D-Link®

Version 1.0 | 12/2/2013

User Manual

Wi-Fi Dual Band Range Extender

DAP-1520

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.0	December 2, 2013	• Initial release for Revision A1

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

The purpose of this product is to create a constant network connection for your devices. As such, it does not have a standby mode or use a power management mode. If you wish to power down this product, please simply unplug it from the power outlet.

Table of Contents

Package Contents

DAP-1520 Wi-Fi Dual Band Range Extender

Wi-Fi Configuration Card

Quick Install Guide

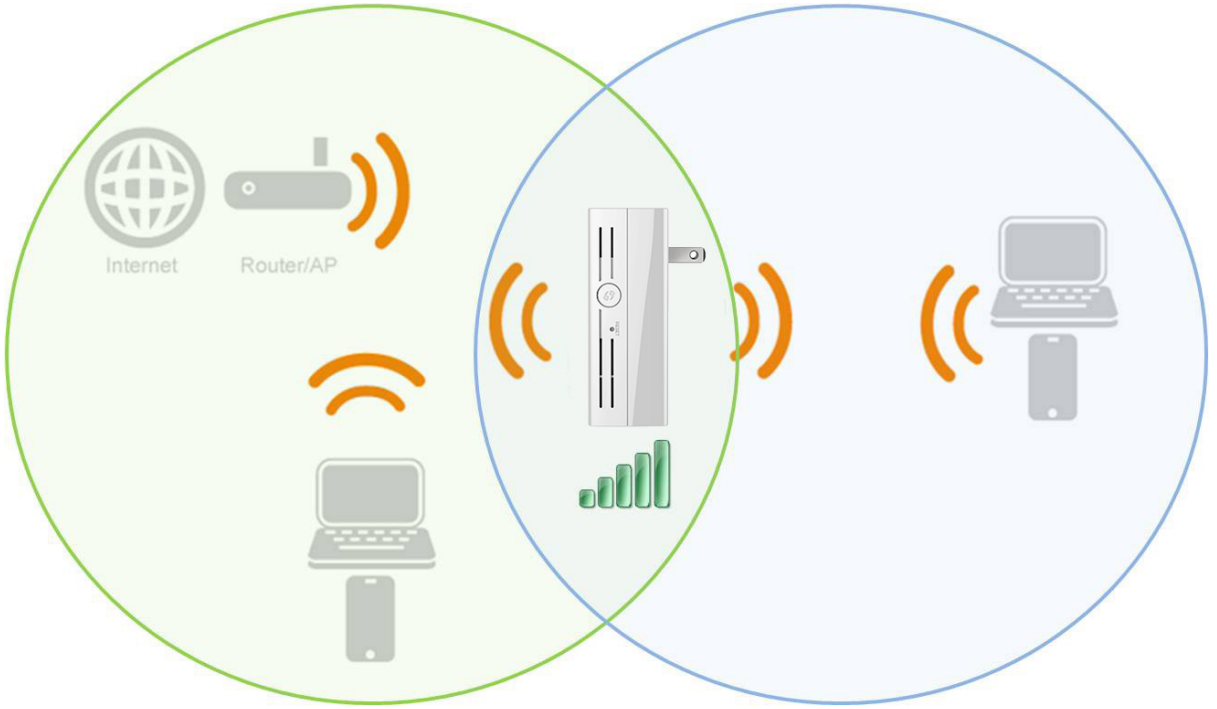
If any of the above items are missing from your package, please contact your reseller.

Minimum Requirements

Network Requirements	• IEEE 802.11ac draft, 802.11n, 802.11g wireless router or access point • IEEE 802.11ac draft, 802.11n, 802.11g, or 802.11a wireless clients/devices
Web-based Configuration Utility Requirements	**Device with the following:** • A Windows®, Macintosh®, Android™, or Linux-based operating system • Wireless adapter or Wi-Fi functionality **Browser Requirements:** • Internet Explorer® 7 • Firefox® • Safari® 4 • Chrome™ **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

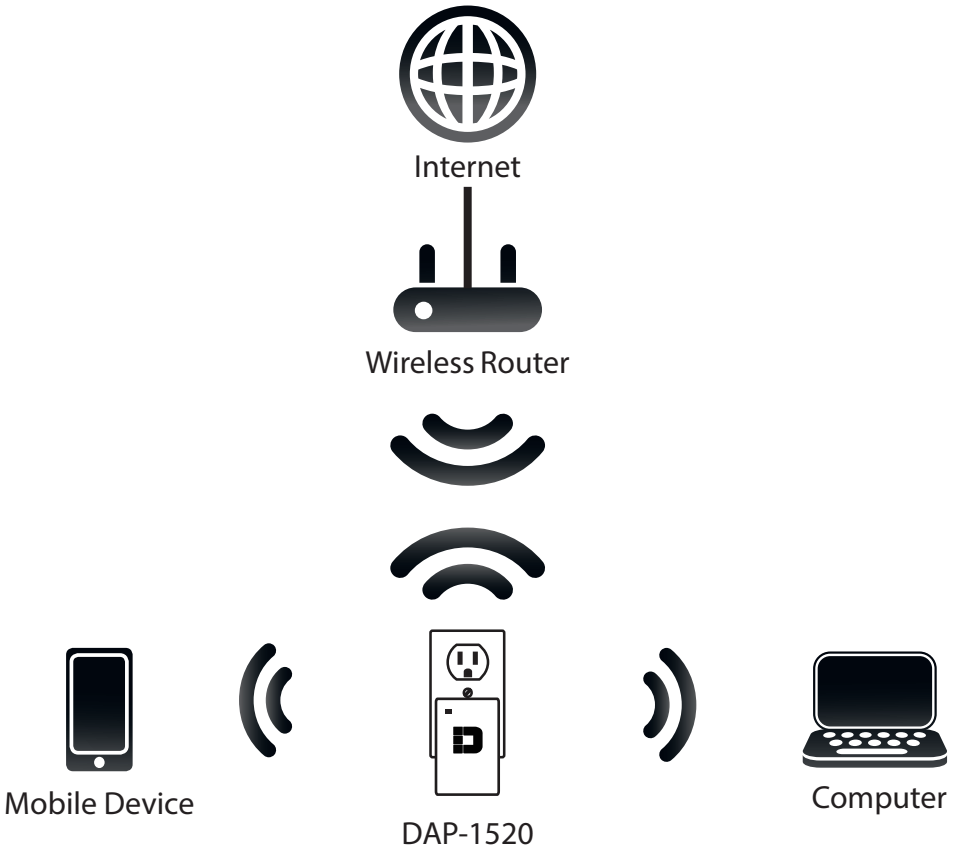
The DAP-1520 enables you to extend your existing wireless network coverage by placing the Wireless Range Extender in between your wireless router and your wireless client devices. This is great for extending your wireless coverage to hard-to-reach places like basements, home offices or upstairs bedrooms that are distant from your wireless router. The Wireless Range Extender is also ideal for mobile device connections.



Note: *Place the DAP-1520 within equal distance of your existing network/router and wireless clients.*

What is a Wireless Extender?

The DAP-1520 acts as a repeater to extend the range of an existing wireless network to provide a better signal for parts of your home or office that may have poor or no reception. Your existing wireless signal will be re-broadcast by the DAP-1520, allowing you to reach the farthest corners of your home or office . The extended network can simply use the same network credentials as the existing network, or you can specify a different network name and password, giving you the flexibility to control network access.



Features

Easily Extend Your Existing Network - The DAP-1520 lets you easily extend a secure wireless network. Connect the extender to a router and share your high-speed Internet access in more places throughout your home or small office.

High-speed Wireless Performance With Wireless 802.11ac Technology - Thanks to the latest Wireless AC technology, the DAP-1520 provides a wireless connection at up to 750 Mbps* with other 802.11ac wireless devices. This feature lets you participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

IEEE 802.11ac draft, 802.11n/g/a Compliant - The DAP-1520 is fully compatible with the IEEE 802.11n/g/a and IEEE draft 802.11ac standards, so you can connect with all of your wireless devices.

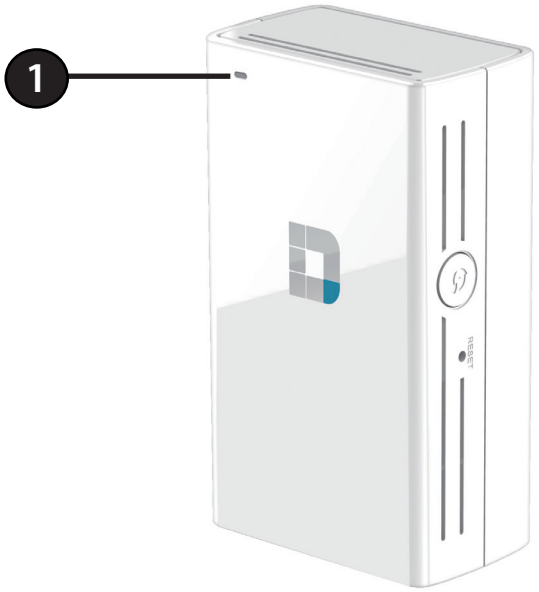
Simple Setup - All it takes is a press of a button to connect compatible WPS devices to the DAP-1520. Its easy-to-use Web UI lets you quickly and easily connect the DAP-1520 to an uplink router, configure the extended wireless network, and manage the administrative settings. The setup wizard will even guide you through the setup process, getting your extended wireless network up and running in no time.

Latest Wireless Network Security and Encryption - The DAP-1520 supports wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA/WPA2 standards ensure that you'll be able to use the best possible encryption methods with your compatible wireless devices.

* Maximum wireless signal rate derived from standard IEEE specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead may lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

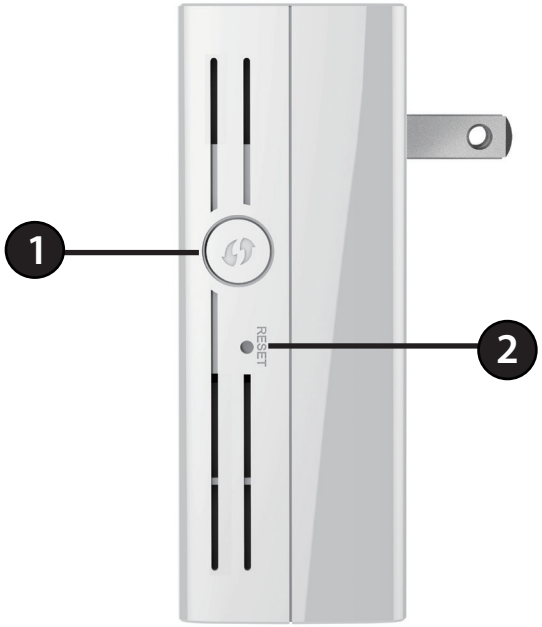
Front/Top



1	Power/Status LED	Solid Green	The device is powered ON and securely connected to a wireless router or access point.
		Blinking Green	The device is processing a connection after the WPS button has been pressed.
		Solid Red	Device is booting up.
		Blinking Red	The device is in recovery mode or the device has malfunctioned.
		Blinking Amber	The device is not connected to a wireless router or access point.
		Off	Device is not receiving power. Try a different outlet.

Hardware Overview

Side



1	WPS Button	Press the WPS (Wi-Fi Protected Setup) button for a minimum of one second to automatically connect with Wi-Fi clients. (Refer to "WPS Button" on page 42.)
2	Reset Button	Use an unfolded paper clip to press and hold the reset button for a minimum of six seconds to reset the DAP-1520 to the factory default settings.

Installation
Wireless Installation Considerations

The DAP-1520 lets you extend the reach of your existing wireless network, allowing you to work wirelessly from more places in your home or office. 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 extender and other network devices to a minimum. Each wall or ceiling can reduce the wireless range by up to 90 feet (approximately 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. At a 45-degree angle, a wall that is 1.5 feet thick (0.5 meters) appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it can appear over 42 feet (approximately 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 make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete can degrade your wireless signal.

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

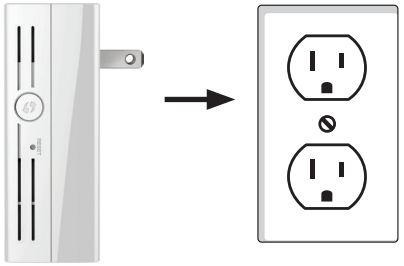
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Installation

Connect the DAP-1520 to Your Router Using WPS

The easiest and most secure way to connect your DAP-1520 to your router or access point is with WPS (Wi-Fi Protected Setup). Refer to your user manual for your router or access point to make sure you understand how to enable WPS. Once you know, follow the steps below:

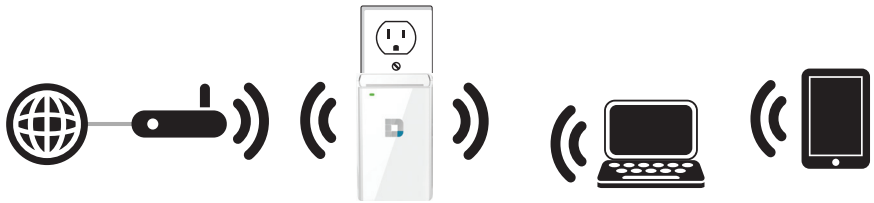
Step 1 - Find an available outlet near your wireless router. Plug in the DAP-1520 and wait until the power LED is blinking amber before continuing.



Step 2 - Press the **WPS button** on your wireless router or access point.

Step 3 - Within one minute, press the **WPS button** on the DAP-1520. The Power/Status LED will start blinking green. When the LED turns solid green, the DAP-1520 is connected securely to your wireless router or access point.

Step 4 - You can now unplug and move the DAP-1520 to a location between your wireless router and the area where you need to extend your wireless coverage.



Note: *When using WPS to connect to the router, the SSID on the DAP-1520 will automatically be assigned the following:*

- *2.4GHz: (Your Router's SSID)-EXT*
- *5GHz: (Your Router's SSID)-EXT5G*

The Wi-Fi passwords for your router will be the same as your passwords for the DAP-1520.

Step 5 - Connect your wireless clients to the DAP-1520. From your wireless device, go to the **Wireless Utility** to display the available wireless networks and select the **Wi-Fi Name** (SSID) for the DAP-1520. Both the **Wi-Fi Name** and **Wi-Fi Password** are on the specification sticker located on the underside of the device.

For instructions about using WPS to connect your devices, refer to "Connecting to a Wireless Client" on page 42. Or consult your device's user manual for more information. Once connected, you can begin the configuration process.

