USER MANUAL

DAP-1555

VERSION 1.0

D-Link®

WIRELESS

Table of Contents

Product Overview 4
Package Contents 4
System Requirements 4
Introduction 5
Features 6
Hardware Overview 7
Connections 7
LEDs 8

Installation 9
Before you Begin 9
Wireless Installation Considerations 10

AP/BRIDGE Mode 11

Configuration for AP Mode 13
Web-based Configuration Utility 13
Setup Wizard 14
Wireless Setup Wizard 15
Add Wireless Device With WPS 22
Manual Configuration 24
Wireless Settings 24
Network Settings 26
DHCP 26
Static IP 27
Advanced 28
MAC Address Filter 28
Advanced Wireless 29
WISH 30
Tools 32
Admin 32
Time 33
System 34
Firmware 35
Status 36
Device Info 36
Wireless 37
Logs 38
Statistics 39
Wish Sessions 40
Help 42

Configuration for Bridge Mode 43
Web-based Configuration Utility 43
Setup Wizard 44
Wireless 52
Network Settings 54
Static 54
DHCP 55
Advanced 56
Advanced Wireless 56
Tools 57
Admin 57
System 58

Firmware 59
Status 60
Device Info 60
Logs 61
Help 62

Wireless Security 63
What is WEP? 63
What is WPA? 64
Configure WEP In AP Mode 65
Configure WPA-Personal (PSK) In AP Mode 66
Configure WPA-Enterprise (RADIUS) In AP Mode 67
Configure WEP In Bridge Mode 69
Configure WPA-Personal (PSK) In Bridge Mode ... 70
Configure WPA-Enterprise (RADIUS) In Bridge Mode 71

Connect to a Wireless Network 73
Using Windows® XP 73
Configure WEP 74
Configure WPA-PSK 76

Troubleshooting 78

Wireless Basics 82
What is Wireless? 83
Tips 85
Wireless Modes 86

Networking Basics 87
Check your IP address 87
Statically Assign an IP address 88

Technical Specifications 89

Contacting Technical Support 90

Warranty 91

Registration 97

Package Contents

- D-Link DAP-1555 Wireless N Dualband MediaBridge
- 2 Detachable Antennas
- Power Adapter
- CAT5 Ethernet Cable
- Mounting Kit
- Rubber Feet
- CD-ROM with Installation Wizard, User Manual, and Special Offers

Note: Using a power supply with a different voltage rating than the one included with the DAP-1555 will cause damage and void the warranty for this product.

System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0, Mozilla 1.7.12 (5.0), or Firefox 1.5 and above (for configuration)

Introduction

TOTAL PERFORMANCE
Combines award winning access point features and Draft 802.11n wireless technology to provide the best wireless performance

TOTAL SECURITY
The most complete set of security features including WPA2 and MAC Address Control to protect your network against outside intruders

TOTAL COVERAGE
Provides greater wireless signal rates even at farther distances for best-in-class Whole Home Coverage.

ULTIMATE PERFORMANCE
The D-Link Xtreme N™ MediaBridge (DAP-1555) is a draft 802.11n compliant device that delivers real world performance of up to 650% faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the Xtreme N™ MediaBridge to router and share your high-speed Internet access with everyone on the network. In addition, this MediaBridge includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

EXTENDED WHOLE HOME COVERAGE
Powered by Xtreme N™ technology, this high performance MediaBridge provides superior Whole Home Coverage while reducing dead spots. The Xtreme N™ MediaBridge is designed for use in bigger homes and for users who demand higher performance networking. Add a Xtreme N™ notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

TOTAL NETWORK SECURITY
The Xtreme N™ MediaBridge supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA and WEP standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices.

* Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and Draft 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 conditions will adversely affect wireless signal range.

Features

- **Faster Wireless Networking** - The DAP-1555 provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless access point gives you the freedom of wireless networking at speeds 650% faster than 802.11g.

- **Compatible with 802.11a, 802.11b and 802.11g Devices** - The DAP-1555 is still fully compatible with the IEEE 802.11a/b/g standard, so it can connect with existing 802.11a/b/g PCI, USB and Cardbus adapters.

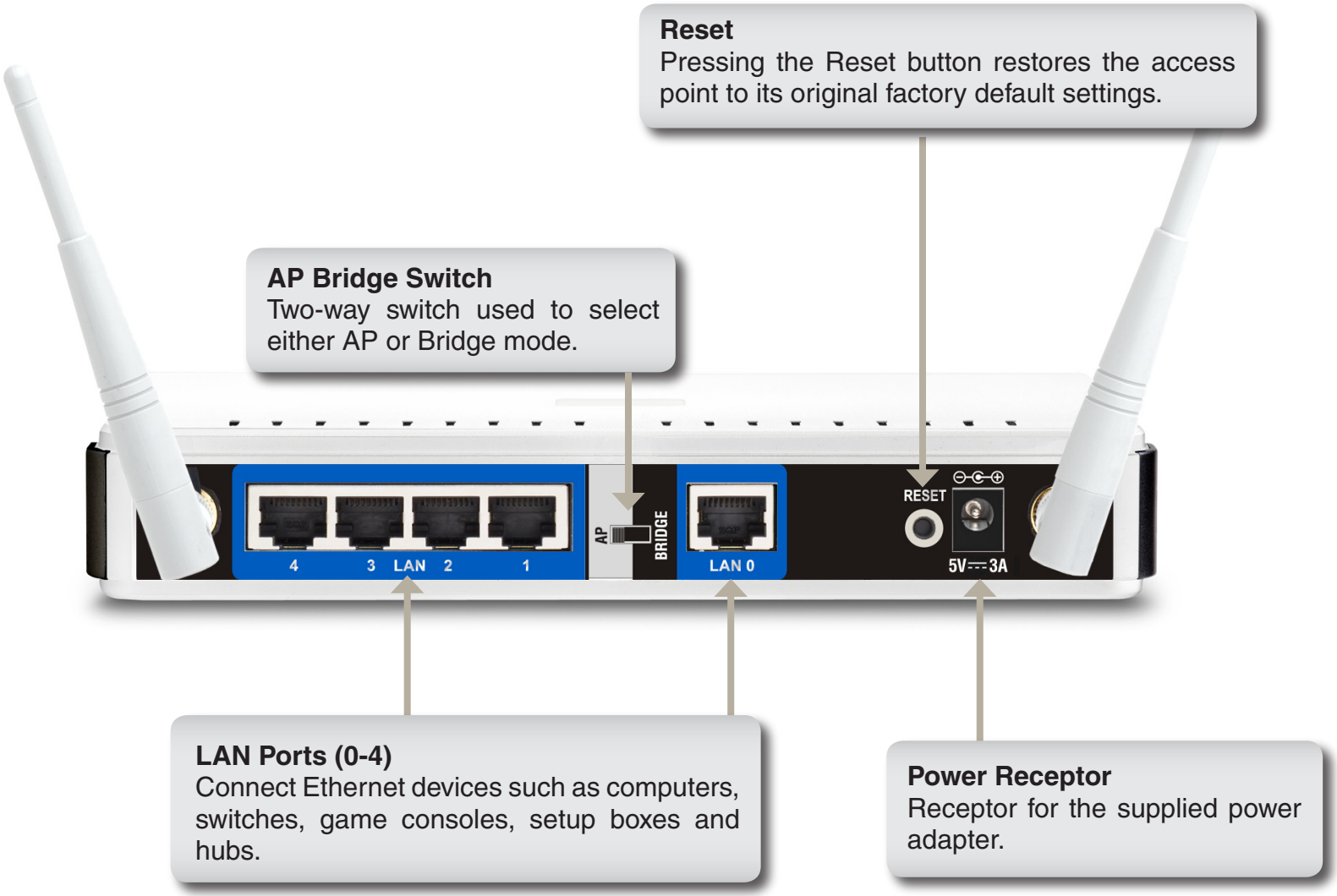
- **Advanced Firewall Features** - The Web-based user interface displays advanced network management features including:

  Content Filtering - Easily applied content filtering based on MAC Address.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DAP-1555 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your access point to your specific settings within minutes.

