WLR-6001

Wireless Gigabit VPN Router N750 X6

(802.11a/b/g/n)

User Manual

TABLE OF CONTENTS

1 KEY FEATURES 5

2 PACKAGE CONTENTS 6

3 CAUTIONS 7

4 PRODUCT LAYOUT 8

5 NETWORK + SYSTEM REQUIREMENTS 11

6 WLR-6001 PLACEMENT 11

7 SETUP LAN, WAN 12

8 PC NETWORK ADAPTER SETUP 13

9 BRING UP THE WLR-6001 17

10 INITIAL SETUP WLR-6001 17

11 CONFIGURATION WIZARD 26

11.1 Connecting to an external VPN service 27

12 WIRELESS SETTINGS 31

13 FIREWALL SETTINGS 42

14 ADVANCED SETTINGS 48

15 VPN 58

16 TOOLBOX SETTINGS 107

17 ADDENDUM: USB PORT CONTROL CENTER 119

Revision 1.1
© Sitecom Europe BV 2012

Note: All the information contained in this manual was correct at the time of publication.
However, as our engineers are always updating and improving the product, your device’s software may have a slightly different appearance or modified functionality than presented in this manual.

Introduction

Congratulations on your purchase of the Wireless Gigabit VPN Router N750 X6. The WLR-6001 is compliant with 802.11a and 802.11n and up to 6 times faster than standard 802.11g based routers while still being compatible with 802.11g & 802.11b devices. The WLR-6001 is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Gigabit switch that connects your wired-Ethernet devices together at 10/100/1000 Mbps speeds.

At 300/450 Mbps wireless transmission rate, the Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel, giving you seamless access to multimedia content. The robust RF signal travels farther, eliminates dead spots and extends the network range. For data protection and privacy, the WLR-6001 encodes all wireless transmissions with WEP, WPA, or WPA2 encryption.

With the built-in DHCP Server & powerful SPI firewall, the WLR-6001 protects your computers against intruders and most known Internet attacks and also provides safe VPN pass-through. With the incredible speed and QoS function of 802.11n the WLR-6001 is ideal for media-centric applications like streaming video, gaming, and VoIP telephony to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

With Sitecom Cloud Security, Sitecom goes one step further and ensures that you can surf the Internet even more safely, not only on your PC, but on all the devices in your home which you use to access the Internet. All the Internet devices in your home are protected against the dangers of Internet criminality.

You can use the WLR-6001 as a VPN client to access an external VPN server or you can configure the router as a VPN server to be able to access your home network from any location using the Internet. With VPN technology you always make use of a highly secured and encrypted VPN tunnel.

1 Key Features

Features	Advantages
Incredible Data Rate up to 450Mbps*	**Heavy data payloads such as MPEG video streaming**
IEEE 802.11n Compliant and backwards compatible with 802.11b/g	**Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices with legacy protection**
Four 10/100/1000 Mbps gigabit Switch Ports (Auto-Crossover)	**Scalability, extend your network.**
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	**Avoids the attacks of Hackers or Viruses from Internet**
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	**Provide mutual authentication (Client and dynamic encryption keys to enhance security**
WDS (Wireless Distribution System)	**Make wireless AP and Bridge mode simultaneously as a wireless repeater**
Sitecom Cloud Security	**Protect your home against cybercrime while browsing.**

** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. The WLR-6001 Router
2. A 100V~240V to 12V 1.25A Switching Power Adapter
3. A Quick Install Guide
4. A CD (with User Manual)
5. A Warranty card
6. An UTP cable

3 Cautions

This router's design and manufacturer has your safety in mind. In order to safely and effectively use this router, please read the following before usage.

3.1 Usage Cautions

The user should not modify this router. The environmental temperature should be within +5 ~ +35 degrees Celsius.

3.2 Power

The router's power voltage is DC 12V 1.25A.
When using this router, please connect the supplied AC adapter or AC adapter cable to the router's power jack. When placing the adapter cable, make sure it can not get damaged or be subject to pressure. To reduce the risk of electric shock, unplug the adapter first before cleaning it. Never connect the adapter to the router in a humid or dusty area. Do not replace the adapter or cable's wire or connector.

3.3 Repair

If the router has a problem, you should take it to an appointed repair centre and let the specialists do the repair. Never repair the router yourself, you might damage the router or endanger yourself.

3.4 Disposing of the Router

When you dispose of the router, be sure to dispose it appropriately. Some countries may regulate disposal of an electrical device, please consult with your local authority.

3.5 Others

When using this router, please do not let it come into contact with water or other liquids. If water is accidentally spilled on the router, please use a dry cloth to absorb the spillage. Electronic products are vulnerable, when using please avoid shaking or hitting the router, and do not press the buttons too hard.

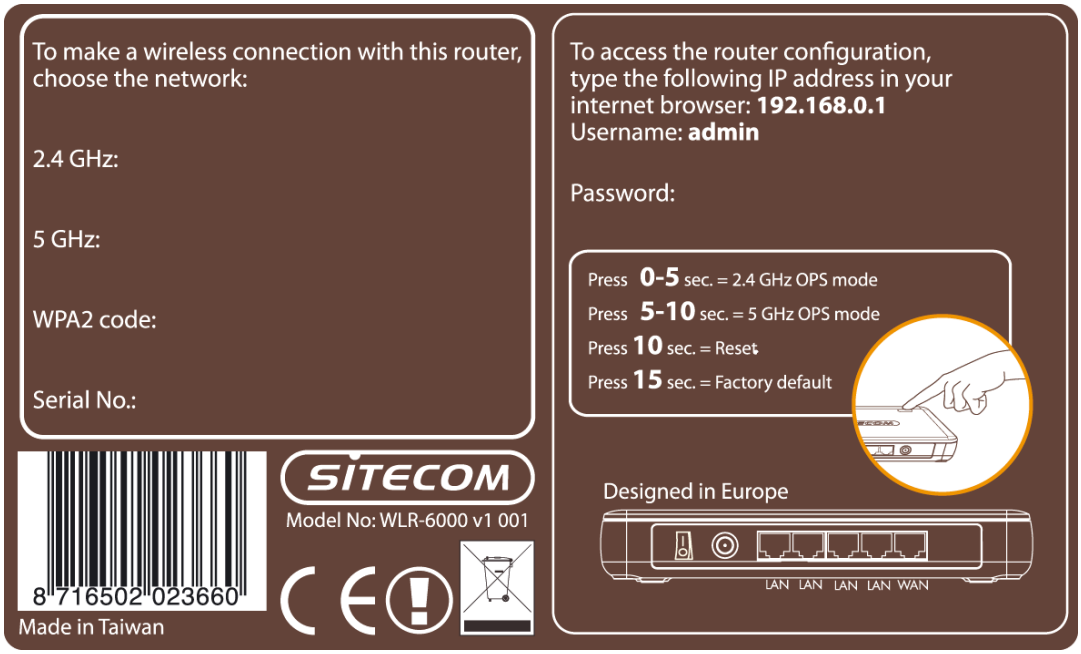
- Do not let the router come into contact with water or other liquid.
- Do not disassemble the router, repair the router or change the design of the router, any damage done will not be included in the repair policy.
- Avoid hitting the router with a hard object, avoid shaking the router and stay away from magnetic fields.
- If during electrostatic discharge or a strong electromagnetic field the product will malfunction, unplug the power cable. The product will return to normal performance the next time it is powered on.

4 Product Layout

Port	Description
Power connector	Connect the 12V DC adapter to this port
LAN (Yellow)	Connect your PC's or network devices to this port
WAN (Blue)	Connect your ADSL/Cable modem to this port
USB	Connect your Printer or Storage device to this port

Backlabel

The backlabel describes the IP address, login details, SSID, security code and WPS button functionality.



Button	Description
WPS BUTTON	Press 0-5 seconds for 2.4 GHz WPS mode Press 5-10 seconds for 5 GHz WPS mode Press 10 seconds to reset the router Press 15 Seconds to reset the router to factory defaults.

LED Definition

From left to right.

Port	Description
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
WAN (Blue)	Shows the cable is connected.
WiFi (White)	Shows 5GHz WiFi activity.
WiFi (Blue)	Shows 2.4GHz WiFi activity.
Power (Red)	Shows the device is turned on.
OPS (White)	Shows OPS activity.

5 Network + System Requirements

To begin using the WLR-6001, make sure you meet the following as minimum requirements:

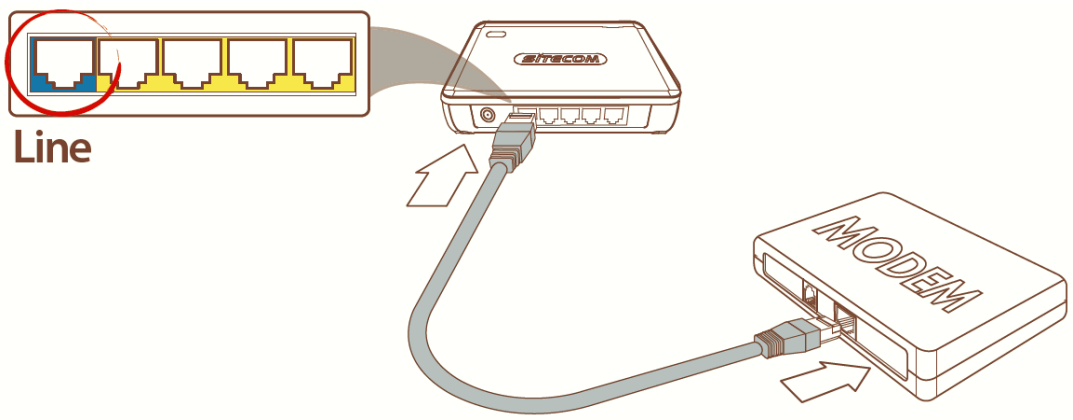
- PC/Notebook.
- Operating System – Microsoft Windows XP/2000/VISTA/7
- 1 Free Ethernet port.
- WiFi card/USB dongle (802.11 b/g/n) – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5e cables.

6 WLR-6001 Placement

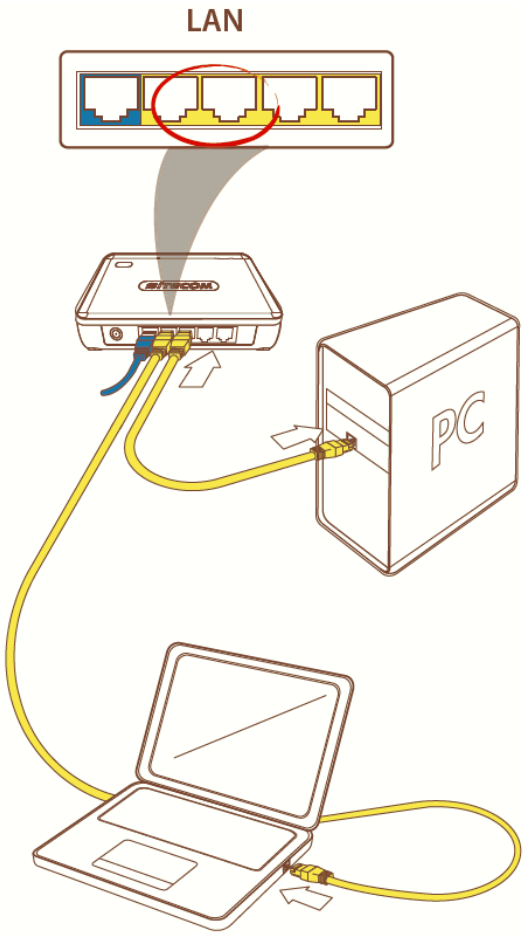
You can place the WLR-6001 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Router in the center of your home (or your office) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem.

7 Setup LAN, WAN

WAN connection:



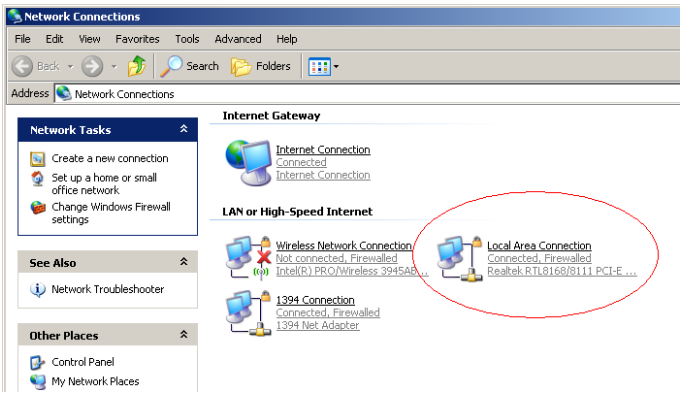
LAN connection:



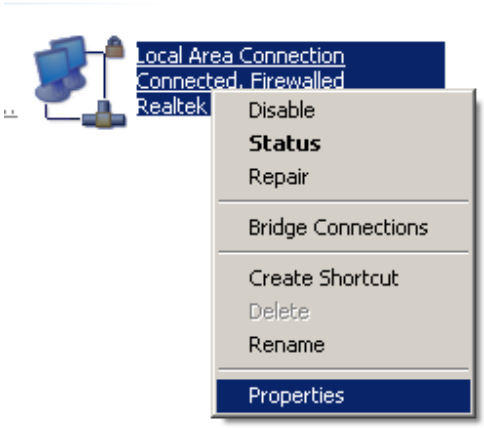
8 PC Network Adapter setup

Windows XP

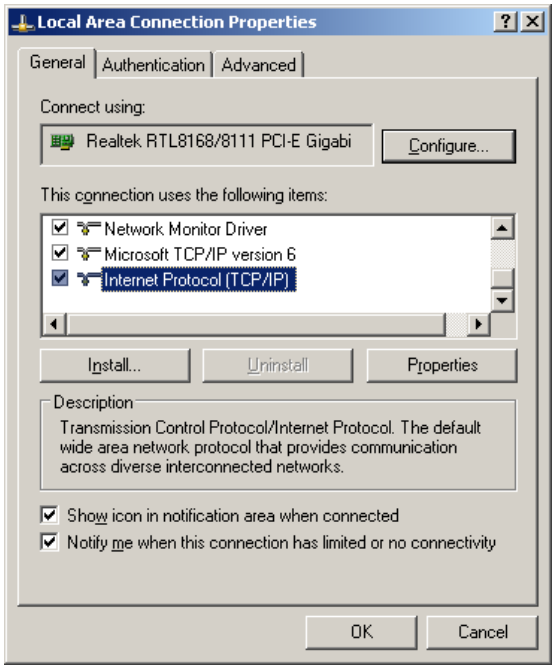
- Enter [Start Menu] → select [Control panel] → select [Network].

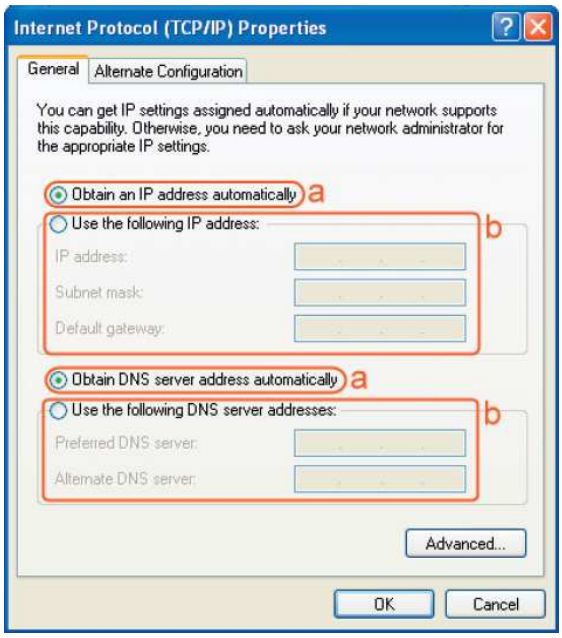


- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol (TCP/IP)] =>Click [Properties].



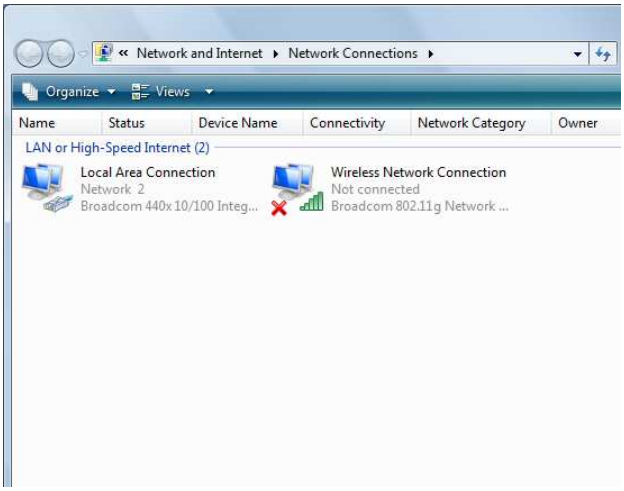


- Select the [General] tab.

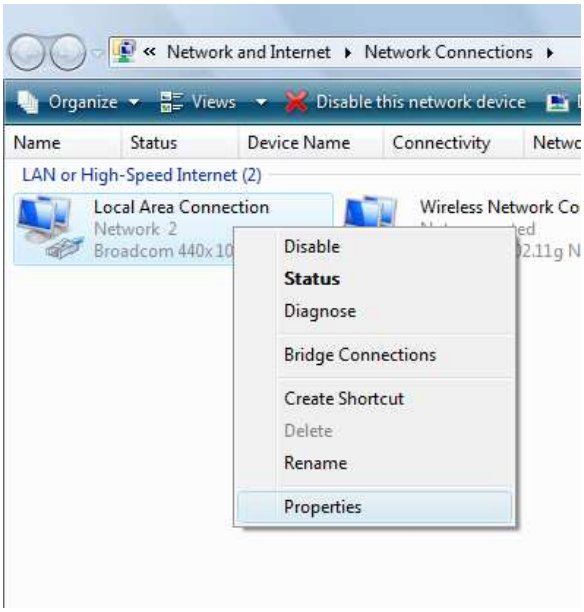
  The WLR-6001 supports a [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

Windows Vista/Seven

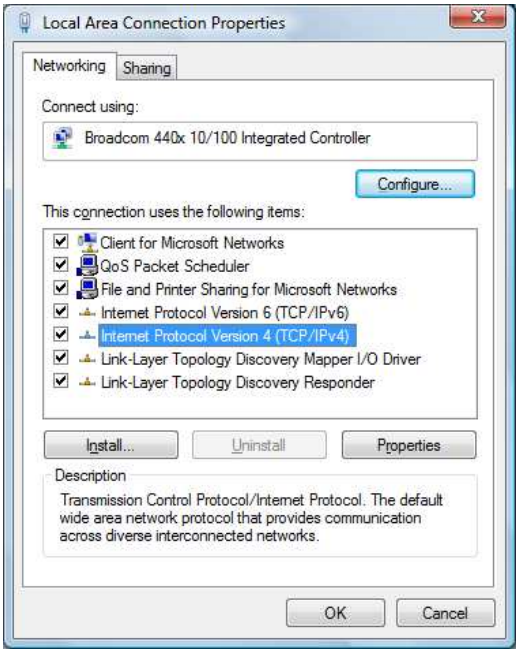
- Enter [Start Menu] → select [Control panel] → select [View network status and tasks] -> select [Manage network connections].

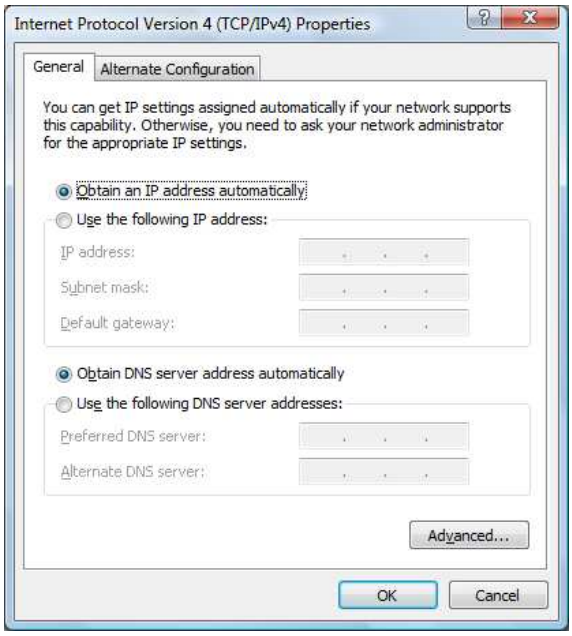


- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol Version 4 (TCP/IPv4)] =>Click [Properties].





- Select the [General] tab.

The WLR-6001 supports a [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

9 Bring up the WLR-6001

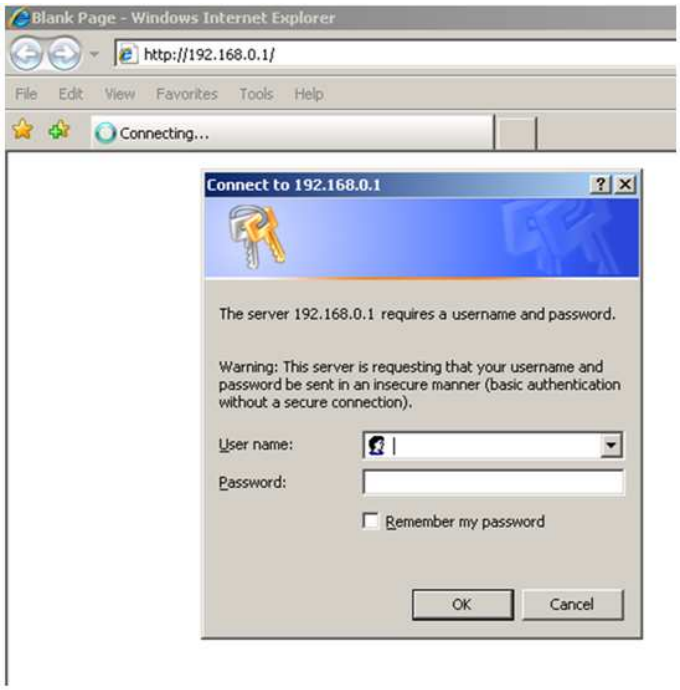
Connect the supplied power-adapter to the power inlet port and connect it to a wall outlet. Switch the WLR-6001 on by flipping the switch on the back of the device. The WLR-6001 automatically enters the self-test phase. During self-test phase, the Power LED will be lit continuously to indicate that this product is in normal operation.