Note: *For instructions for changing your **Wi-Fi Name** and **Wi-Fi Password**, refer to* "Extended Wi-Fi Settings" on page 30.

Configuration
Configuring Your DAP-1520

There are two ways to configure your DAP-1520; using the *QRS Mobile App* on your smartphone or tablet, or using a wireless device or computer to access the *Web-based Configuration Utility*.

For detailed information on either of the methods above, refer to the following sections of the manual:

- "QRS Mobile App Setup" on page 12
- "Web-based Configuration" on page 17

QRS Mobile App Setup

The DAP-1520 can be set up from your iOS or Android smartphone or tablet device using the QRS Mobile app.

Search for *QRS Mobile* in the App Store or Google Play, or use your mobile device to scan the **QR code** on the right to download a *QRS Mobile* app from the App Store (left) for your iOS device, or from Google Play (right) for your Android device.

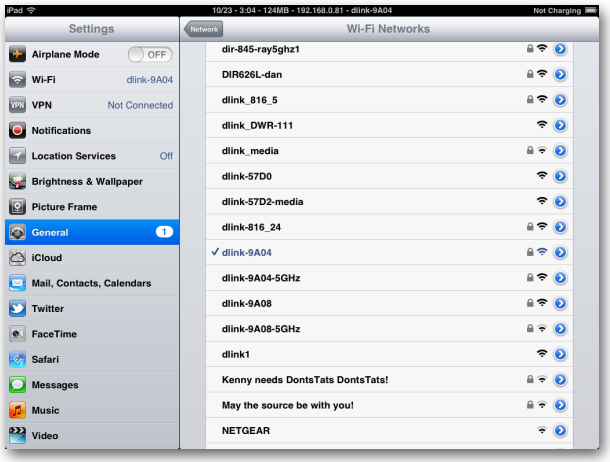
Available on the App Store

For iOS

ANDROID APP ON Google play

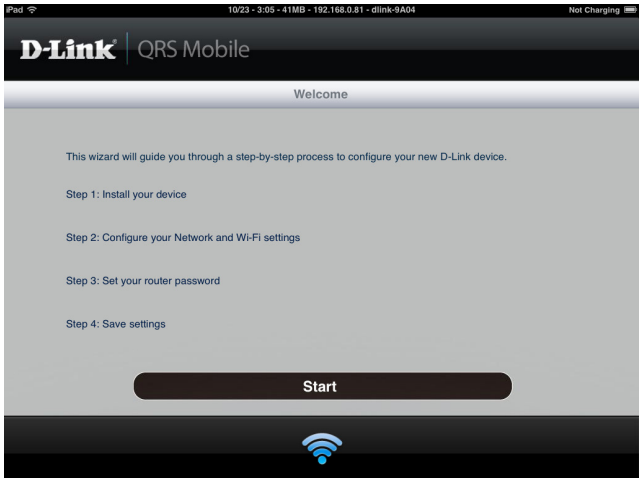
For Android

Connect to the **Wi-Fi Network** that is displayed on the Wi-Fi Configuration Card included in your package (ex: **dlink-a8fa).** Then, enter the **Wi-Fi Password** also printed on the Wi-Fi Configuration Card (ex: **akbdj19346).**

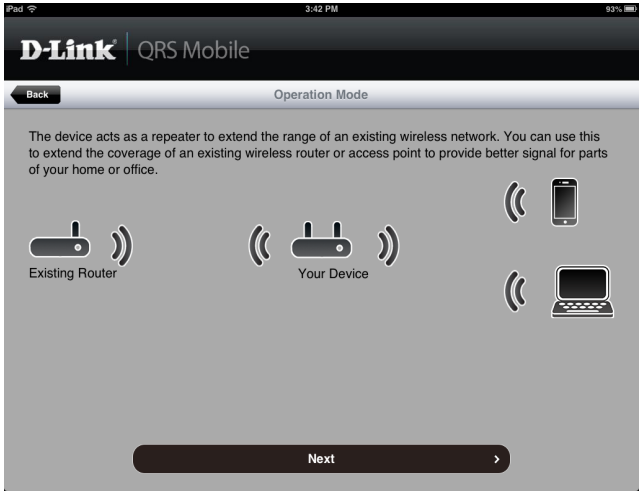


Once your mobile device is connected, tap on the **QRS Mobile** icon.

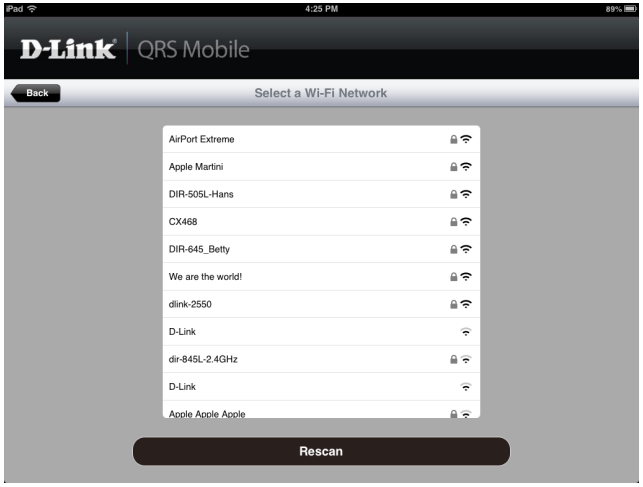
Tap **Start** to continue.



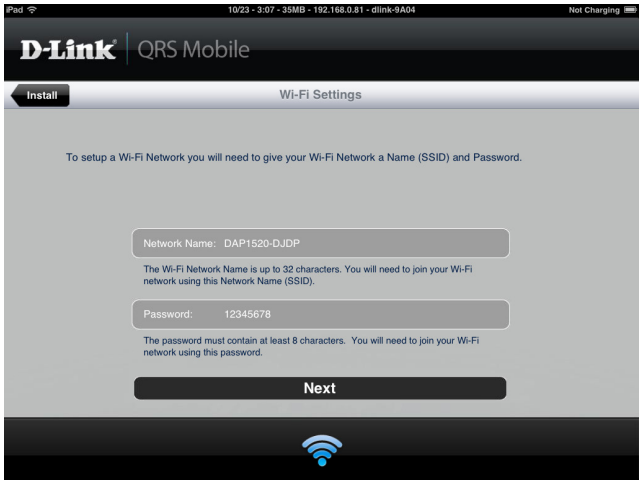
Tap **Next** to continue.



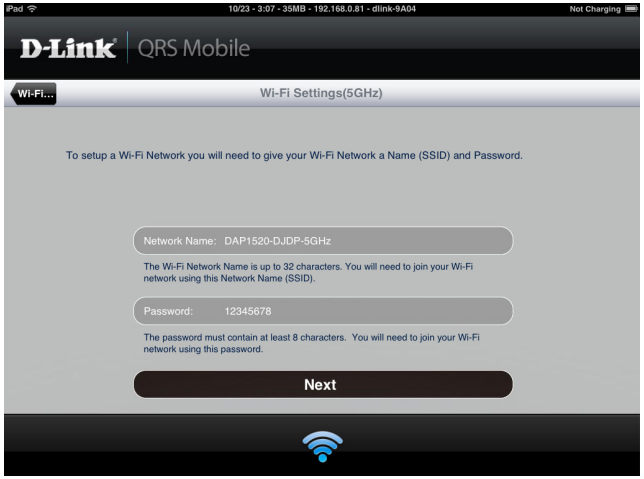
QRS Mobile will first detect your DAP-1520, then scan for available Wi-Fi networks. Select the **Wi-Fi Network** you wish to extend. Enter the **Password** if required.



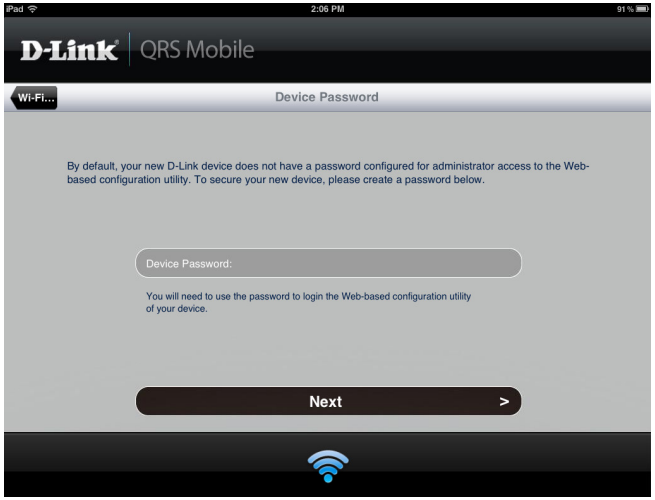
Enter a **Network Name** (SSID) and **Password** for the extended 2.4 GHz Wi-Fi network. You may keep the existing SSID and password if you wish. Click **Next** to continue.



Enter a **Network Name** (SSID) and **Password** for the extended 5 GHz Wi-Fi network. Click **Next** to continue.

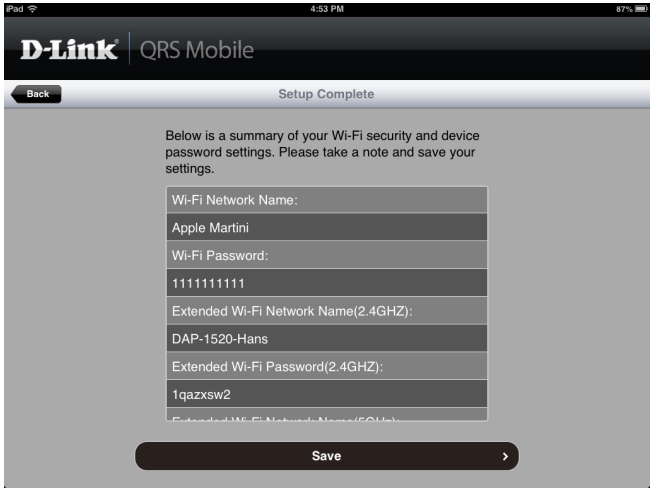


By default, your DAP-1520 does not have an admin password for the Web-based configuration utility. You can create a **Device Password**. Click **Next** to continue.

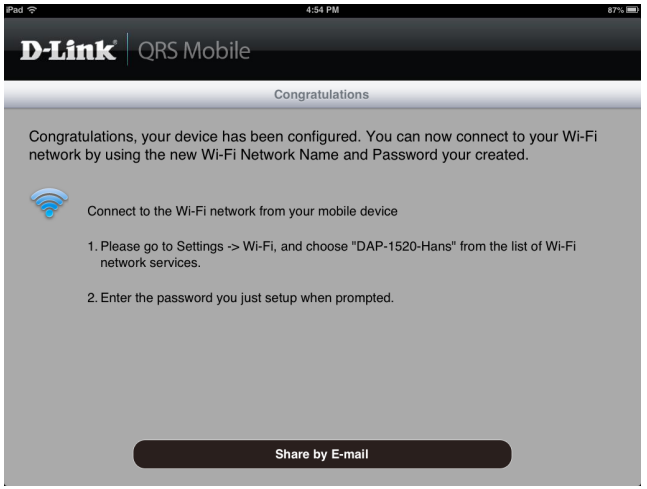


A summary of your settings will be displayed. Click **Save** to save your settings and reboot the device.

Make a note of your new Wi-Fi Network Name and Password. This completes your setup.



The confirmation screen will appear. To connect to the extended network, you can now change your mobile device and laptop wireless settings to the **Wi-Fi Network Name** and **Password** you just created. You can also share your Wi-Fi information by tapping on the **Share by E-mail** button at the bottom of the screen.

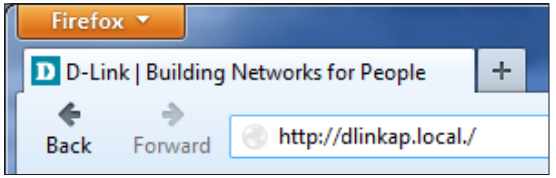


Web-based Configuration

You may use a wireless device or computer to access the *Web-based Configuration Utility* on the DAP-1520 for the following tasks:

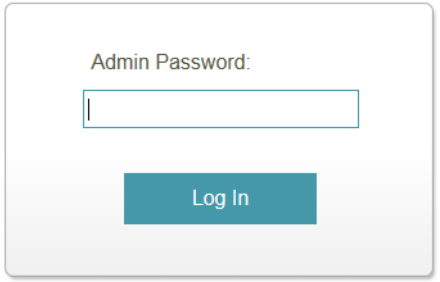
- Run the *Setup Wizard*
- Upgrade the Firmware
- Change the Wireless and Network Settings

Step 1 - Plug the DAP-1520 into an available outlet near your router. You can move it to a more suitable location after configuration.



Step 2 - Open the wireless utility on your wireless device or computer. Select the **Wi-Fi Name** (from your Wi-Fi Configuration Card) and enter the **Password**.

Step 3 - Open a web browser (e.g., Internet Explorer) and enter **http://dlinkap.local./** in your browser's URL field. You may also enter the IP address of the DAP-1520*. Windows XP users should enter **http://dlinkap**. You will see the *Log In* screen.

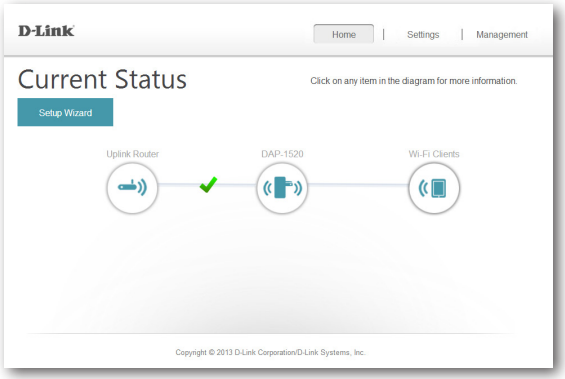


Note: *The default IP address is 192.168.0.50. Once your DAP-1520 connects to your router, it will be assigned a new IP address based on your network's DHCP settings. You will need to log in to your router to see what IP address was assigned to your DAP-1520.*

Step 4 - Enter your **Password** and click **Log In**. By default, the password is blank.

Note: *If this is your first time logging in to the DAP-1520, you will automatically be directed to the Setup Wizard.*

Step 5 - The Home page will display your *Current Status*. A green check mark represents a successful connection to your wireless router or Access Point (AP). If you see a red X to the left of the DAP-1520 icon, click on the **Uplink Router** icon to connect to your wireless router or AP.

