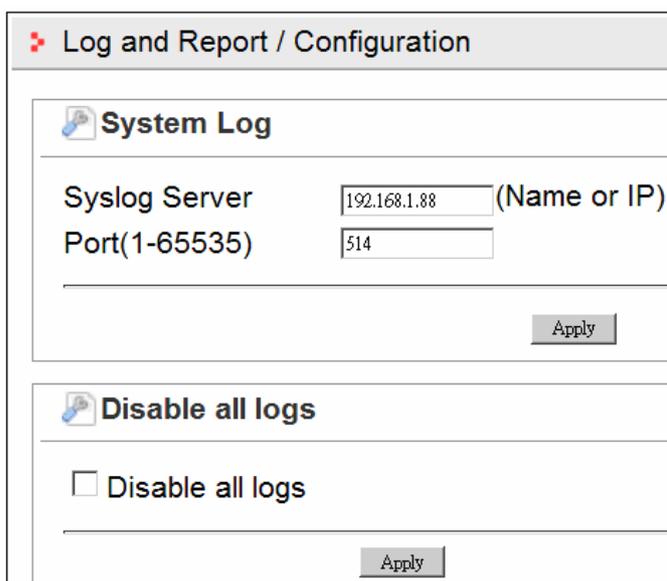


5.9.1. Logs and Report / Configuration

In this page, you can fill in a server name or IP address with network port information of system log server so that all system logs will be passed to the assigned server(Default syslog port: 514).

Click **“Apply”** to validate the setting.

Tick the **“Disable all logs”** and then validate by **“Apply”** bottom to bypass the transmission of system logs to syslog server.



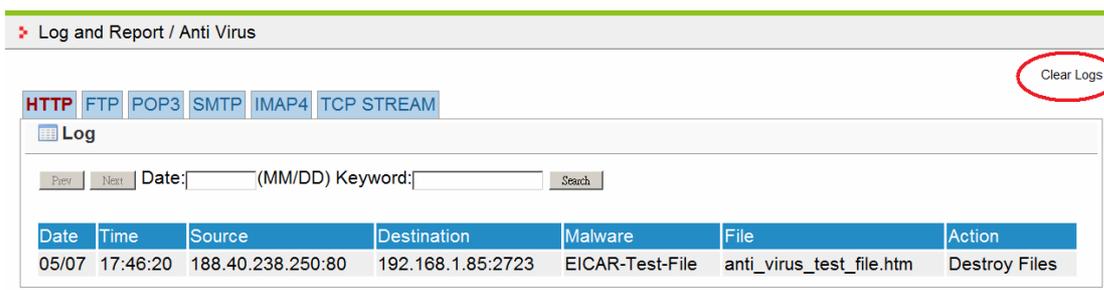
5.9.2. Logs and Report / Anti-Virus

Anti-Virus Log records are distinguished into different protocols and listed. Please check **HTTP / FTP / SMTP / POP3 / IMAP4 / TCP STREAM** pages for each single protocol.

Enter Date information (Format: MM/DD, i.e: 09/30) or keyword and then click “**Search**” to view the logs.

Click the “**Prev / Next**” button to view the previous / next page of log records when the logs get more than one page.

Click the “**Clear Logs**” to erase log data.



The screenshot shows the 'Log and Report / Anti Virus' interface. At the top right, there is a 'Clear Logs' button circled in red. Below it, there are tabs for different protocols: HTTP, FTP, POP3, SMTP, IMAP4, and TCP STREAM. Under the 'Log' section, there are 'Prev' and 'Next' buttons, a 'Date:' field with '(MM/DD)' format, a 'Keyword:' field, and a 'Search' button. Below the search fields is a table with the following data:

Date	Time	Source	Destination	Malware	File	Action
05/07	17:46:20	188.40.238.250:80	192.168.1.85:2723	EICAR-Test-File	anti_virus_test_file.htm	Destroy Files

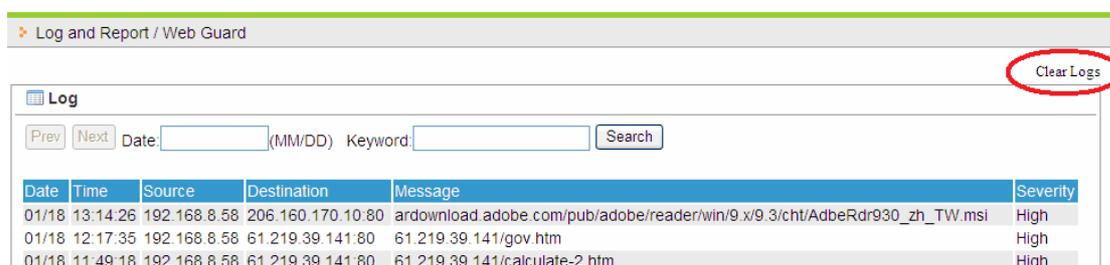
5.9.3. Logs and Report / Web Guard

This page shows the log records of Web Guard function.

