D-Link *Air*Plus Xtreme G™ DWL-G510

High-Speed 802.11g
Wireless PCI Adapter

Manual

Rev. B1

D-Link

Building Networks for People

Contents

Package Contents

Contents of Package:

- **D-Link *Air*Plus Xtreme G™ DWL-G510**
  High-Speed 2.4 GHz/802.11g Wireless PCI Adapter
- Manual and Drivers on CD
- Quick Installation Guide

If any of the above items are missing, please contact your reseller.

System Requirements:

- A computer or laptop with an available 32-bit PCI slot
- Windows XP/2000/Me/98SE
- At least 32 MB of memory and a 300 MHz processor
- An **802.11g** or **802.11b** *Access Point (for Infrastructure mode),* or another **802.11g** or **802.11b** wireless adapter (for Ad-Hoc, Peer-to-Peer networking mode).

Introduction

The D-Link *Air*Plus *X*treme *G*™ DWL-G510 Wireless PCI Adapter is an 802.11g high-performance, wireless adapter that supports high-speed wireless networking at home, at work or in public places.

Unlike most network cards, the DWL-G510 provides data transfers at up to 54 Mbps. The 802.11g standard is backwards compatible with 802.11b products.

The DWL-G510 has the newest, strongest, and most advanced security features available today. When used with other 802.11 WPA (Wi-Fi Protected Access) and 802.1x compatible products in a network with a RADIUS server, the security features include:

WPA: Wi-Fi Protected Access which authorizes and identifies users based on a secret key that changes automatically at regular intervals. **WPA** uses **TKIP** (**Temporal Key Integrity Protocol**) to change the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This ensures much greater security than the standard WEP security. (By contrast, the older WEP encryption required the keys to be changed manually.)

802.1x: Authentication which is a first line of defense against intrusion. In the authentication process, the Authentication Server* verifies the identity of the client attempting to connect to the network. Unfamiliar clients would be denied access.

For home users that will not incorporate a RADIUS server in their network, the security for the DWL-G510, used in conjunction with other WPA-compatible 802.11 products, will still be much stronger than ever before. Utilizing the **Pre Shared Key mode** of WPA, the DWL-G510 will obtain a new security key every time it connects to the 802.11 network. You only need to input your encryption information once in the configuration menu. No longer will you have to manually input a new WEP key frequently to ensure security. With the DWL-G510, you will automatically receive a new key every time you connect, vastly increasing the safety of your communication.

** Not all servers can provide Authentication.*

Features & Benefits

- **Five times faster** - achieve data transfer speeds up to 54 Mbps; up to 5x faster than conventional 802.11b networks, when used with other 802.11g devices
- **Fully compliant with the 802.11b** standard and interoperable with all existing 802.11b-compliant and 802.11g compliant devices
- **Provides a simple and inexpensive way** to connect your desktop computer to a wireless network at home, at the office, or in public places
- **Quick and Easy Installation**- The DWL-G510 installs quickly and easily into a standard PCI 2.2 slot in a desktop computer. By following the simple steps outlined in the *Quick Installation Guide*, you can connect to an available wireless network in a matter of seconds
- **High Performance 32-bit PCI** - The high capacity PCI interface utilized by the DWL-G510 ensures optimal performance in transmitting a wireless signal within the desktop computer. By utilizing a standard PCI 2.2 interface, the DWL-G510 ensures a wide range of compatibility with motherboards used by PC manufacturers
- **Operates in the 2.4GHz** frequency range
- **Maximum reliability**, throughput and connectivity with automatic data rate switching
- **Supports Infrastructure** networks via an access point and Peer-to-Peer communication in Ad-Hoc mode
- **User-friendly** configuration and diagnostic utilities
- **Provides a measure of security** for the information transmitted over a wireless network with high data encryption at 64-, 128-, and 152-bit WEP
- **Stronger Security than ever before with WPA -** Wi-Fi Protected Access authorizes and identifies users based on a secret key that changes automatically at regular intervals, for example:
    - **TKIP** (Temporal Key Integrity Protocol), in conjunction with a RADIUS server, changes the temporal key every 10,000 packets, ensuring greater security
    - **Pre-Shared Key** mode means that the home user, without a RADIUS server, will obtain a new security key every time he or she connects to the network, vastly improving the safety of communications on the network
- **Extra Protection** - 802.1x **Authentication** in conjunction with the RADIUS server verifies the identity of wireless clients wishing to gain access to the WLAN

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. D-Link wireless products will allow you access to the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking brings.

A Wireless Local Area Network (WLAN) is a computer network that transmits and receives data with radio signals instead of wires. WLANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

People use WLAN technology for many different purposes:

Mobility - Productivity increases when people have access to data in any location within the operating range of the WLAN. Management decisions based on real-time information can significantly improve worker efficiency.

Low Implementation Costs – WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLANs ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation and Network Expansion - Installing a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Wireless technology allows the network to go where wires cannot go - even outside the home or office.

Scalability – WLANs can be configured in a variety of ways to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to larger infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Inexpensive Solution - Wireless network devices are as competitively priced as conventional Ethernet network devices.