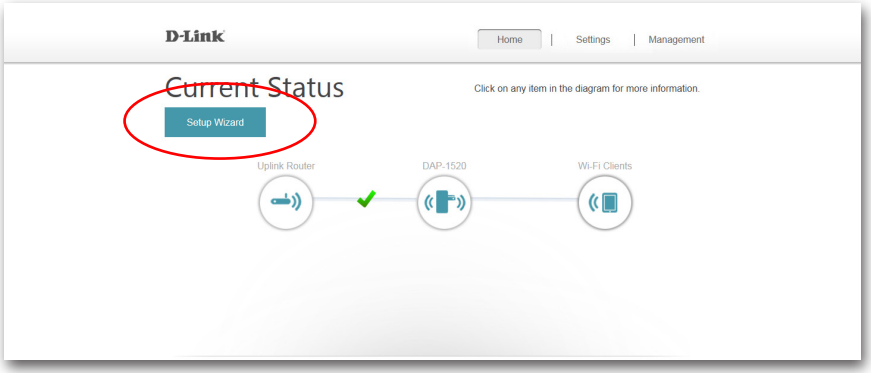


For detailed information on manually setting up your DAP-1520 to extend an existing wireless network, refer to "Using the Manual Method" on page 23.

Setup Wizard

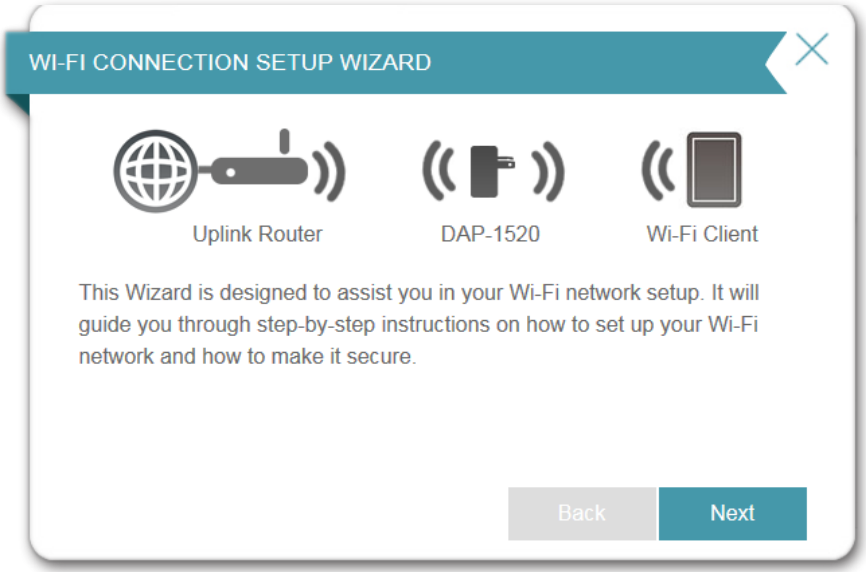
The *Wi-Fi Connection Setup Wizard* will guide you through the configuration process for your DAP-1520. If you already have a Wi-Fi network set up, and you prefer to configure your Wi-Fi network settings manually, click **Settings** at the top right corner of the page that displays *Current Status,* and select **Wi-Fi** from the drop-down menu. (Refer to "Wi-Fi Settings" on page 29.) To set up the extended Wi-Fi network, select **Extended Wi-Fi.** (Refer to "Extended Wi-Fi Settings" on page 30.)

From the Home page, under *Current Status*, click the **Setup Wizard** button.



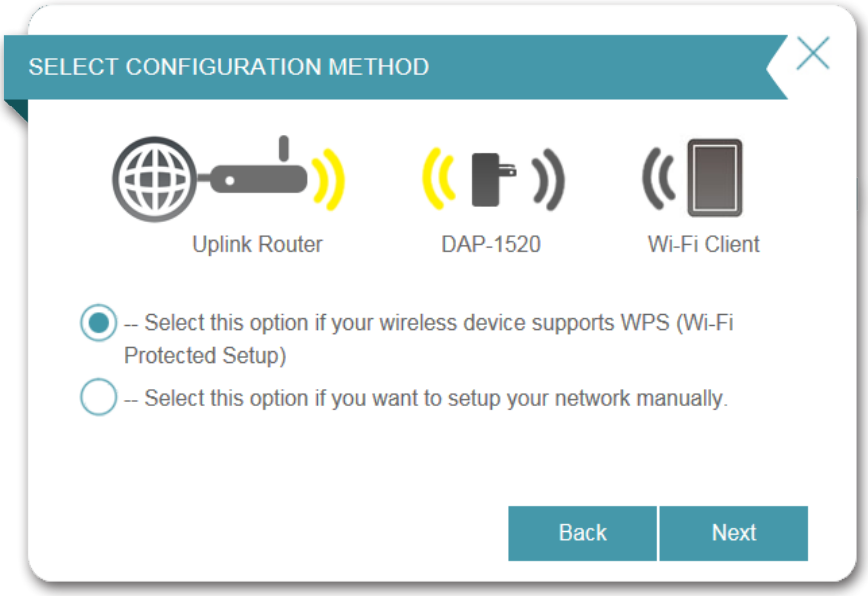
The *Wi-Fi Connection Setup Wizard* will guide you through step-by-step instructions on how to set up your Wi-Fi network.

Click **Next** to continue.



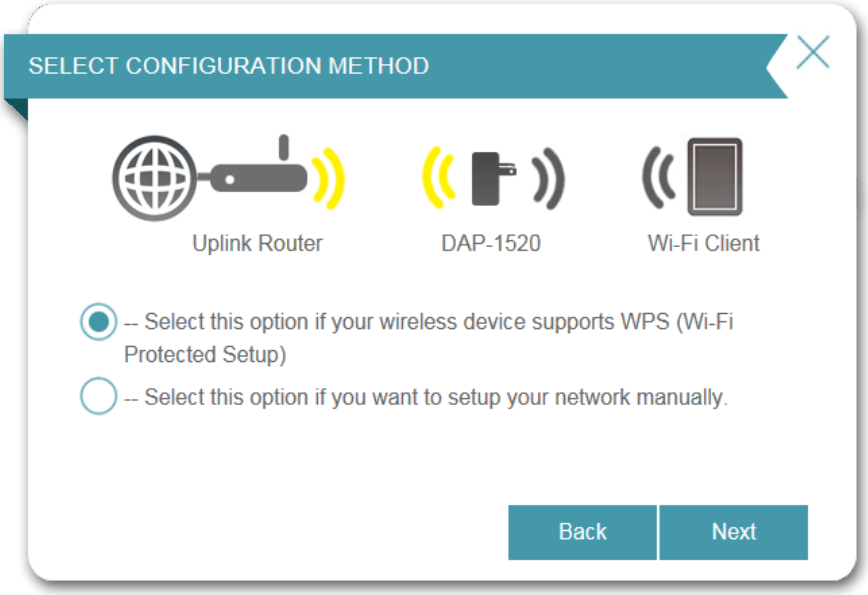
If your devices support WPS (Wireless Protected Setup), select the **WPS** configuration method and refer to "Using the WPS Method" on page 20. Otherwise, select the manual method and refer to "Using the Manual Method" on page 23.

Click **Next** to continue.



Using the WPS Method

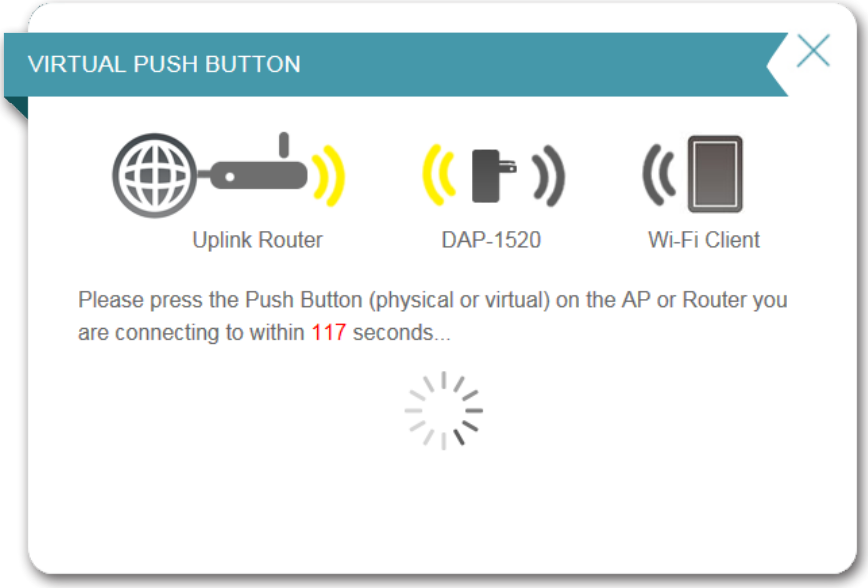
The *Wi-Fi Connection Setup Wizard* gives you the option to use the WPS configuration method. Click **Select this option if your wireless device supports WPS**. Click **Next** to continue.



You will see instructions on the screen that say, *Press the Push Button (physical or virtual) on the AP* (access point) *or Router...* You have 120 seconds to press the button.

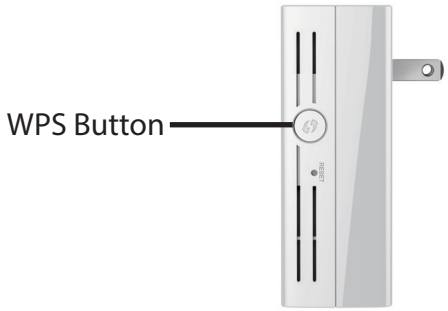
Press and hold the WPS button on your wireless router or access point until the light starts blinking*. Allow up to two minutes for the WPS process to complete.

When a connection is successfully made, you will see a notice on the screen and the LED on the device will turn solid green.

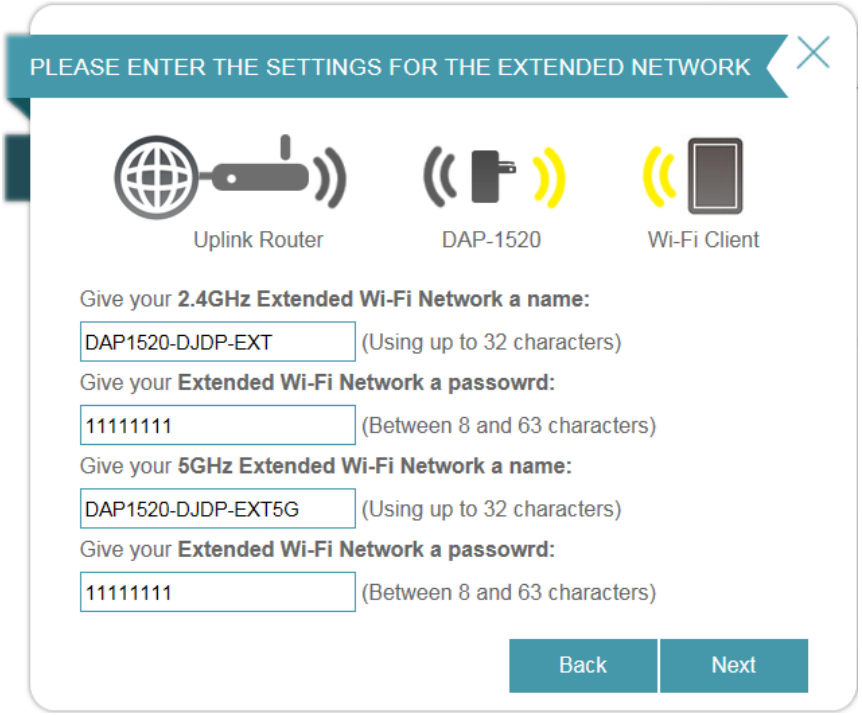


*__Note:__ *For LED indicator details, refer to the user manual for your router or access point.*

Note: *You can also use the WPS button on the side of the DAP-1520 to initiate a WPS connection with the uplink router. After pressing the WPS button on the DAP-1520, you will have 120 seconds to press the WPS button on your access point or router. The LED on the DAP-1520 will turn solid green when a connection has been successfully established with your router. Refer to "Connecting to a Wireless Client" on page 42.*

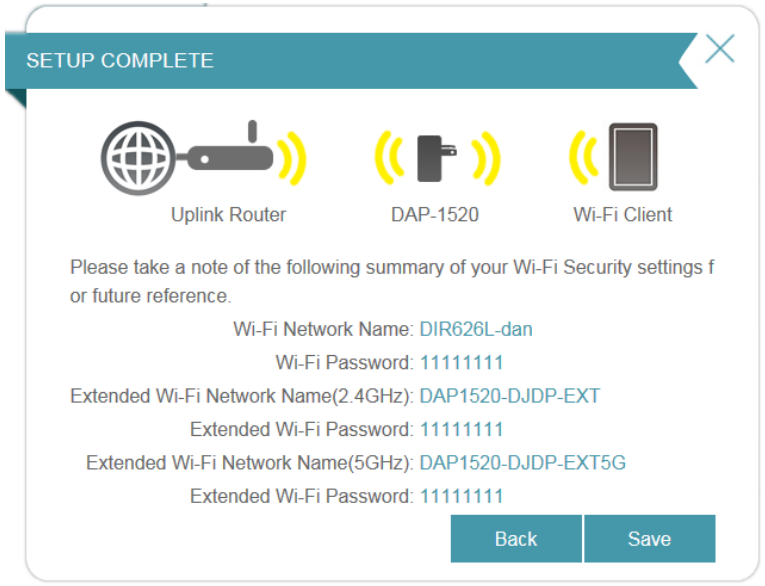


Once your connection has been established, you can then enter your *Extended Network* settings for both 2.4GHz and 5GHz. Click **Next** to continue.



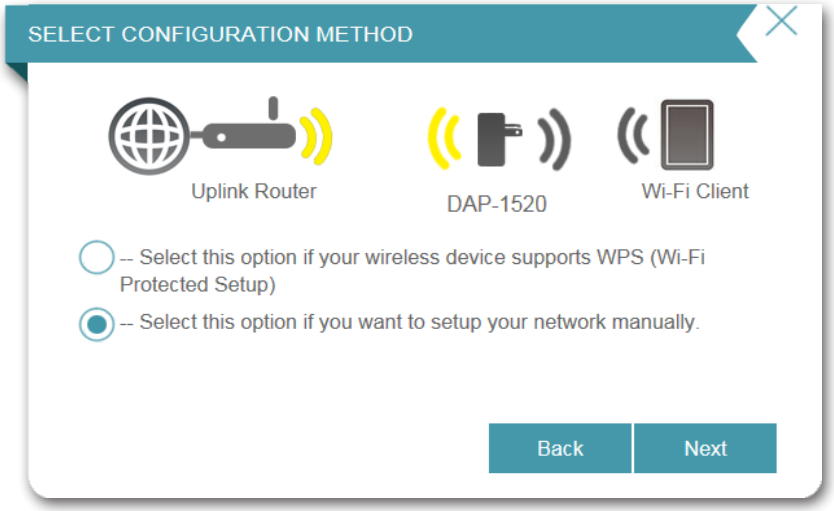
The next screen will show your *Wi-Fi Security* settings you entered in the previous step. Make a note of your Wi-Fi Network Name and Password.