10 Initial Setup WLR-6001

LOGIN procedure

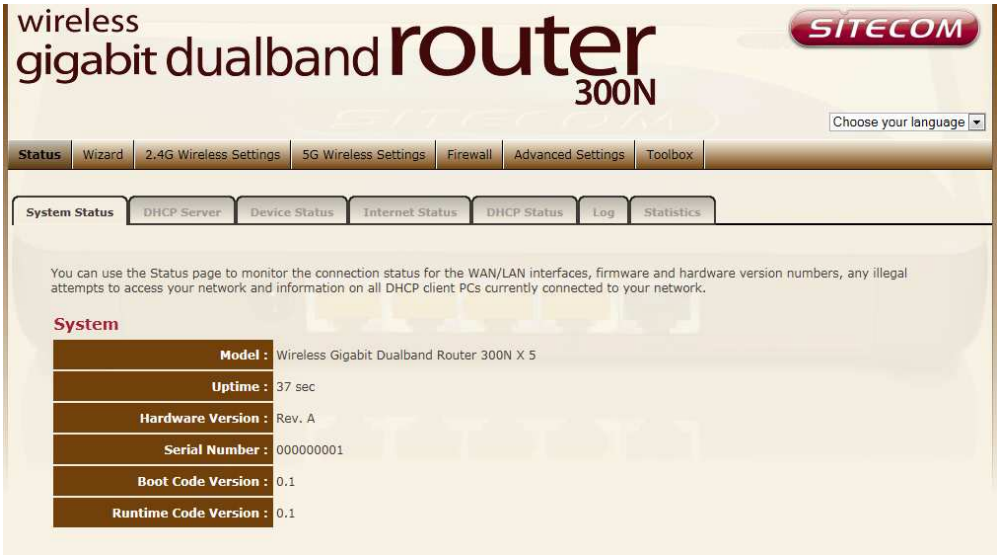
1. OPEN your browser (e.g. Internet Explorer).

2. Type http://192.168.0.1 in the address bar and press [Enter]



3. Type user name and password. The default username is admin, the password can be found on the back label on the bottom of your router.

4. Click **OK**.
5. You will see the home page of the WLR-6001.



The System status section allows you to monitor the current status of your router, the UP time, hardware information, serial number as well as firmware version information is displayed here.

LAN settings

The LAN tab gives you the opportunity to change the IP settings of the WLR-6001.

Click **<Apply>** at the bottom of this screen to save any changes.

IP address 192.168.0.1. It is the router's LAN IP address (Your LAN clients default gateway IP address).

IP Subnet Mask 255.255.255.0 Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree is Disabled by default. If the 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server Enabled by default. You can enable or disable the DHCP server. When DHCP is disabled no ip-addresses are assigned to clients and you have to use static ip-addresses. When DHCP server is enabled your computers will be assigned an ip-address automatically until the lease time expires.

Lease Time Forever. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.

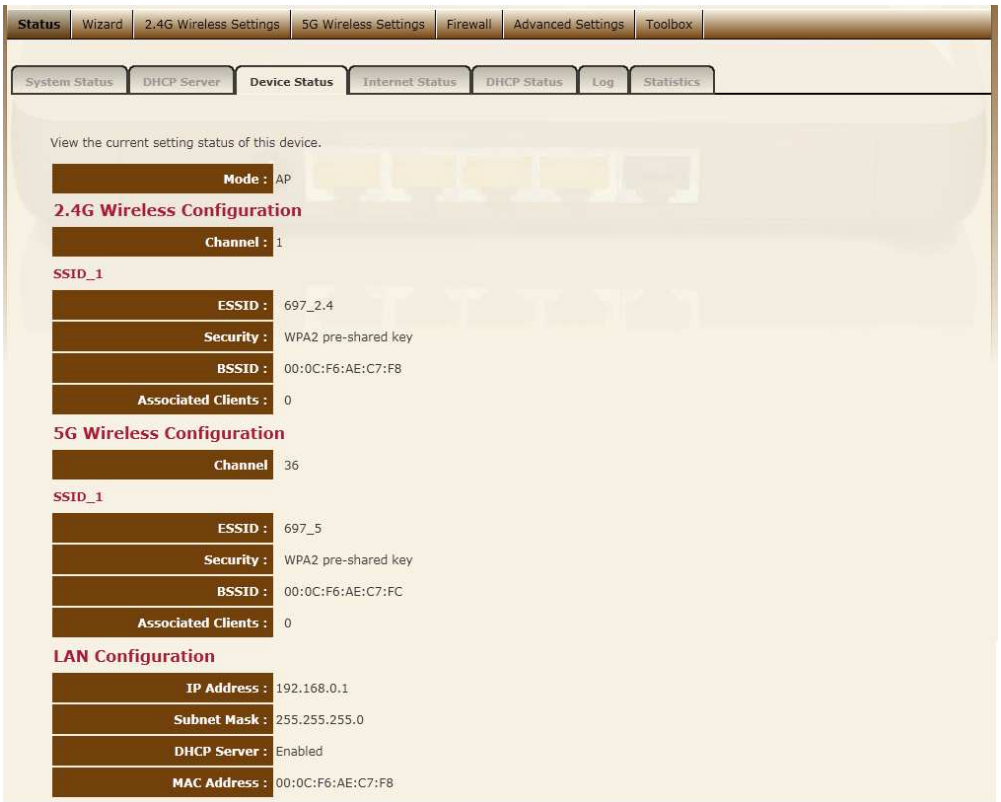
IP Address Pool You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.

***Note**: default IP range is 192.168.0.100 ~ 192.168.0.200. If you want your PC(s) to have a static/fixed IP address, then you'll have to choose an IP address outside this IP address Pool*

Domain Name You can specify a Domain Name for your LAN. Or just keep the default (sitecomwlr6001).

Device Status

View the Broadband router's current configuration settings. Device Status displays the configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section.



Internet Status

This page displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press **Renew** button to renew your WAN IP address.

DHCP Client Status

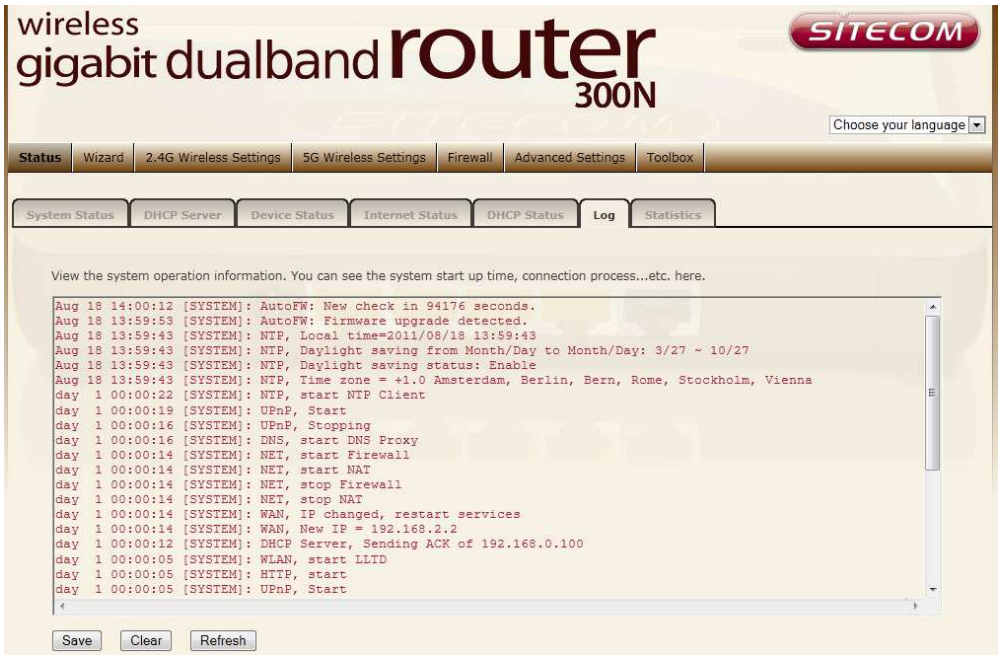
DHCP This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the Refresh button to update the available information.

You can check **Enable Static DHCP IP**. It is possible to add more static DHCP IPs. They are listed in the table **Current Static DHCP Table**. IP can be deleted at will from the table.

Click the **Apply** button to save the changed configuration.

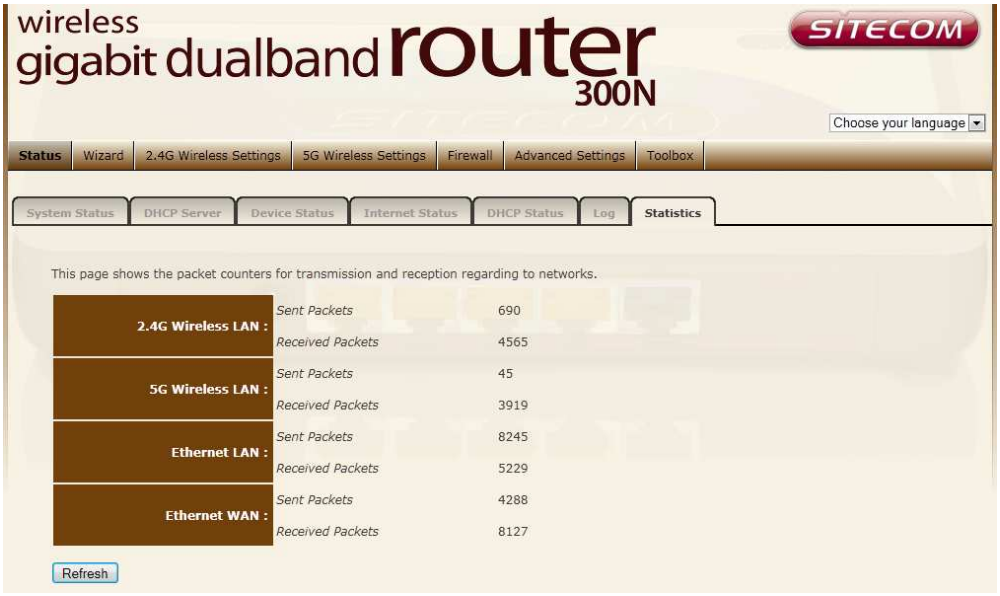
WLR-6001 Log

View the operation log of the WLR-6001. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.



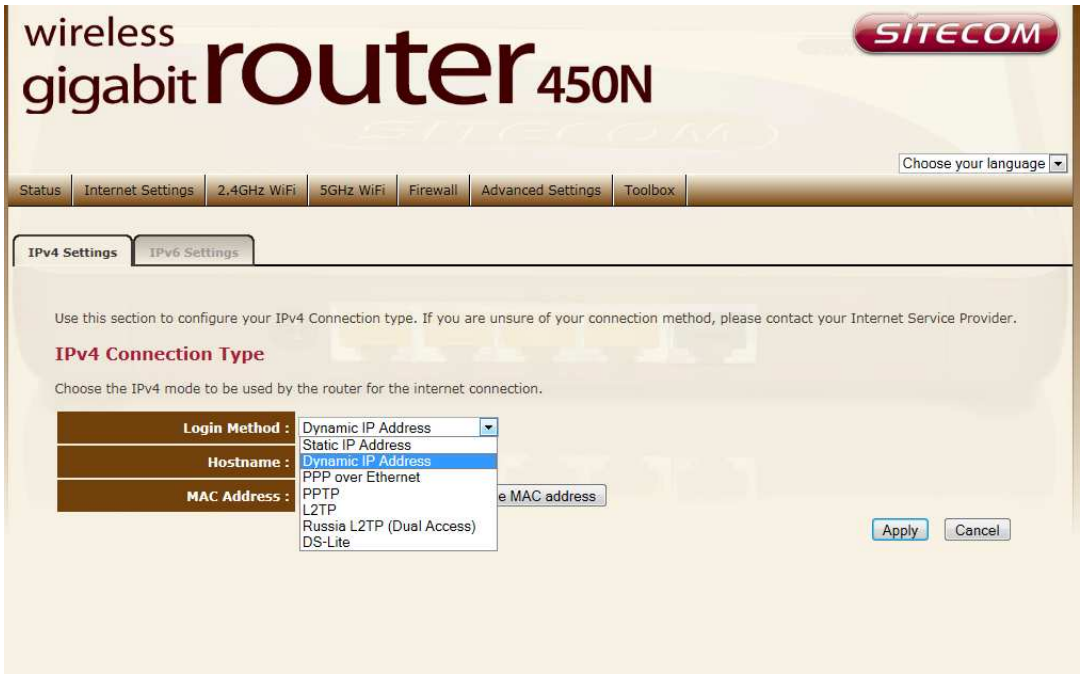
WLR-6001 Statistics

Shows the counters of packets sent and received on WAN, LAN & WLAN.



11 Configuration Wizard

Click **Internet Settings** to configure the router. Here you can choose your internet connection type.



Depending on the chosen setting, you may need to enter your user name and password, MAC address or hostname in the following window. After you have entered the correct information, click **Apply** to save the settings.

11.1 Connecting to an external VPN service

This section explains how to connect the WLR-6001 to an external VPN service by making use of the supported protocols **PPTP**, and **L2TP+IPSec**. If you want to set up the WLR-6001 as a VPN server, you should go to Section 15 "WLR-6001 as a VPN server"**.**

In order to properly connect to an external VPN service you must first make sure that your WLR-6001 is connected to the Internet. The Internet connection can be configured as either "Dynamic IP Address" or "PPP over Ethernet". Once you are successfully connected to the Internet with either of these two methods you may continue with the set-up of the VPN connection.

Once you are sure the WLR-6001 has Internet connectivity, please follow the following steps:

1. First of all, make sure you are connected to the WLR-6001. It does not matter if you are connected either wirelessly or via a cable connected to one of the LAN ports (yellow ports) of the device.
2. Open your web browser and type in the address bar the LAN IP address of the device. Note: the default value for the LAN IP is "192.168.0.1"
3. Click on the Tab called "Internet Settings" where you can see your current Internet configuration.
4. Click on "Login Method". This action will display a small menu containing the different connectivity options, as you can see in the following image:

This is a configuration example, where the default configuration for the Internet connection is Dynamic IP Address, but you may also have PPP over Ethernet established as default.

5. At this point you must choose the type of VPN connection you want to set-up. Depending on the VPN service you want to connect to, choose out of:

   5a. Connect to a **PPTP** service.

   Click on the "PPTP" option in the menu. You should see the following page:

Although most of the VPN servers will give you an IP address dynamically, some VPN servers must be configured statically. If you want to configure your IP address dynamically, please skip this step. If you want to configure the VPN statically, click on "Use the following IP address". Next, fill in the information provided from your VPN service regarding:

1. *IP address.* This is the IP address that the VPN service has assigned to you.
2. *Subnet mask*. If you are configuring your IP address statically, your VPN service should have provided you with a subnet mask value along with your IP address.
3. *Default Gateway***.** If connected statically, this value is also provided from your VPN service to route packets properly to the VPN server.

   Fill in the Login information to connect to the VPN service. VPN servers use this information for user authentication. Please fill in the following information:

4. *Username* and *Password*. This information must have been provided from your VPN service provided.
5. *PPTP Gateway***.** This value corresponds to either the **domain name** or **public IP address** of the VPN server you are trying to connect to. It must have been also provided from your VPN service provider.

   Click on "Apply". Now your router will save the new configuration, and it will restart with the new configuration, trying to connect to the VPN server.

5b. Connect to a **L2TP + IPSec** service.

Click on the "L2TP IPSec" option in the menu. You should see the following page:

Although most of the VPN servers will give you an IP address dynamically, some VPN servers must be configured statically. If you want to configure your IP address dynamically, please skip this step. If you want to

configure the VPN statically, click on "Use the following IP address". Next, fill in the information provided from your VPN service regarding:

1. *IP address.* This is the IP address that the VPN service has assigned to you.
2. *Subnet mask*. If you are configuring your IP address statically, your VPN service should have provided you with a subnet mask value along with your IP address.
3. *Default Gateway**.*** If connected statically, this value is also provided from your VPN service to route packets properly to the VPN server.

Fill in the Login information to connect to the VPN service. VPN servers use this information for user authentication. Please fill in the following information:

4. *Username, Password*, and *Shared Key*. This information must have been provided from your VPN service provider.

5. *PPTP Gateway**.*** This value corresponds to either the **domain name** or **public IP address** of the VPN server you are trying to connect to. It must have been also provided from your VPN service provider.

Click on "Apply". Now your router will save the new configuration, and it will restart with the new configuration, trying to connect to the VPN server.

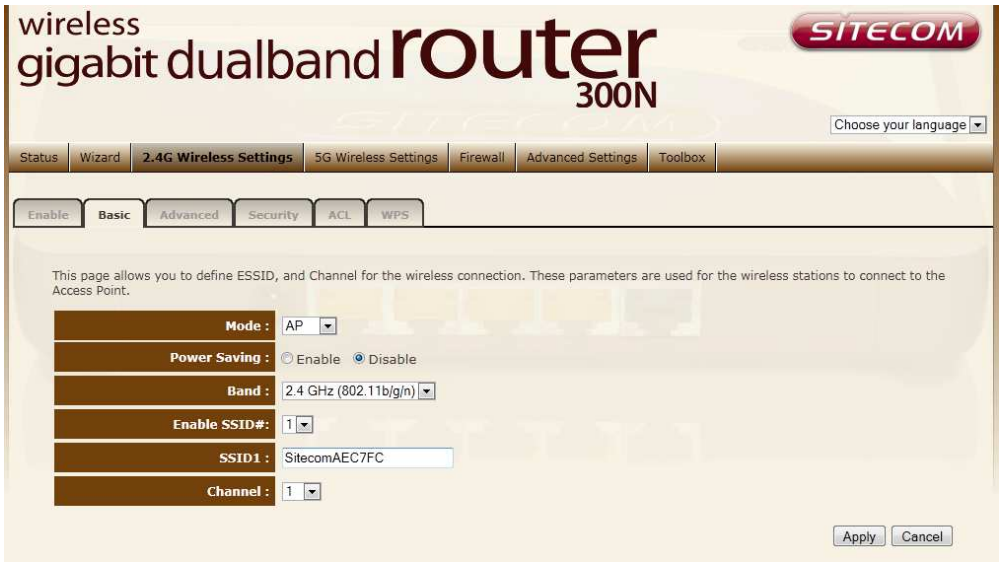
12 Wireless Settings

You can set parameters that are used for the wireless stations to connect to this router for the **2.4Ghz** radio or **5Ghz** radio. The parameters include Mode, ESSID, Channel Number and Associated Client.

Wireless Function

Enable or Disable Wireless function here. Click **Apply** and wait for module to be ready & loaded.

Basic Settings



Mode Allows you to set the AP to AP, Station, Bridge or WDS mode.

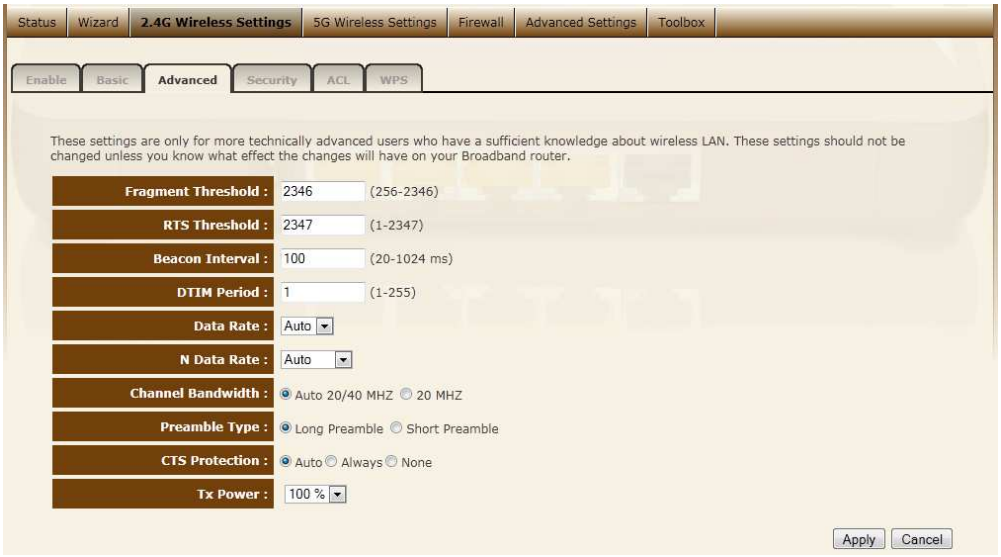
Band Allows you to set the AP fixed at 802.11b or 802.11g mode. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time. For the 5GHz mode you can set 802.11a, 802.11n or 802.11a/n mode.

ESSID This is the name of the wireless signal which is broadcasted. All the devices in the same wireless LAN should have the same ESSID.

Channel The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Advanced Settings

This tab allows you to set the advanced wireless options. The options included are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.



Authentication Type There are two authentication types: "Open System" and "Shared Key". When you select "Open System", wireless stations can associate with this wireless router without WEP encryption. When you select "Shared Key", you should also setup a WEP key in the "Encryption" page. After this has been done, make sure the wireless clients that you want to connect to the device are also setup with the same encryption key.

Fragment Threshold "Fragment Threshold" specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold When the packet size is smaller then the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth is the range of frequencies that will be used.

Preamble Type The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.

Broadcast ESSID If you enabled "Broadcast ESSID", every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast ESSID" can provide better security.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

TX Power can be set to a bare minimum or maximum power.

WMM WiFi Multi Media if enabled supports QoS for experiencing better audio, video and voice in applications.

Security

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.

Disable

When you choose to disable encryption, it is very insecure to operate the WLR-6001.

Enable 802.1x Auth

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication

WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.

Key Length You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Format You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Key1 - Key4 The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

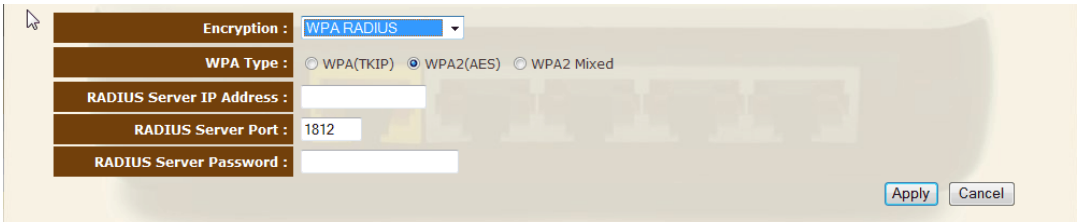
Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.