The DWL-G510 is compatible with 802.11g and 802.11b wireless products, which include:

- **D-Link *Air* DWL-650,D-Link *Air*Plus DWL-650+,**
  D-Link *Air*Plus Xtreme G™ DWL-G650
  2.4GHz Wireless Cardbus Adapter used with laptop computers
- **D-Link *Air* DWL-520, D-Link *Air*Plus DWL-520+**
  2.4GHz Wireless PCI cards used with desktop computers
- **D-Link *Air*Plus DWL-900AP+, D-Link *Air*Plus Xtreme G™ DWL-2000AP**
  2.4GHz Wireless Access Points
- **D-Link *Air*Plus DI-614+, DI-714P+**
  2.4GHz Wireless Routers

Standards-Based Technology

The DWL-G510 Wireless PCI Adapter utilizes the new **802.11g** standard.

The IEEE **802.11g** standard is an extension of the 802.11b standard. It increases the data rate up to 54 Mbps within the 2.4GHz band, utilizing **OFDM technology.**

This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing **OFDM** (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) technology. **OFDM** works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. **OFDM** reduces the amount of **crosstalk** (interference) in signal transmissions. The D-Link DWL-G510 will automatically sense the best possible connection speed to ensure the greatest speed and range possible.

802.11g offers the most advanced network security features available today, including: *WPA , 802.1x, TKIP, AES and Pre-Shared Key mode*. These security features are explained in more detail in the *Introduction* and the *Features* section of this manual.

The DWL-G510 is backwards compatible with 802.11b devices. This means that if you have an existing 802.11b network, the devices in that network will be compatible with 802.11g devices at speeds up to 11Mbps in the 2.4GHz range.

Installation Considerations

The D-Link *Air*Plus Xtreme G™ DWL-G510 lets you access your network using a wireless connection from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the DWL-G510 and other network devices to a minimum - each wall or ceiling can reduce your DWL-G510's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

Getting Started

With its default settings, the DWL-G510, when activated, will connect with other D-Link *Air*Plus Xtreme G™ products, right out of the box.

There are basically two modes of networking:

- **Infrastructure** – using an Access Point or Router, such as the DI-624
- **Ad-Hoc** – directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DWL-G510 wireless network adapters

On the following pages we will show you an example of an **Infrastructure Network** and an **Ad-Hoc Network**.

An **Infrastructure** network contains an Access Point or Router. The **Infrastructure Network** example shown on the following page contains the following D-Link network devices (your existing network may be comprised of other devices):

- A wireless Router - **D-Link *Air*Plus Xtreme G™ DI-624**
- A desktop computer with a wireless adapter - **D-Link *Air*Plus *Xtreme G*™ DWL-G510, D-Link Air DWL-520,** or **D-Link AirPlus DWL-520+** (**D-Link *Air*** devices have speeds up to 11Mbps)
- A Cable modem - **D-Link DCM-201**

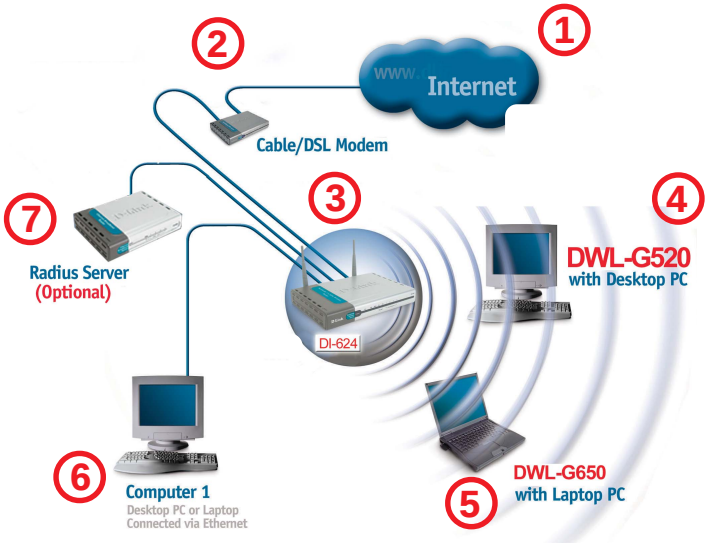
LEDs

LED stands for **L**ight-**E**mitting **D**iode.

Power: Solid **green** light indicates connection to the network

Network: Blinking **green** light indicates activity on the network

Setting up a Wireless Infrastructure Network



*Please remember that **D-Link AirPlus Xtreme G**™ wireless devices are pre-configured to connect together, right out of the box, with their default settings.*

For a typical wireless setup at home (as shown above), please do the following:

1. You will need broadband Internet access (a Cable or DSL-subscriber line into your home or office).
2. Consult with your Cable or DSL provider for proper installation of the modem.
3. Connect the Cable or DSL modem to your broadband router (*see the **Quick Installation Guide** included with your router.*)
4. Install the D-Link *AirPlus Xtreme G*™ DWL-G510 Wireless PCI Adapter into an available PCI slot on your desktop computer. *(See the **Quick Installation Guide** included with the DWL-G510.)*
5. Install the D-Link *AirPlus Xtreme G*™ DWL-G650 Wireless PC Card Adapter into a laptop computer. (*See the **Quick Installation Guide** included with the DWL-G650.*)
6. If you wish, you may connect a computer that is equipped with an Ethernet network adapter (such as a DFE-530TX+) to the router also.
7. A RADIUS Server is optional. Connect a RADIUS Server to your network to use all the features of WPA. (Without a RADIUS Server you can still use the *WPA Pre-Shared Key* mode.) RADIUS Authentication can also be provided by another service provider over the Internet and remote to your network site.