Click **Save** to save your settings and exit the wizard. Your changes will be saved and the device will reboot.



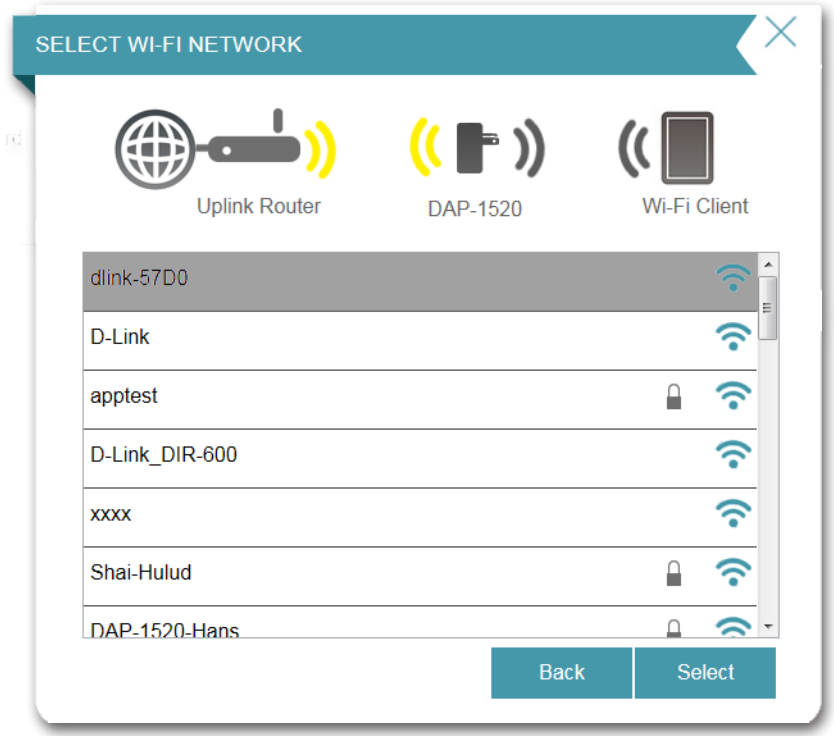
Using the Manual Method

The *Wi-Fi Connection Setup Wizard* gives you the option to set up your network manually. Click **Select this option if you want to setup your network manually**. Click **Next** to continue.



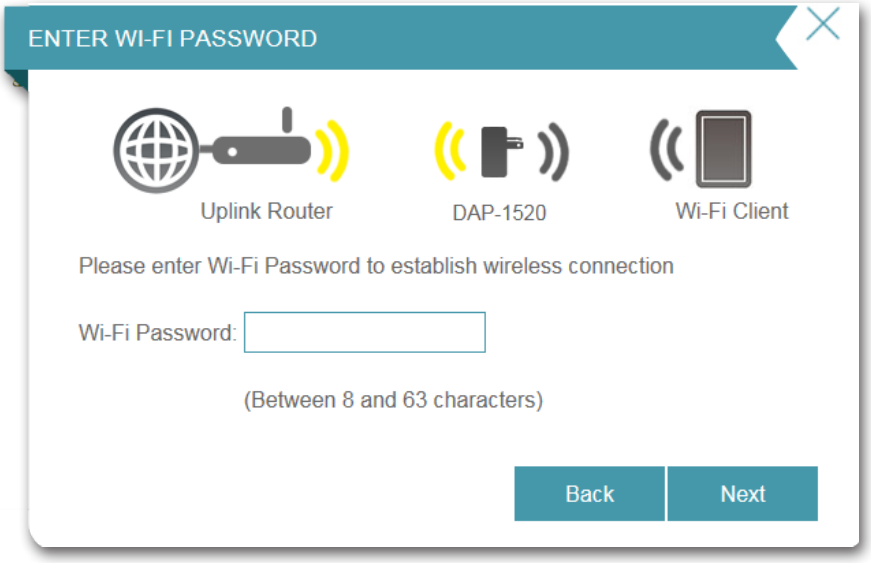
The DAP-1520 will first scan for available Wi-Fi networks and list the networks it has found. If the network you would like to connect to isn't listed, click **Back** and select the manual option again to perform another scan.

Click to highlight the **Wi-Fi Network** you wish to use, then click the **Select** button.



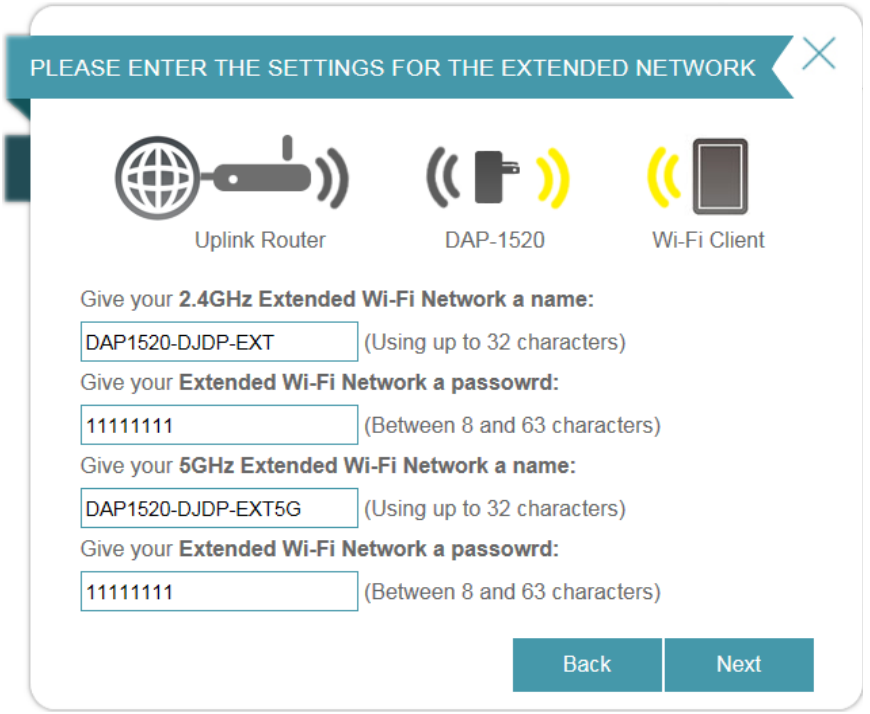
If the wireless network you selected is secure, you will be prompted to enter the **Wi-Fi Password**.

Click **Next** to continue. Click **Back** to return to the previous step if you need to select a different wireless network.



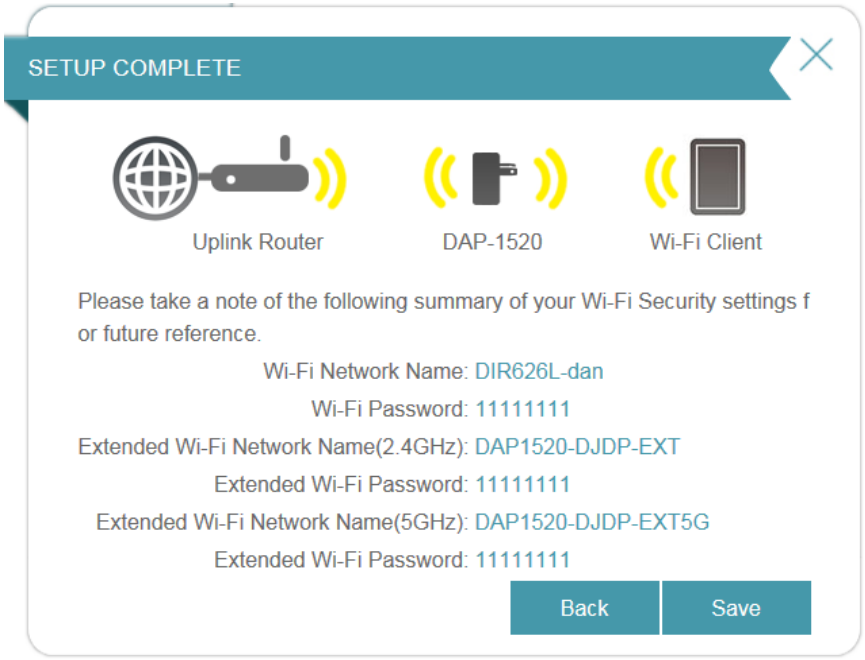
The DAP-1520 will re-broadcast the Wi-Fi connection from the uplink router as *Extended* 2.4GHz and 5GHz *Wi-Fi Networks*. Enter the **Wi-Fi Network Name** (SSID) and **Password** that you wish to apply to each of the extended Wi-Fi networks.

Click **Next** to continue.



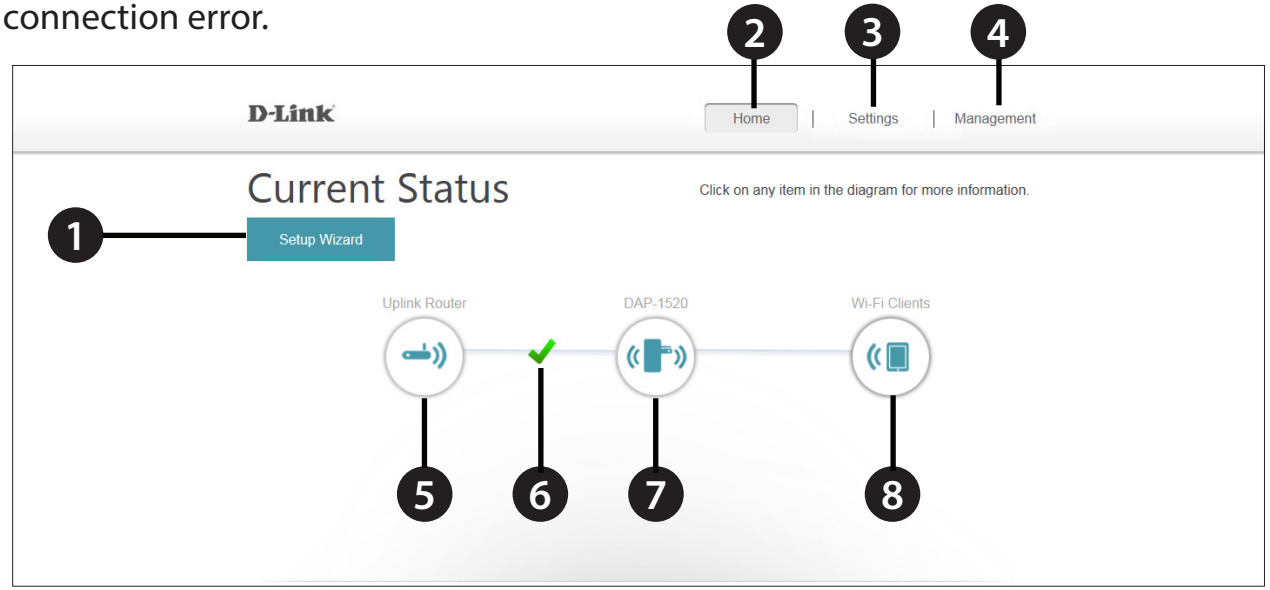
The next screen will show your *Wi-Fi Security* settings you entered in the previous step. Make a note of your Wi-Fi Network Name and Password.

Click **Save** to save your settings and exit the wizard. Your changes will be saved and the device will reboot.



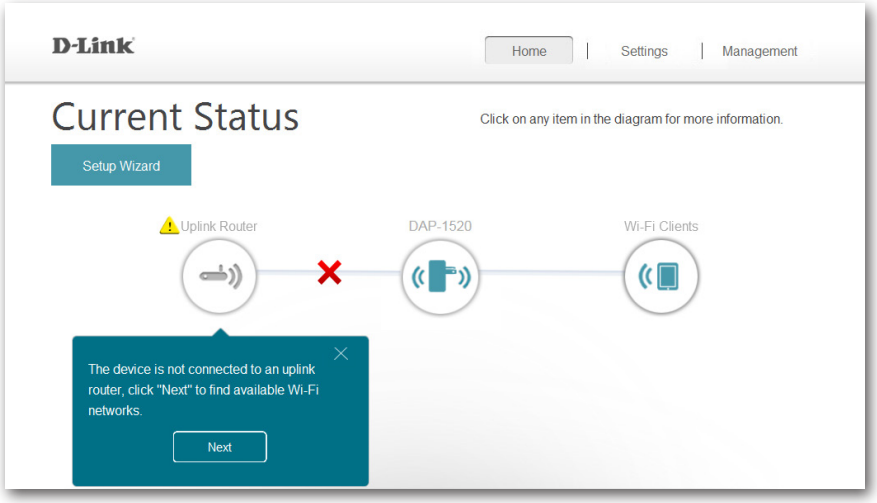
Home Screen

The Home screen shows the *Current Status* of devices connected to the DAP-1520. A green check mark between the *Uplink Router* icon and the *DAP-1520* icon indicates that there is an active connection. A red X indicates that there is no connection present, or there is a connection error.