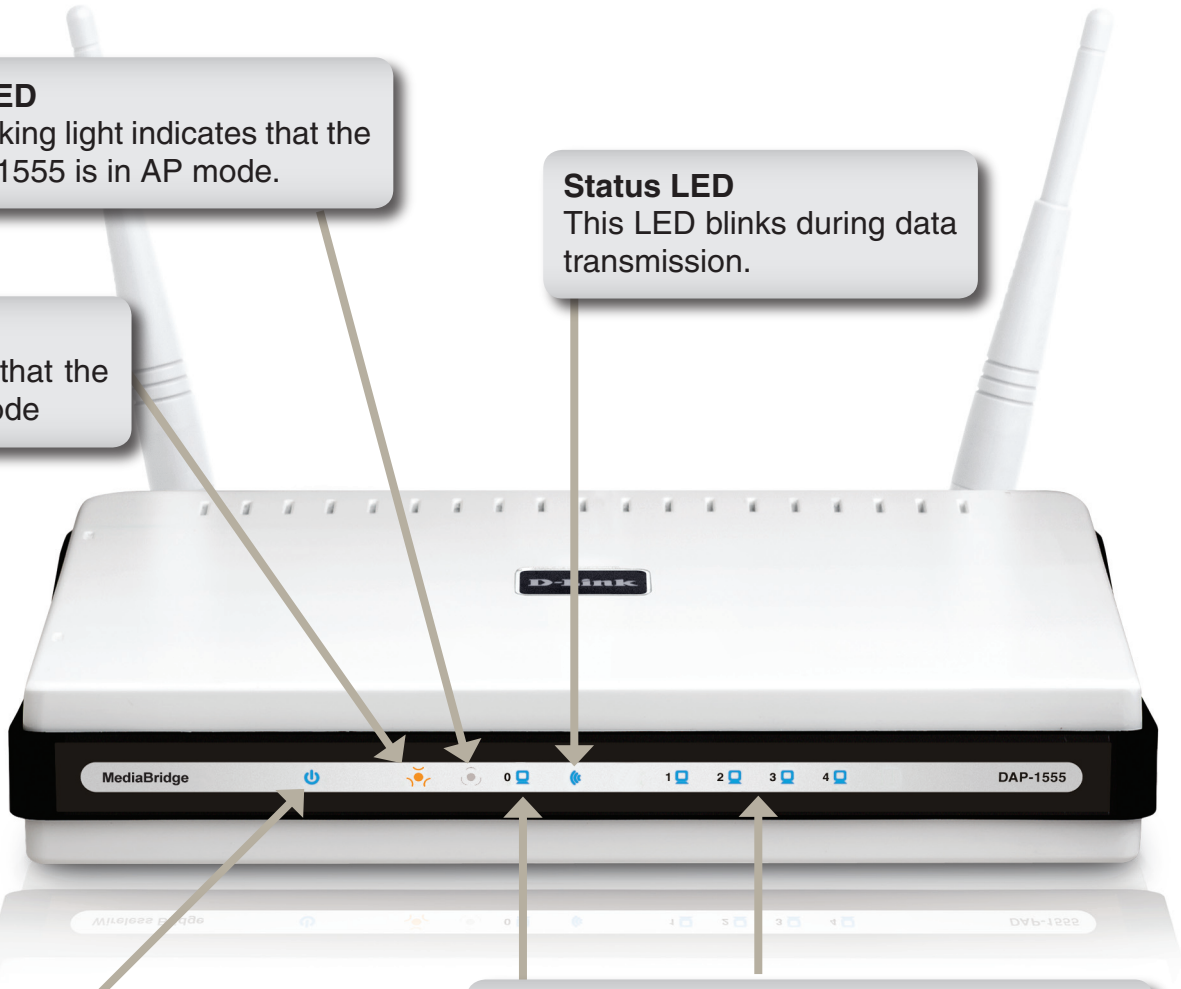
* Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data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

Hardware Overview
Connections



Hardware Overview

LEDs



AP LED
A blinking light indicates that the DAP-1555 is in AP mode.

Status LED
This LED blinks during data transmission.

Bridge LED
A blinking light indicates that the DAP-1555 is in bridge mode

Power LED
A solid light indicates a proper connection to the power supply.

Local Network LEDs
A solid light indicates a connection to an Ethernet-enabled device on ports 0-4. This LED blinks during data transmission.

Installation

This section will walk you through the installation process. Placement of the DAP-1555 is very important. Do not place the DAP-1555 in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before you Begin

Please configure the MediaBridge with the computer that was last connected directly to your modem. Also, you can only use the Ethernet port on your modem. If you were using the USB connection before using the MediaBridge, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the MediaBridge, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).

If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.

Wireless Installation Considerations

The D-Link wireless access point lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. 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 D-Link access point and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

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

3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless access points, 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 will 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.

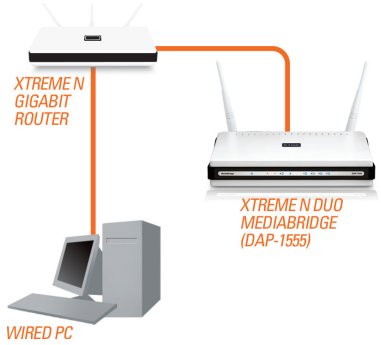
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits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

AP/BRIDGE Mode

Depending on how you want to use your DAP-1555 will determine which mode you use on the DAP-1555. This section will help you figure out which setting works with your setup.

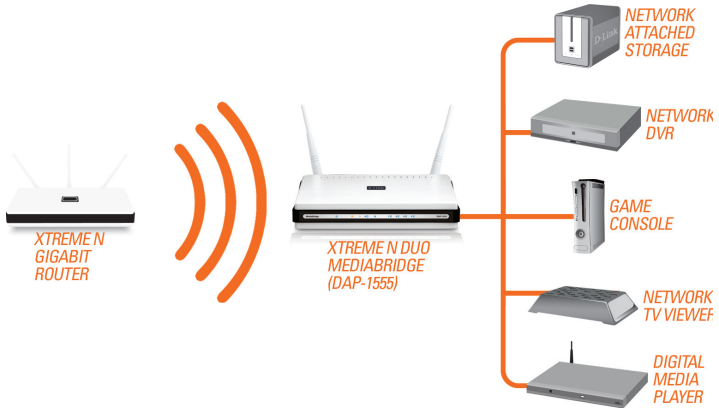
AP Mode

If you already have a wired or wireless router, and want to add a MediaBand (5GHz wireless), to your network, you will need to move the switch on the back panel of the DAP-1555 to “AP”.



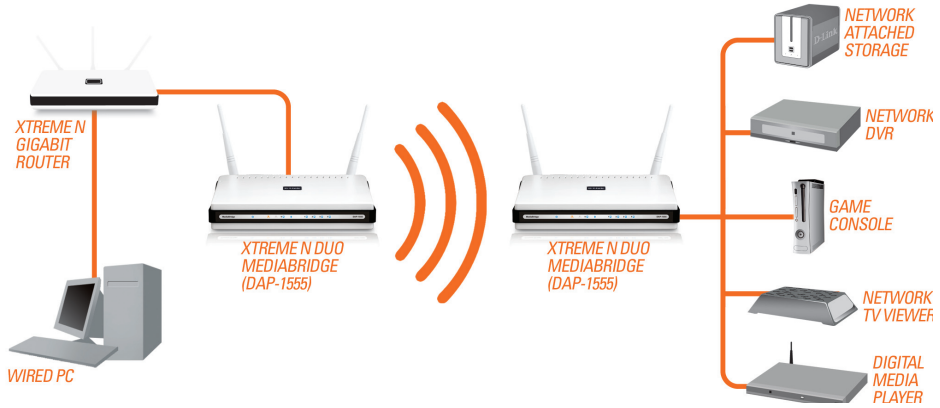
Bridge Mode

If you want to wirelessly connect multiple Ethernet enabled devices such as game consoles, media players, or network attached storage devices you will need to move the switch on the back panel of the DAP-1555 to “BRIDGE”.



Create a Full MediaBand (5GHz wireless) Network

If you have two DAP-1555 devices and want to create a wireless network with full MediaBand technology you will need to connect one MediaBridge to your router and move the switch on the back panel to “AP”. The second MediaBridge will need to be placed next to your Ethernet-enabled devices and you will need to move the switch on the back panel to “BRIDGE”.

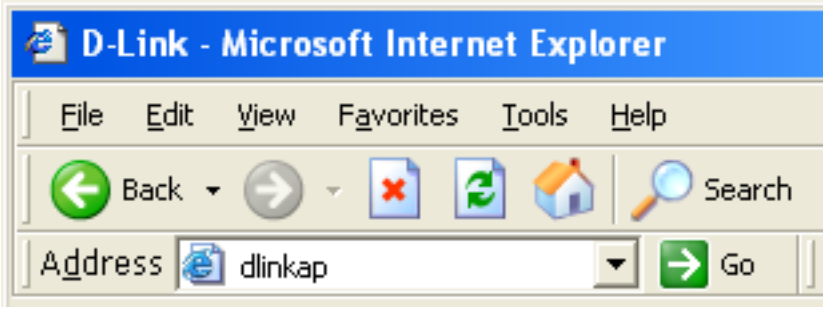


Configuration for AP Mode

This section will show you how to configure your new D-Link wireless access point using the web-based configuration utility.

Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter the friendly address for AP mode (dlinkap).



Select **Admin** from the drop-down menu and then enter your password. Leave the password blank by default.