WPA-Radius

Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses **TKIP** or CCMP (**AES**) to change the encryption key frequently. Press **Apply** button when you are done.



ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

Enable wireless access control Enables the wireless access control function

Adding an address into the list Enter the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

Remove an address from the list If you want to remove a MAC address from the "Current Access Control List ", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPS

Wi-Fi Protected Setup (WPS) is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

WPS Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.

Self Pin Code This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID This is the network broadcast name (SSID) of the router.

Authentication Mode It shows the active authentication mode for the wireless connection.

Passphrase Key It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

WPS via Push Button Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

13 Firewall Settings

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select Enable and click Apply

DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

Enable DMZ Enable/disable DMZ

Public IP Address The IP address of the WAN port or any other Public IP addresses given to you by your ISP

Client PC IP Address Fill-in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

Ping of Death Protections from Ping of Death attack

Discard Ping From WAN The router's WAN port will not respond to any Ping requests

Port Scan Protects the router from Port Scans.

Sync Flood Protects the router from Sync Flood attack.

Access

You can restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Deny If you select "Deny" then all clients will be allowed to access Internet accept for the clients in the list below.

Allow If you select "Allow" then all clients will be denied to access Internet accept for the PCs in the list below.

Filter client PCs by IP Fill in "IP Filtering Table" to filter PC clients by IP.

Add PC You can click Add PC to add an access control rule for users by IP addresses.

Remove PC If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button.

Filter client PC by MAC Check "Enable MAC Filtering" to enable MAC Filtering.

Add PC Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.

Remove PC If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

Click <**Apply**> at the bottom of the screen to save the above configuration.

URL block

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

Enable URL Blocking Enable/disable URL Blocking

Add URL Keyword Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block.

Remove URL Keyword If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keywords from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

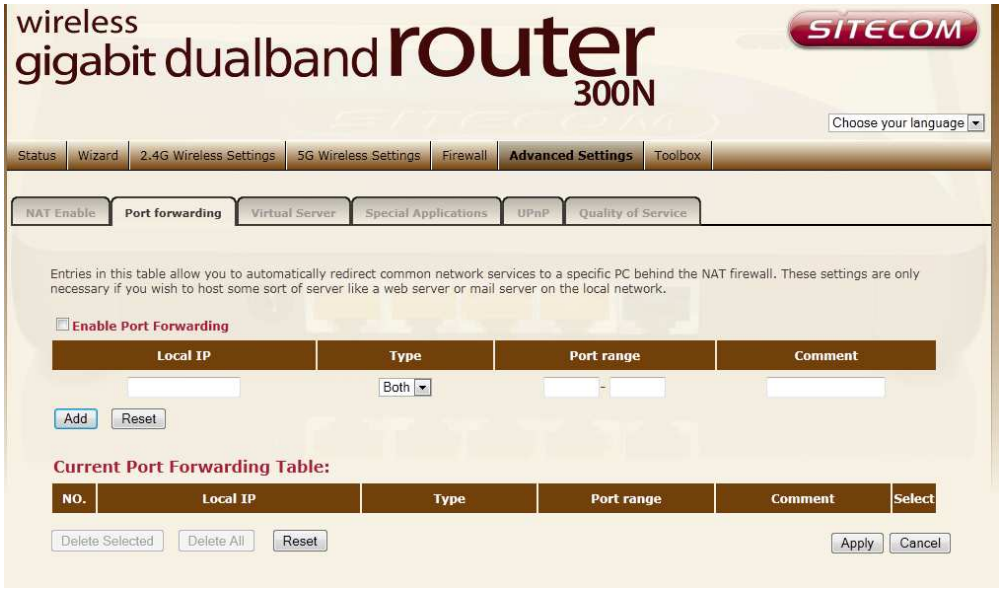
Click <**Apply**> at the bottom of the screen to save the above configurations

14 Advanced Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.

Port Forwarding

Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.



Enable Port Forwarding Enable Port Forwarding

Local IP This is the private IP of the server behind the NAT firewall.

Type This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only, or select “both” to forward both “TCP” and “UDP” packets.

Port Range The range of ports to be forward to the private IP.

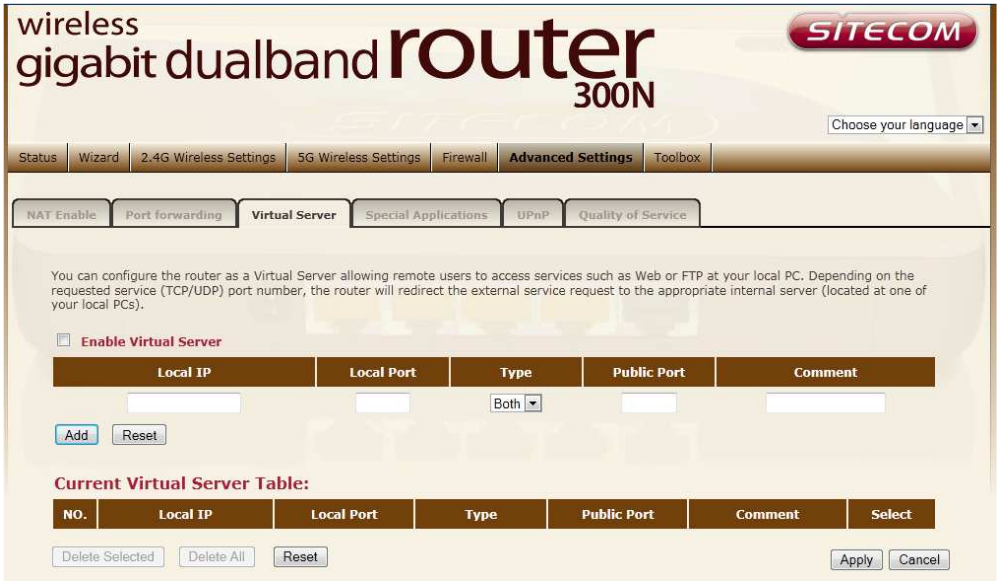
Comment description of this setting.

Add Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below.

Remove If you want to remove a Port Forwarding setting from the "Current Port Forwarding Table", select the Port Forwarding setting that you want to remove in the table and then click "Delete Selected". If you want to remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number.



Enable Virtual Server Enable Virtual Server.

Local IP This is the LAN client/host IP address that the Public Port number packet will be sent to.

Local Port This is the port number (of the above Private IP host) that the below **Public Port** number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).

Type Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "both" setting. Public Port Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN

Comment The description of this setting.

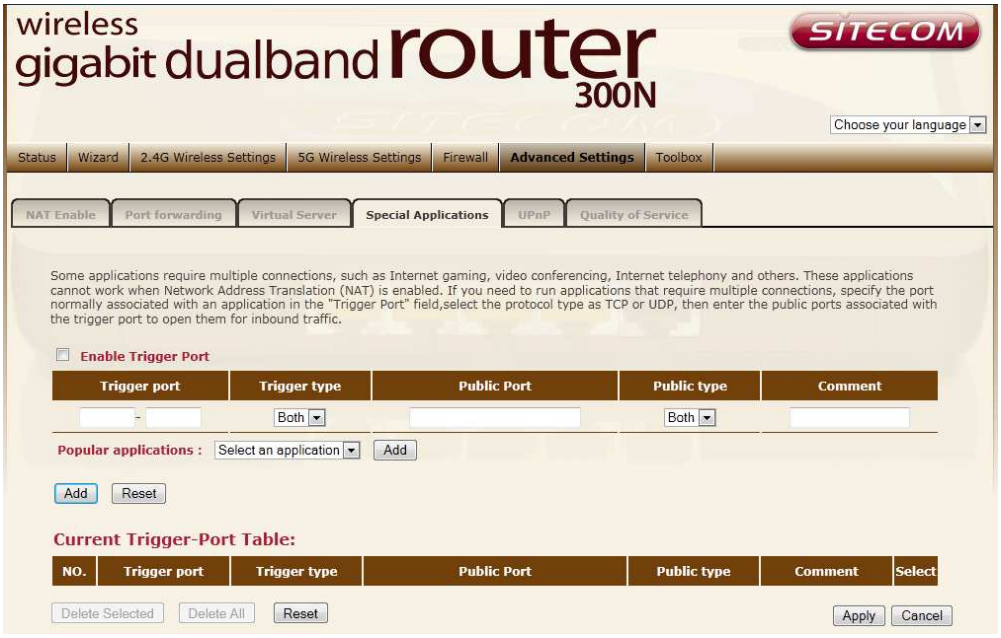
Add Fill in the "Private IP", "Private Port", "Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below.

Reset If you want to remove Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want to remove all Virtual Server settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Special Applications

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Enable Trigger Port Enable the Special Application function.

Trigger Port This is the out going (Outbound) range of port numbers for this particular application.

Trigger Type Select whether the outbound port protocol is “TCP”, “UDP” or both.

Public Port Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624)

Public Type Select the Inbound port protocol type: “TCP”, “UDP” or both
Comment The description of this setting.

Popular applications This section lists the more popular applications that require multiple connections. Select an application from the Popular

Applications selection. Once you have selected an application, select a location (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

Add Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". The Special Application setting will be added into the "Current Trigger-Port Table" below. If you happen to make a mistake, just click "Clear" and the fields will be cleared.

Reset If you want to remove Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

UPNP

With UPnP, all PCs in you Intranet will discover this router automatically, so you don’t have to configure your PC and it can easily access the Internet through this router.

UPnP Feature You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

QoS

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference …etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

Enable/Disable QoS You can check "Enable QoS" to enable QoS functionality for the WAN port.

Add a QoS rule into the table Click "Add" then enter a form of the QoS rule. Click "Apply" after filling out the form the rule will be added into the table.

Remove QoS rules from the table If you want to remove QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete Selected". If you want remove all QoS rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Edit a QoS rule Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "**Apply**" after editing the form and the rule will be saved.

Adjust QoS rule priority You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

USB port

You can use the USB port in Server mode as a Samba server for filesharing in your home network or in NetUSB mode as a virtual USB port on your computer. Please note that for NetUSB mode you need the Control Center software installed on your computer.

Server name Enter a name for the network share.
Workgroup If you wish to add the share to your workgroup enter the workgroup name here.
Description Enter a desired description for the share.
Administrator Enter a desired username for access to the share.
New Password Enter the password for access to the share and confirm this password by re-entering it in the **Confirm password** field

For **netUSB** make sure the radio button next to netUSB is selected and press apply. Please see Addendum MultiFunction Printserver Control Center for more information about netUSB.

15 VPN

WARNING: This section explains how to set-up the WLR-6001 as a VPN server, so you may connect VPN clients (MacOS, Windows, Android, or any other VPN-ready devices) and establish a Virtual Private Network. If your need is to connect to an external VPN server (i.e. HideMyAss, StrongVPN, SwitchVPN) please refer to Section 11 "Connecting to an external VPN service".

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet.
It provides authentication to ensure that the information is going to and from the correct parties and security to protect the information from viewing or tampering en route. The WLR-6001 supports IPSec (Site to Site, Remote to Site) and L2TP over IPSec methods to establish VPN connections and the maximum VPN session number is up to 5.

Status

This page displays the connect status of VPN connection. You can select one of them to connect or disconnect the VPN connection.

To **Connect** or **Disconnect** an existing tunnel. Select the tunnel from the list by ticking the corresponding check box and click connect or disconnect.

Note: If the connection type is remote dial-in (Client to Site or L2TP over IPSec), you can't disconnect this session manually.

Using the Wizard to Configure the WLR-6001 for a PPTP VPN tunnel.

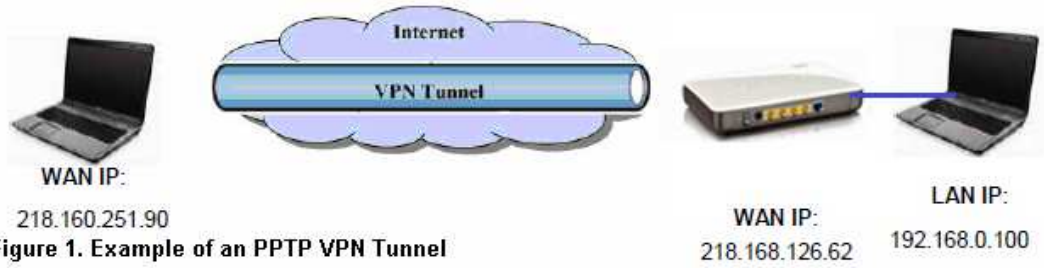


Figure 1. Example of an PPTP VPN Tunnel

1. In the Top Menu on the right side, click **VPN**.
2. In the submenu, click **Wizard** to add a VPN profile.
3. Click **Next** to create a VPN profile.

4. In the **Name** field, enter a name for the PPTP VPN tunnel. This name is for reference purposes. Click **Next** to continue.

5. Click **PPTP** and click **NEXT** to continue.

6. Complete the following fields :

User Name Enter a name for authentication.
Password Enter a password for authentication.
Server IP Enter any private IP address on a different subnet than the LAN IP address of the computer connected behind the WLR-6001.(When WLR-6001 is on default settings, the LAN IP address is 192.168.0.100. In this case you can select any private IP address other than 192.168.0.x, for example 192.168.3.x).
Remote IP Range Enter an IP range that is on the same subnet as the Server IP address you have entered in the Server IP address field, but the range should not include Server IP.(For example if you specified a Server IP address of 192.168.2.1, you can define a Remote IP Range of 192.168.2.100 – 200.)

Click **Next** to continue.

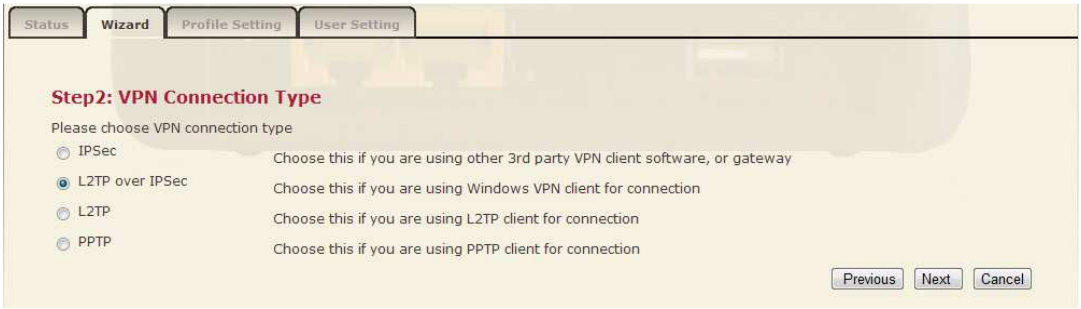
8. Enable the VPN policy, and then click **Apply** to save the VPN profile.

Using the Wizard to Configure the WLR-6001 for L2TP over IPSec VPN tunnel.

1. In the Top Menu on the right side, click **VPN**.
2. In the submenu, click **Wizard** to add a VPN profile.
3. Click **Next** to create a VPN profile.

4. In the **Name** field, enter a name for the L2TP VPN tunnel. This name is for reference purposes. Click **Next** to continue.

5. Click **L2TP** and click **NEXT** to continue.



6. Complete the following fields:

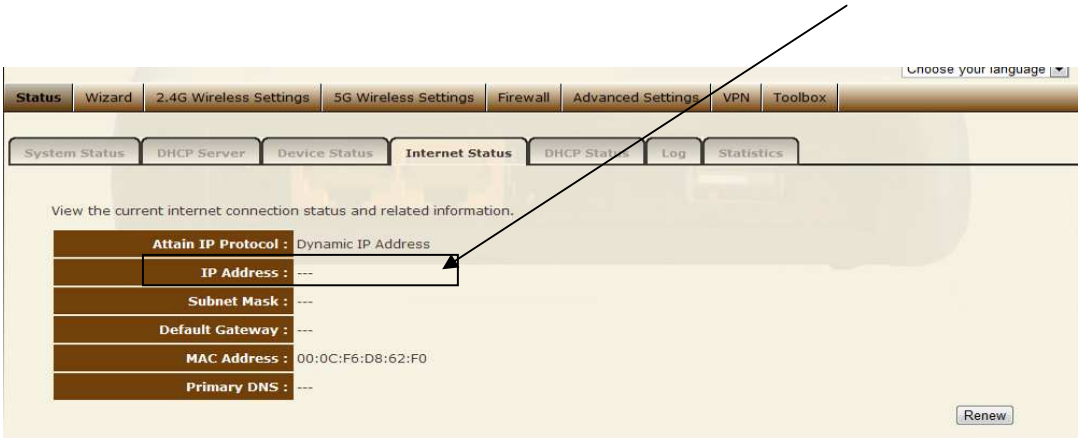
User Name	Enter a name for authentication.
Password	Enter a password for authentication.
Server IP	Enter any IP address on a different subnet than the LAN IP address of the computer connected behind the WLR-6001.(When WLR-6001 is on default settings, the LAN IP address is 192.168.0.1. In this case you can select any IP address other than 192.168.0.x).
Remote IP Range	Enter an IP range that is on the same subnet as the Server IP address you have entered in the Server IP address field, but the range should not include Server IP.(For example if you specified a Server IP address of 192.168.2.1, you can define a Remote IP Range of 192.168.2.100 – 200.)

Click **Next** to continue.

7. In the **Shared Key** field, enter the Security key you wish to use.

8. **Enable the VPN policy**, and then click **Apply** to save the VPN profile.

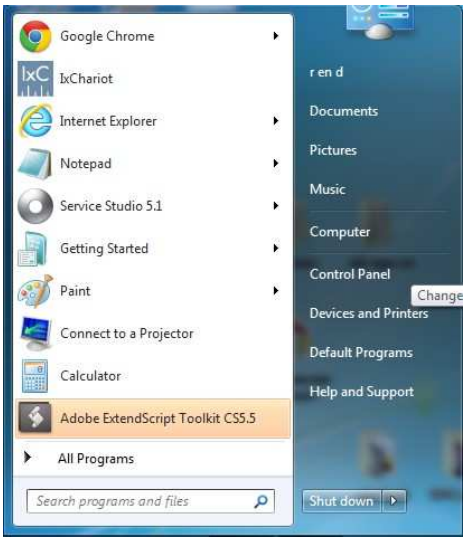
In the following examples it is assumed that the WLR-6001 is placed behind a bridged modem. This means that the Router will receive a public IP address on the WAN side. The **WAN/Internet IP address** can be found on the Internet status page of the WLR-6001.



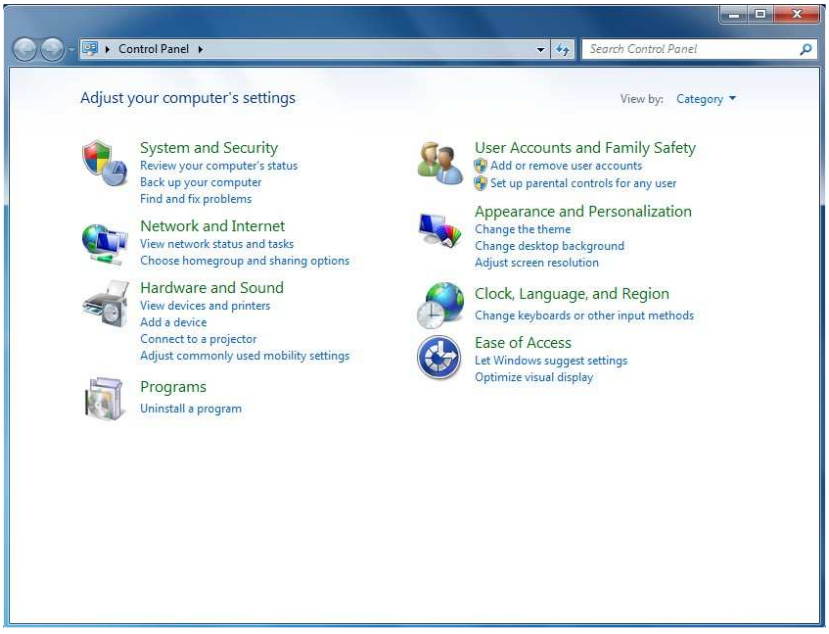
If the WAN IP address of the WLR-6001 is not a public IP address but a local IP address (for example any IP address in the following ranges: 10.X.X.X, 172.16.X.X or 192.168.X.X)
In this situation your WLR-6001 is placed behind a NAT enabled modem. In this case consult your manual to make sure your modem supports VPN pass through and the GRE47 protocol and set it up to allow access to the VPN server behind the modem.