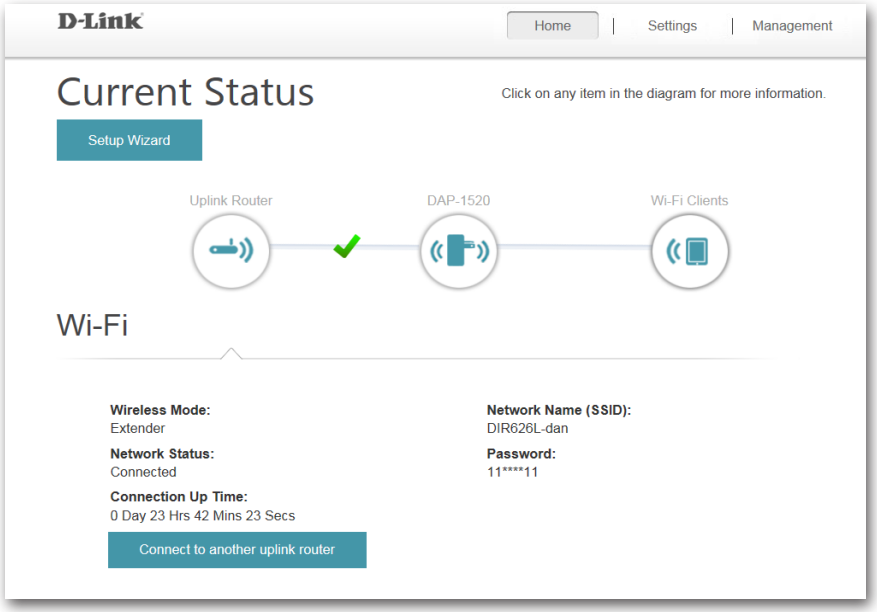


1	Setup Wizard	Click to launch the *Wi-Fi Connection Setup Wizard*. Refer to "Setup Wizard" on page 18.
2	Home	Click to navigate to the *Current Status* page (as shown above).
3	Settings	Click to view or change your *Wi-Fi*, *Extended Wi-Fi*, and *Network* settings.
4	Management	Click to change the login password, upgrade firmware, view data traffic statistics, save or load configuration files, reboot, and restore the DAP-1520 back to the factory default settings.
5	Uplink Router	Click to display the network settings of the wireless network (if connected) or to connect to a network if not connected.
6	Uplink Router Status	Displays the status of your connection to the wireless network you are "repeating". A green check mark (✔) indicates a successful connection to your wireless router or access point. A red (✘) indicates no connection. Click the **Uplink Router** icon to display a list of wireless networks you can connect the DAP-1520 to.
7	DAP-1520	Click to view the details for both the uplink router network and the extended Wi-Fi network.
8	Wi-Fi Clients	Click to display a list of clients (devices) currently connected to the DAP-1520.

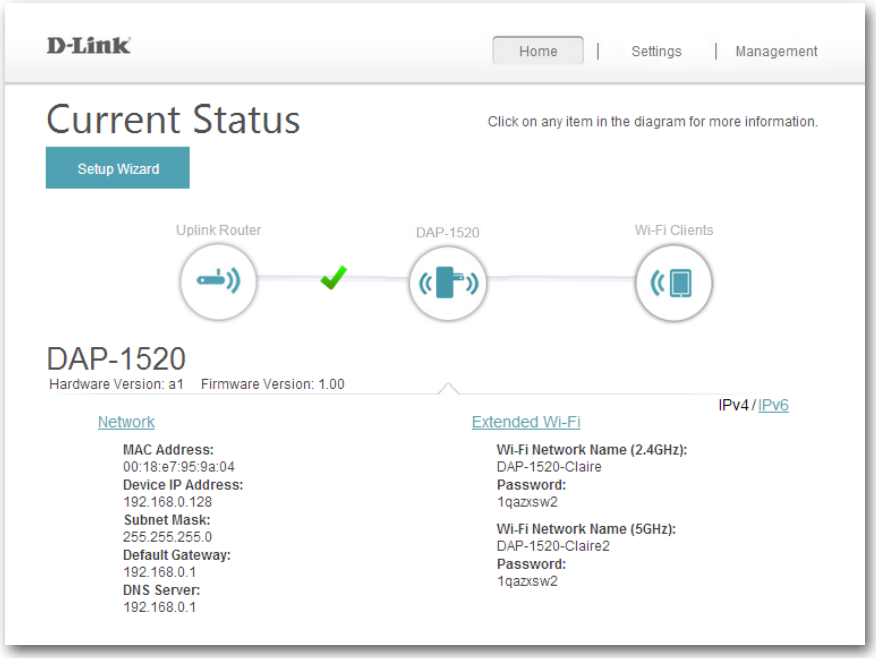
When the red (✖) indicates that the DAP-1520 is not connected to your router, click on the **Uplink Router** icon to search for an available Wi-Fi network.



At any time, you can click on a device icon on the Home screen to view the device details.



You can view the details of both the *Network* and the *Extended Wi-Fi Network* by clicking on the **DAP-1520** icon.



Wi-Fi Settings

This page lets you configure the Wi-Fi Network you would like the DAP-1520 to connect to. From the Home page, click on the **Settings** drop-down menu at the top of the page, and select **Wi-Fi**.

Wireless Mode: This is set to *Extender* mode and cannot be changed.

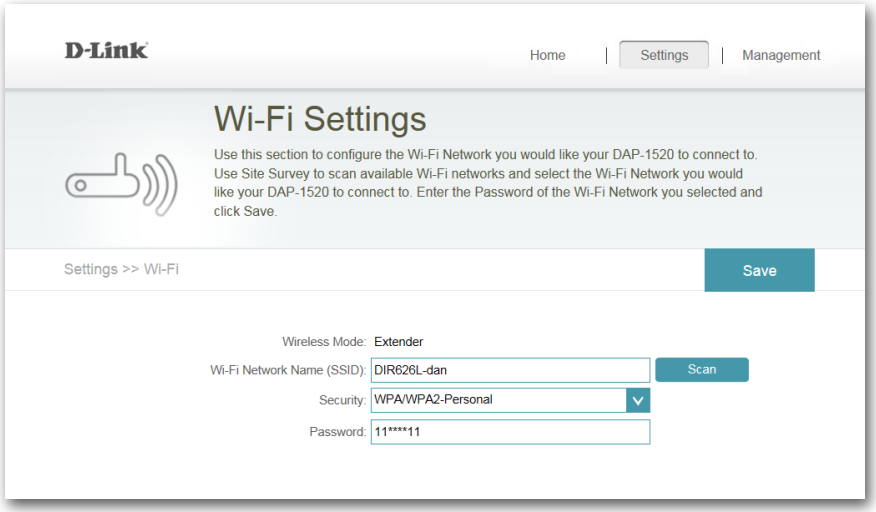
Wi-Fi Network Name (SSID): Click **Scan** to use Site Survey to scan for available wireless networks within range of the DAP-1520. Select the one you want to extend. You can also type in the name (SSID) of the wireless network.

Security: Select the security method that is being used by the wireless network that you have selected: **WEP**, **WPA/WPA2**, or **None**.

Password: If you selected **WEP** or **WPA/WPA2**, you will be required to enter the password or security key for the network you are attempting to join.

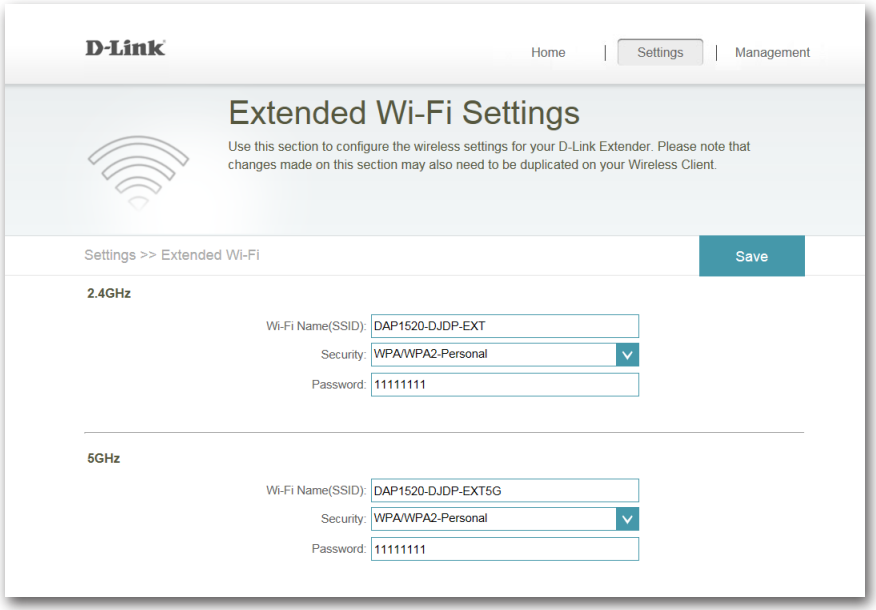
You can also use WPS to connect your wireless devices to the DAP-1520's extended network. For further information on how to do this, refer to "Connecting to a Wireless Client" on page 42.

Save: Click **Save** to save the settings and return to the Home page.



Extended Wi-Fi Settings

This page lets you configure the settings for the DAP-1520's extended wireless network. From the Home page, click on the **Settings** drop-down menu at the top of the page, and select **Extended Wi-Fi**.



2.4GHz

Wi-Fi Name (SSID): This is the name of the DAP-1520's extended network. The DAP-1520 will rebroadcast the uplink router's Internet connection under this SSID. You can also choose to make the SSID for the extended network the same as the SSID for the uplink network.

Security: Select the type of wireless security you wish to use for the extended network. Choose **None**, **WEP**, or **WPA/WPA2 Personal**.

Password: Enter the password or network key that you wish to use for the extended network.

5GHz

Wi-Fi Name (SSID): Enter the SSID for the extended 5 GHz network here.

Security: Select the type of wireless security you wish to use for the extended 5GHz network. Choose **None**, **WEP**, or **WPA/WPA2 Personal**.

Password: Enter the password or network key that you wish to use for the extended 5 GHz network.

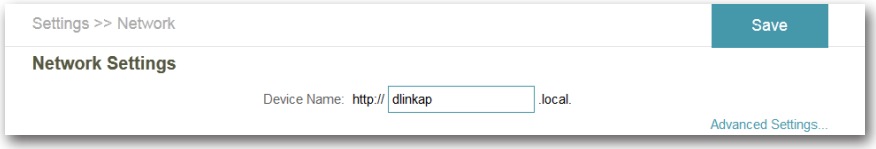
Note: *You can make the password for the extended network the same as the password for the uplink network.*

Save: Click **Save** to save the settings and return to the Home page.

Network Settings

This page lets you configure the network settings for the DAP-1520. To access this page, point to the **Settings** drop-down menu at the top of the page, then select **Network**. Click **Save** at any time to save the changes you have made on this page.

Device Name: You can change the URL name of the device by editing the text in the text box. If you change the name of the device, you will need to enter **http://xxxx.local./** (where "xxxx" corresponds to the name of the device) in the address bar of your web browser in order to access the configuration utility.



Advanced Settings

The *Advanced Settings* section of the *Network Settings* page allows you to configure both *IPv4* and *IPv6* settings that will be used by the DAP-1520's extended network.

IPv4 Device Management Interface

My LAN Connection is: Select whether you want the IP to have a **Dynamic IP** or **Static IP** address. If you select **Dynamic IP**, the IP address information is obtained automatically from your ISP. (The fields below become irrelevant.)

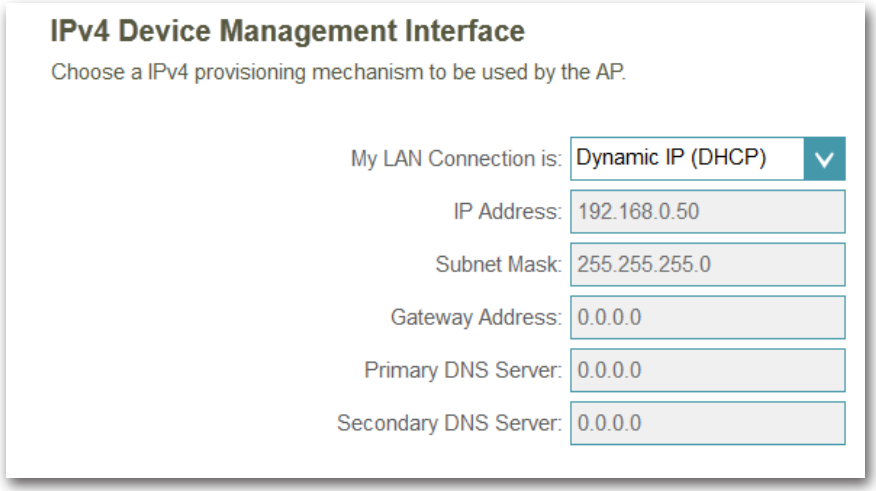
IP Address: Enter the Static **IP Address** that you want to assign to the extended network AP. This address should be outside of the uplink router's DHCP address pool.

Subnet Mask: Enter the **Subnet Mask**.

Gateway Address: Enter the **Gateway Address**. (This is usually the IP address of the uplink router.)

Primary DNS Server: Enter the address of the **Primary DNS Server.**

Secondary DNS Server: Enter the address of the **Secondary DNS Server**. This is optional but will provide backup if the primary server fails.



Autoconfiguration (SLAAC/DHCPv6)

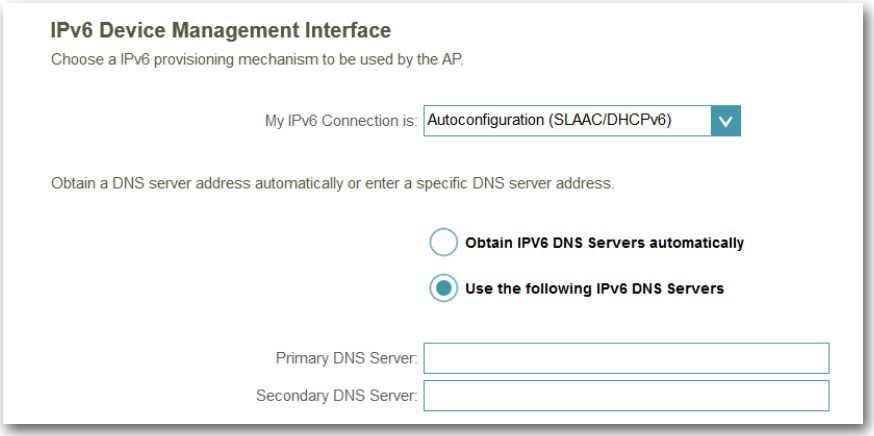
IPv6 Device Management Interface

My IPv6 Connection is: Select **Autoconfiguration (SLAAC/DHCPv6)** to have the DAP-1520 automatically receive an IPv6 address from the uplink router.

Obtain DNS Server Address: You can select **Obtain IPv6 DNS Servers automatically**, or you can select **Use the following IPv6 DNS Servers** to configure DNS servers manually.

Primary DNS Server: If you selected the manual option above, enter the **Primary** IPv6 **DNS Server** address.

Secondary DNS Server: If you selected the manual option above, enter the **Secondary** IPv6 **DNS Server** address. This is optional but will provide backup if the primary server fails.



Static IPv6

IPv6 Device Management Interface

My IPv6 Connection is: Select **Static IPv6** to manually assign an IP address to the DAP-1520.