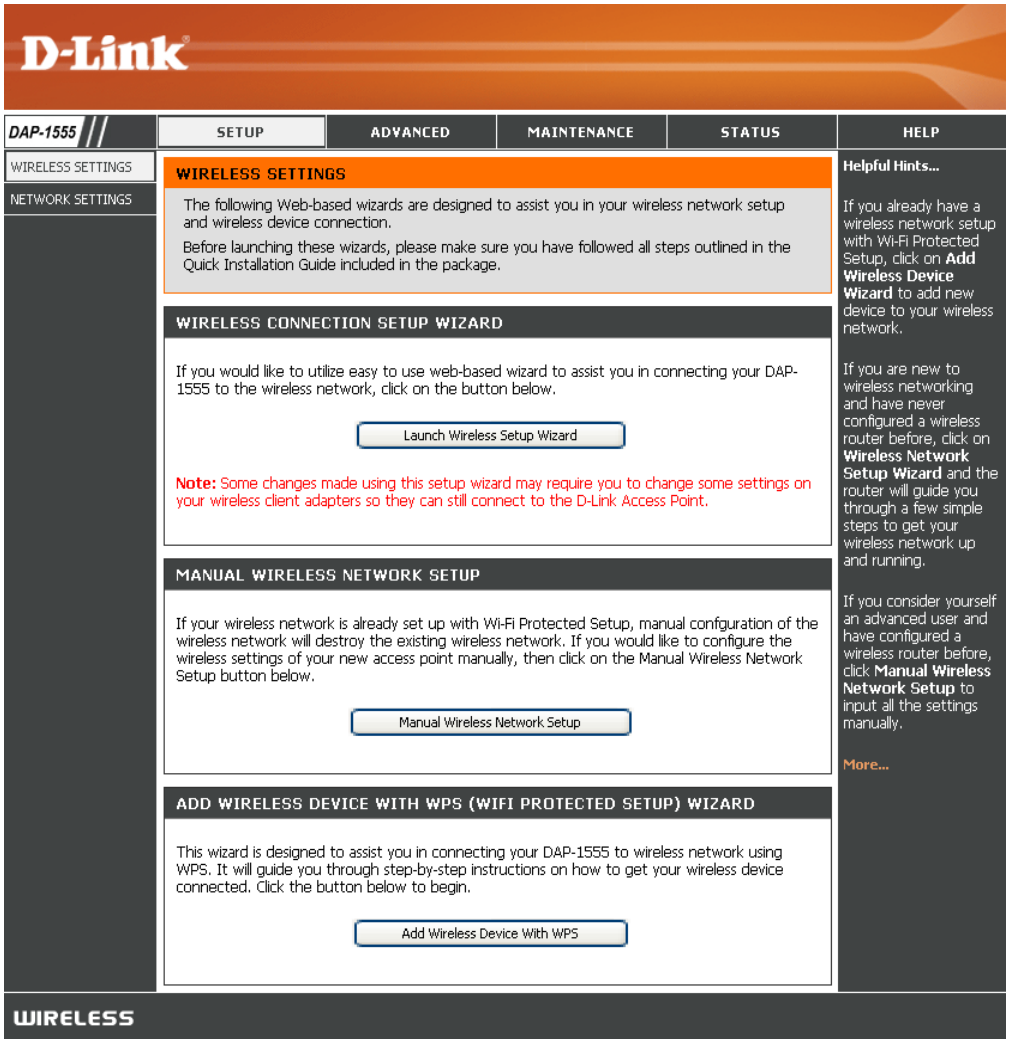
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.

Setup Wizard

Click **Launch Wireless Setup Wizard** to quickly configure your access point.

To setup your wireless network click **Add Wireless Device With WPS** and skip to page 22.

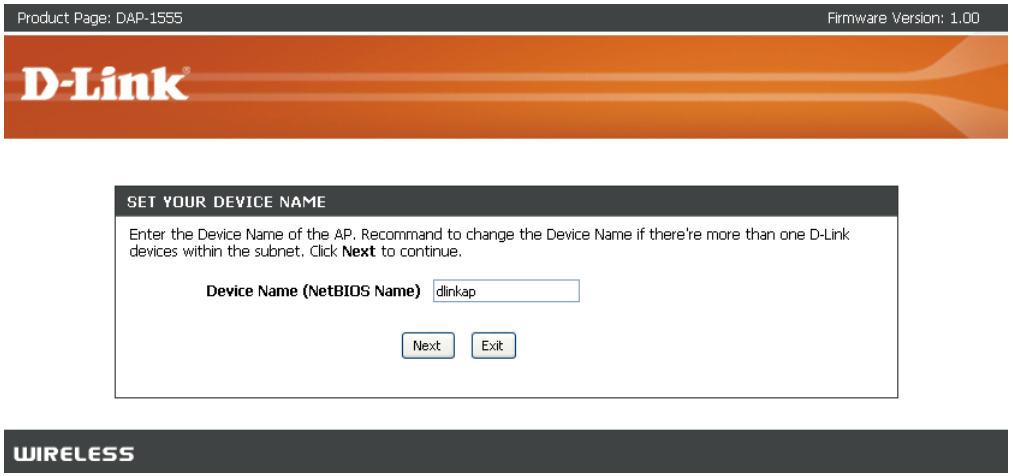
If you want to enter your settings without running the wizard, click **Manual Wireless Network Setup** and skip to page 24.



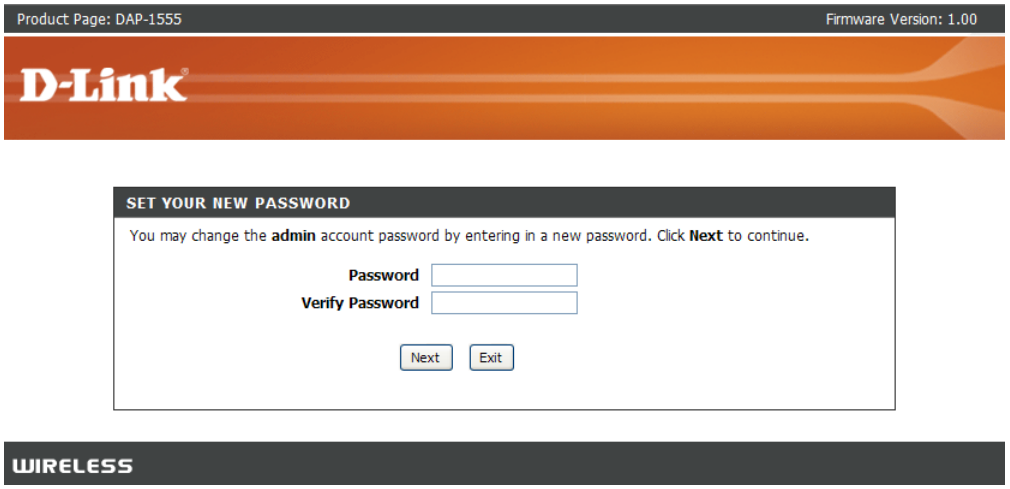
Wireless Setup Wizard

This Wizard is designed to assist you in connecting you wireless device to your access point. It will guide you through step-by-step instructions on how to get your wireless device connected.

Enter the Device Name of the AP and click **Next** to continue. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.



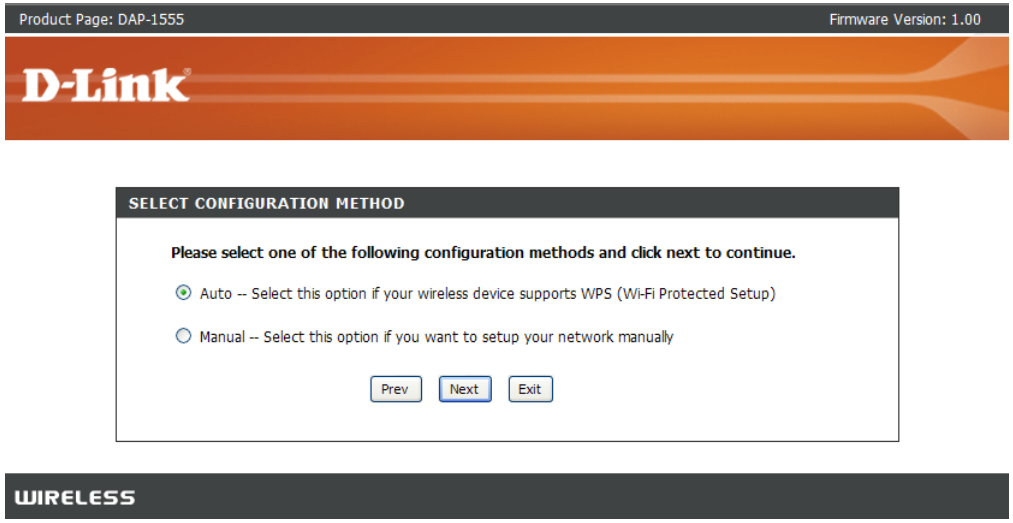
If you want to change the admin account password, enter a new password and click **Next**.