Configuring a Microsoft Windows 7 VPN Client

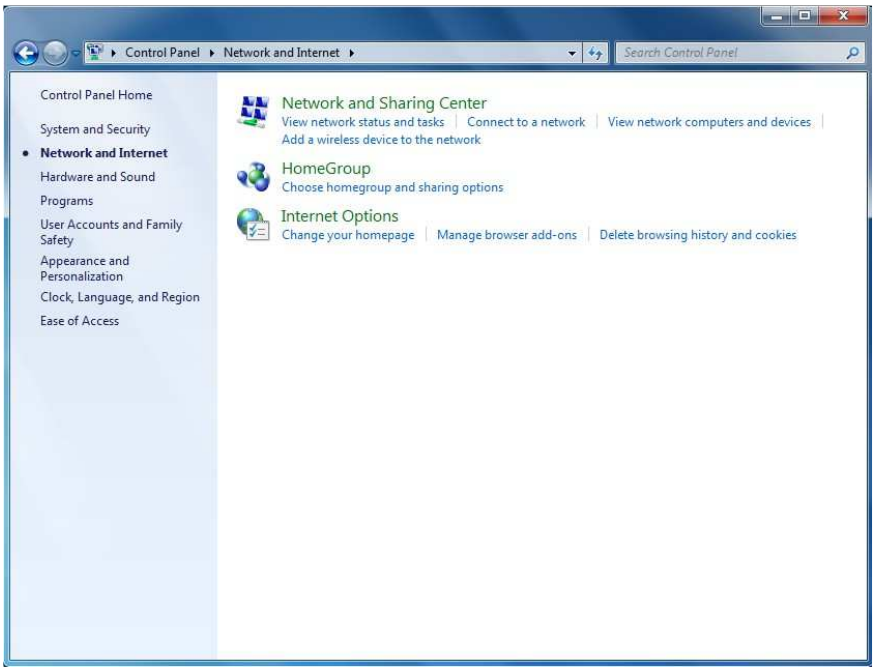
Click the **Start** button and open the **Control Panel.**



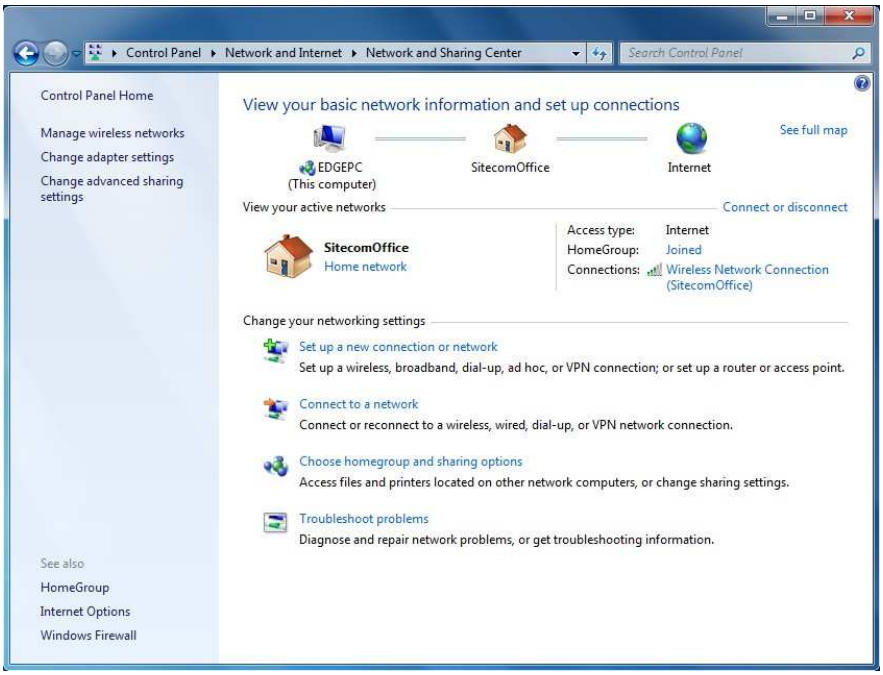
From the **Control Panel**, select **Network and Internet**.(If your control panel view has been set to Icons you can directly go to step 4)



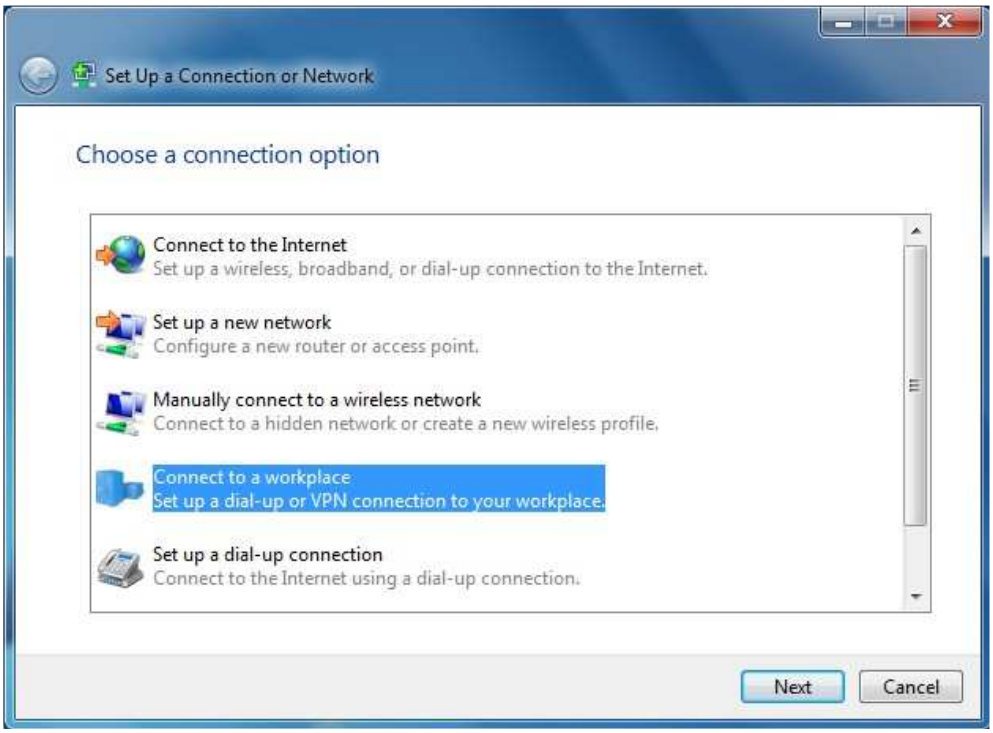
3. From **Network and internet**, select **Network and Sharing center** .

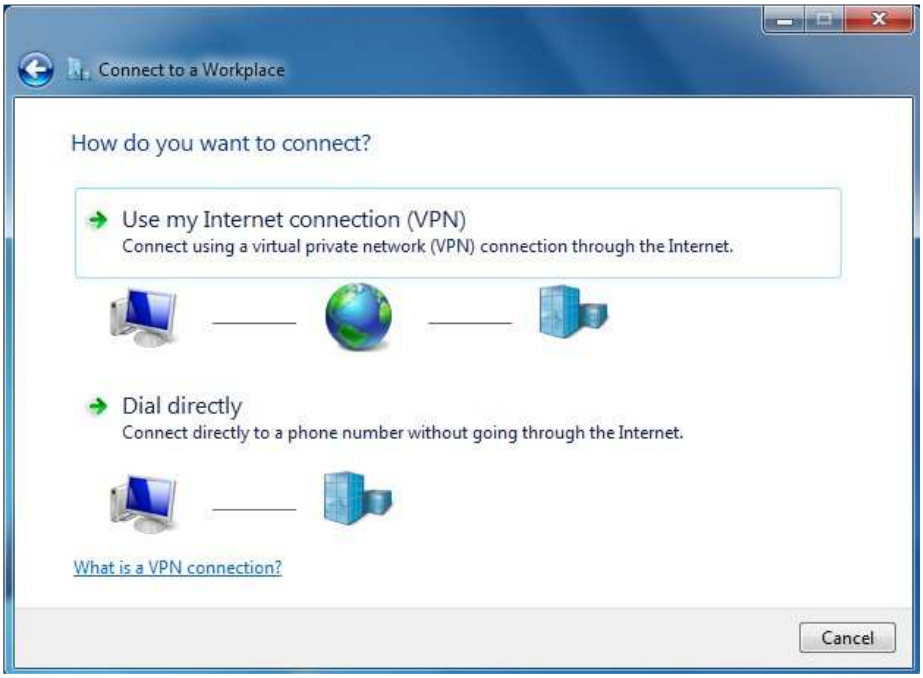


4. Under **Network and Sharing Center**, select **Setup a new connection or network**.



5. Click **Connect to a workplace**, and click **Use my internet connection (VPN)**.



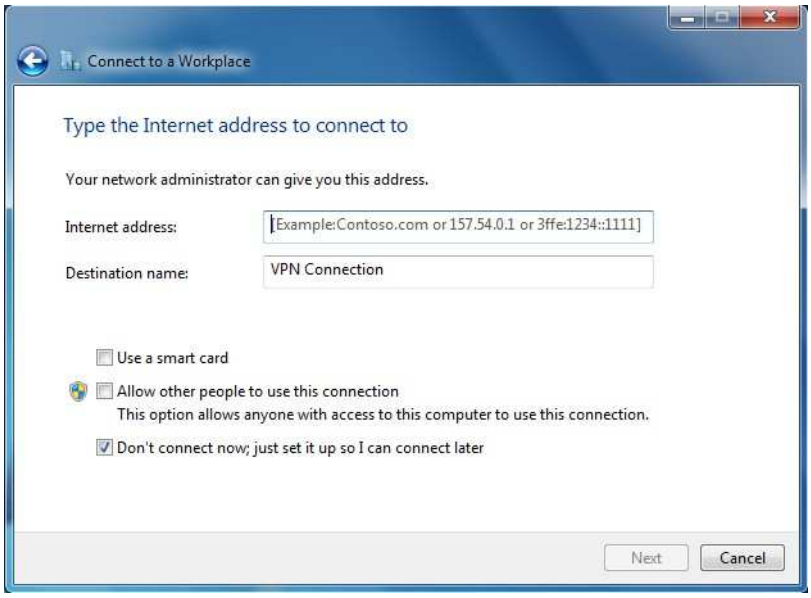


6. Complete the following fields:

Internet Address Enter the WLR-6001 WAN IP address.
Destination name Enter a name for the VPN client.

We recommend to select: Don't connect now. Just set it up so I can connect later.

Click **next** to continue.

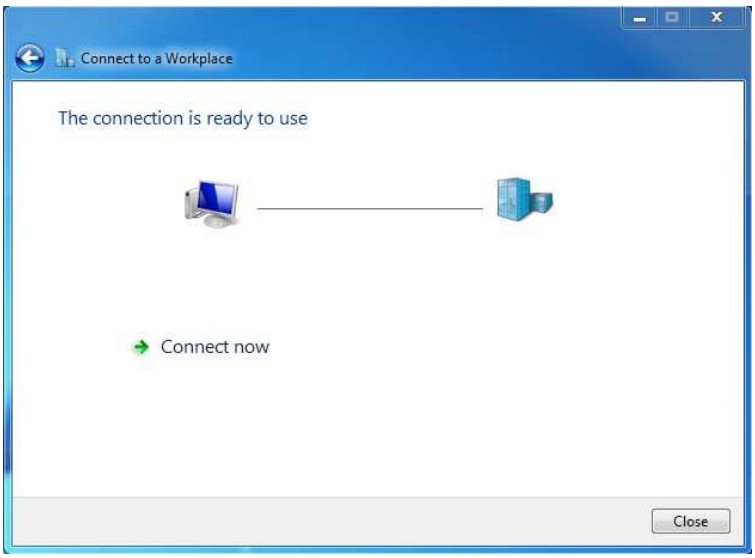


7. Complete the following fields:

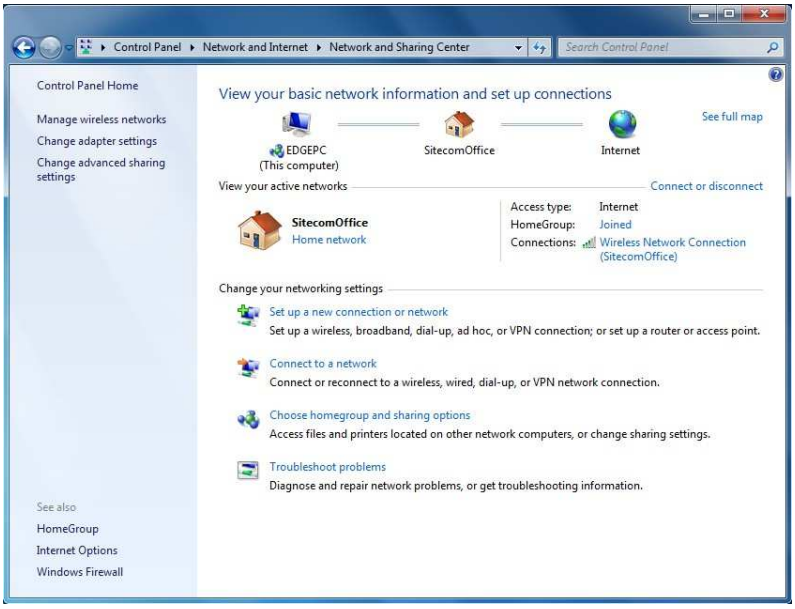
User name Enter the username used to log onto the VPN tunnel.
Password Enter the password used to log onto the VPN tunnel.

Click **Create** to continue.

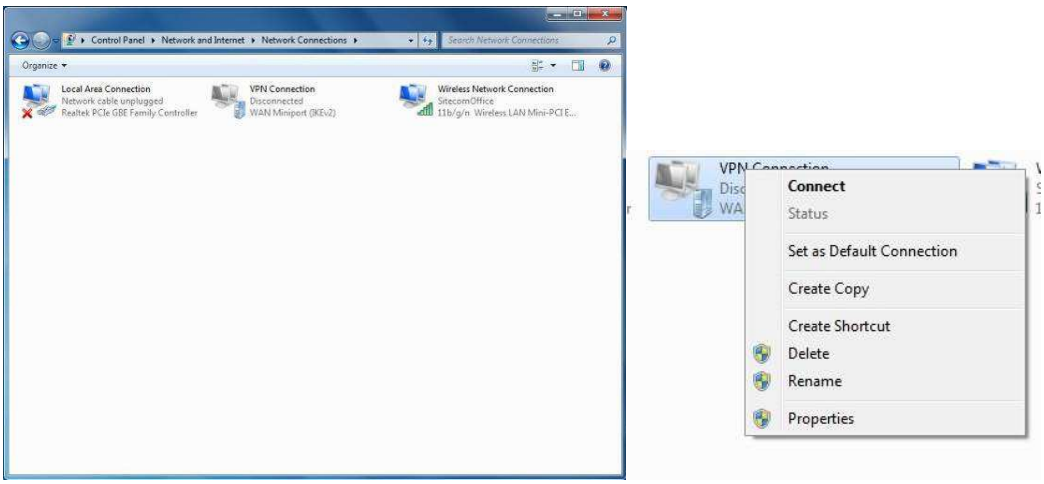
8. When the following screen appears, click the **Close** button to close the VPN connection setting.



9. Select **Change adapter settings** on the left side of the window.



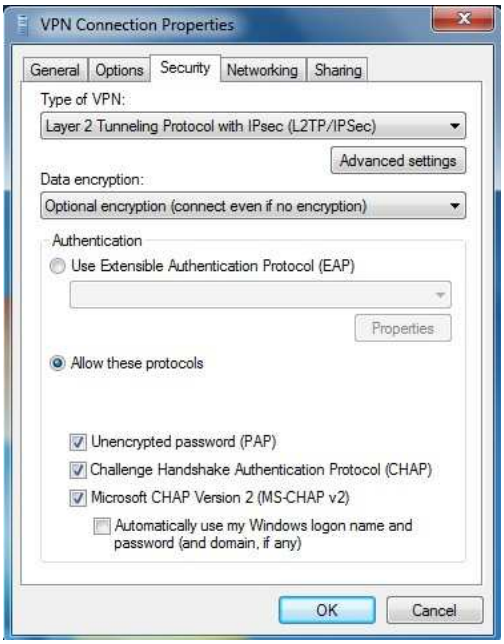
10. Select the VPN connection you just set, right-click VPN Connection, and select **Properties.**

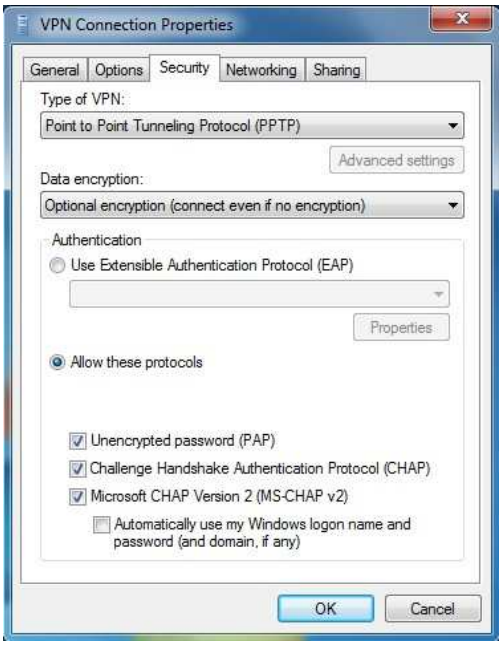


11. Go to the Security tab and configure the following settings :

Under the **Type of VPN**, select the Protocol that has been set in the WLR-6001, **Point to point tunneling protocol(PPTP)** or **Layer 2 Tunneling Protocol with IPsec (L2TP-IPSec)** .

Check **unencrypted password (PAP)**.
Check **Challenge Handshake Authentication Protocol (PPTP).**
Check **Microsoft CHAP Version 2 (MS-CHAP v2)**.





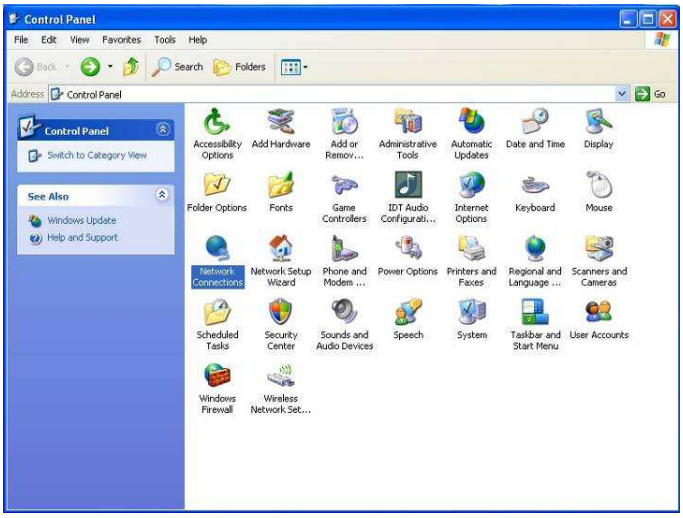
12. Go to **Network and Sharing Center** on the bottom-right of the windows.

Under VPN Connection click **Connect.**

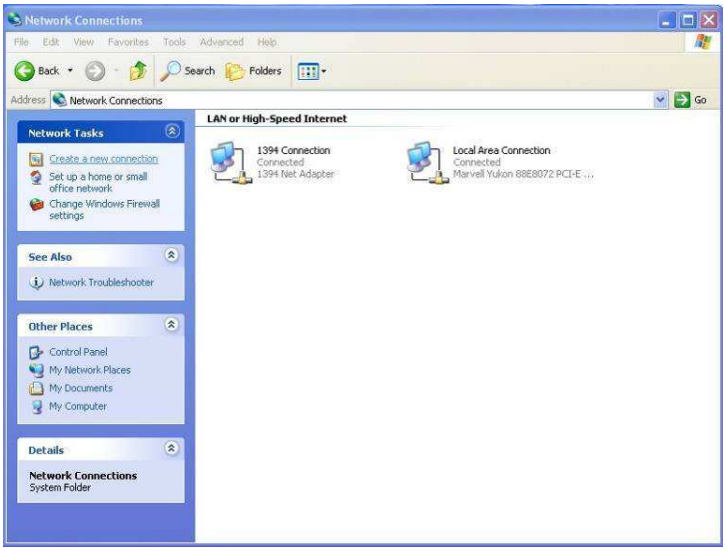
Configuring a Microsoft Windows XP VPN Client

1. Click the **Start** button and open the **Control Panel**.

2. From the **Control Panel**, Click on **Network Connections**.



3. Click on **Create a network** from the left side of the window.



4. Click **Next** to continue to setup the VPN client.

5. Select **Connect to the network at my workplace** and click Next to continue.

6. Select **Virtual Private network connection** and click **Next** to continue.

7. Enter a **Company name**, this name is only for reference purposes.

8. Enter the **Hostname** , this should be the WLR-6001 WAN IP address and click **Next** to continue.

9. Click **Finish** to continue, you may choose to add a shortcut for this connection on the Desktop by clicking the checkbox before you click **Finish**.

10. Click on **Properties**.

11. Click on the **Security** Tab from the top in the window and select **Advanced,** click **Settings** to continue.

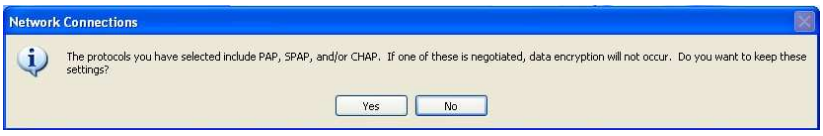
12. Configure the following settings:

Under **Data encryption**, select Optional encryption (connect even if no encryption)

Check	**Unencrypted password (PAP)**
Check	**Challenge Handshake Authentication Protocol (SPAP)**
Uncheck	**Microsoft CHAP (MS-CHAP)**
Check	**Microsoft CHAP Version 2 (MS-CHAP v2)**

Click **OK** to continue.

13. Click **Yes** to continue. If the VPN type you have configured in the WLR-6001 is PPTP you can skip step 14.



14a. If the VPN Type of the tunnel you have set up in the WLR-6001 is L2TP over IPSec You have also entered a **Shared key** in the WLR-6001(see step 7 of chapter **Using the Wizard to Configure the WLR-6001 for L2TP over IPSec** for reference**)**.

Click on **IPSec Settings…**

14b. Check Use pre-shared key for authentication.
Key, Enter the shared key you have entered in the WLR-6001.

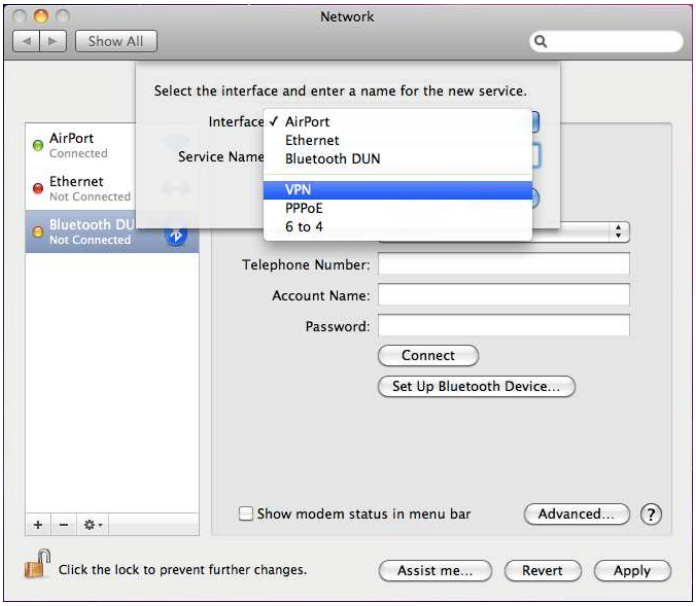
Configuring a MacOS VPN Client

1. Select **System Preferences.**

2. On the **System preferences** panel, Click **Network**.

3. Click on the **+** sign on the bottom left.

4. Select the **VPN** interface.

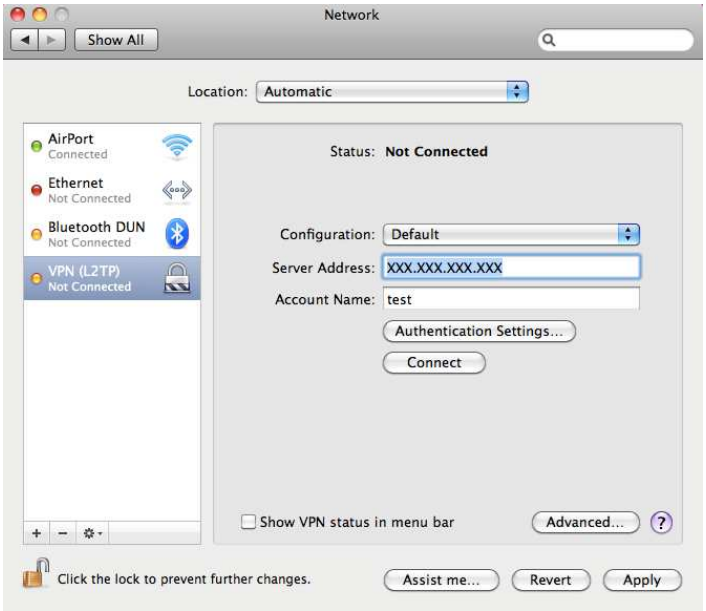


5. Under the **VPN Type** dropdown**,** select the option that corresponds to the **VPN Type** you have configured in the WLR-6001. Enter a name for this profile (this name is for reference purpose only)

6. Complete the following fields:

Server address	Enter the WAN IP address of the WLR-6001.
Account Name	Enter the name used to log onto the VPN tunnel (this must be one of the users you have set in the VPN user table of the WLR-6001)

Click **Authentication Settings** to continue.