1. Install the DWL-G510 into the desktop computer.
*(See the **Quick Installation Guide** included with the product for installation instructions.)*

2. Install the DWL-G650 Wireless PC Card Adapter into a laptop computer.
*(See the **Quick Installation Guide** included with the product.)*

3. Set the wireless configuration for the adapters to Ad-Hoc mode, set the adapters to the same channel, and assign an IP Address to each computer on the Ad-Hoc network. *(See Box below).*

IP Address

When assigning IP Addresses to the computers on the network, please remember that the **IP Address for each computer must be in the same IP Address range as all the computers in the network**, and the subnet mask must be exactly the same for all the computers in the network.

For example: If the first computer is assigned an IP Address of 192.168.0.2 with a Subnet Mask of 255.255.255.0, then the second computer can be assigned an IP Address of 192.168.0.3 with a Subnet Mask of 255.255.255.0, etc.

IMPORTANT: If computers or other devices are assigned the same IP Address, one or more of the devices may not be visible on the network.

Using the Configuration Utility

D-Link *AirPlus Xtreme G*™ DWL-G510 uses the **Configuration Utility** as the management software. The utility provides the user an easy interface to change any settings related to the wireless adapter. After you have completed the installation of the DWL-G510 (refer to the ***Quick Installation Guide*** that came with your purchase) whenever you start the computer, the **Configuration Utility** starts automatically and the system tray icon is loaded in the toolbar (see illustration below*.) Clicking on the utility icon will start the **Configuration Utility**. Another way to start the **Configuration Utility** is to click on **Start>Programs>D-Link *AirPlus* Xtreme G>D-Link *Air*Plus Xtreme G Utility.**

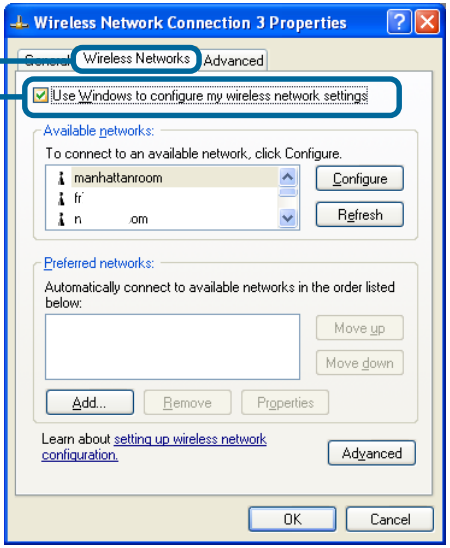
If you are using Windows XP, you can use either the Zero Configuration Utility or the D-Link Configuration Utility.

To use the D-Link Configuration Utility with XP, right-click on the Wireless network icon in the taskbar in the lower right-hand corner of your computer screen.

In the window that appears, select **View Available Wireless Networks** and click the **Advanced** button. The screen at right will appear.

Select the **Wireless Networks** tab.

Uncheck the box in the properties window that enables windows configuration.



After you have done this, you can then use the D-Link Configuration Utility with XP by clicking on the D-Link Configuration Utility icon.

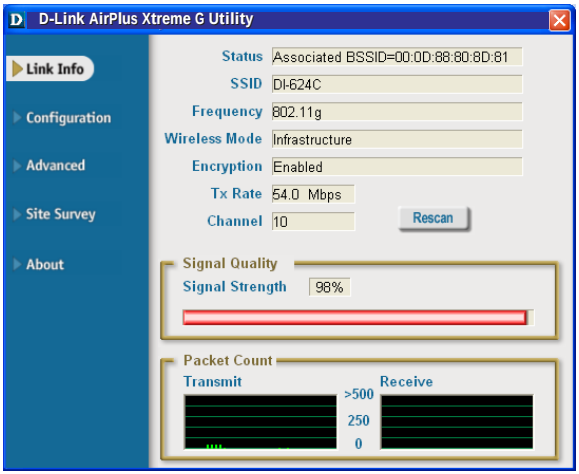
**Configuration Utility icon in the system tray*

If the icon does not display in the taskbar, then click on this icon on your desktop to open.

Using the Configuration Utility *(continued)*

After clicking on the Configuration Utility icon, the **Link Info** screen will display the settings for the DWL-G510:

Link Info



Status:

Displays the MAC Address of the Access Point or Router to which the DWL-G510 is associated

SSID:

The Service Set Identifier is the name assigned to the wireless network. The factory SSID setting is **default**.

Frequency:

802.11g indicates that the DWL-G510 is communicating in the 2.4GHz band.