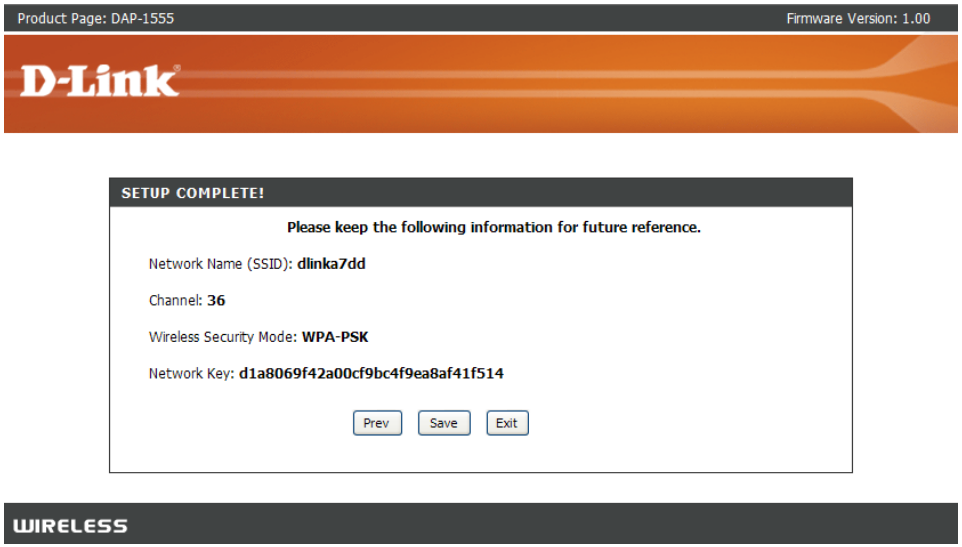
Select **Auto** as the configuration method only if your wireless device supports Wi-Fi Protected Setup.

Skip to page 17 for **Manual** configuration.

Click **Next** to continue.

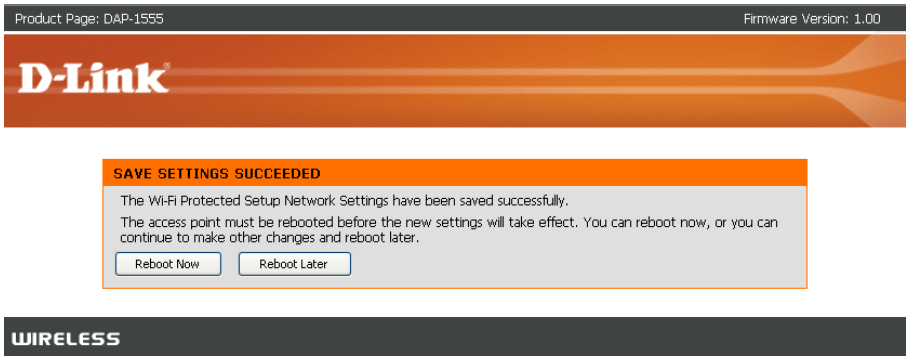


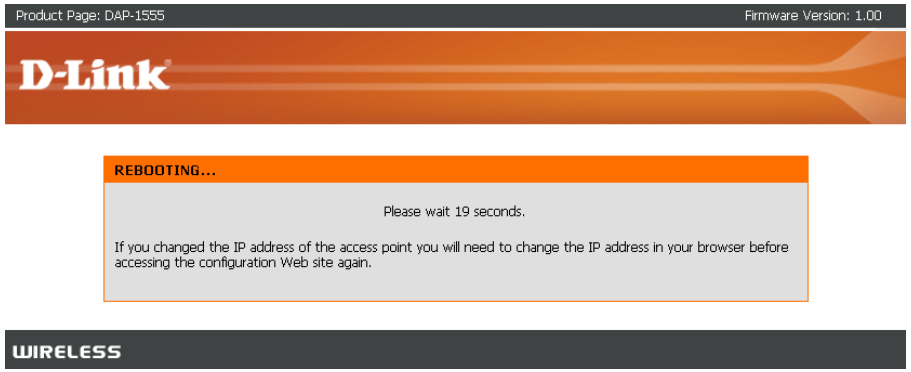
Click **Save** to save your network settings.



In order for your network settings to take effect you must reboot the access point by clicking **Reboot Now**.

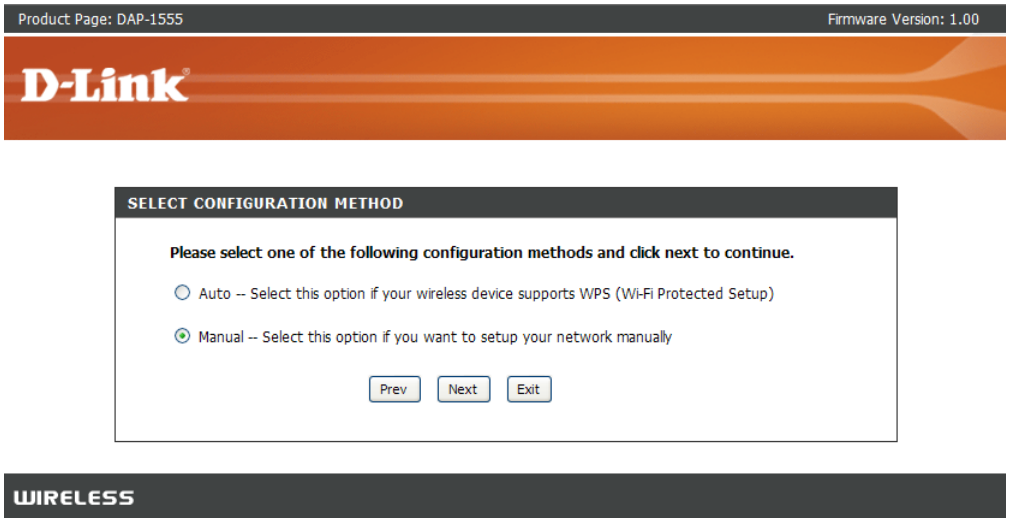
Choose **Reboot Later** to make other changes and reboot later.





Select **Manual** as the configuration method to setup your network manually.

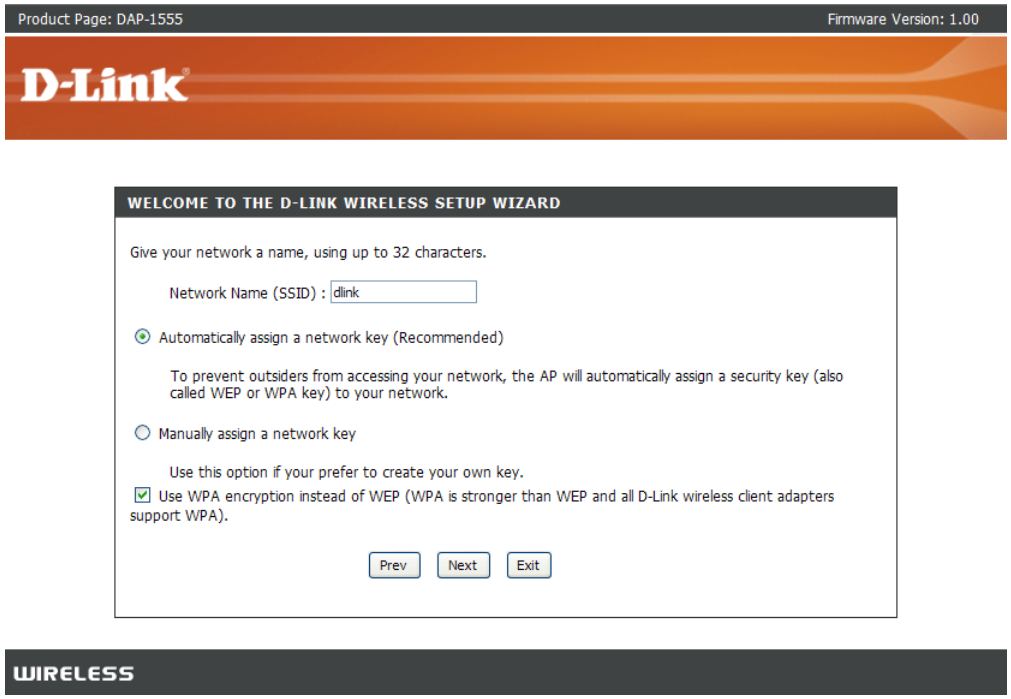
Click **Next** to continue.



Enter a network name and choose Automatically assign a network key.