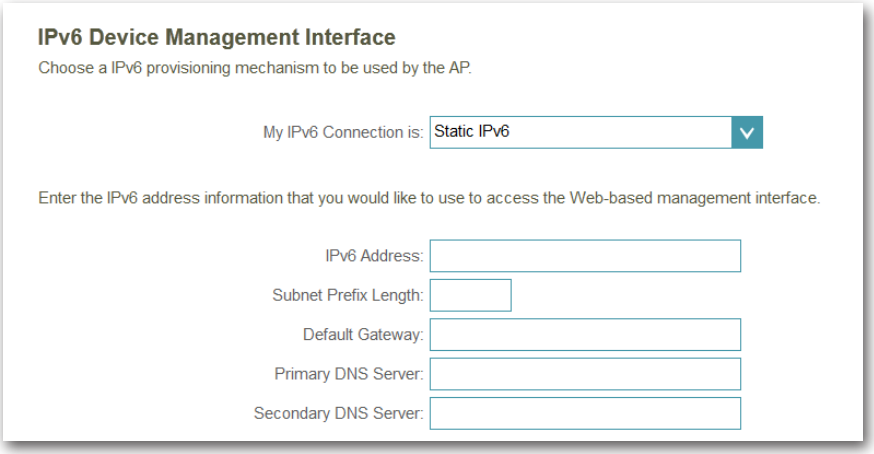
IPv6 Address: Enter the **IPv6 Address** that you want to assign to the extended network AP. This address should be outside of the uplink router's DHCP address pool.

Subnet Prefix Length: Enter the length of the IPv6 subnet prefix.

Default Gateway: Enter the **Default Gateway**. (This is usually the IP address of the uplink router.)

Primary DNS Server: Enter the **Primary** IPv6 **DNS Server** address.

Secondary DNS Server: Enter the **Secondary** IPv6 **DNS Server** address. This is optional but will provide backup if the primary server fails.

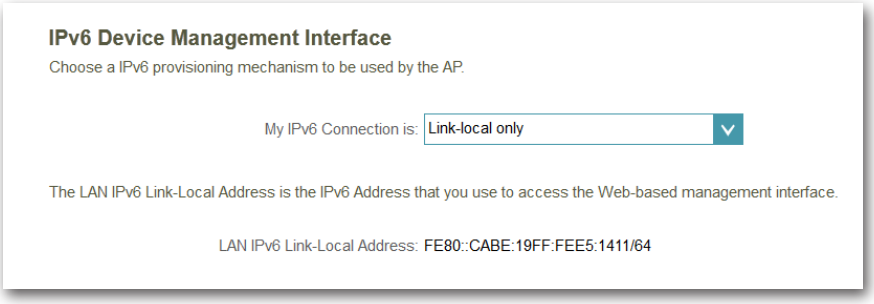


Link-local Only

IPv6 Device Management Interface

My IPv6 Connection is: Select **Link-local only** to only set an IPv6 address for the local network.

LAN IPv6 Link-Local Address: Displays the *Link-Local Address* of the DAP-1520 that you use to access the Web-based management interface.



Tools
Admin

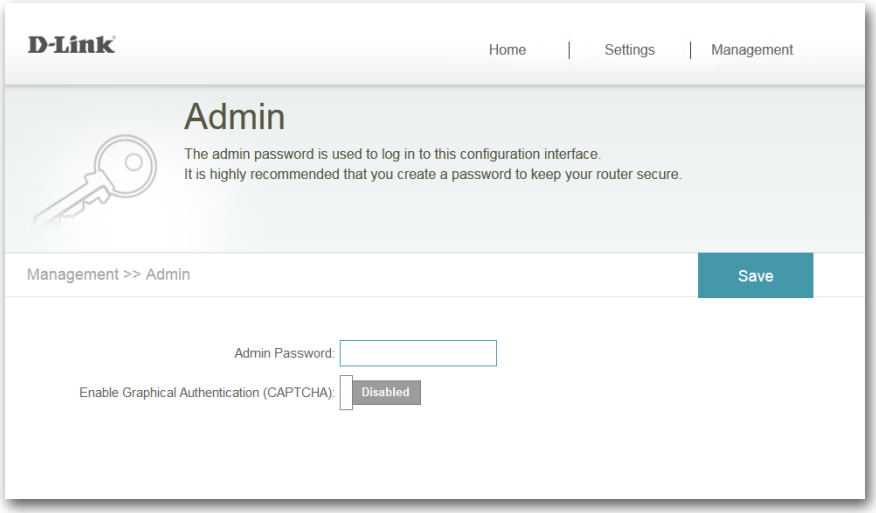
This page will allow you to set a new password for the administrator account used to configure the DAP-1520. You can also enable graphical authentication (CAPTCHA) on this page. From the Home page, click on the **Management** drop down menu at the top of the page, and select **Admin**. Click **Save** at any time to save the changes you have made on this page.

Admin Password: Enter the **Admin Password**.

Enable Graphical Authentication: Use the slider to **Enable Graphical Authentication**, or CAPTCHA. This provides an extra layer of security by requiring you to enter a code that is displayed on-screen. This can help prevent unauthorized users from gaining access to your wireless network using automated methods.

Save: Click **Save** to save the settings.

Note: *The device will reboot after saving the changes, and then the password will take effect.*



System

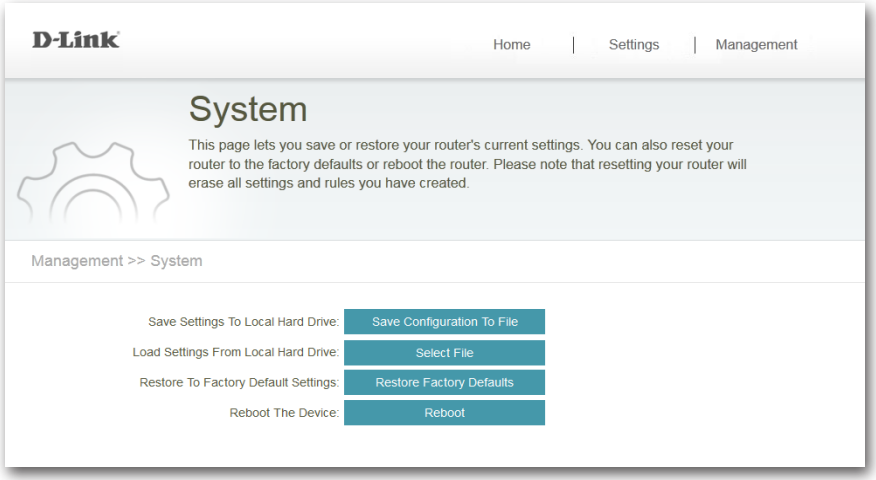
This page allows you to save or restore your system configuration, reset, or reboot the DAP-1520. From the Home page, click on the **Management** drop down menu at the top of the page, and select **System**.

Save Settings To Local Hard Drive: Save the system settings to a file on the local hard drive of your computer. You will then see a file dialog, allowing you to select a location and enter a file name for the configuration file.

Load Settings From Local Hard Drive: Load the system settings from a previously saved file on the local hard drive.

Restore to Factory Default Settings: Restore the system settings to factory default settings. This will erase all currently stored settings.

Reboot the Device: Click **Reboot** to reboot the DAP-1520.



Upgrade

You can check for the latest firmware version, then upgrade your firmware and language pack from this page. From the Home page, click on the **Management** drop down menu at the top of the page, and select **Upgrade**.

Firmware Information

Firmware Information: This section displays the currently installed *Firmware Version*, as well as the date on which the *Current Firmware Version* was released.

Click **Check For New Firmware** to find out if there is new firmware available. If there is, you can download it to your computer.

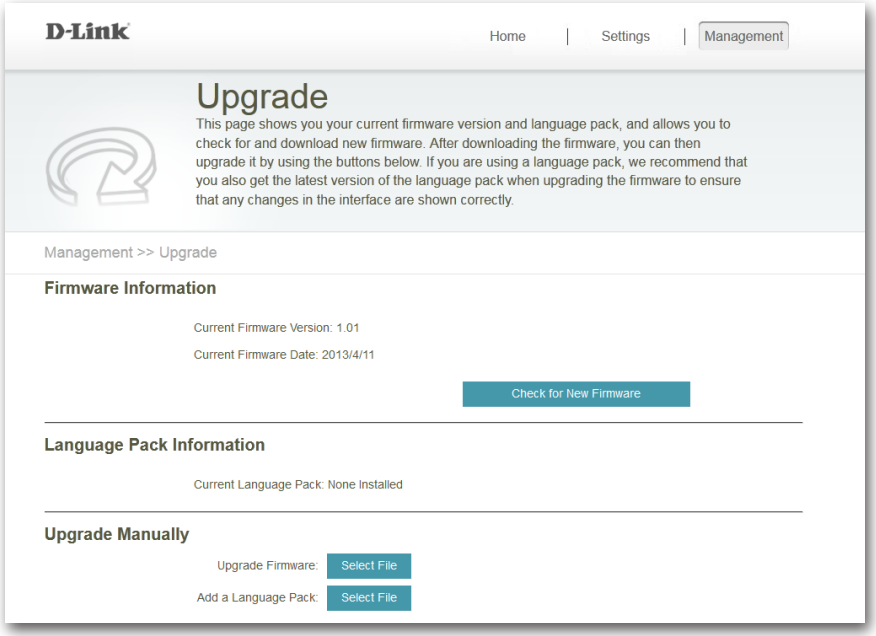
Language Pack Information

Language Pack: This section will show the details of any language packs currently installed, or will say *None Installed*.

Upgrade Manually

Upgrade Firmware: Click **Select File** to locate the firmware file on your local hard drive of your computer and perform a manual firmware upgrade.

Add a Language Pack: Click **Select File** to locate a language pack file on your local hare drive of your computer and add the language pack to the user interface.



Statistics

This page displays traffic statistics for your *Wi-Fi* and and *Extended Wi-Fi* connections. From the Home page, click on the **Management** drop-down menu at the top of the page, and select **Statistics**.

Wi-Fi

Click on the **Wi-Fi** tab to display the traffic statistics for the connection between the DAP-1520 and the uplink router.

The Blue line indicates the upload speeds and the red line indicates the download speeds.

The table displays the following in real-time:

- Total Packets
- Total Byte(s)
- Total Kbit(s)
- Kbits/sec

Extended Wi-Fi

Click on the **Extended Wi-Fi** tab to display the traffic statistics for the connection between the DAP-1520 and any connected clients.

Click **Clear** to reset the statistics.

Wireless Security Options

What is the best way to secure your wireless computer network? There are several security protocols with various versions from which to choose. Depending on the wireless device, you may have to select from different levels of security. The description of security protocols, encryption and authentication that follows is intended to help you better understand your choices.

Security Protocols

WPA (Wi-Fi Protected Access) and **WPA2** (Wi-Fi Protected Access II) are two security protocols that were developed by the Wi-Fi Alliance (WFA) to replace the less-secure **WEP** (Wired Equivalent Privacy). The WFA is a trade association that certifies Wi-Fi® products that are compliant with standards of interoperability. IEEE 802.11 is the set of specifications for implementing WLAN (Wireless Local Area Network) computer communication within the 2.4 to 5GHZ frequency bands. WLAN typically provides a connection between wireless devices to the Internet using an AP (access point).

WPA was originally referred to as the draft IEEE 802.11i standard, since it became available first, and was intended as an intermediate solution pending the availability of a full IEEE 802.11i standard. **WPA2** was known as IEEE 802.11i-2004, the year it first became available. Wi-Fi devices that have been certified since 2006 generally support both **WPA** and **WPA2**.

WPS (Wi-Fi Protected Setup™) provides the easiest way to establish a secure wireless network for home or small office (SOHO) environments. Introduced in 2007, **WPS** was created by WFA so that users who might otherwise be intimidated by the available security options could set up a secure network, and later add new devices, with a simple automated process. PBC (Push Button Configuration) requires just the push of a button. Today most wireless devices, from routers to wireless printers and cameras, have a **WPS** button. **WPS** enables WPA2 security protocol.

Encryption

WPA typically provides data encryption using **TKIP** (Temporal Key Integrity Protocol), which dynamically generates a new 128-bit key for each data packet that is transmitted between networks. WPA also has an integrity checking feature, designed to prevent a hacker from altering and re-sending the data packets.

WPA2 uses **CCMP**, for Counter Cipher Mode with Block Chaining Message Authentication Code Protocol, which uses a higher standard known as **AES** (Advanced Encryption Standard). Therefore **CCMP** provides stronger security than **TKIP**. It was designed to provide data confidentiality, user authentication, and access control. WPS also uses a form of **AES**.

Authentication

With both WPA and WPA2, there are two types of authentication. For home or small office environments, **WPA-Personal** and **WPA2-Personal** are widely used. Enterprise networks for business use **WPA-Enterprise** and **WPA2-Enterprise**.

WPA-Personal, also called **WPA-PSK** (for Pre-shared key) / **WPA2-Persona**l or **WPA2-PSK**:
Was designed for home and small office networks, and does not require an authentication server. Instead, each network device authenticates with the AP (access point) using the same key generated from an alpha-numeric password or passphrase. The password must be between 8-64 characters, and should not be a commonly known phrase.

WPA-Enterprise, also known as **WPA-802.1X** / **WPA2-Enterprise** or **WPA2-802.1X**:
Was designed for enterprise networks, and requires a RADIUS authentication server. The server uses a set of protocols to implement secure access for devices attempting to communicate with the network.

Although this is a more complicated setup, it provides the best security through **EAP,** for Extensible Authentication Protocol. **EAP** is actually a general framework, or architecture, for creation of keying material for message authentication. For example, when **EAP** is implemented in an 802.1X-enabled Network Access Server (NAS) device, **EAP** methods are used to generate a secure private key that can be used for wireless encryption. This will ensure that only authorized network devices can access the network.

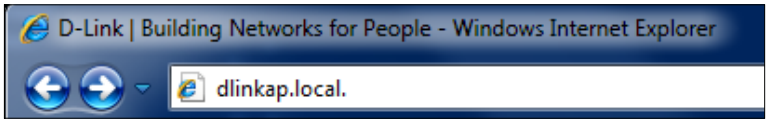
The WPS protocol uses **EAP** message exchanges for authentication. There are two methods:

1. Push-Button-Method means the user simply pushes a button on the access point or router, and within a minute or two pushes a button on the new wireless client device, in order to connect it to the wireless network.
2. The PIN method uses a Personal Identification Number that must be read from either a sticker, wireless configuration card, or the display on the wireless device. Support for this mode is mandatory for access points. However, there is some concern that the messages sent between the AP and the wireless client when attempting to validate the PIN could make the network vulnerable to attack. Most companies have fixed this issue with updated firmware.