Wireless Mode:

Either **Infrastructure** or **Ad-Hoc** will be displayed here. (Please see the *Getting Started* section in this manual for an explanation of these two modes.)

Encryption:

You can see if WEP (Wired Equivalent Privacy) is **Enabled** or **Disabled** here.

Tx Rate:

Tx Rate settings are automatically determined for an optimal speed up to a maximum of 54Mbps.

Channel:

The channel selection is automatically determined by the DWL-G510.

Signal Strength:

Displays the Link Quality for the DWL-G510 wireless connection to the Access Point. The Signal Strength represents the wireless signal between the Access Point and the DWL-G510. The percentage coincides with the graphical bar.

Packet Count:

Displays the statistics of the data packets that are transmitted and received.

Rescan Button:

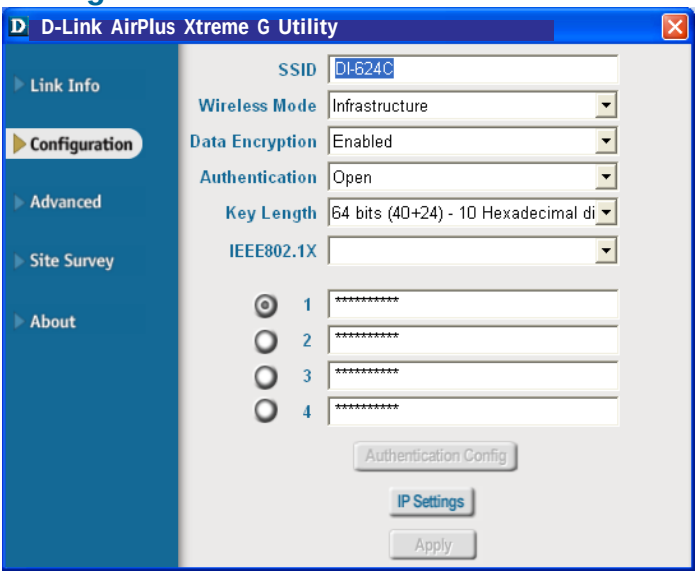
Rescans for the strongest signal in your environment and associates with that Access Point or Router.

Using the Configuration Utility *(continued)*

Configuration

After you have configured the network through the Site Survey section of the D-Link *Air*Plus Utility, you can make minor adjustments and check on settings in this **Configuration** screen.

*For a complete explanation of the configuration of a network, please refer to the **Site Survey** section in this chapter.*



SSID:

Service Set Identifier is a name that identifies a wireless network. Access Points and wireless devices attempting to connect to a specific WLAN (Wireless Local Area Network) must use the same SSID. The default setting is **default**.

Wireless Mode:

Click on the pull-down menu; select from the following options:

Infrastructure - connecting to the WLAN using an Access Point. (This is the **default** setting).

Ad-Hoc – wireless mode used when connecting directly to a computer equipped with a wireless adapter in a peer-to-peer environment.

Data Encryption:

Select **Enabled** or **Disabled.**

Authentication:

Choose one of the following modes:

Open Authentication – the DWL-G510 is visible to all devices on the network

Shared Authentication – allows communication only with other devices with identical WEP settings

WPA – Wi-Fi Protected Access which authorizes and identifies users based on a secret key that changes automatically at a regular interval. (A RADIUS Server is required for this mode.)

WPA-PSK - WPA Pre-Shared Key mode ensures that the DWL-G510 will obtain a new security key every time it connects to the 802.11 network. (A RADIUS Server is not required for this mode.)

Using the Configuration Utility *(continued)*

Key Length:
Select the key length and either ASCII or hexadecimal format.

IEEE 802.1x:
Authentication which is a first line of defense against intrusion. In the Authentication process the Authentication Server* verifies the identity of the client attempting to connect to the network. Unfamiliar clients are denied access.

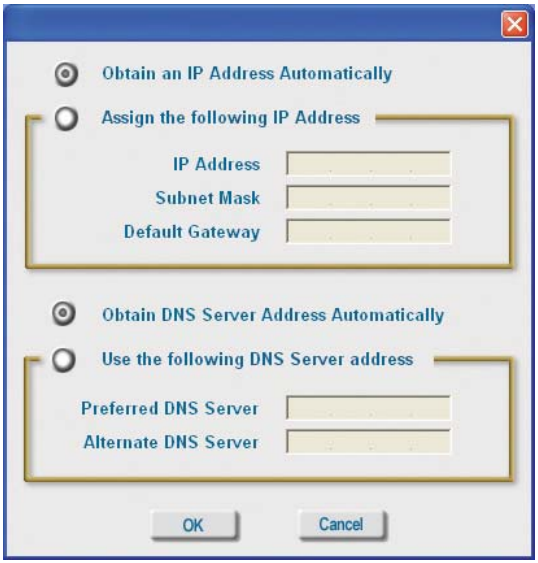
Keys 1-4:
Select the default key

Hexadecimal *digits consist of the numbers 0-9 and the letters A-F*

ASCII *(American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127*

IP Settings

When you click **IP Settings** in the Configuration window, this pop-up screen will appear. Configure the IP Settings in this window.



Click **Apply** to save changes.