Enter Date information (Format: MM/DD, i.e: 09/30) or keyword and then click “**Search**” to view the logs.

Click the “**Prev / Next**” button to view the previous / next page of log records when the logs get more than one page.

Click the “**Clear Logs**” to erase log data.



Log and Report / Web Guard

Clear Logs

Log

Prev Next Date: (MM/DD) Keyword: Search

Date	Time	Source	Destination	Message	Severity
01/18	13:14:26	192.168.8.58	206.160.170.10:80	ardownload.adobe.com/pub/adobe/reader/win/9.x/9.3/cht/AdobeRdr930_zh_TW.msi	High
01/18	12:17:35	192.168.8.58	61.219.39.141:80	61.219.39.141/gov.htm	High
01/18	11:49:18	192.168.8.58	61.219.39.141:80	61.219.39.141/calculate-2.htm	High

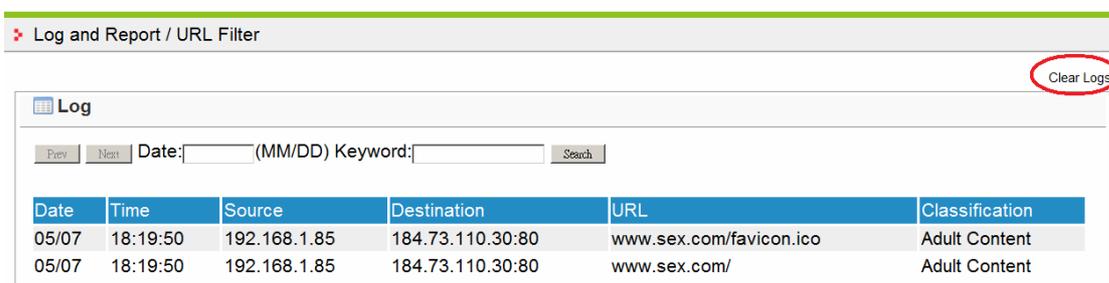
5.9.4. Logs and Report / URL Filter

This page shows the log records of URL Filter function.

Enter Date information (Format: MM/DD, i.e: 09/30) or keyword and then click **“Search”** to view the logs.

Click the **“Prev / Next”** button to view the previous / next page of log records when the logs get more than one page.

Click the **“Clear Logs”** to erase log data.



Log and Report / URL Filter

Clear Logs

Log

Prev Next Date: (MM/DD) Keyword: Search

Date	Time	Source	Destination	URL	Classification
05/07	18:19:50	192.168.1.85	184.73.110.30:80	www.sex.com/favicon.ico	Adult Content
05/07	18:19:50	192.168.1.85	184.73.110.30:80	www.sex.com/	Adult Content

5.9.5. Logs and Report / IP Blacklist

This page shows the log records of IP Blacklist function.

Enter Date information (Format: MM/DD, i.e: 09/30) or keyword and then click “**Search**” to view the logs.

Click the “**Prev / Next**” button to view the previous / next page of log records when the logs get more than one page.

Click the “**Clear Logs**” to erase log data.

Log and Report / IP Blacklist

Clear Logs

Log

Prev Next Date: (MM/DD) Keyword: Search

Date	Time	Source	Destination	Drop
------	------	--------	-------------	------

6. Troubleshooting

Problem	Corrective Action
None of the LEDs turn on when you turn on the AC-FW0514VP	<ul style="list-style-type: none"> ❖ Make sure the connection of power adaptor to the AC-FW0514VP, and plug the power lead to an appropriate power source. Check all the cable connections. ❖ If LED's still do not turn on, you may have a hardware problem. In this case, please contact with vendor for product service.
Cannot access the AC-FW0514VP from LAN	<ul style="list-style-type: none"> ❖ Check the cable connection between the AC-FW0514VP and your computer. ❖ Ping the AC-FW0514VP (192.168.1.1) from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly.
Cannot access the internet	<ul style="list-style-type: none"> ❖ Check the AC-FW0514VP's connection to the broadband devices such as ADSL / cable modem / Router device. ❖ Check WAN to verify setting.

FCC

Interference Statement:

This device complies with Part 15 of FCC rules.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.**
- (2) This device must accept any interference received, including interference that may cause undesired operations.**

FCC Warning!

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.