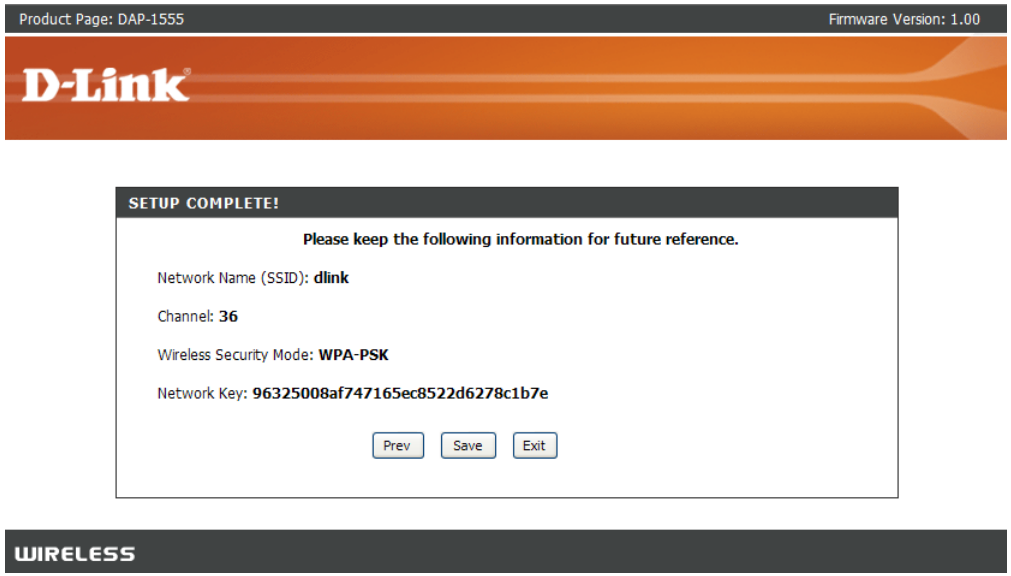
To Manually assign a network key, skip to page 19.

Click **Next** to continue.



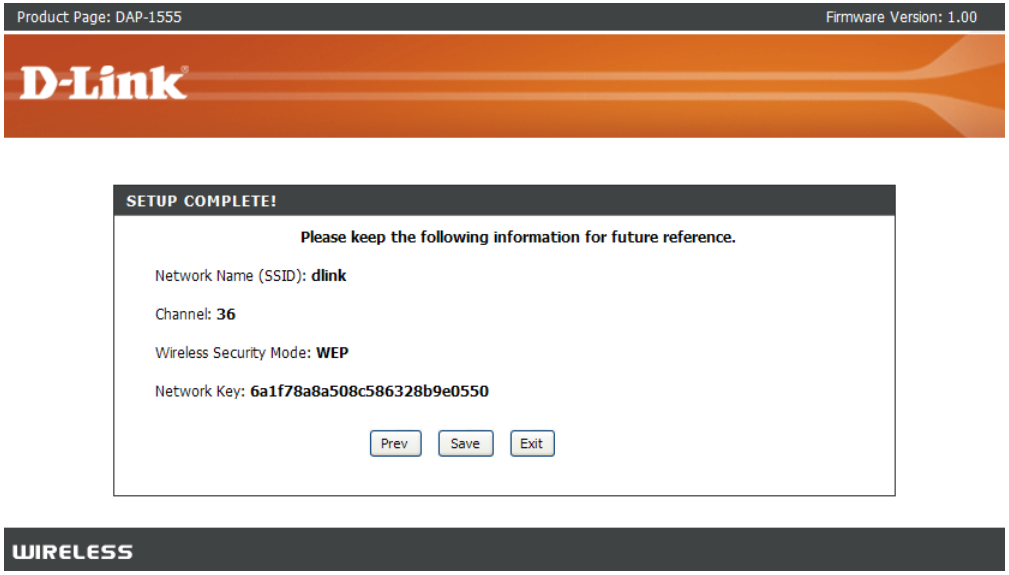
If you choose WPA-PSK encryption, the following screen will show you your Network Key to enter on your wireless clients.

Click **Save** to finish the Setup Wizard.



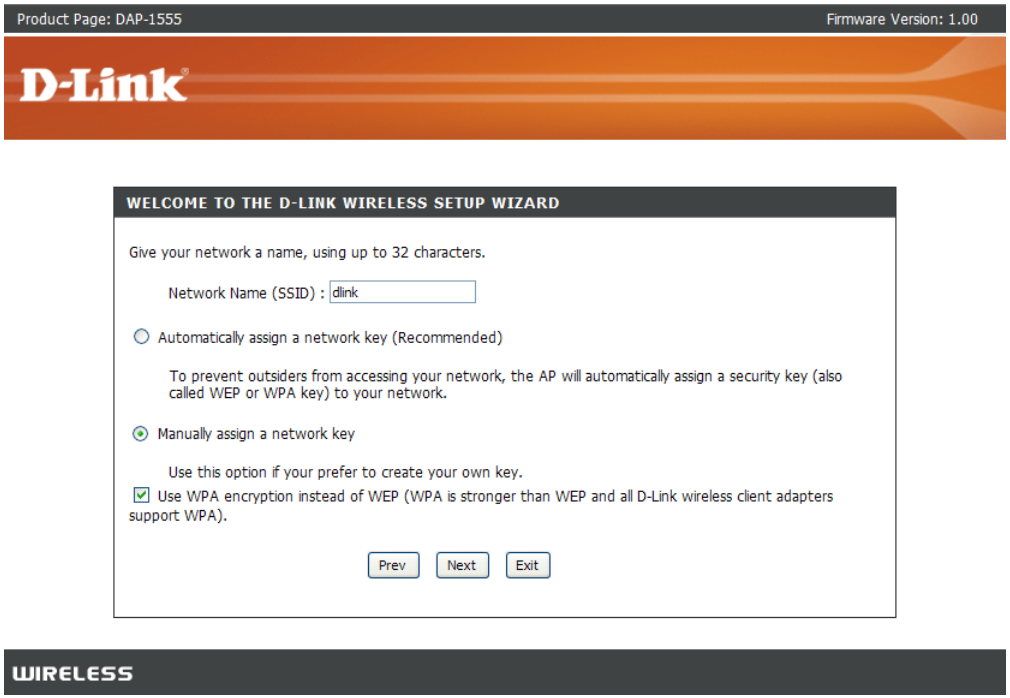
If you choose WEP encryption, the following screen will show you your Network Key to enter on your wireless clients.

Click **Save** to finish the Setup Wizard.



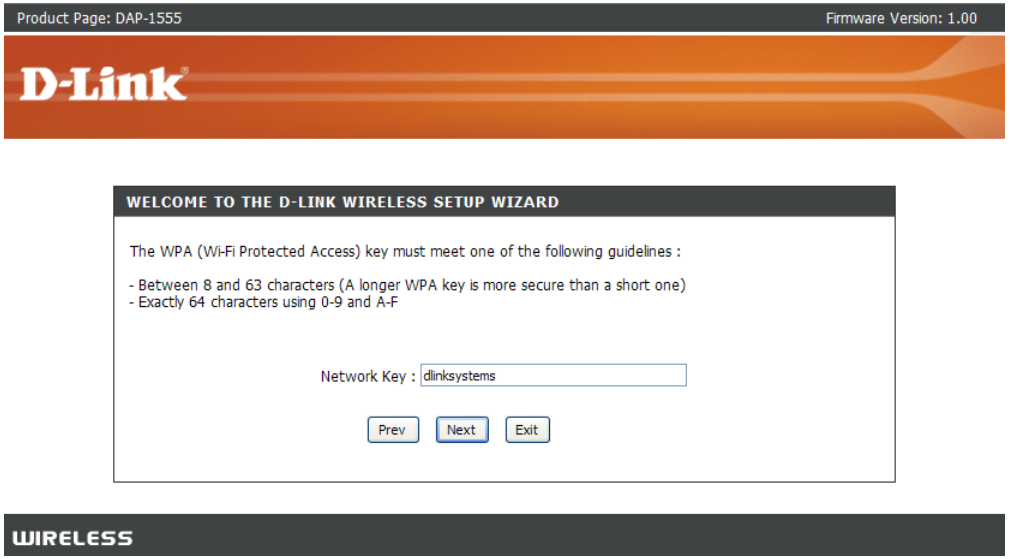
Choose **Manually assign a network key** to create you own key.

Click **Next** to continue.



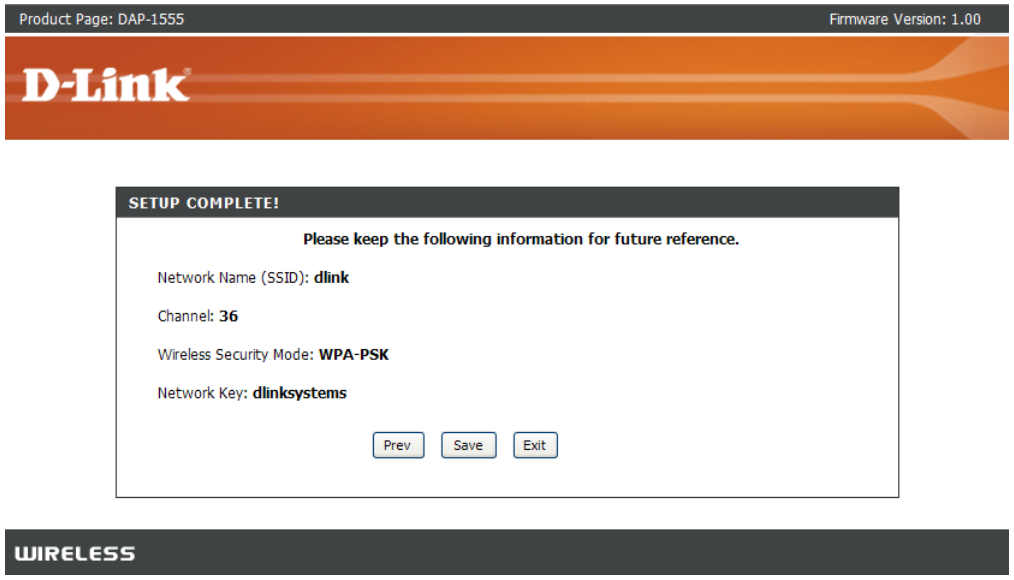
For **WPA** encryption, enter a Network Key between 8 and 63 characters long or enter exactly 64 characters using 0-9 and A-F.