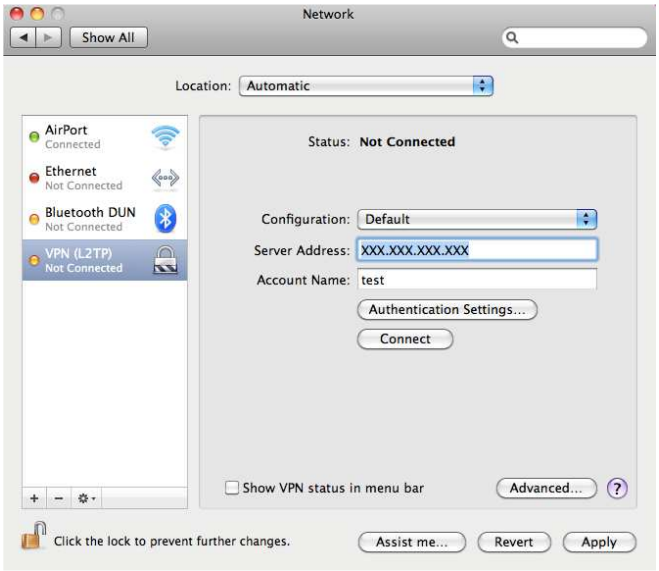
7. Complete the following fields:

Password Enter the password that belongs to the Account name which you have entered in step 6 of this Guide.

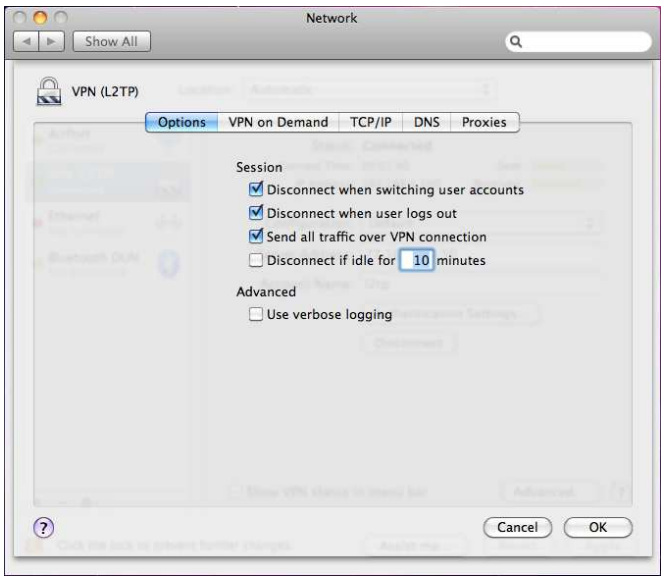
Shared Key If the VPN Type of the VPN tunnel you have set up in the WLR-6001 is L2TP over IPSec You have also entered a **Shared key** in the WLR-6001(see step 7 of chapter **Using the Wizard to Configure the WLR-6001 for L2TP over IPSec** for reference**)** Enter the same key in this field.

Click **OK** to continue.

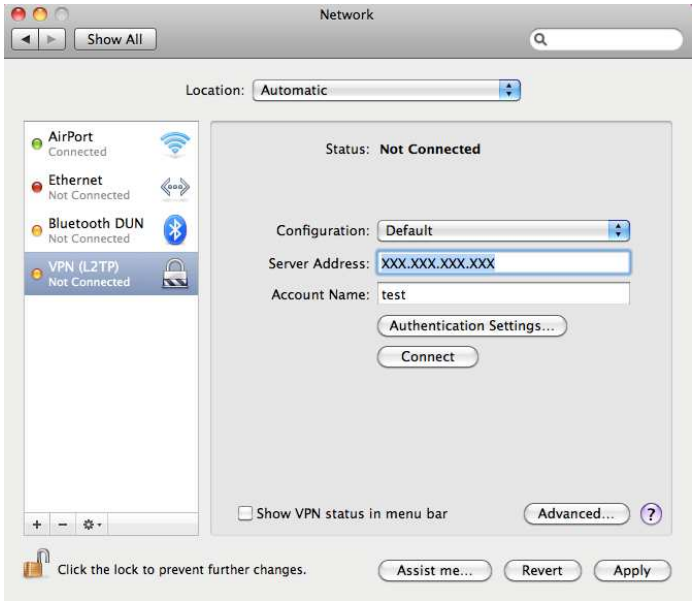
8. Click on **Advanced** in the network panel to continue.



9. Select the checkbox **Send all traffic over VPN connection.** Click **OK** to continue.



10. If the VPN tunnel is already connected, click **Disconnect** and **Connect** again for the changes made in step 9 to take effect.



Configuring a VPN client on iOS

1. Click **Settings** on the Springboard.

2. Select **General** on from the panel of the left side and Click on **Network.**

3. Click on **VPN**.

4. click on **Add VPN Configuration…**

3. Select the **VPN Type** that corresponds to the **VPN Type** you have configured in the WLR-6001.

Complete the following fields:

Description Enter a name for your VPN connection, this name is for reference purposes only.

Server Enter the WLR-6001 WAN IP address

Account Enter the name used to log onto the VPN tunnel(this must be one of the users you have set in the VPN user table of the WLR-6001)

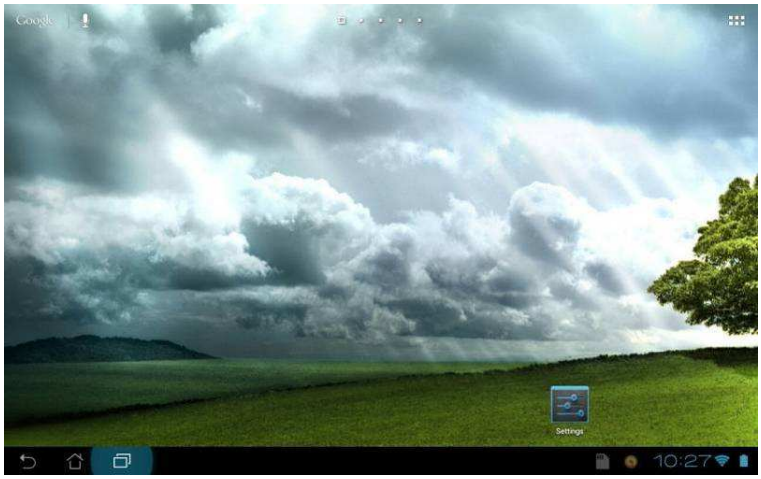
Password Enter the Password used to log onto the VPN tunnel.

Secret(L2TP only) If the VPN Type of the VPN tunnel you have set up in the WLR-6001 is L2TP over IPSec You have also entered a **Shared key** in the WLR-6001(see step 7 of chapter **Using the Wizard to Configure the WLR-6001 for L2TP over IPSec** for reference**)** Enter the same key in this field.

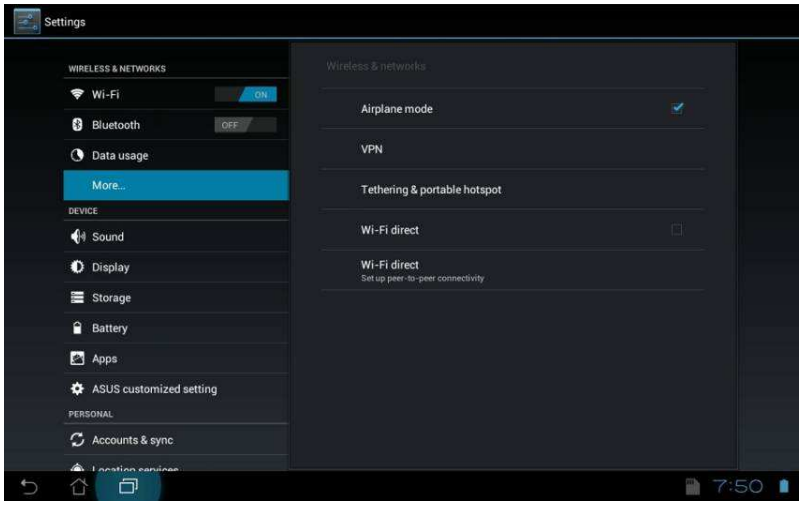
4. Set the Switch to **ON** to connect to the VPN Network.

Configuring a VPN client on Android

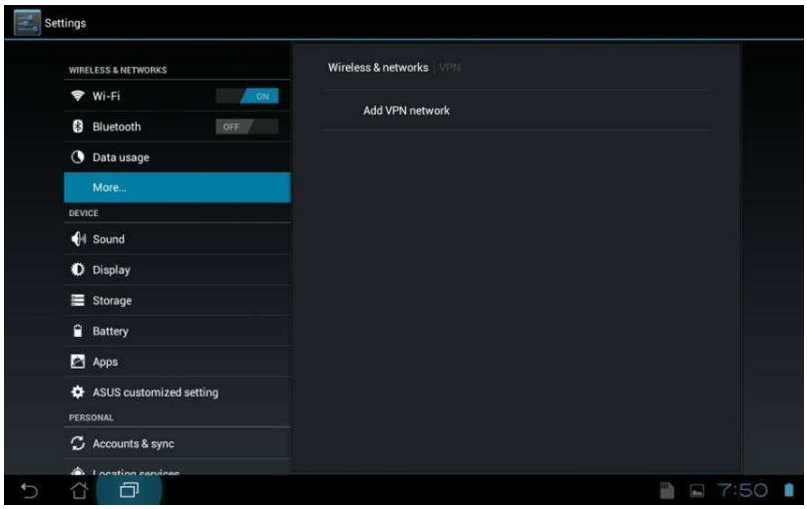
1. Click on **Settings.**



2. click on **More..** from the Settings menu on the upper left. Then Click on **VPN.**



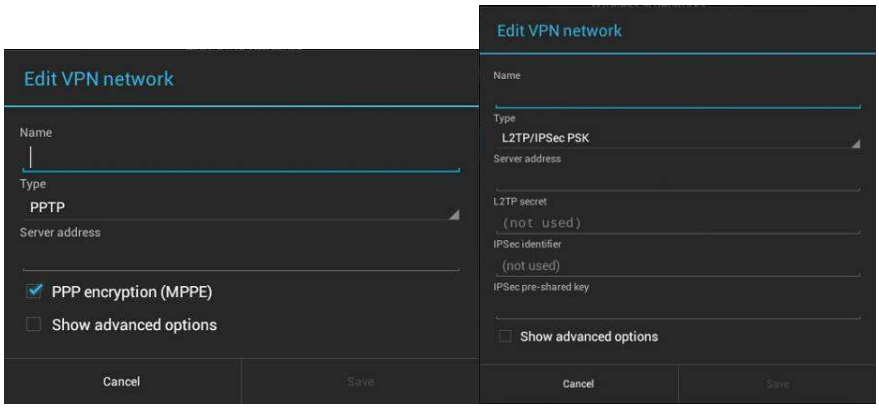
2. Click on **Add VPN Network.**



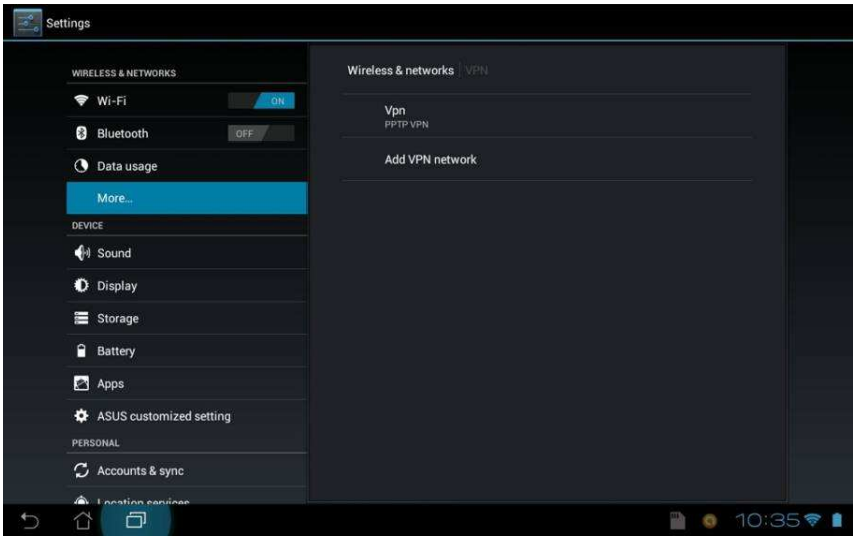
3. Select the **VPN Type** that corresponds to the **VPN Type** you have configured in the WLR-6001.

Complete the following fields:

Description	Enter a name for your VPN connection, this name is for reference purposes only.
Server	Enter the WLR-6001 WAN IP address
Account	Enter the name used to log onto the VPN tunnel (this must be one of the users you have set in the VPN user table of the WLR-6001)
Password	Enter the Password used to log onto the VPN tunnel.
Secret(L2TP only)	If the VPN Type of the VPN tunnel you have set up in the WLR-6001 is L2TP over IPSec You have also entered a **Shared key** in the WLR-6001(see step 7 of chapter **Using the Wizard to Configure the WLR-6001 for L2TP over IPSec** for reference**)** Enter the same key in this field.



4. Click on the VPN network you have just created to connect.



Profile Setting

This page allows you to Add, Edit and Delete VPN profiles.

Add click here if you wish to manually add a new VPN profile.

Edit to edit an existing profile, select one from the list by selecting the corresponding radio button and click 'Edit'.

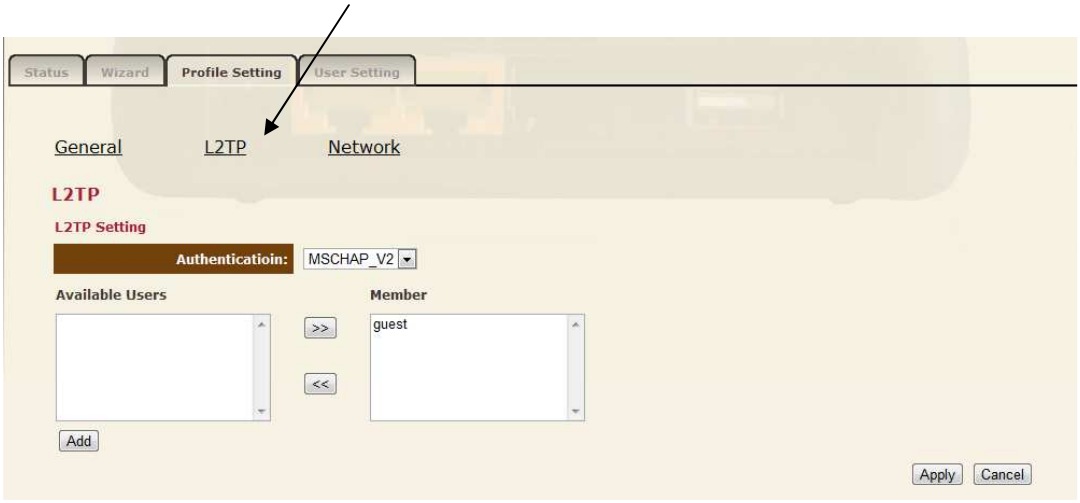
Click "**Apply**" to save the settings and apply the changes.

Add Users to an existing Profile

Click on **Profile Setting**.

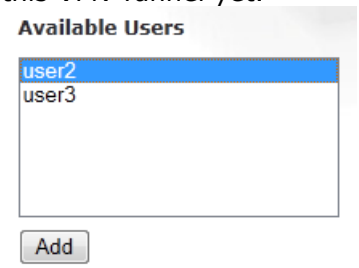
Select the **Profile** for which you wish to modify user settings and click on **Edit**.

Then Click on the protocol name you selected to edit.

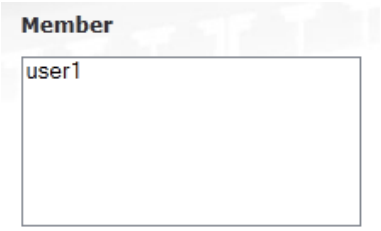


From here all current users that you have created will be shown.

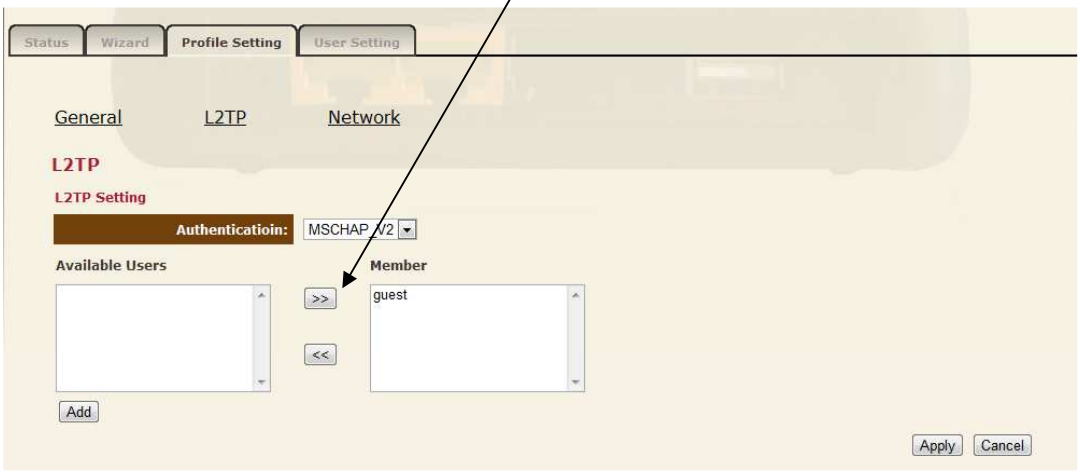
In the **Available** box existing users are be displayed that do not have access to this VPN Tunnel yet.



The **Member** box displays users that already have access to this VPN Tunnel.



To Add or remove users to the VPN Tunnel, click the on the username you wish you Add or Remove and press the ‘**<<**’, ‘**>>**’ buttons to the desired box.



Click Apply Click “**Apply**” to save the settings and apply the changes.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
The PPTP specification does not describe encryption or authentication features and relies on the PPP protocol being tunneled to implement security functionality. However the most common PPTP implementation, shipping with the Microsoft Windows product families, implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide similar levels of security and remote access as typical VPN products.

General

This page allows you to configure the general VPN settings.

Name	Enter a name for your VPN policy
Connection Type	Supports **IPSec** and **L2TP** over **IPSec** methods to establish VPN connection.

PPTP

Authentication	Select the desired authentication protocol (PAP, CHAP, Auto). Select **Auto** by default.
Encryption	Supports **40-bit, 128-bit** or **No** encryption.
User Name	Enter the username for authentication.
Password	Enter the password for authentication.

Network

Server IP	Enter the VPN Server IP address.
Remote IP Range	Assign a range of IP addresses. The assigned IP range should be on the same IP network but not the in the same range as your DHCP IP range.

L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

General

This page allows you to configure the general VPN settings.

Name	Enter a name for your VPN policy
Connection Type	Supports **IPSec** and **L2TP** over **IPSec** methods to establish VPN connection.

L2TP

Authentication	Select the desired authentication protocol (PAP, CHAP, Auto). Select **Auto** by default.
User Name	Enter the username for authentication.
Password	Enter the password for authentication.

Network

Server IP	Enter the VPN Server IP address.
Remote IP Range	Assign a range of IP addresses. The assigned IP range should be on the same IP network but not the in the same range as your DHCP IP range.

IPSec

IPSec (Internet Protocol Security) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.
IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

General

This page allows you to configure the general VPN settings.

Name	Enter a name for your VPN policy
Connection Type	Supports **IPSec** and **L2TP** over **IPSec** methods to establish VPN connection.
Authentication Type	Supports **pre-shared key** method for authentication.
Shared Key	Enter the Shared Key.
Confirm	Enter your Shared Key again for verification.
Local ID Type	Supports **IP Address**, **Domain Name**, **Email Address** methods for Local ID Type.
Local ID	identify and authenticate the local VPN endpoint.
Peer ID Type	Supports **IP Address**, **Domain Name**, **Email Address** methods for Peer ID Type.
Peer ID	Enter an ID to identify and authenticate the remote VPN endpoint.

SA (Security Association)

A Security Association (SA) is the establishment of shared security attributes between two network entities to support secure communication.
An SA may include attributes such as:
cryptographic algorithm and mode; traffic encryption key; and parameters for the network data to be passed over the connection.
Establishment of an SA is described in RFC 2408, the Internet Security Association and Key Management Protocol.

This page allows you to configure SA.

IKE (Phase 1) Proposal

Exchange
Select Main Mode or Aggressive Mode for IKE Phase 1 negotiation.
• Main Mode: Select this option to configure the standard negotiation parameters for IKE Phase 1 of the VPN Tunnel. (Recommended Setting)
• Aggressive Mode: Select this option to configure IKE Phase 1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended - Less Secure)

DH Group
Select a DH Group from the drop-down menu (Group 1, Group2, Group5 and Group14). As the DH Group number increases, the higher the level of encryption implemented for IKE Phase 1.

Encryption
The WLR-6001 supports DES, 3DES, AES128, AES192, AES256 encryption methods for traffic through the VPN.