Configuring WPA/WPA2 Personal

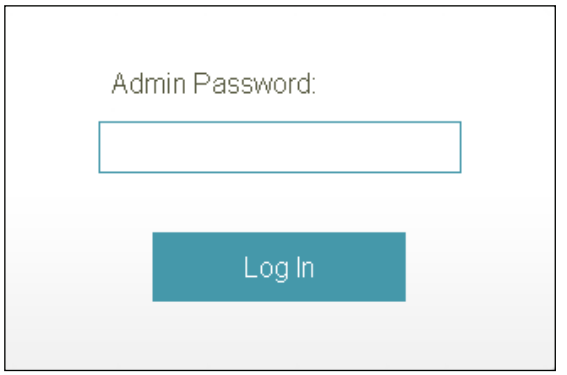
If you did not enable wireless security during initial setup, it is recommended that you do so using the web-based configuration utility. Establish wireless connectivity before enabling wireless security. If you prefer WPS, proceed to "Connecting to a Wireless Client" on page 42.

1. Log into the web-based configuration by opening a web browser and entering **http://dlinkap.local./**.



2. Enter the **Admin Password** (blank by default) and click **Login**.

   ***Note**: By default, Admin is the user name. If you did not create a password, it should be left blank.*



3. The configuration interface will open to the *Home* page. Click on the **Settings** drop-down menu and select **Wi-Fi**. Then configure the Wi-Fi network you would like your DAP-1520 to connect to.

Connecting to a Wireless Client

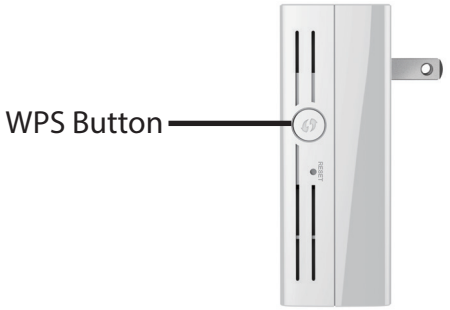
WPS Button

WPS (Wi-Fi Protected Setup) is a simple and secure way to connect your wireless devices with the DAP-1520. Most wireless devices such as wireless routers, media players, printers, and cameras will have a WPS button (or a software utility with WPS). Refer to the user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the **WPS** button on the DAP-1520 for a minimum of one second. The LED on the device will start to blink. You can also use the WPS option in the *Wi-Fi Connection Setup Wizard* (refer to "Setup Wizard" on page 18).

Step 2 - Within 120 seconds, press the **WPS** button on your wireless device.

Step 3 - Allow up to one minute to connect. When the LED stops blinking and turns solid green, you will be connected and your wireless connection will be secured with WPA2.

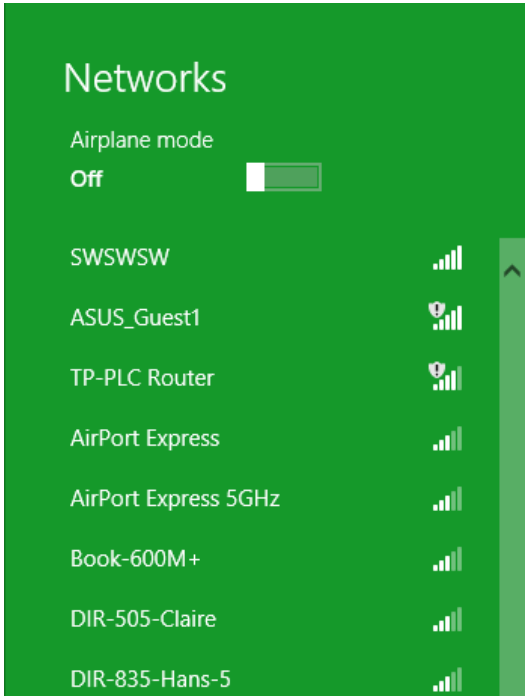


Windows® 8
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

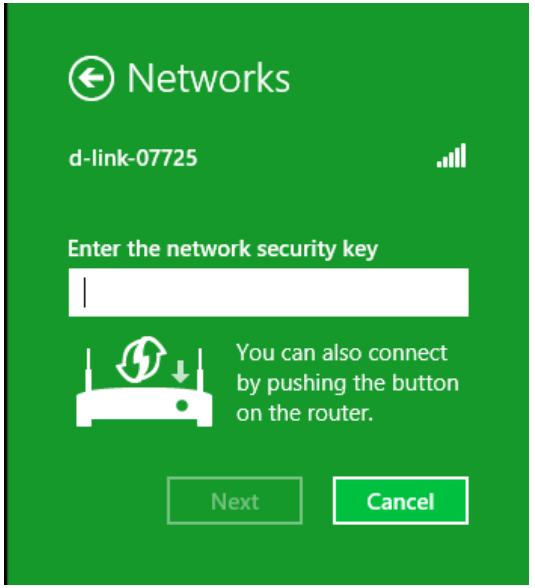
To join an existing network, locate the wireless network icon in the taskbar, next to the time display.

Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

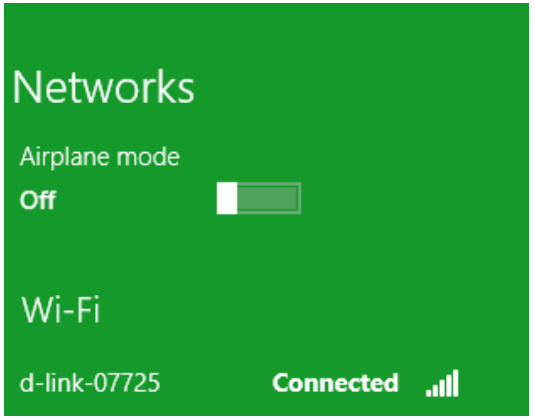


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at this point to enable the WPS function.



When you have established a successful connection with a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Windows® 7
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).

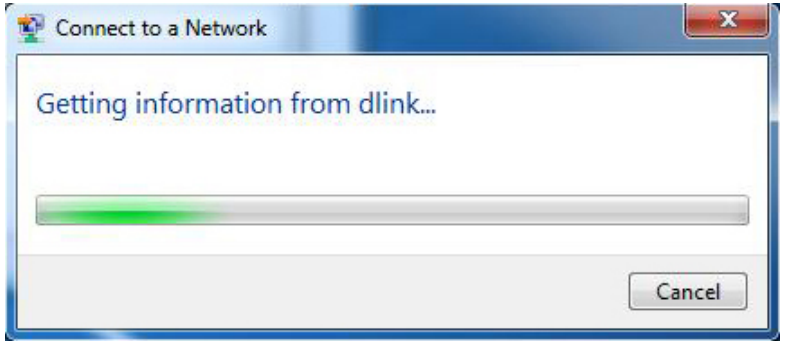
Wireless Icon

2. The utility will display any available wireless networks in your area.

3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

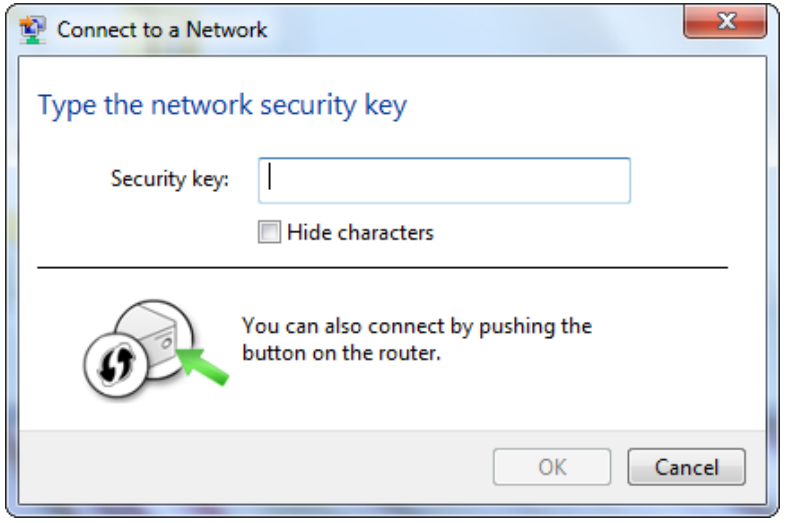
   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Wireless Basics section in this manual for more information.

4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



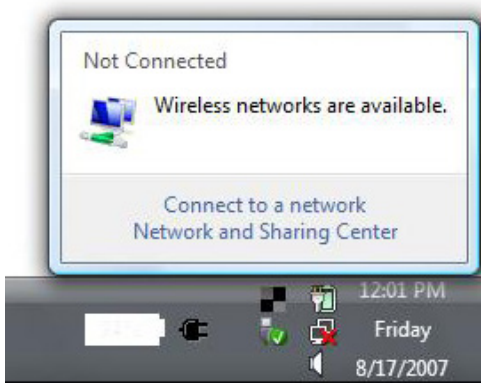
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the "Wireless Networks Are Available" bubble, click on the center of the bubble to access the utility.

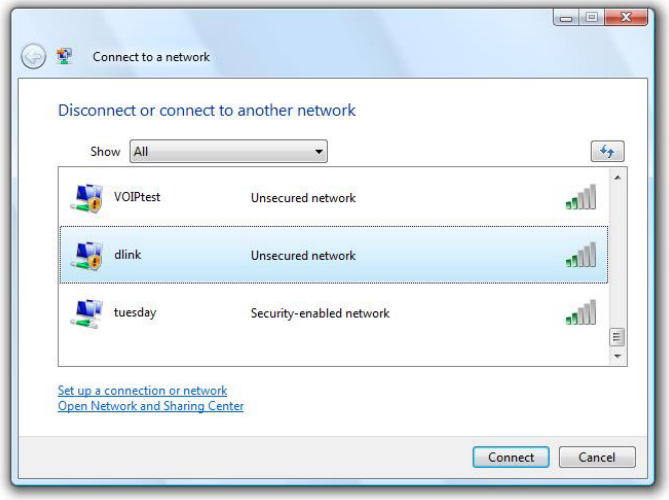
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click **Connect**.

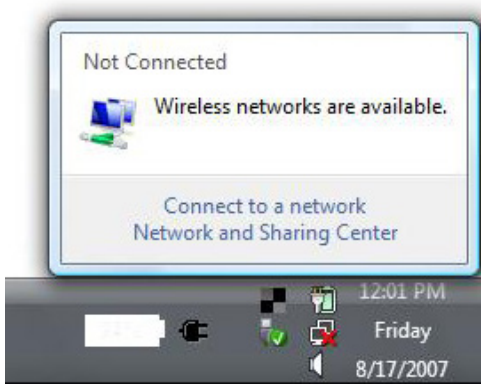
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Troubleshooting" on page 54 for more information.



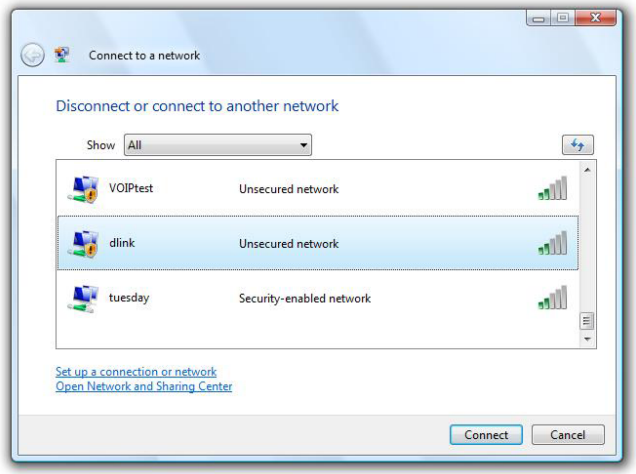
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



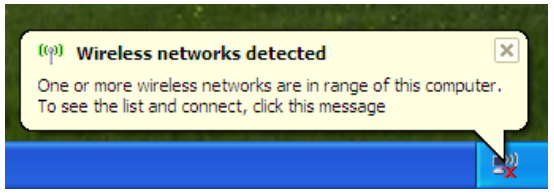
3. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

Windows® XP

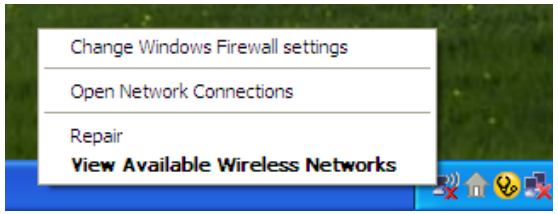
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.



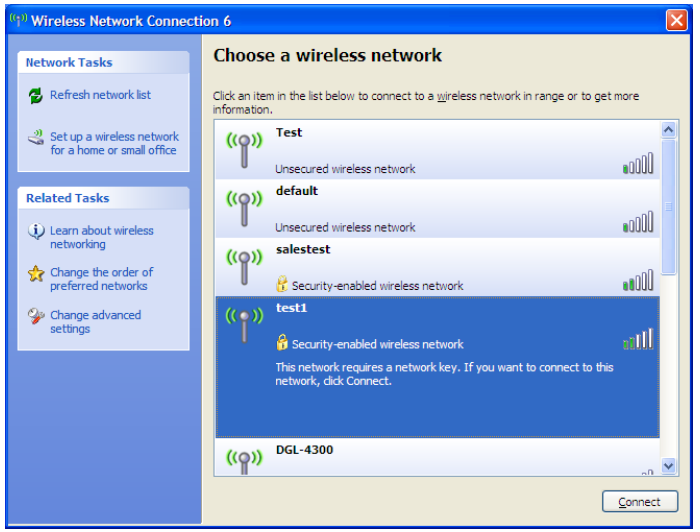
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

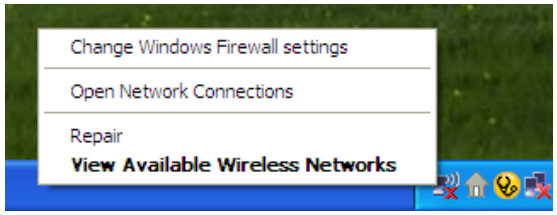
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the **Wireless Basics** section in this manual for more information.