Click **Next** to continue.



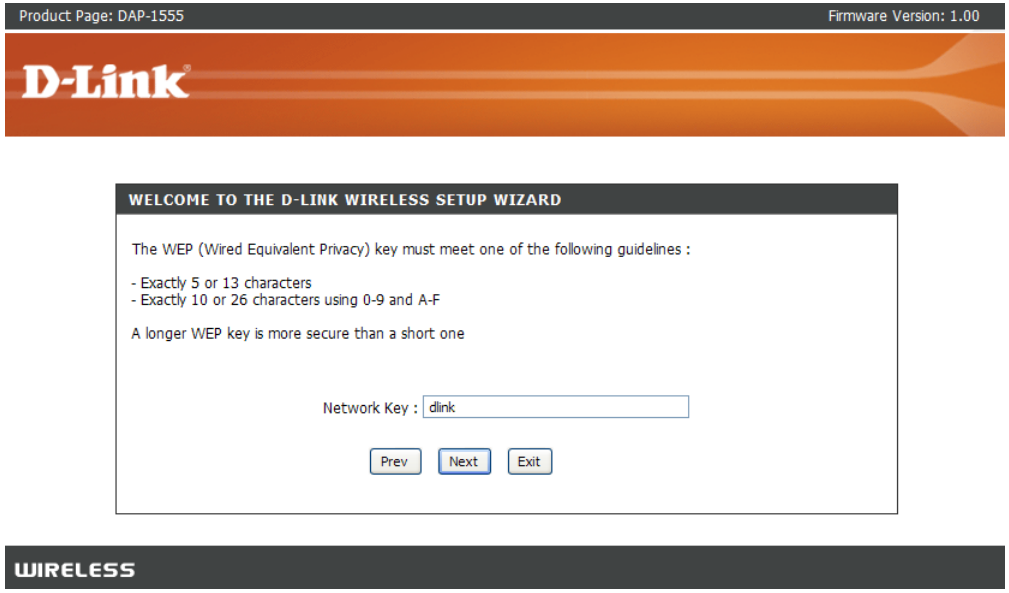
If you select **WPA** encryption, the following screen will show you your network key to enter on your wireless clients.

Click **Save** to finish the Setup Wizard.



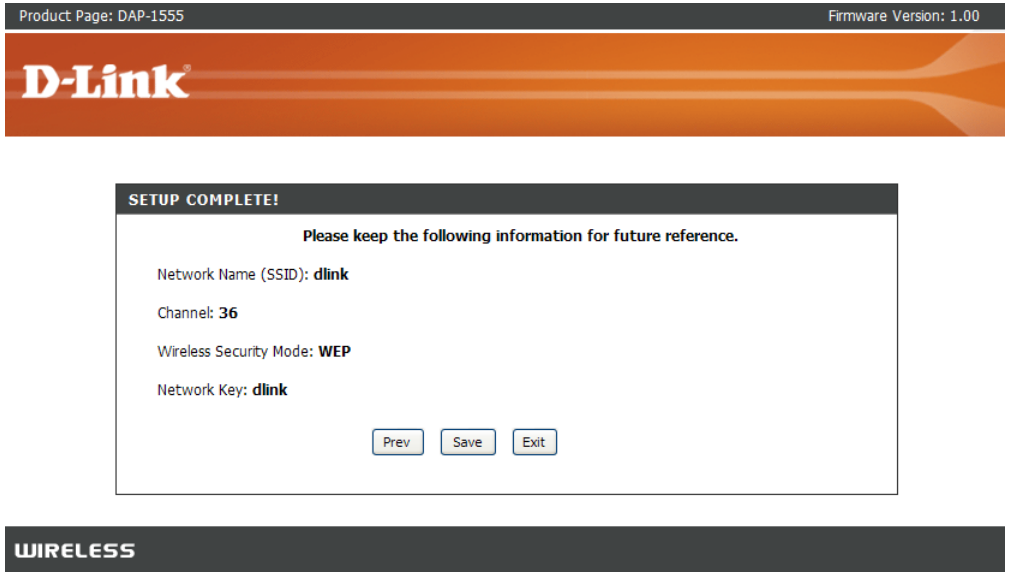
For **WEP** encryption, enter a Network Key exactly 5 or 13 characters long or exactly 10 or 26 characters using 0-9 and A-F.

Click **Next** to continue.



If you select **WEP** encryption, the following screen will show you your network key to enter on your wireless clients.

Click **Save** to finish the Setup Wizard.



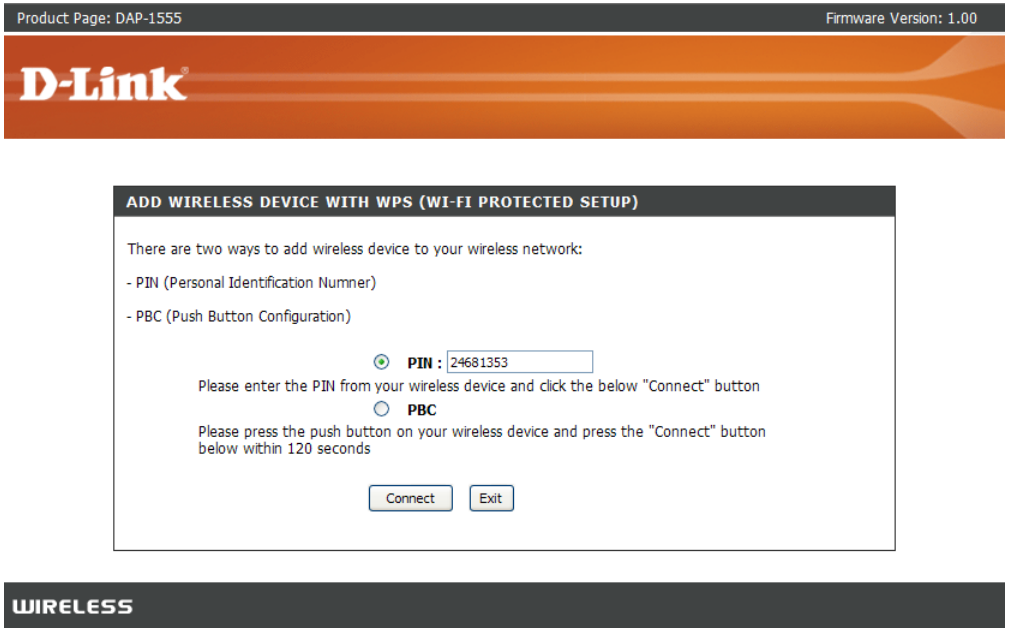
Add Wireless Device With WPS

This Wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

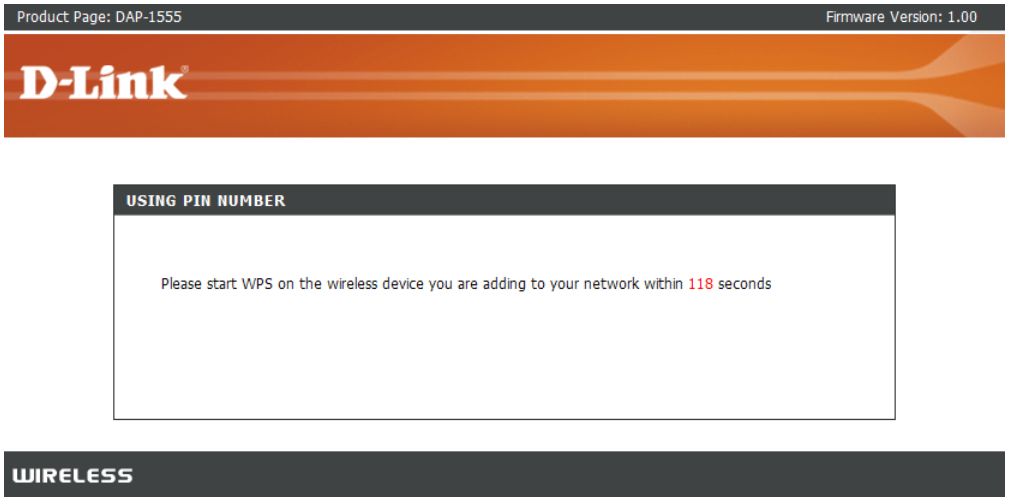
Select **PIN** to use your PIN number from your wireless device to connect to your network.