Authentication
The WLR-6001 supports SHA1, MD5 methods for authentication.
Life Time Enter the number of seconds for the IKE Lifetime. The period of time to pass before establishing a new IKE security association (SA) with the remote endpoint. The default value is 28800.

IPSec (Phase 2) Proposal

Protocol
Select ESP (Encapsulating Security Payload) or AH (Authentication Header) for traffic through the VPN.
• **AH (Authentication Header)** to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replay attacks.
• **ESP (Encapsulating Security Payload)** to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

Encryption
The WLR-6001 supports **DES**, **3DES**, **AES128**, **AES192**, **AES256** encryption methods for traffic through the VPN.

Authentication
The WLR-6001 supports **SHA1**, **MD5** methods for authentication.

Perfect Forward Secrecy
Select Enable or Disable to enable or disable PFS (Perfect Forward Secrecy). PFS is an additional security protocol.

DH Group
Select a PFS DH Group from the drop-down menu (**Group 1, Group2, Group5, Group14**). As the DH Group number increases, the higher the level of encryption implemented for PFS.

Life Time
Enter the number of seconds for the IPSec Lifetime. The period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 28800.

Network

This page allows you to configure the VPN server and local/remote subnet.

Security Gateway Type	Security Gateway Type supports IP Address and Domain Name. Select one of them.
Security Gateway	The IP address or domain name of the VPN server.
Local Network	Enter the local (LAN) subnet and mask. (ex. 192.168.0.0/255.255.255.0)
Remote Network	Enter the remote subnet and mask. (ex. 192.168.9.0/255.255.255.0)

Advanced

This page allows you to configure advanced VPN settings.

Nat Traversal	Enabling **NAT Traversal** allow IPSec traffic from this endpoint to traverse through the translation process during NAT. The remote VPN endpoint must also support this feature and it must be enabled to function properly over the VPN.
Dead Peer Detection	Enable **DPD (Dead Peer Detection)** to delete the VPN tunnel if there is no traffic detected. The VPN will re-establish once traffic is again sent through the tunnel.

L2TP over IPSec

L2TP over IPSec VPNs enable a business to transport data over the Internet, while still maintaining a high level of security to protect data.
You can use this type of secure connection for small or remote office clients that need access to the corporate network. You can also use L2TP over IPSec VPNs for routers at remote sites by using the local ISP and creating a demand-dial connection into corporate headquarters.

General

Name	Enter a name for your VPN policy
Connection Type	Supports **IPSec** and **L2TP** over **IPSec** methods to establish VPN connection.
Authentication Type	Supports **pre-shared key** method for authentication.
Shared Key	Enter the Shared Key.
Confirm	Enter your Shared Key again for verification.

L2TP/PPTP

Authentication	Select the desired authentication protocol (PAP, CHAP, Auto). Select **Auto** by default.
User Name	Enter the username for authentication.
Password	Enter the password for authentication.

Network

Server IP	Enter the VPN Server IP address.
Remote IP Range	Assign a range of IP addresses. The assigned IP range should be on the same IP network but not the in the same range as your DHCP IP range.

User Setting

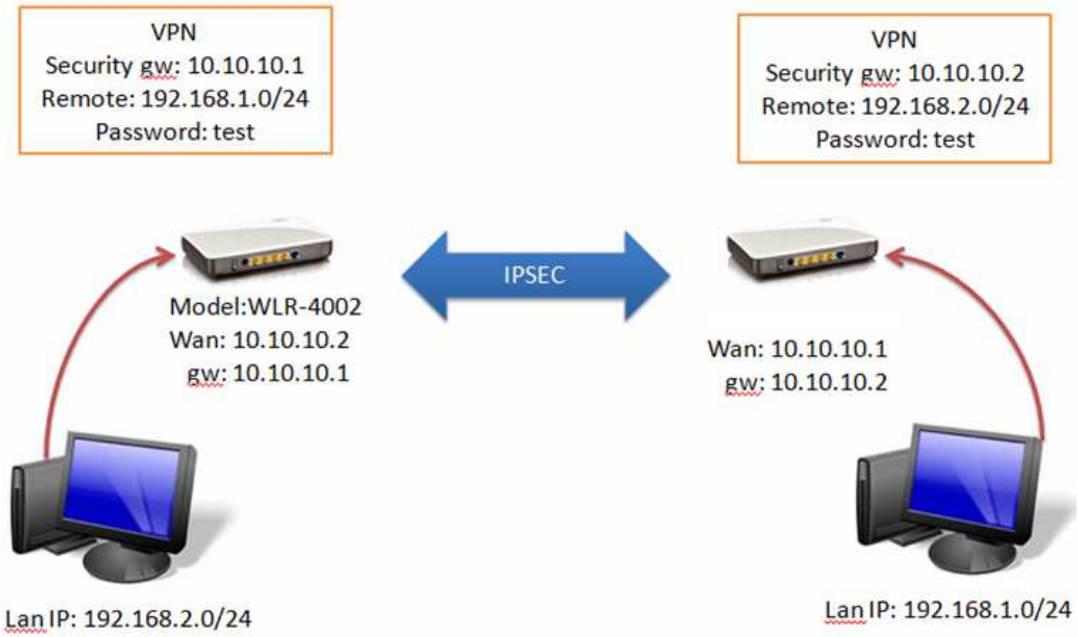
This page allows you to maintain VPN users.

Add	a user Enter the desired name and password, for verification the password has to be entered twice. Click 'Add' to add the user to the current VPN user table
Reset	This button will clear all values from the input boxes.
Current VPN user table	shows all existing VPN users.
Delete Selected	Select a user from the table and Click Delete Selected to delete this user.
Delete ALL	This deletes all current VPN user from the current table.

Click "**Apply**" to save the settings and apply the changes.

Example of configuring IPSec Site to Site architecture

In this guide we give an example how to set up a IPSec Site to Site architecture. The values in this example are only to give an impression of how to do the configuration.

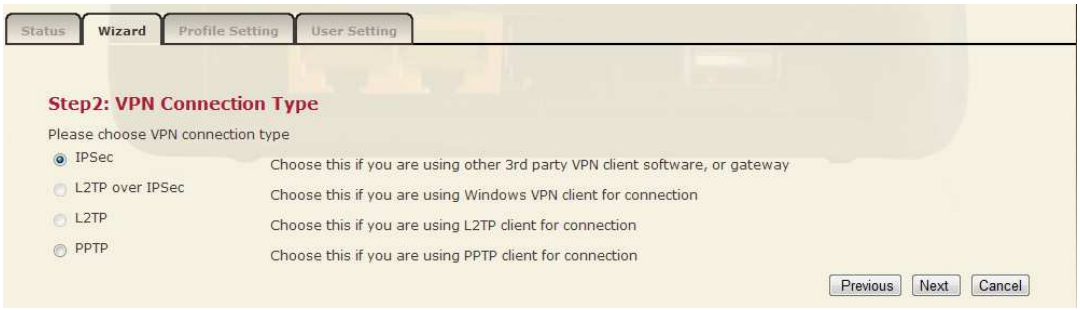


Configuring Location B

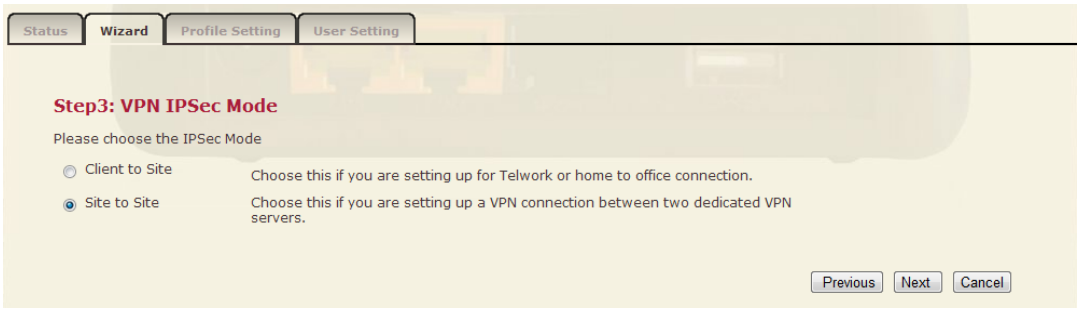
1. Click on **VPN** in the top menu then click **Wizard** in the submenu. Click **Next** to continue.

2. In the **Name** field, enter a name for the IPSec VPN tunnel. This name is for reference purposes. Click **Next** to continue.

3. Click **IPSec** and click **NEXT** to continue.



4. Click **Site to Site** and click **NEXT** to continue.



5. Complete the following fields :

Security Gateway Type Choose the type of **Security Gateway** you wish to use(In this example we use IP address.

Security Gateway Enter the **WAN IP address** of the **remote VPN Server**(In our example this is the WAN IP address of the WLR-6001 in Location A, 77.193.12.20)

Remote Address Enter an **IP address** that is on the same **Subnet** as the Local LAN of the remote VPN server (In our example the WLR-6001 in location A has a **local IP** of 192.168.2.1 so we set the **Remote address** to 192.168.2.0)

Remote Netmask Enter the Netmask of the Remote Local LAN(In our example the WLR-6001 in Location A has a **IP Subnet Mask** of 255.255.255.0)

click **NEXT** to continue.

6. Enter the **Shared Key** you wish to use, this shared key must be used in both VPN servers.(In this example we used 'sharedkey')

7. **Enable the VPN policy**, and then click **Apply** to save the VPN profile.

8. Repeat these steps 1~7 for the other VPN server.

9. Once Both VPN routers have been completely set up.
Click on **Status** in the submenu of the VPN menu and click **Connect** to establish the IPSec Site to Site connection.

16 TOOLBOX Settings

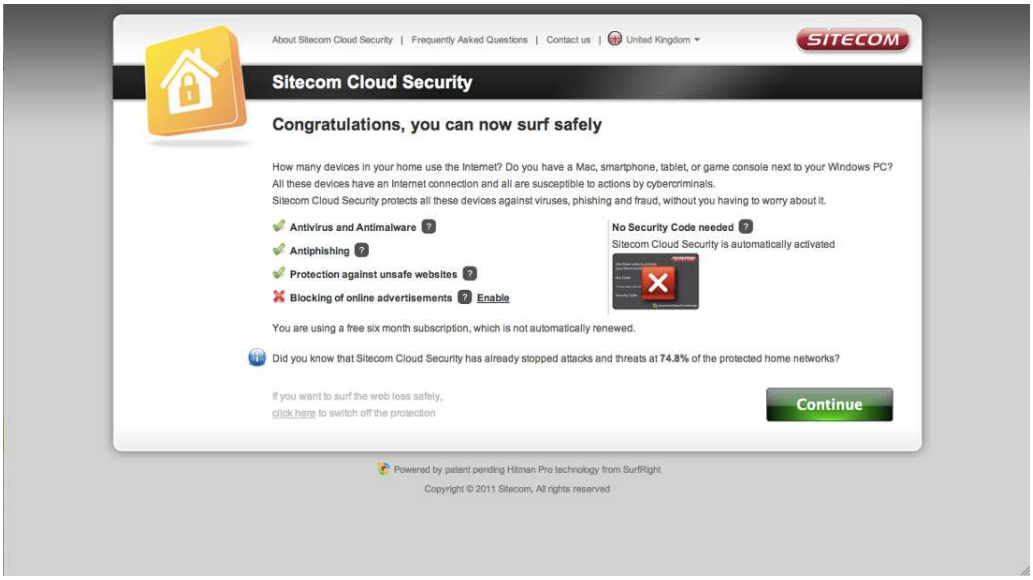
Sitecom Cloud Security

Antivirus software alone is not safe enough. You can now benefit from additional built-in security in your modem or router. Protect all devices in your home network against cybercrime while browsing. Activate in just one click, your network and devices are better secured than ever before.

Your Sitecom device comes with a 6 month free *Sitecom cloud security* subscription.

After you have set up your Sitecom device for internet access, open the webbrowser and enter http://www.sitecomcloudsecurity.com in the address bar.

If the device has been properly configured the following web page should be shown.



Here you can select which security features you would like to use.

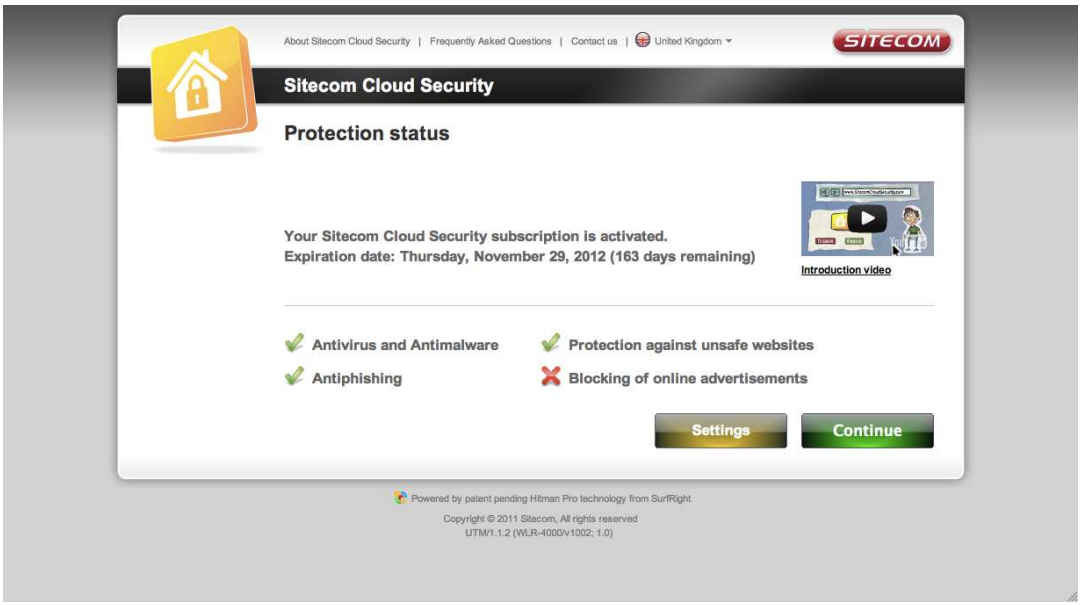
The S*itecom Cloud Security* service offers the following protection options:

- Anti-Malware
- Anti-Phishing
- Protection against unsafe websites
- Advertisement blocking

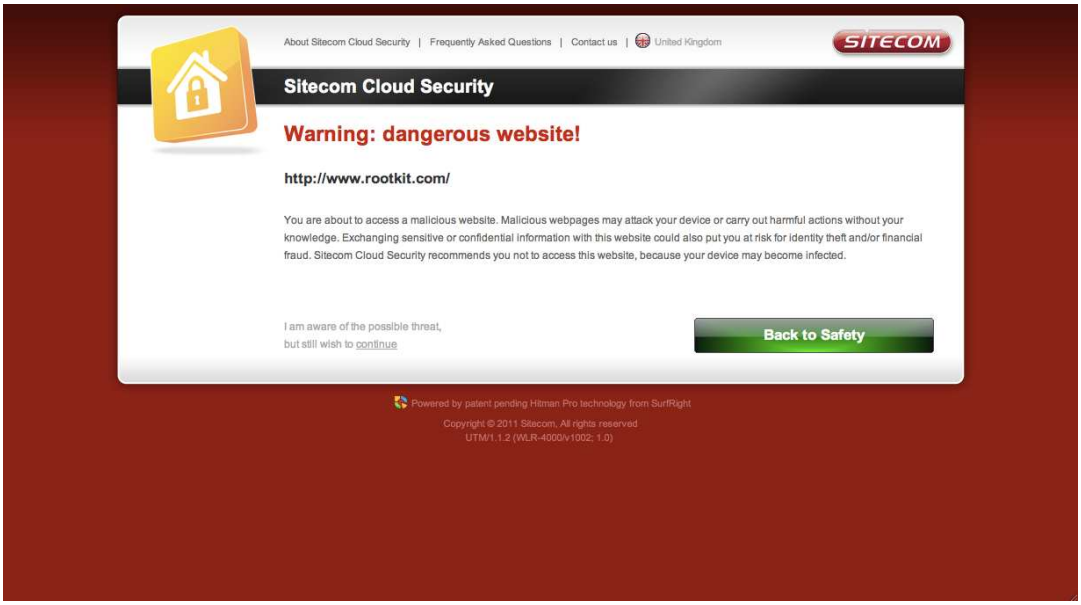
After selecting your preferred protection options, enter the Key code and

Security code that you have received with your Sitecom product.

Before you can now activate your subscription you will have to accept the license agreement. After this click the activation button. You will be shown the status of your *Sitecom cloud security* and the expiration date of your current subscription.



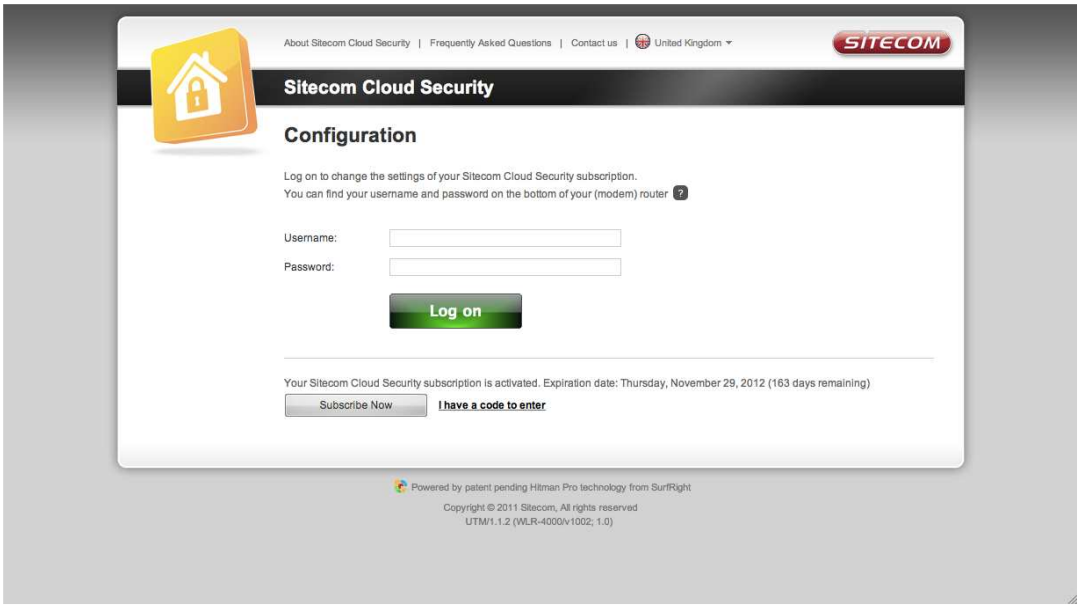
With the protection of *unsafe websites* activated the S*itecom Cloud Security* will always check if a website is safe. If it is not safe it will inform you that is not safe to enter.



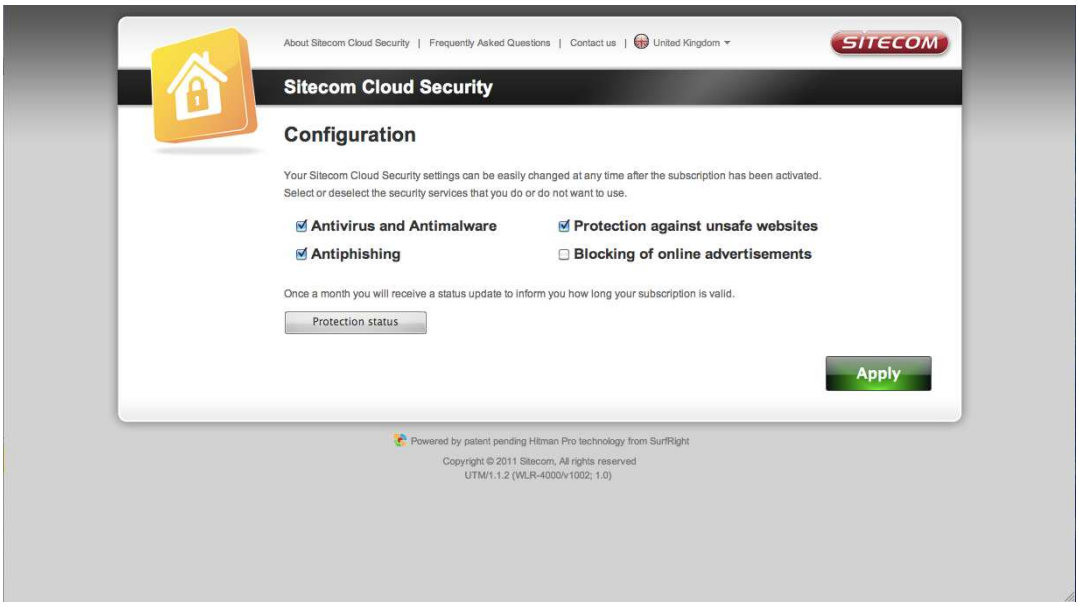
If you still wish to visit this webpage click on ‘proceed anyway’. Alternatively click ‘Back to Safety’ so that your security will not be breached.

If you wish to change your security options or to extend your subscription at any time, open http://www.sitecomcloudsecurity.com from your web browser.

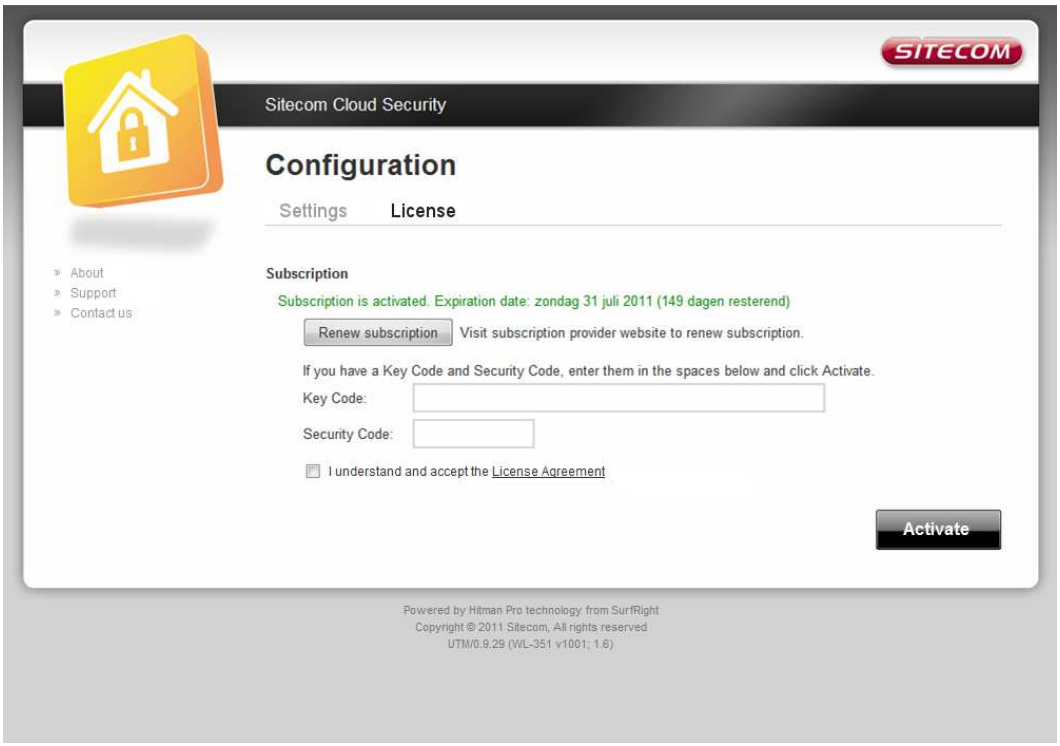
You will be asked for a username and password. These can be found on the backlabel on the bottom of your Sitecom router or modem.