*Not all servers can provide Authentication

Using the Configuration Utility *(continued)*

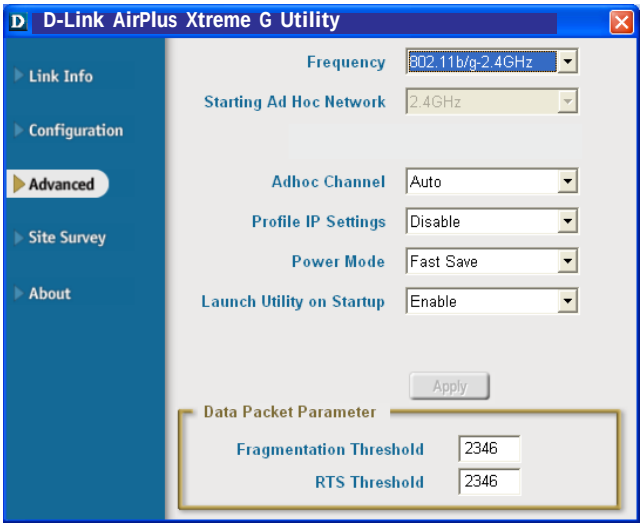
Frequency:
Select the Frequency

Starting Ad-Hoc Network:
Select the Ad-Hoc Network

Ad-Hoc Channel:
All devices in the Ad-Hoc network must be set to the same channel

Profile IP Settings:
You can **Enable** or **Disable** the *IP Settings* portion of your profile here. If you select **Disable** you will need to configure the IP Address information each time you connect to a network. If you select **Enable** you will maintain the same IP Address information each time you connect to a network.

Advanced



Power Mode:
Disable -this default setting consumes the most power
Enable - this setting consumes the least power.

Launch Utility on Startup:
Select **Enable** or **Disable**

Data Packet Parameter:
Set the *Fragmentation Threshold* and the *RTS Threshold*. Please see below.

Fragmentation Threshold:
This value should remain at its default setting of 2432. If you experience a high packet error rate, you may slightly increase your Fragmentation Threshold within the value range of 256 to 2432. Setting the Fragmentation Threshold too low may result in poor performance.

RTS Threshold:
This value should remain at its default setting of 2432. If inconsistent data flow is a problem, only a minor modification should be made.

Click **Apply** if you have made any changes

Using the Configuration Utility *(continued)*

Available Network:
The top section of the window displays the **Available Networks**. Scroll up and down the list and highlight the network to which you wish to connect. Click on the **Connect** button.

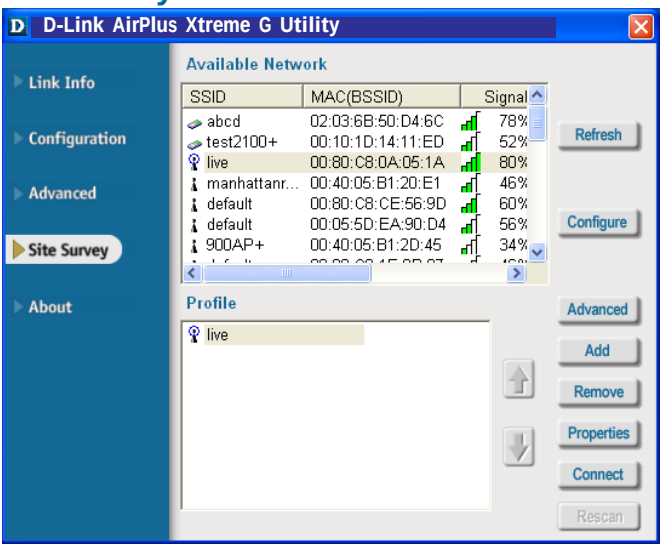
Profile:
In the lower half of the screen, you can manage the profiles that you have created for the wireless network at home, at the office and in public places. Scroll up and down and highlight the profile that you wish to configure. You can **Add** or **Remove** a profile, or configure the **Properties** of the profile in order to connect with an available network.

Refresh:
Click on **Refresh** to get the most updated list of available networks.

Configure:
Highlight an existing network and click **Configure**; the configuration window on the next page will appear.

Advanced:
Highlight a network; click **Advanced** and the screen on the next page will appear.

Site Survey



Add:
Click **Add** and the screen on the next page will appear.

Remove:
Highlight a network profile; click **Remove** to remove a network from the profile list.

Properties:
Highlight a network profile; click **Properties** and the screen on the next page will appear.

Connect:
Highlight a network profile; click **Connect** to connect to that network.

Rescan:
Click Rescan to rescan and connect to the strongest signal.

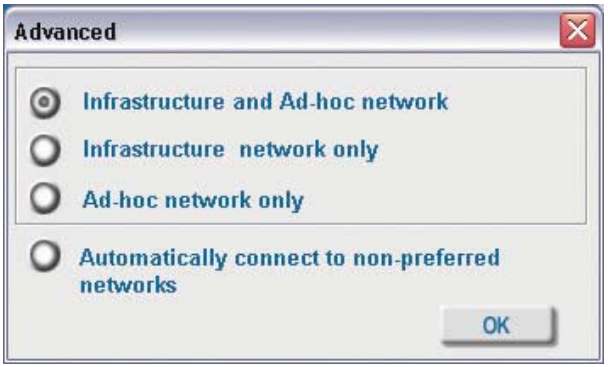
Using the Configuration Utility *(continued)*

Site Survey > Add

Advanced

In this window you can select the type of network connection.