For **PBC** configuration, skip to page 23.

Click **Connect** to continue.

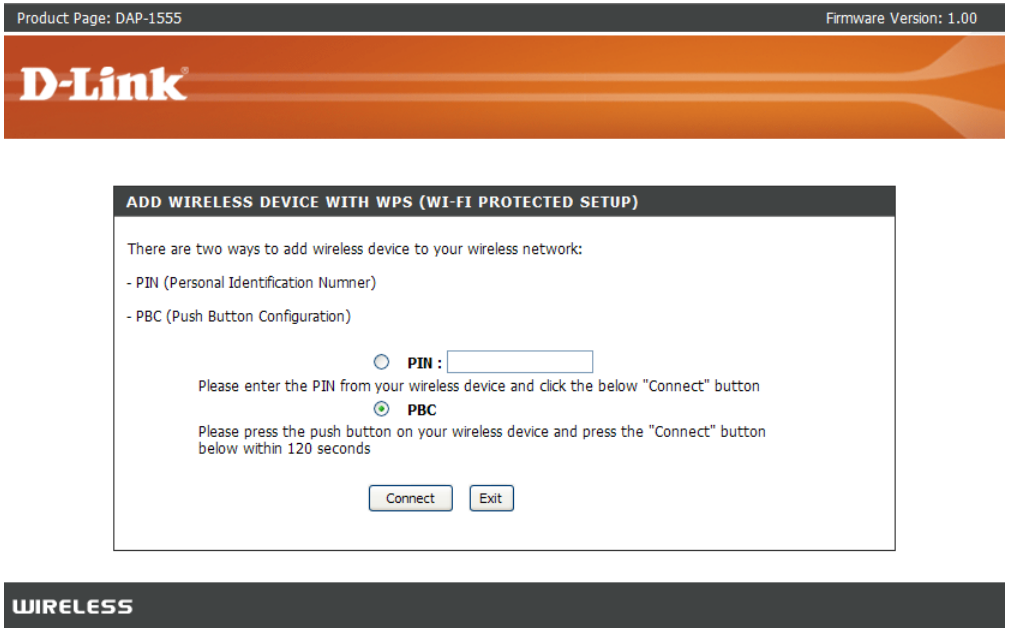


Start WPS on the wireless device you are adding to you wireless network to complete the setup.

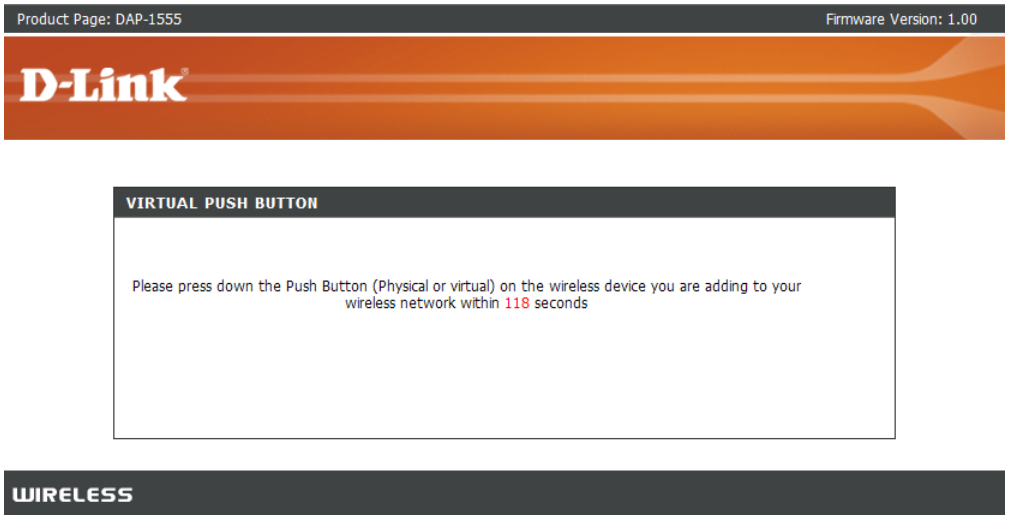


Select **PBC** to use the Push Button Configuration to connect to your network.

Click **Connect** to continue.



Press down the Push Button on the wireless device you are adding to your network to complete the setup.



Manual Configuration
Wireless Settings

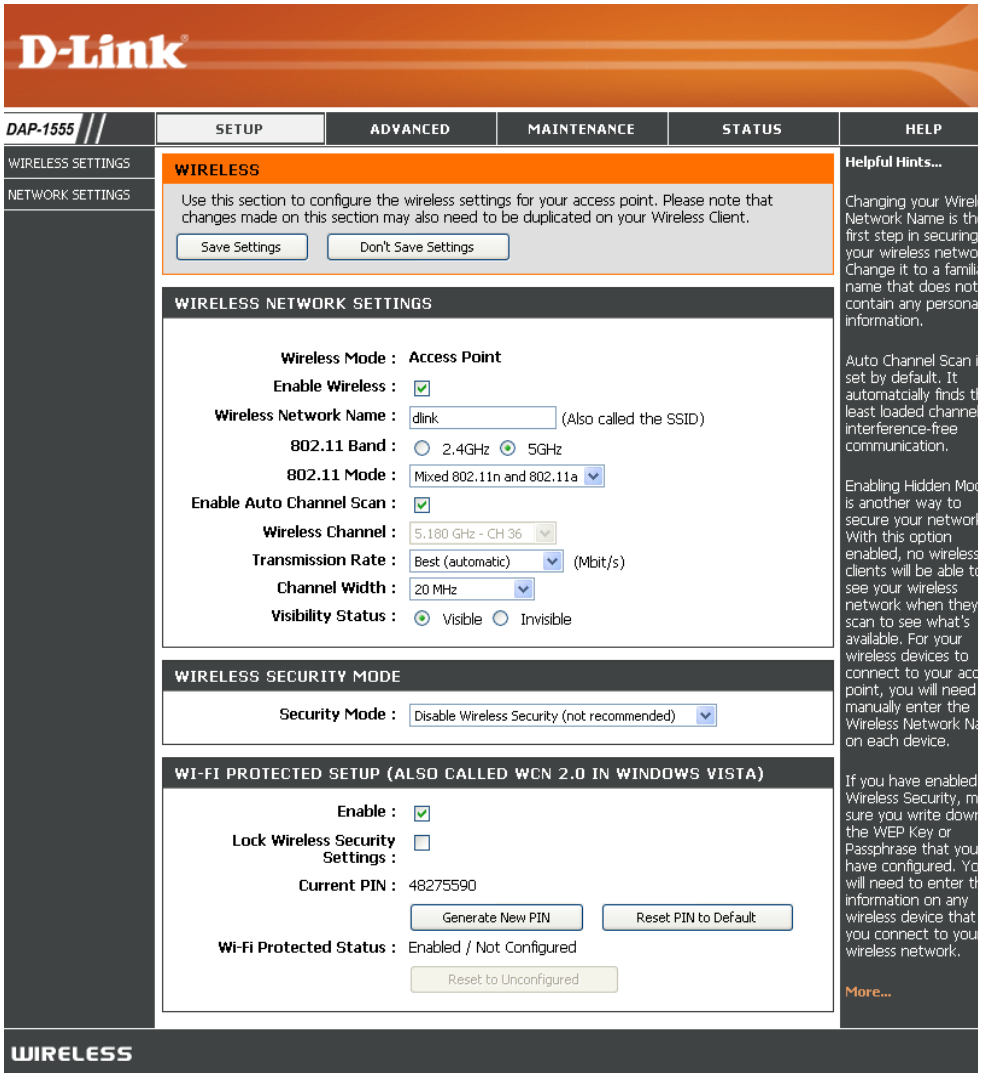
Wireless Mode: The current wireless mode is set to Access Point, it will create a wireless infrastructure network.

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.

802.11 Band: Operating frequency band. Choose 2.4GHz for visibility to legacy devices and for longer range. Choose 5GHz for least interference.

802.11 Mode: If you choose 2.4GHz band, than select one of the following:
802.11b Only - Select if all of your wireless clients are 802.11b.
802.11g Only - Select if all of your wireless clients are 802.11g.
802.11n Only - Select only if all of your wireless clients are 802.11n.
Mixed 802.11g and 802.11b - Select if you are using both 802.11b and 802.11g wireless clients.
Mixed 802.11n and 802.11g - Select if you are using both 802.11n and 802.11g wireless clients.
Mixed 802.11n, 802.11b, and 802.11g - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.
If you choose 5GHz band, then select either **802.11a only**, **802.11n only**, or **Mixed 802.11n and 802.11a**.



Enable Auto Channel Scan: The Auto Channel Scan setting can be selected to allow the DAP-1555 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DAP-1555. By default the channel is set to 6 for 2.4GHz band. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Scan, this option will be greyed out.

Transmission Rate: Select the transmit rate. It is strongly suggested to select **Best (Auto)** for best performance.