If the login succeeded you can click on 'Settings' to change your security options.



Or click 'License' to renew your subscription.



If you wish to disable to Sitecom cloud security at any time, open the webpage of your Sitecom product and log in with the supplied credentials (these can be found on the back label on the bottom of your Sitecom device).

Go to Toolbox and select "Sitecom Cloud Security".

Click the "Disable" radio button and click 'Apply' for the settings to take effect.

Password change options

You can change the password required to log into the broadband router's system web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

Current Password Fill in the current password to allow changing to a new password.

New Password Enter your new password.

Confirmed Password Enter your new password again for verification purposes.

Click <**Apply**> at the bottom of the screen to save the above configurations

Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

Set Time Zone Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address You can set an NTP server address.

Enable Daylight Savings The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).

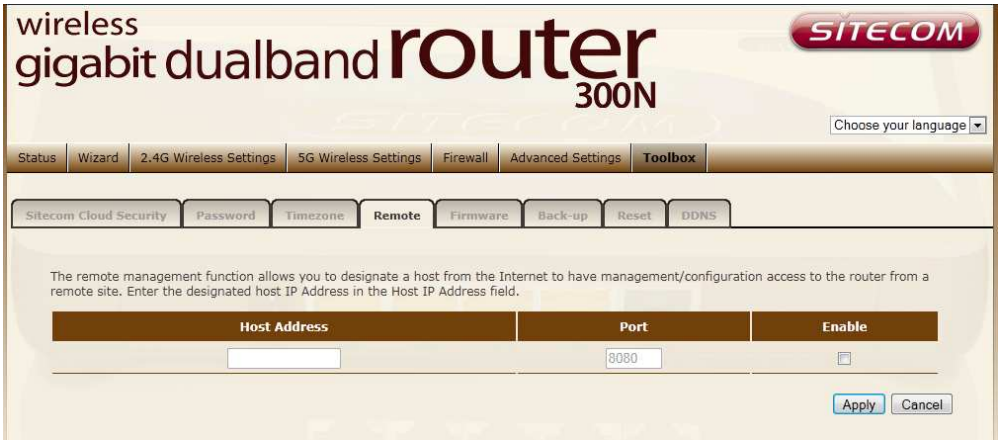
Start Daylight Savings Time Select the period in which you wish to start daylight Savings Time

End Daylight Savings Time Select the period in which you wish to end daylight Savings Time

Click <**Apply**> at the bottom of the screen to save the above configurations

Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.



Host Address This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

Port The port number of the remote management web interface.

Enabled Select "**Enabled**" to enable the remote management function.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Firmware Upgrade

Firmware Upgrade This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process

Backup Settings

The Backup screen allows you to save (Backup) the router's current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).

Use the "Backup" tool to save the Broadband router current configuration to a file named "**config.bin**" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system.

DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

Enable/Disable Enable or disable the DDNS function of this router

Provider Select a DDNS service provider

Domain name Fill in your static domain name that uses DDNS

Account/E-mail The account that your DDNS service provider assigned to you

Password/**Key** The password you set for the DDNS service account above

Click <**Apply**> at the bottom of the screen to save the above configurations.

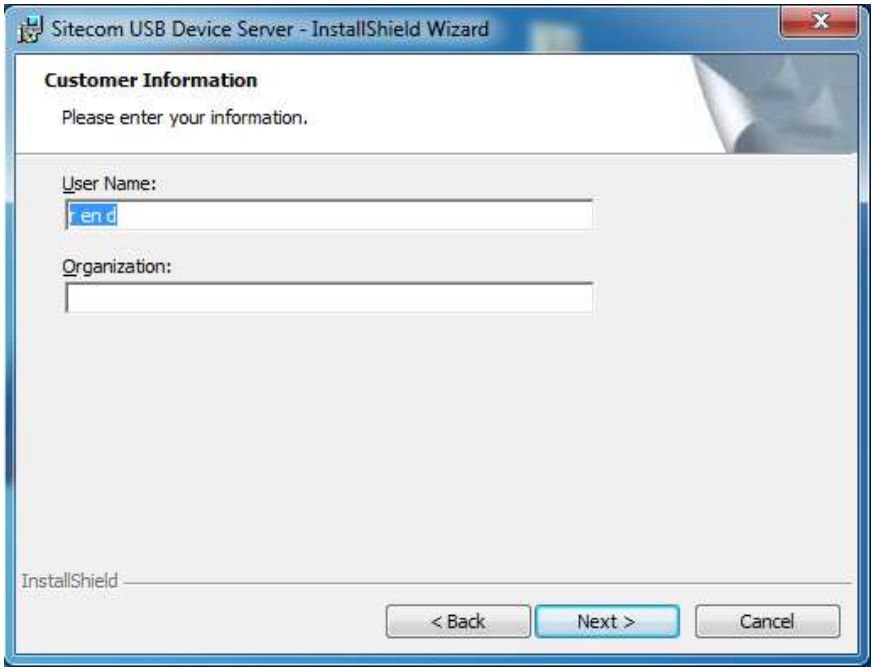
17 Addendum: USB Port Control Center

The netUSB functionality of your router requires additional software to work with your computer. The following will describe how the software can be installed and used.

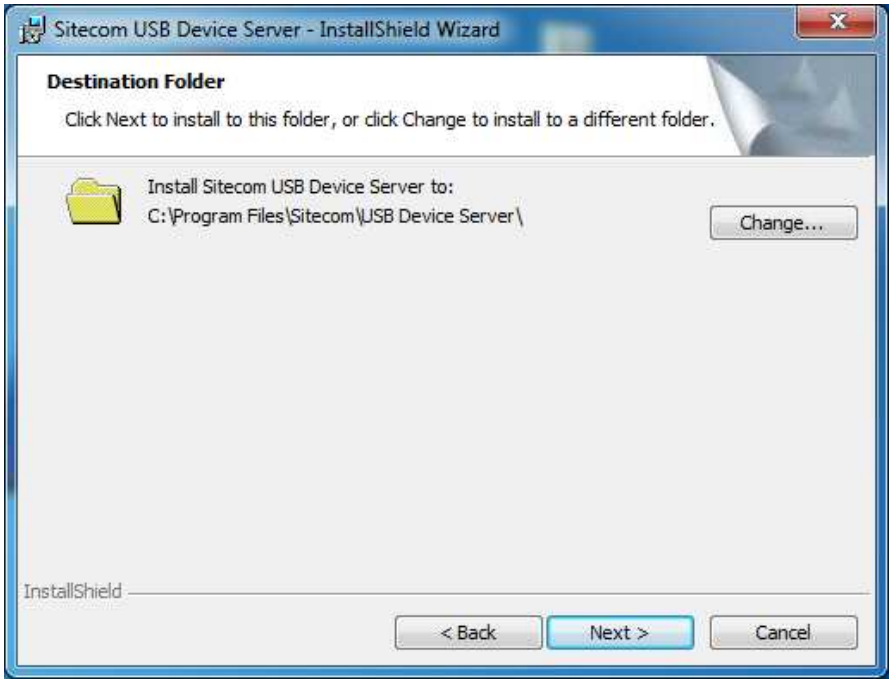
Windows

Insert the cd-rom that was included with your router and select install utility from the cd-menu.
The software will inform you about what will be installed.

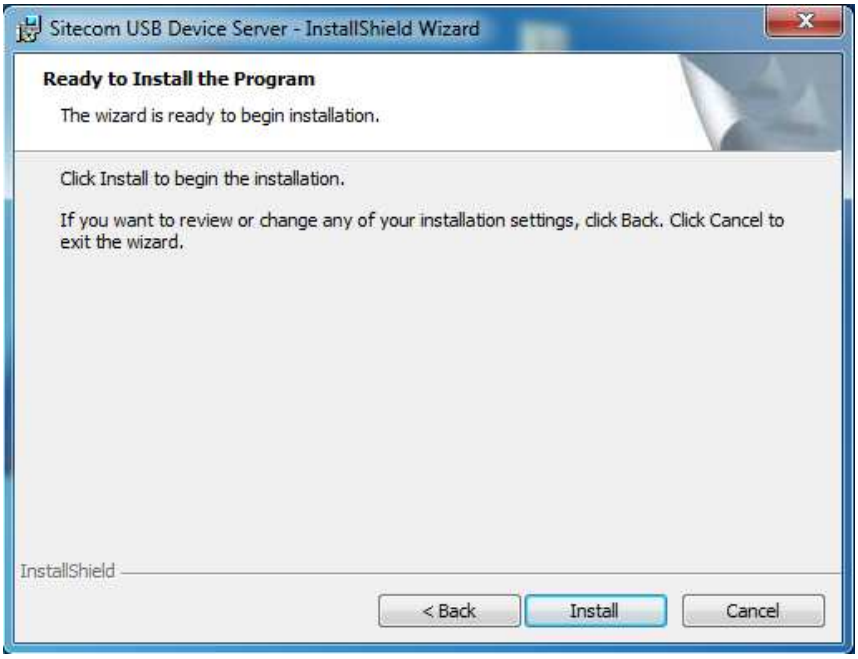
Click **Next** to continue the installation.



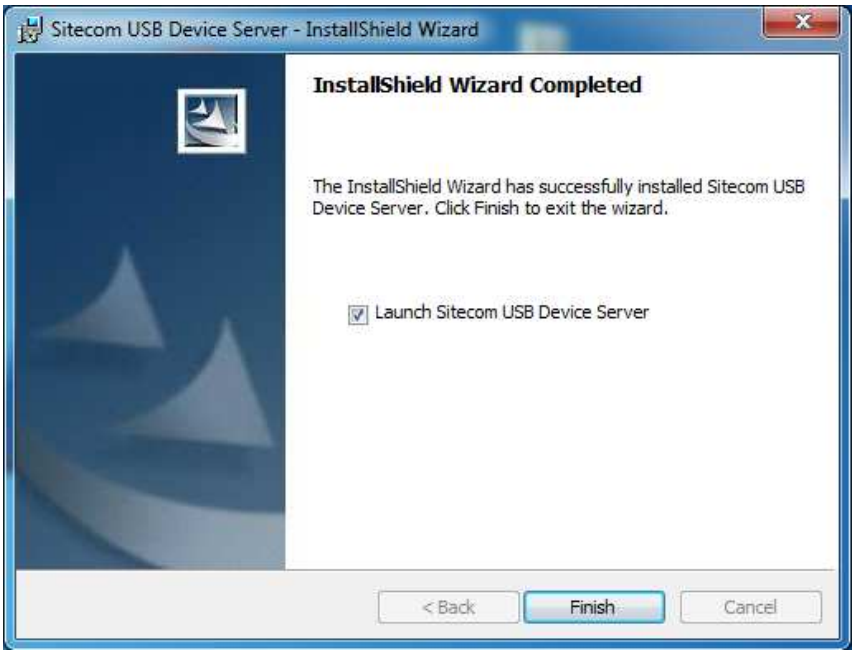
Enter your username and organization if applicable and click **Next** to continue.



Choose a folder where the software should be installed or keep it to default and click **Next** to continue.



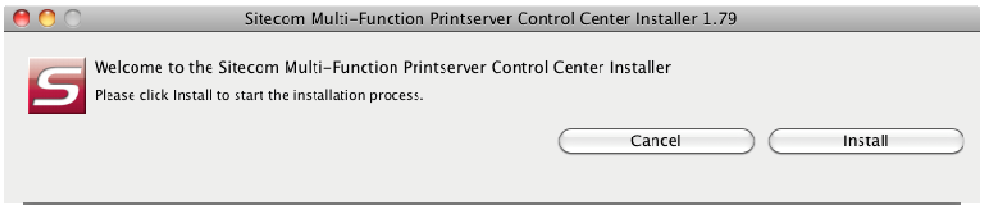
The software is now ready to be installed, Click **Install** to continue.



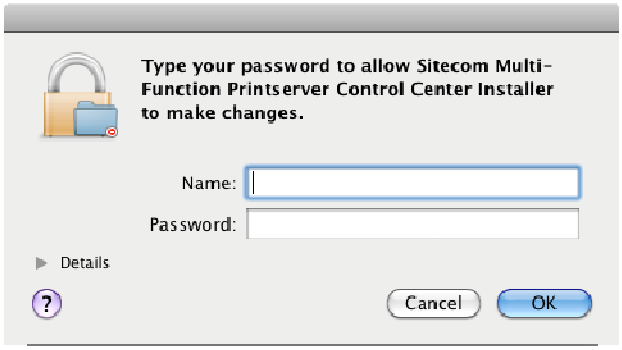
Once the installation is finished the software will inform you. If **Launch Sitecom USB Device Server is** checked the software will automatically be launched after you clicked **Finish.**

Mac

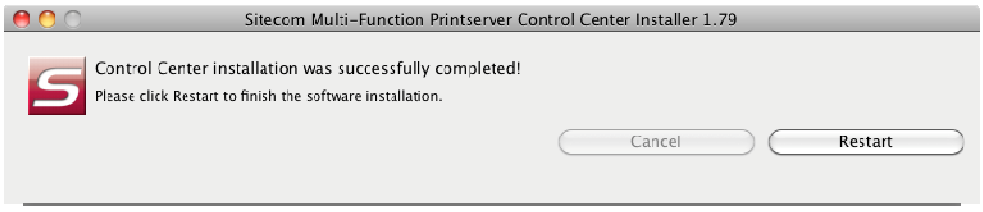
Insert the cd-rom that was included with your router and select install utility from the cd-menu.



Click **Install** to continue installation.



Enter your Mac username and password and click **OK** to continue.



Once the installation is finished the software will inform you and requires to restart the system.

Connect & Disconnect

"NetUSB" allows you to use USB printers when they're actually connected to the Sitecom USB server.

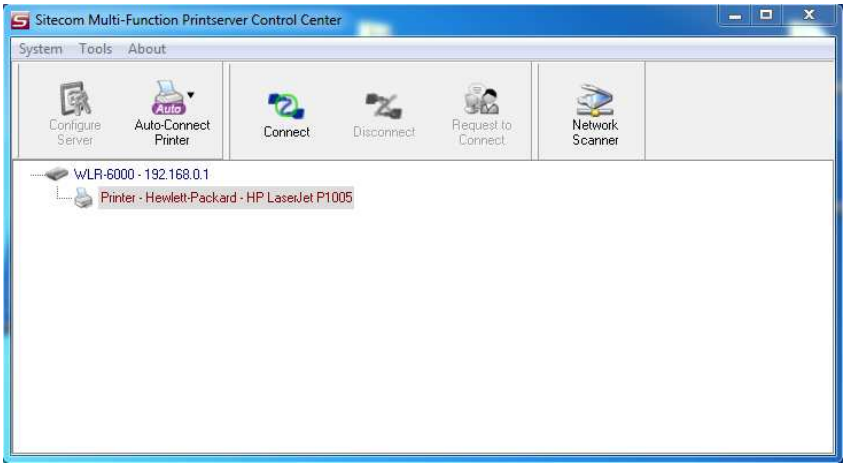
The "connect" operation is a software operation that simulates an actual USB device plug-in. Therefore, when you do a "connect" operation in the Control Center, the PC can detect a USB device's plug-in, although actually you do not plug in any USB device to your PC. Similarly, the "disconnect" operation is a software operation that simulates the disconnection of the USB device.

Note
If a USB device is "connected" by a PC, we say that PC has the ownership of the USB device. Only one PC can get the ownership of a USB device at the same time.

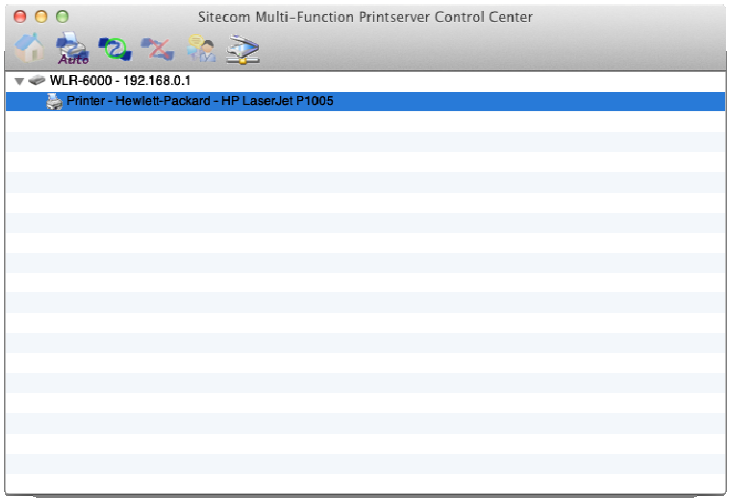
NetUSB installation

The steps to do installation for USB devices, like MFPs:

- Make sure the Sitecom WLR-6001 is turned on.
- Connect the USB device to Sitecom WLR-6001.
- Run the Control Center. In the "USB MFP Server List" window, you can see the host names and IP addresses all of the Sitecom servers (in blue) on the network, as shown below.

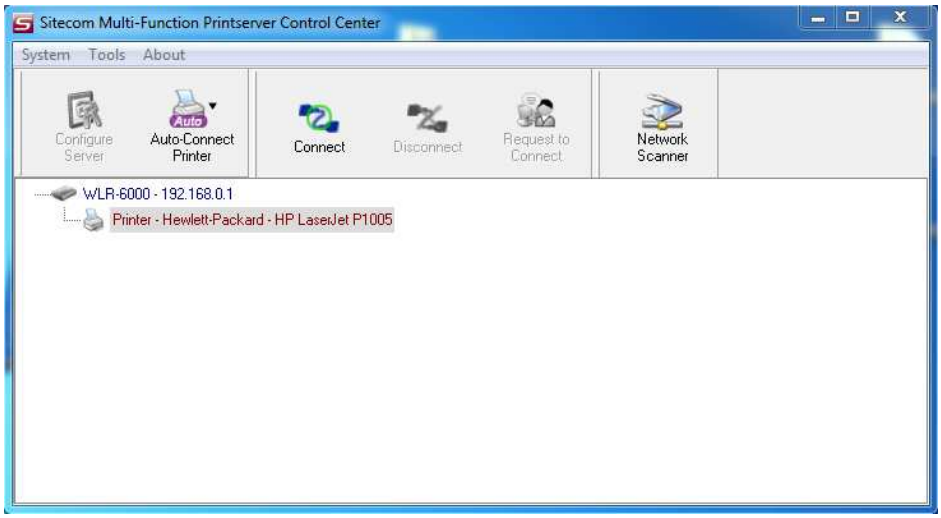


Windows



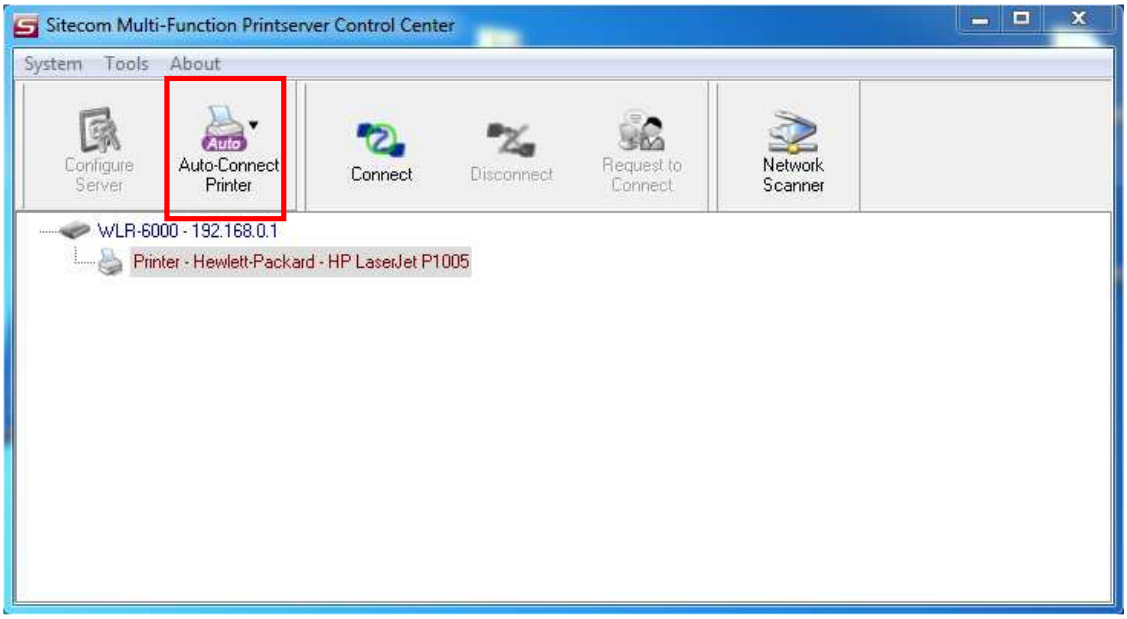
Mac OS

- Click the server. Then all USB devices attached to the server will be shown.