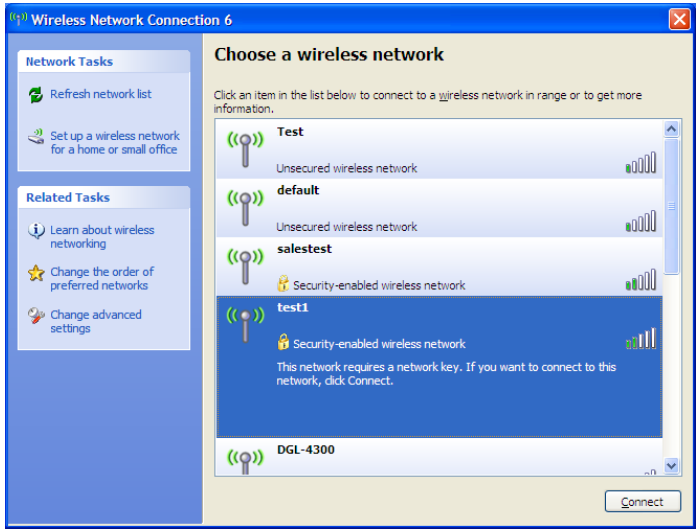
WPA/WPA2

It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

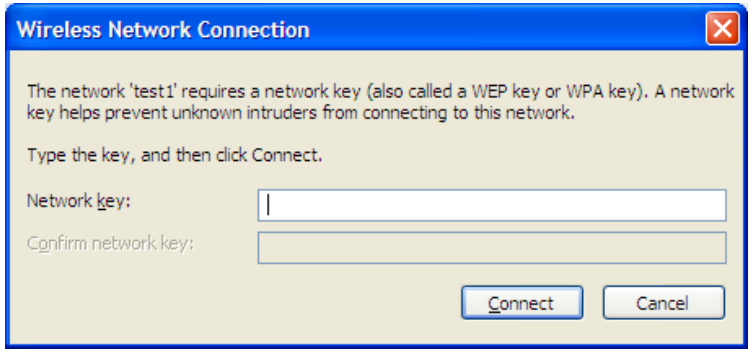
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect**.



It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.

Troubleshooting

This section provides solutions to problems that can occur during the installation and operation of the DAP-1520. Read the following instructions if you are having problems:

1. Why can't I access the web-based configuration utility?

When you enter the IP address of the DAP-1520 (**192.168.0.50** for example), or even if you enter **http://dlinkap.local./**, you are not connecting to a website on the Internet. The DAP-1520 has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Microsoft Internet Explorer® 7 and higher
  - Mozilla Firefox®
  - Apple Safari® 4 and higher
  - Google Chrome™

- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings on your web browser:
  - Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.
  - Click the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click the **LAN Settings** button. Make sure nothing is checked. Click **OK**.
  - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
  - Close your web browser (if open) and re-open it.

- To access the web management interface, open your web browser and enter **http://dlinkap.local./** or **http://192.168.0.50*** in the address bar. This should open the login page for the web-based configuration utility.

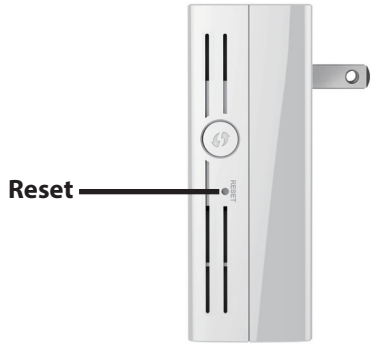
  ***Note**: This is the default IP address. Once the DAP-1520 connects to your router, it will be assigned a new IP address based on your router/network's DHCP settings. You will have to log in to your router and view the DHCP table to see what IP address was assigned to the DAP-1520. If you are using a D-Link router, follow these instructions to find the IP address that was assigned:*
  *Using the router's Web-based configuration utility, go to **Setup** > **Network Settings**. Scroll down to the bottom of the page, below the heading that says **Number of Dynamic DHCP Clients**, to view the list of connected devices. Refer to the MAC address that is printed on the label that is attached to the bottom of the DAP-1520 to find the corresponding IP address.*

- If you still cannot access the configuration, unplug the extender from the power outlet for at least 10 seconds and plug it back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your extender. Unfortunately this process will change all your settings back to the factory default settings.

To reset the extender, locate the reset button (hole) on the side of the unit. With the extender powered on, use an unfolded paper clip to hold the button down for 10 seconds. Release the button and the extender will go through its reboot process (as indicated when the LED turns solid red).



Wait for at least 30 seconds to access the extender. The default IP address is **http://dlinkap.local./**. When logging in, the username is **admin** and leave the password field empty.

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. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely and conveniently access your network. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs 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 adapters used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

Tips

Here are a few things to keep in mind when you are installing your Wireless AC750 Dual Band Range Extender.

Centralize the extender's location

For best performance, make sure you place the extender in a centralized location within your desired usage area. Try to place the extender so that there are minimal obstructions between it and the uplink router. If possible, use an elevated power outlet, so the signal can be dispersed more easily. If you have a large home or usage area, you may need several extenders in order to achieve optimal coverage.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the extender. This can significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let your neighbors or intruders connect to your wireless network. Secure your wireless network by utilizing the WPA or WEP security feature on the extender and uplink router. Refer to "Wireless Security Options" on page 39 for more information.

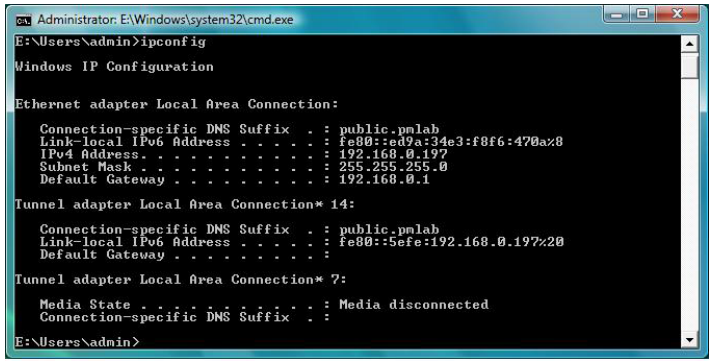
Networking Basics

Check your IP address

After you install your new D-Link wireless adapter and have established a wireless connection, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e., router) automatically. To verify your IP address, please follow the steps below.

Windows® 8 Users

- Press the **Windows key** and **R** together. Type **cmd** in the box and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.

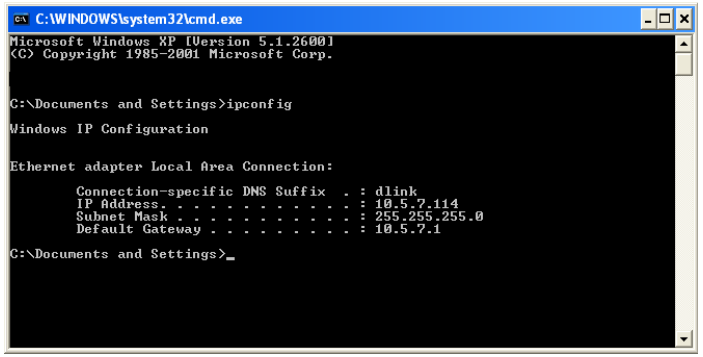


Windows® 7/Vista® Users

- Click **Start**, type **cmd** in the search box and then click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.

Windows® XP Users

- Click on **Start** > **Run**. In the run box type **cmd** and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and the default gateway of your adapter.



If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

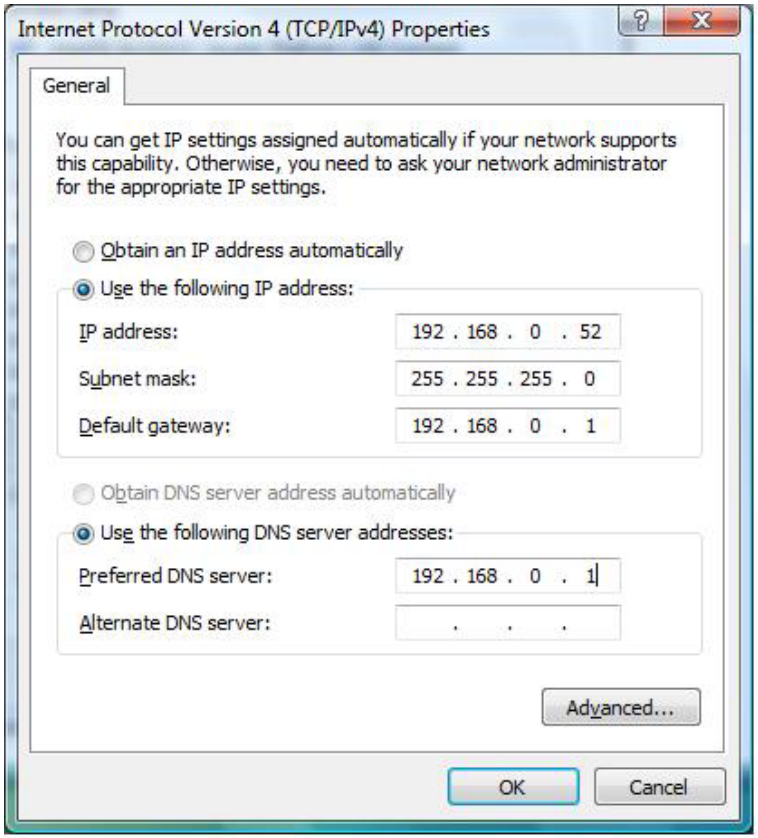
Statically Assign an IP Address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Windows® 8 Users

- Press the **Windows** key and then type **IP**. Click **Settings** on the right side and then click **View Network Connections**.
- Right-click on the adapter which represents your D-Link wireless network adapter.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router or network.

  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.
- Set **Default Gateway** the same as the LAN IP address of your router or gateway.
- Set **Primary DNS** the same as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.



Windows® 7/ Vista® Users

- Click on **Start** > **Control Panel** (make sure you are in Classic View). Double-click on the **Network and Sharing Center** icon. If you are using Windows Vista, click on **Manage network connections** along the left panel in the window. For Windows® 7, click on **Change adapter settings**.

- Right-click on the **Local Area Connection** which represents your D-Link wireless network adapter which will be connected to your network.

- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.

- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router or network.

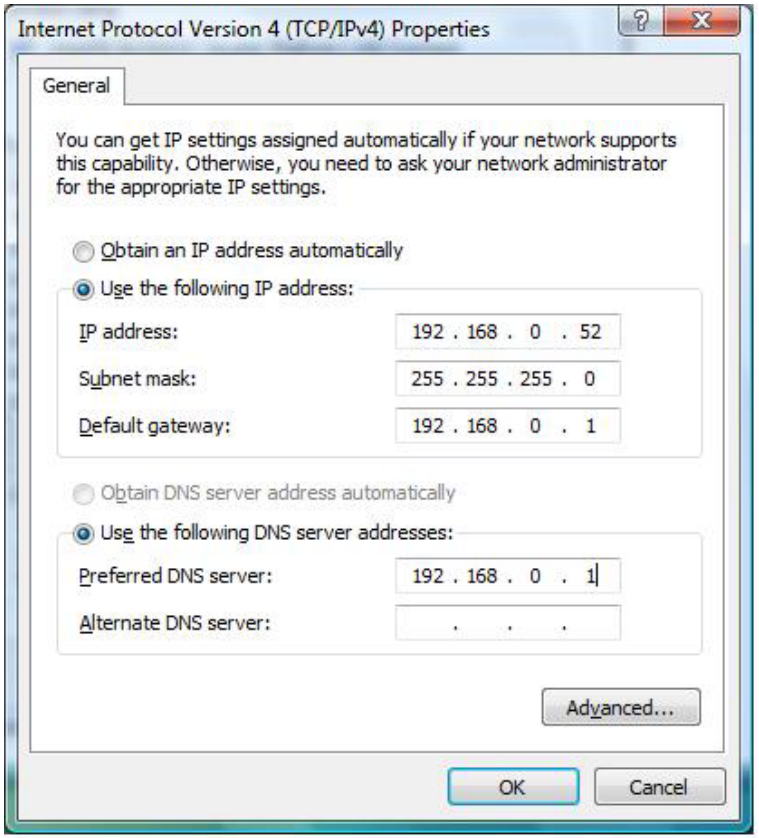
  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.

- Set **Default Gateway** the same as the LAN IP address of your router or gateway.

- Set **Primary DNS** the same as the LAN IP address of your router or gateway.

- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).

- Click **OK** to save your settings.



Technical Specifications

Standards [1]
- IEEE 802.11ac draft
- IEEE 802.11a
- IEEE 802.11n
- IEEE 802.11g

Wireless Frequency Range [2]
- 2.4GHz to 2.4835GHz
- 5.18MHz to 5.85MHz

Antenna
- Internal Antenna

Security
- Wi-Fi Protected Access (WPA/WPA2)
- Wi-Fi Protected Setup (WPS)

Advanced Features
- QRS Mobile setup app for iOS and Android devices

Device Management
- Web UI

Diagnostic LEDs
- Status/WPS

Operating Temperature
- 32 to 104˚F (0 to 40˚C)

Operating Humidity
- 0% to 90% non-condensing

Power Input
- AC 110-240 V

Maximum Power Consumption
- 5.5 W

Certifications
- EMI/EMC
- FCC
- CE
- IC
- C-Tick
- UL
- Wi-Fi Certified

Dimensions
- 3.62 x 2.28 x 1.35 inches (92 x 58 x 34.2 mm)

Weight
- 3.67 ounces (104 grams)

Warranty
- 1-Year Limited Warranty

1 Maximum wireless signal rate derived from IEEE Standard 802.11ac (draft), 802.11a, 802.11g, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

2 Frequency Range varies depending on country's regulation.

Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DAP-1520)
- Hardware Revision (located on the label on the device (e.g. rev A1))
- Serial Number (s/n number located on the label on the device).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

For customers within the United States:

Phone Support:
(877) 453-5465

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

GPL Code Statement

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

http://tsd.dlink.com.tw/GPL.asp

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPLsource code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:
Email: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble
The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. 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 them 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 prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. 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.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.
All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.
No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention
is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.
You may convey 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; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.
You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work). You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights

from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If 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 convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.
The Free Software Foundation may publish revised and/or new versions of the GNU 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 that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.
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.

16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS 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.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim (USA):

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

Submitting A Claim (Canada):

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-800-361-5265, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.ca/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:
Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:
This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Declaration d'exposition aux radiations:
Cet equipement est conforme aux limites d'exposition aux rayonnements IC etablies pour un environnement non controle. Cet equipement doit etre installe et utilise avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Registration

Register your product online at registration.dlink.com

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
December 2, 2013