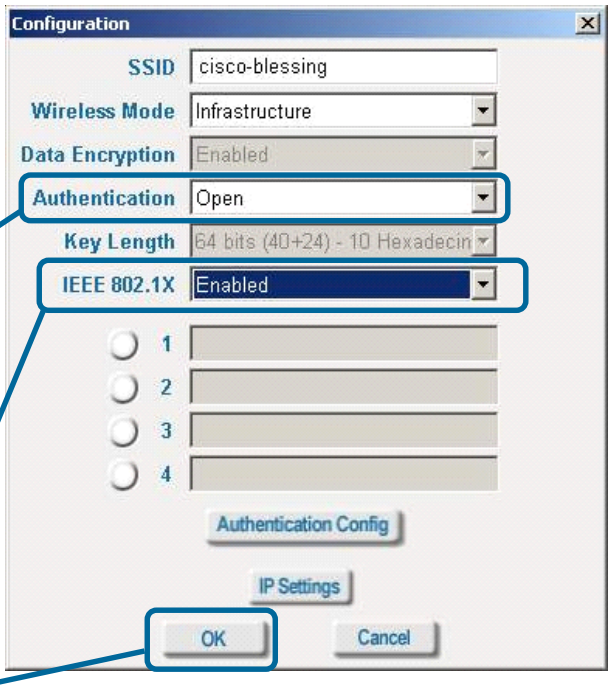
Click **OK** to save the changes.



Configuration, Add or Properties

If you clicked on **Add,** you can configure, in this window, all the properties of a profile that you wish to add to the network.

If you clicked on **Configuration or Properties** you can configure, in this window, all the properties of a profile that already exists in the network.



If you select **WPA** in the *Authentication* field, please see detailed instructions for configuring WPA on the following pages.

If you choose to use the **IEEE 802.1x** feature, please see the detailed instructions on the following pages.

Click **OK** to save the changes.

Using the Configuration Utility *(continued)*

Site Survey > Configuration > 802.1x

To use 802.1x and to configure its settings, please do the following:

IEEE 802.1x - Select **Enabled**.

Click **Authentication Config.**

Advanced Security Settings

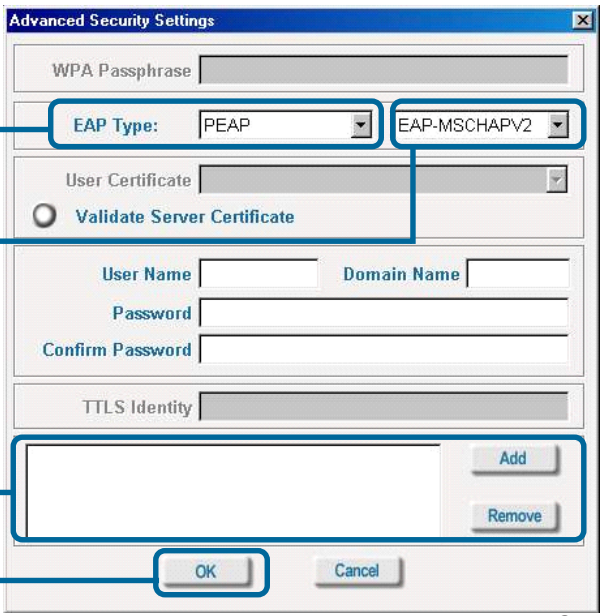
Select the **EAP Type** you want to use. Configure the information needed for authenticating.

Inner Authentication Protocol.

For an explanation of the terms shown in this window please see the following pages.

Trusted CA List.

Click **OK**



Using the Configuration Utility *(continued)*

802.1x > Advanced Security Settings > EAP Types

EAP Type	Inner Authentication Protocol	Information needed for Authenticating
EAP-TLS		Certificate User Name
EAP-MSCHAPv2		User Name Password Domain Name
LEAP		User Name Password
EAP-TTLS	PAP	TTLS Identity User Name Password
	CHAP	TTLS Identity User Name Password
	MSCHAP	TTLS Identity User Name Password Domain Name
	MSCHAPv2	TTLS Identity User Name Password Domain Name

Using the Configuration Utility *(continued)*

802.1x > Advanced Security Settings > EAP Types (continued)

EAP Type	Inner Authentication Protocol	Information needed for Authenticating
EAP-TTLS	EAP-MD5	TTLS Identity User Name Password
	EAP- Generic Token card	TTLS Identity User Name Password
	EAP-MSCHAPv2	TTLS Identity User Name Password Domain Name
PEAP	EAP-MD5	User Name Password
	EAP-MSCHAPv2	User Name Password Domain Name
	EAP- Generic Token card	User Name Password

802.1x > Advanced Security Settings > Definitions of Terms

Validate Server Certificate:

Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using EAP-TTLS, PEAP, and EAP-TLS. (This is checked by default.)