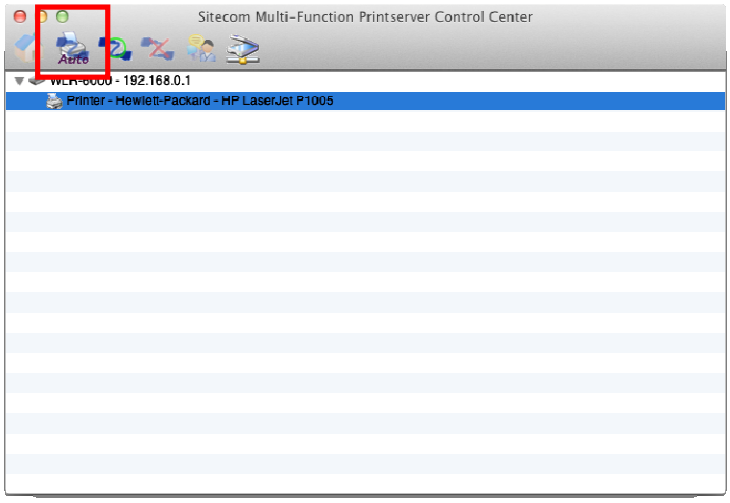


- Please follow the user manual of the USB device to install its driver. For example, you may put the driver CD of the USB device in the CDROM player to install the driver.

- When you are asked to plug in the USB device into PC's USB port, click the desired USB device in the Control Center and then click the "Auto-Connect Printer" button to do the connect operation and get the ownership of the USB device. The computer name of the device owner will be shown at the end of the device.



Windows



Mac OS

- PC will automatically detect that the USB device is plugged-in. On the right side of the Windows Task Bar, you can see the information of the new device. Continue to follow the user manual of the USB device to do the rest jobs of installation, until the driver installation has finished.

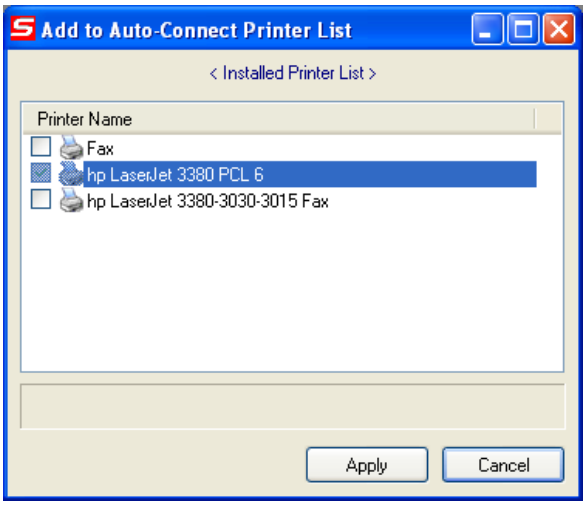
After the installation, you can see the newly created devices on the PC. If the USB device is a MFP, you can see a new printer and a new scanner from the "Control Panel".

NetUSB Printing using Auto-Connect Printer

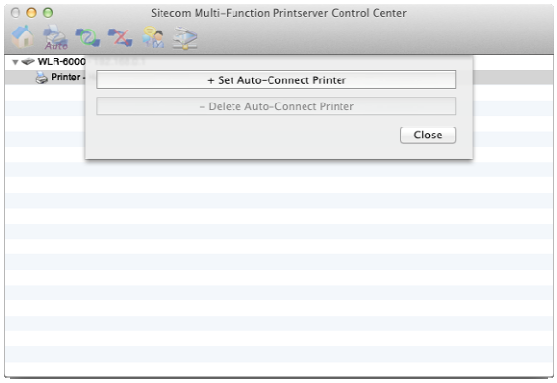
After the driver is installed, you can see a newly created printer in the Control Panel. Follow the steps below to perform NetUSB printing.

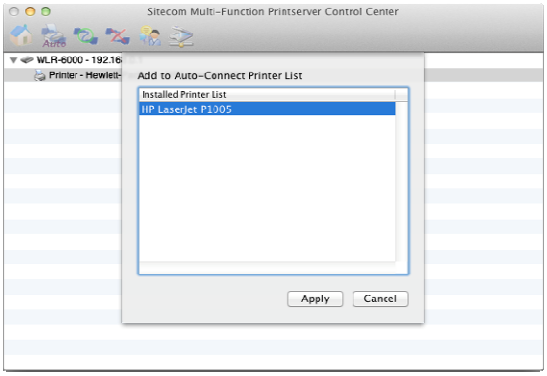
- In the Control Center, click the MFP server that has the desired printer (or MFP) attached.
- Click the desired printer (or MFP).
- Click the "Auto Connect Printer" button and choose "Set Auto-Connect Printer". The following figure will appear.

- Choose the desired printer. The desired printer must be the Windows printer (this is a logical printer) that matches the printer attached on the MFP server (this is a physical printer). Then click the "Apply" button.



Windows

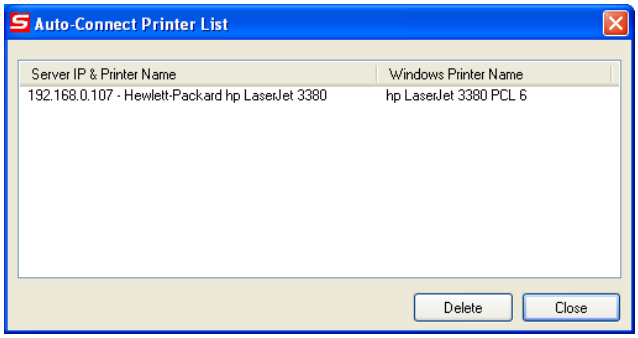




Mac OS

- Then, the printer will be marked as an "Auto-Connected Printer" in red.

- If you choose "Auto-Connected Printer List" in the "Tools" menu, you can see a newly created item that describes the association between the Windows printer and the physical printer on the server.



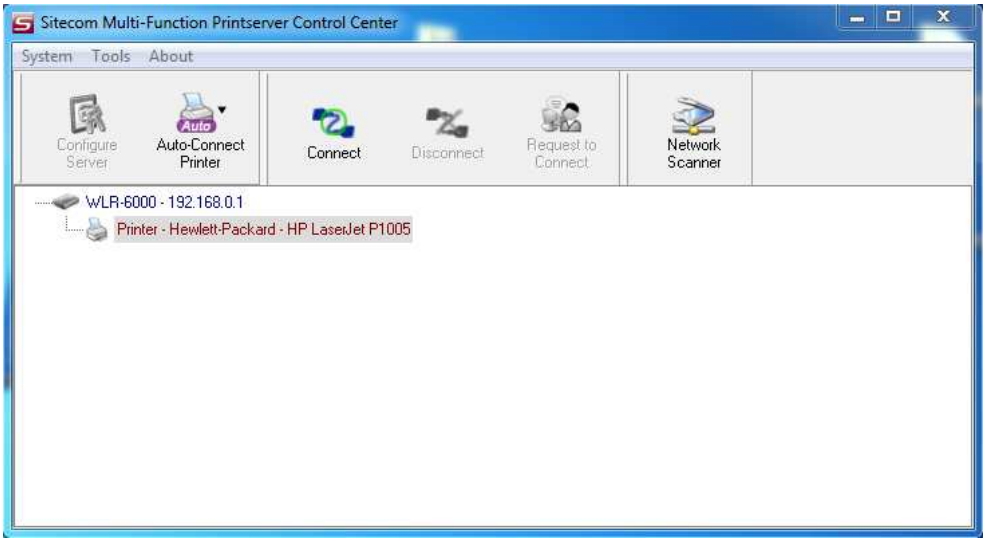
- Then try to issue a print job to the desired printer. You will see the Control Center will automatically do a connect operation and, once the print job finished, it will hold the connection. However, the connection will be released immediately when another user do the printing afterward. At the same time, the printer is automatically disconnected with your PC.

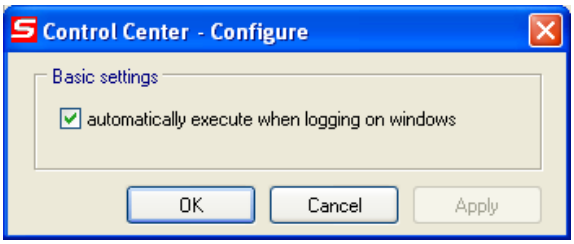
- When you do a print job again. The control center will automatically do a connecting operation on printing again. This is so-called "Auto Connect / Disconnect" operation.

Note

Under the "Auto-Connected Printer" setting, it is **NOT necessary to manually press the "Connect" button** when printing. If you press the "Connect" button for printing, please make sure to **click "Disconnect" button after you finish the printing**. Otherwise, other users cannot print properly. It is because you are the only ownership of the connected printer.

- You can make the Control Center be run automatically after you login Windows. To do this, you choose the "Configuration" item in the "Tools" menu. The following window will appear. Click on the check box and then on the "OK" button. This feature is enabled by default.

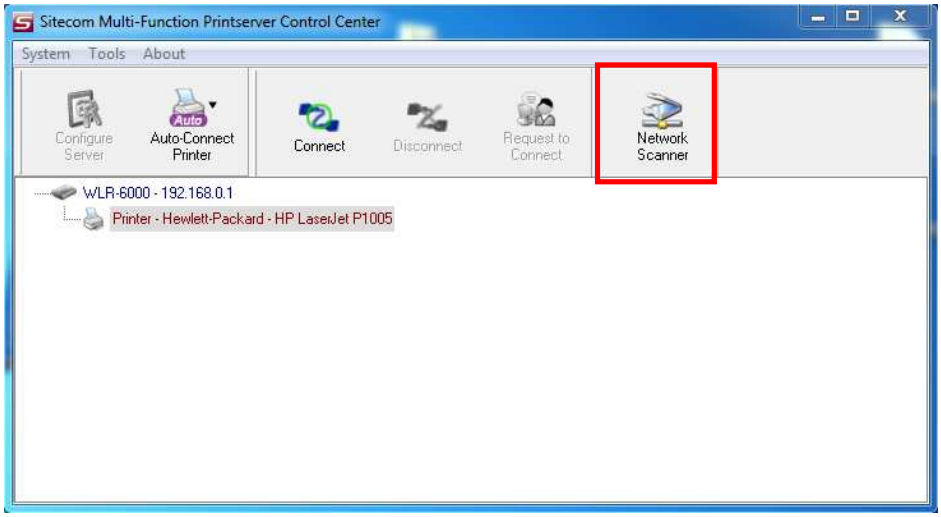




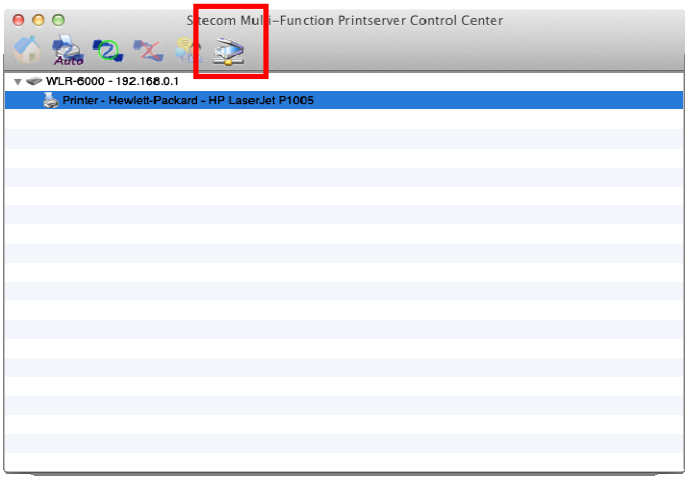
- If you would like to break the association between the Windows printer and the physical printer, just highlight the association and click the "Delete" button in the "Auto-Connected Printer List".

NetUSB Scanning using Network Scanning

- In the Control Center, click the MFP server that has the desired MFP attached.
- Click the desired MFP.
- Click the "Network Scanner" button.

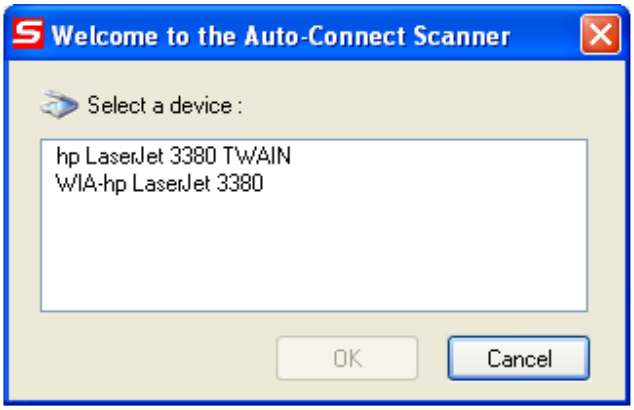


Windows

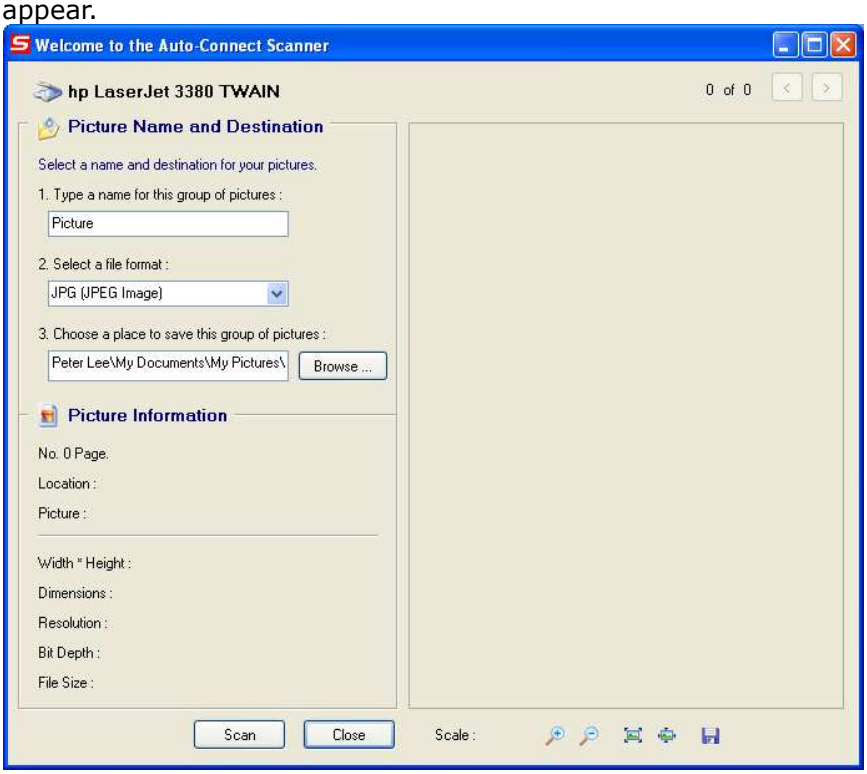


Mac OS

- Then you can see that the Control Center will automatically do a "connect" operation. The following window will appear.



- Choose one of TWAIN or WIA item. Click "OK". The following window will appear.



- Follow the usual steps to do scanning.

Parts of the firmware of the WLR-6001v1001 Wireless Broadband Router are subject to the GNU general public license.

Appendix A: Licensing Information

This product includes third-party software licensed under the terms of the GNU General Public License.. You can modify or redistribute this free software under the terms of the GNU General Public License. Please see Appendix B for the exact terms and conditions of this license.

Specifically, the following part of this product is subject to the GNU GPL:

#	Package name	Source
1	Linux v2.6.21	www.kernel.org
2	busybox v1.7.5	http://www.busybox.net/
3	termcap v1.3.1	ftp://ftp.gnu.org/gnu/termcap
4	libupnp v1.6.0	http://pupnp.sourceforge.net/
5	pcre v6.x	http://www.pcre.org/
6	popt v1.7	http://freecode.com/projects/popt
7	dnsmasq v2.39	http://thekelleys.org.uk/dnsmasq/doc.html
8	iproute2 v2.6.16	http://www.linuxfoundation.org/en/Net:Iproute2
9	rp-pppoe v3.8	http://www.roaringpenguin.com/products/pppoe
10	iptables v1.3.8	http://www.netfilter.org/projects/iptables/index.html
11	wget-1.11.x	http://www.gnu.org/software/wget/
12	linuxigd v1.0	http://linux-igd.sourceforge.net/index.php
13	wireless_tools v28	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
14	updatedd-2.6	http://freecode.com/projects/updatedd
15	igmpproxy v0.1-beta2	http://sourceforge.net/projects/igmpproxy
16	pptp-client v1.7.1	http://pptpclient.sourceforge.net/
17	accel-pptp/pppd-plugin v0.8.3-rc5	http://accel-pptp.sourceforge.net/
18	ppp v2.4.3	http://ppp.samba.org/
19	udhcp v0.9.9-pre	http://sources.busybox.net/index.py/trunk/udhcp-web/index.html?revision=9967
20	ez-ipupdate v3.0.11b8	http://ez-ipupdate.com
21	uboot v1.1.4	http://www.denx.de/wiki/U-Boot
22	gcc v4.3.4	http://gcc.gnu.org/
23	uclibc v0.9.29	http://www.uclibc.org
24	zlib v1.2.3	http://www.zlib.net/
25	mtd-utils v1.2	http://git.infradead.org
26	openl2tp-1.x	http://www.openl2tp.org/
27	rpcbind-0.2.x	http://rpcbind.sourceforge.net/
28	ippool-1.3	http://sourceforge.net/projects/openl2tp/files/ippool/
29	openswan-2.6.2x	https://www.openswan.org/projects/openswan
30	gmp-4.3.x	http://gmplib.org/
31	libtirpc-0.2.x	http://sourceforge.net/projects/libtirpc/
32	libreadline v5.2	http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html

Availability of source code

Sitecom Europe BV has made available the full source code of the GPL licensed software, including any scripts to control the compilation and installation of the object code on the CD-ROM that's shipped with this product.

No Warranty

The free software included in this product is distributed in the hope that it will be useful, but WITHOUT ANY LIABILITY OF OR ANY WARRANTY FROM THE LICENSOR.

Appendix B: GNU GENERAL PUBLIC LICENSE

Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights. We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0.
This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
1.
You may copy and distribute verbatim copies of the Program's source code as you receive it, in

any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2.
You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3.
You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.
4.
You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5.
You are not required to accept this License, since you have not signed it. However, nothing else

grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7.
If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8.
If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9.
The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10.
If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11.
BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,

INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Sitecom Europe BV

EC Declaration of Conformity

We
Sitecom Europe BV
Linatebaan 101
3045 AH Rotterdam
The Netherlands

Hereby declare under our sole responsibility that the Sitecom product:

Product number: **WLR-6001 v1 001**
Product description: **Wireless Gigabit VPN Router N750 X6**

To which this declaration relates is in conformity with the requirements of the following standards:

CE/LVD
- EN 60950-1: 2006+A11 (2009)

CE/EMC
- EN 301 489-1 V1.8.1
- EN 301 489-17 V2.1.1

RADIO SPECTRUM
- EN 300 328 V1.7.1 2006-10
- EN 50385 2002
- EN 301 893 V1.5.1.

This certifies that the following designated Sitecom product:

Product description: Wireless Gigabit VPN Router N750 X6
Product No.: WLR-6001 v1 001

Complies with the requirements of the following directives and carries the CE marking accordingly:
R&TTE Directive 99/5/EC, EMC directive 2004/95/EC and Low Voltage Directive 2006/95/EC.
This declaration is the responsibility of the manufacturer / importer:

Sitecom Europe B.V.
Rotterdam, 11 June 2012

P. Schoonenberg,

CEO

SITECOM

(UK) CE COMPLIANCE

Hereby Sitecom Europe BV declares that this product is in accordance with essential requirements and other relevant terms of the European regulation 1999/5/EC.

(FR) CONFORMITE CE

Par la présente Sitecom Europe BV, déclare que l'appareil est conforme aux exigences essentielles et aux dispositions pertinentes de la Directive Européenne 1999/5/EC.

(DE) CE-CONFORMITAT

Hiermit erklärt Sitecom Europe BV, dass dieses Produkt die erforderlichen Voraussetzungen und andere relevante Konditionen der europäischen Richtlinie 1999/5/EC erfüllt.

(IT) CONFORMITA ALLE NORME CE

Con la presente Sitecom Europe BV dichiara che questo prodotto è conforme ai requisiti essenziali e agli altri termini rilevanti della Direttiva Europea 1999/5/EC.

(NL) CE GOEDKEURING

Hierbij verklaart Sitecom Europe BV dat dit product in overeenstemming is met de essentiële eisen en andere relevante bepalingen van Europese Richtlijn 1999/5/EC.

(ES) CONFORMIDAD CON LA CE

Por la presente Sitecom Europe BV declara que este producto cumple con los requisitos esenciales y las otras provisiones relevantes de la Directiva Europea 1999/5/EC.

(PT) CONFORMIDADE CE

Pela presente a Sitecom Europe BV declara que este produto está em conformidade com os requisitos essenciais e outras condições relevantes da regulamentação Europeia 1999/5/EC.

(SE) CE-FÖRSÄKRAN

Härmed försäkrar Sitecom Europe BV att denna produkt uppfyller de nödvändiga kraven och andra relevanta villkor EU-direktivet 1999/5/EC.

(DK) OVERENSSTEMMELSESERKLÆRING

Sitecom Europe BV bekræfter hermed, at dette produkt er i overensstemmelse med væsentlige krav og andre betingelser i henhold til Rådets direktiv 1999/5/EC.

(NO) CE-OVERENSSTEMMELSE

Sitecom Europe BV erklærer herved at dette produktet er i overensstemmelse med de avgjørende kravene og andre relevante vilkår i den europeiske forskriften 1999/5/EC.

(FI) CE-HYVÄKSYNTÄ

Täten Sitecom Europe BV ilmoittaa, että tämä tuote on yhdenmukainen direktiivin 1999/5/EC olennaisten vaatimusten ja muiden asiaankuuluvien sopimusehtojen kanssa.

(RU) СООТВЕТСТВИЕ ТРЕБОВАНИЯМ CE

Настоящим компания Sitecom Europe BV заявляет, что ее продукция соответствует основным требованиям и условиям Европейской Директивы 1999/5/EC.

(PL) CERTYFIKAT ZGODNOSCI CE

Sitecom Europe BV niniejszym oświadcza, że ten produkt spełnia wszelkie niezbędne wymogi, a także inne istotne warunki dyrektywy europejskiej 1999/5/WE.

(GR) ΣΥΜΜΟΡΦΩΣΗ ΜΕ CE

Η Sitecom Europe BV δηλώνει, διά του παρόντος, ότι αυτό το προϊόν συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τους λοιπούς όρους του ευρωπαϊκού κανονισμού 1999/5/EC.

CE

FOR USE IN:			
NL	BE	LU	FR
ES	CH	PT	UK
DE	AT	SE	DK
IT	NO	SF	IE