Certain protocols, such as EAP-TTLS, PEAP, and EAP-TLS, allow you to verify the identity of the authentication server as the server verifies your identity. This is called mutual authentication.

You can select trusted authentication server certificates using the **Add** button at the **Trusted CA List** (at the bottom of the **Advanced Security Settings** page).

Domain Name:

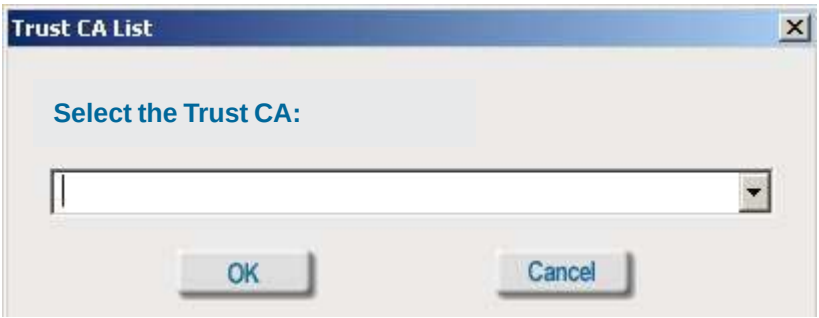
Each server has a domain name that uniquely identifies it. That domain name is normally contained in the ***Subject CN*** field of the server certificate. A server domain name ends with the name of a larger administrative domain, to which the server belongs.

TTLS Identity:

Tunneled Transport Layer Security satisfies a requirement for strong encryption and mutual authentication on Wireless networks. EAP-TTLS has a unique feature that other protocols do not offer. Because it sets up an encrypted tunnel for your credentials, it is also able to pass your login name through that tunnel. That means that not only are your credentials secure from eavesdropping, but your identity is protected as well. Thus, with EAP-TTLS you have two identities: an inner one, and an outer one. The inner identity is your actual user name. Your outer identity can be completely anonymous. Set your outer identity in the ***TTLS Identity*** field.

Trusted CA List:

The **Trusted CA List** allows you to configure which authentication servers you trust for the purpose of logging you in to the network.
Click **Add** at the **Trusted CA List** at the bottom of the *Advanced Security Settings* page. Select the **Trusted CA** that you want to add and click **OK**.

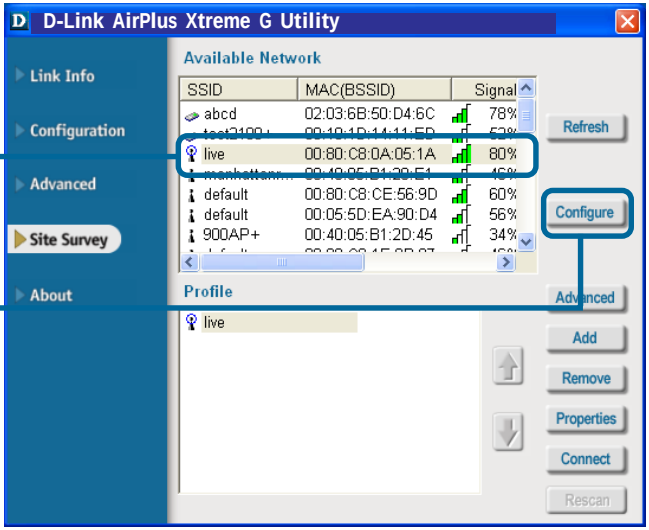


Using the Configuration Utility *(continued)*

Authentication > WPA

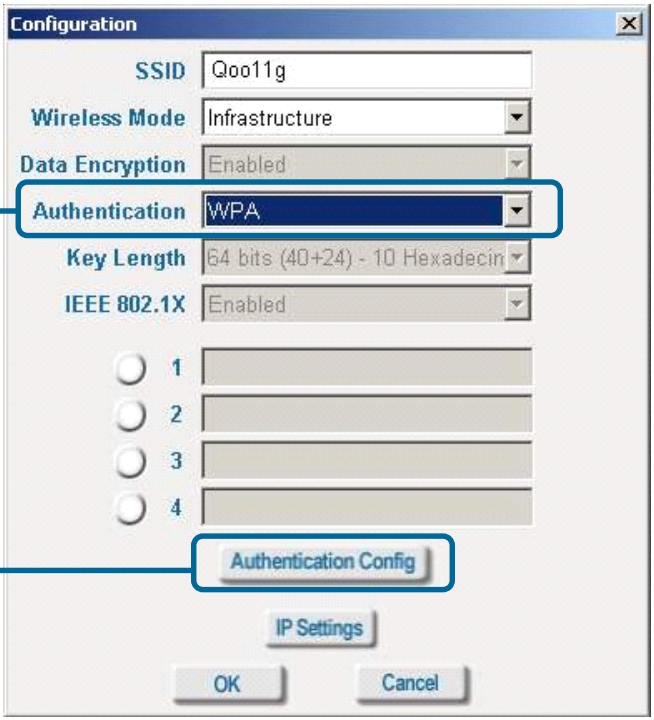
Select the available network to which you want to connect.

Click **Configure**.



Select **WPA** in the *Authentication* field.

Click **Authentication Config**



After you click **Authentication Config**, the *Advanced Security Settings* screen will appear. Complete the *Advanced Security Settings* configuration. Please see pages 19-22 of this manual to find out more about the *Advanced Security Settings*.

Using the Configuration Utility *(continued)*

Authentication > WPA-PSK

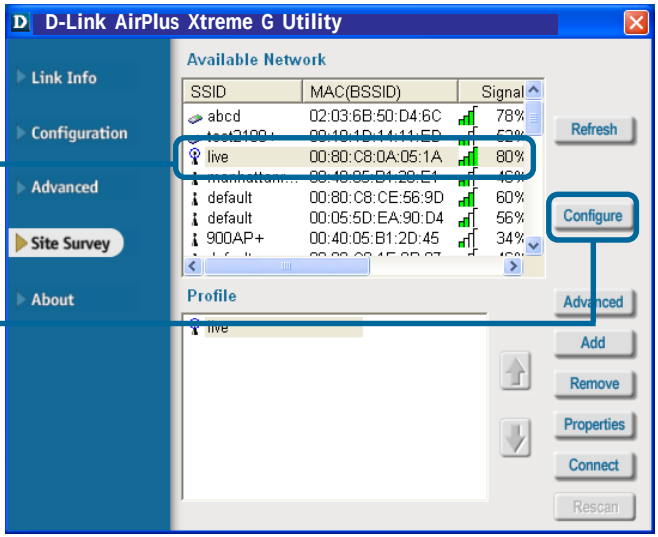
Select the available network to which you want to connect.

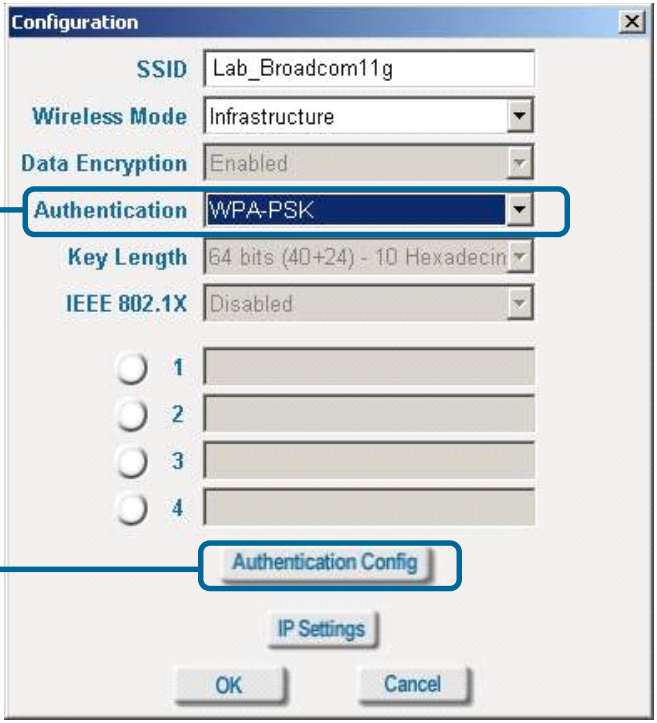
Click **Configure**.

WPA-PSK does not require a RADIUS Server in the network.

Select **WPA-PSK** in the *Authentication* field.

Click **Authentication Config**



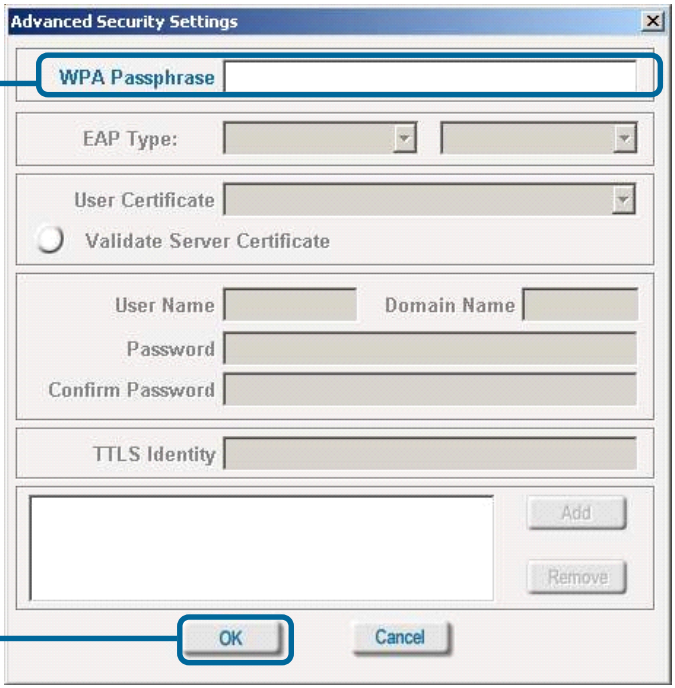


Using the Configuration Utility *(continued)*

Authentication > WPA-PSK (continued)

Advanced Security Settings

Enter the **WPA Passphrase.**



Click **OK**.
The configuration is done.