Channel Width: Select the Channel Width:
Auto 20/40 - Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DAP-1555. If Invisible is selected, the SSID of the DAP-1555 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DAP-1555 in order to connect to it.

Security Mode: Refer to page 65 for more information regarding the wireless security.

Enable: Enable the Wi-Fi Protected Setup feature.

Lock Wireless Security Settings: Locking the wireless security settings prevents the settings from being changed by any new external registar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup. It is still possible to change wireless network settings with Manual Wireless Network Setup, Wireless Network Setup Wizard, or an existing external WLAN Manager Registar.

Current PIN: Shows the current value of the access point's PIN.

Generate New PIN: Create a random number that is a valid PIN. This becomes the access point's PIN. You can then copy this PIN to the user interface of the registrar.

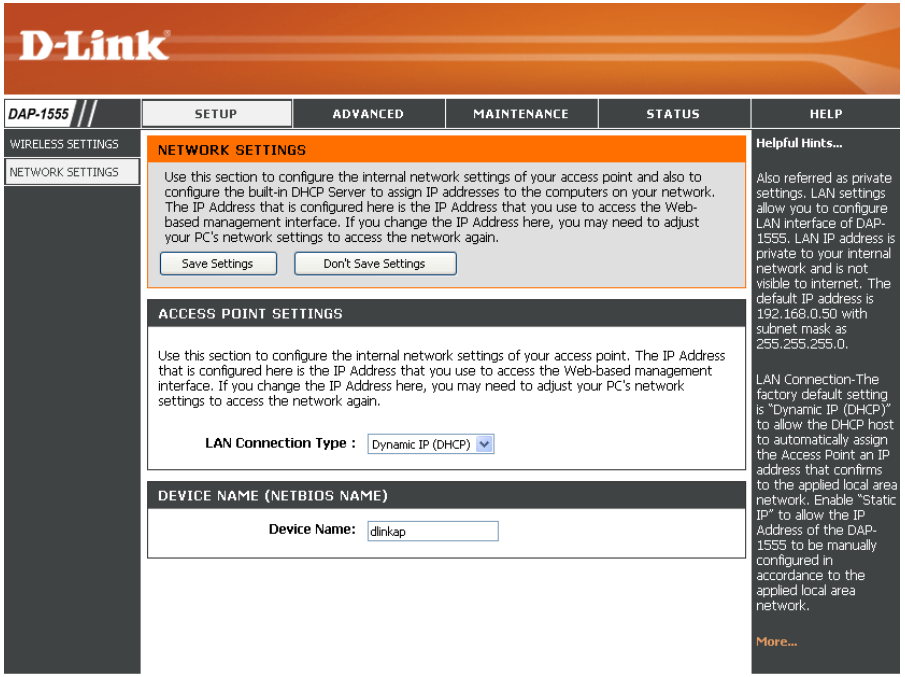
Reset PIN to Default: Restore the default PIN of the access point.

Reset to Unconfigured: Resets Wi-Fi Protected Status to Not Configured. Vista WPS icon will only be displayed when the Wi-Fi Protected Status is Not Configured.

Network Settings
DHCP

This section will allow you to change the local network settings of the access point and to configure the DHCP settings.

Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.



Static IP

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Access point will not accept the IP address if it is not in this format.

Access Point IP Address: Enter the IP address of the access point. The default IP address is 192.168.0.50. If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

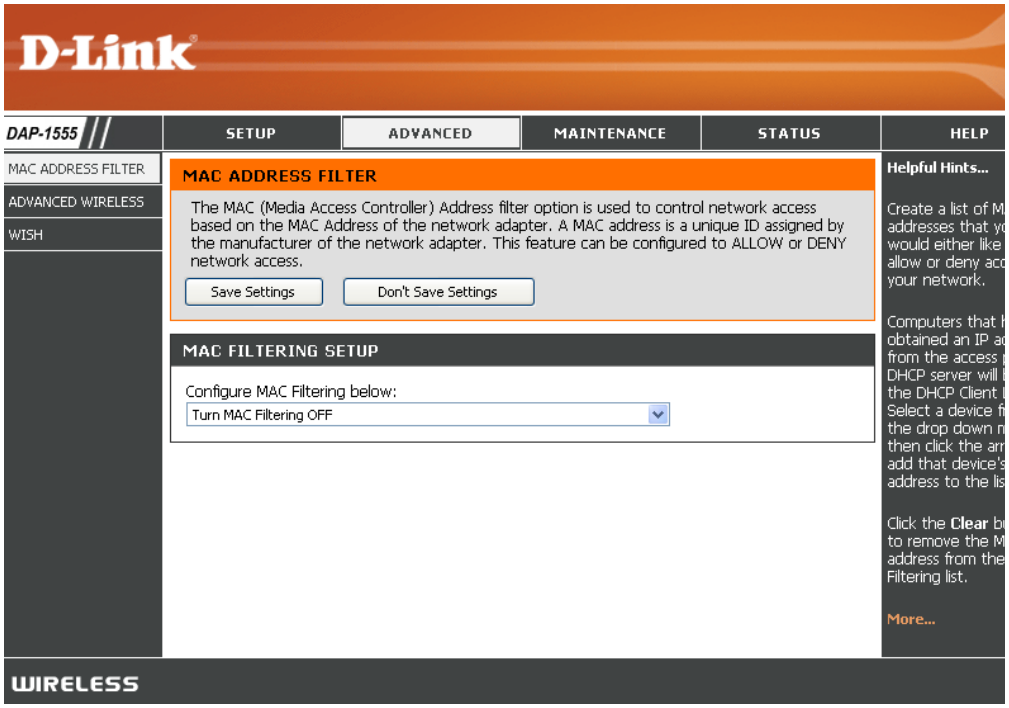
Default Gateway: Enter the Gateway assigned by your ISP.

Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.

Advanced
MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

Configure MAC Filtering: When “OFF” is selected, MAC addresses are not used to control network access. When “ALLOW” is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When “DENY” is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.



Advanced Wireless

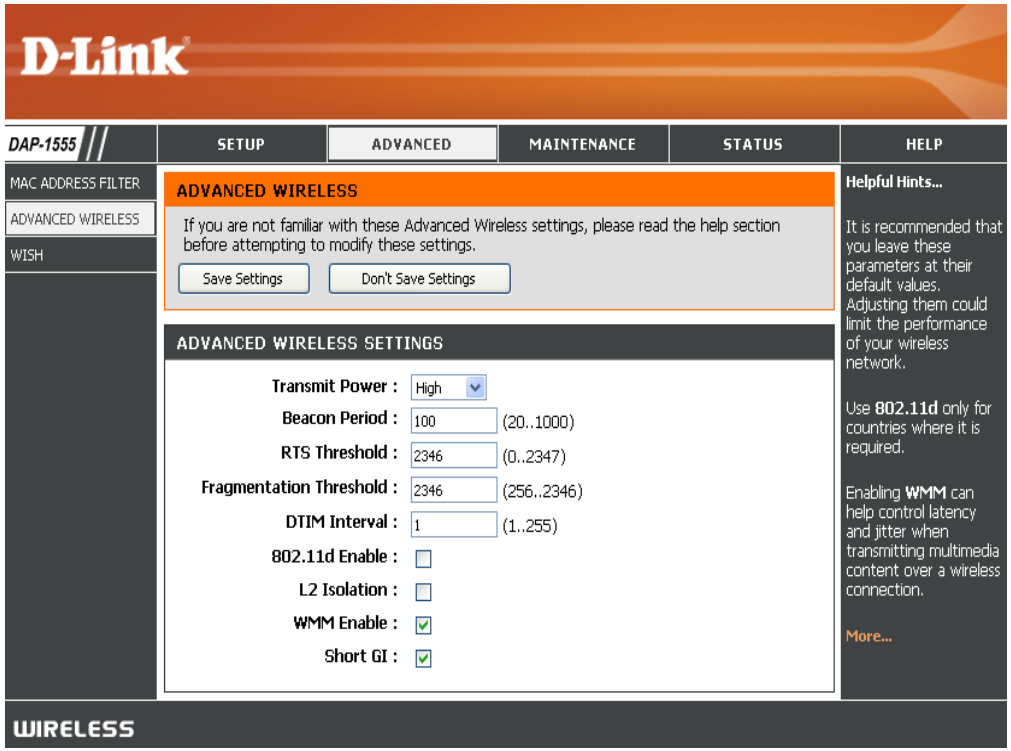
Transmit Power: Set the transmit power of the antennas.

Beacon Period: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

DTIM Interval: (Delivery Traffic Indication Message) 1 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.



802.11d Enable*: This enables 802.11d operation. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

L2 Isolation: Enabling L2 (Layer 2) Isolation prevents associated wireless clients from communicating with each other.

WMM Enable: WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

***Note:** Transmit power is regulated by international standards and users are forbidden to change its maximum limit. Regarding the frequency of 802.11d, every country limits the frequency range used within its territory. Consumers are only allowed to purchase products that operates with the country regulated frequency.

WISH

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

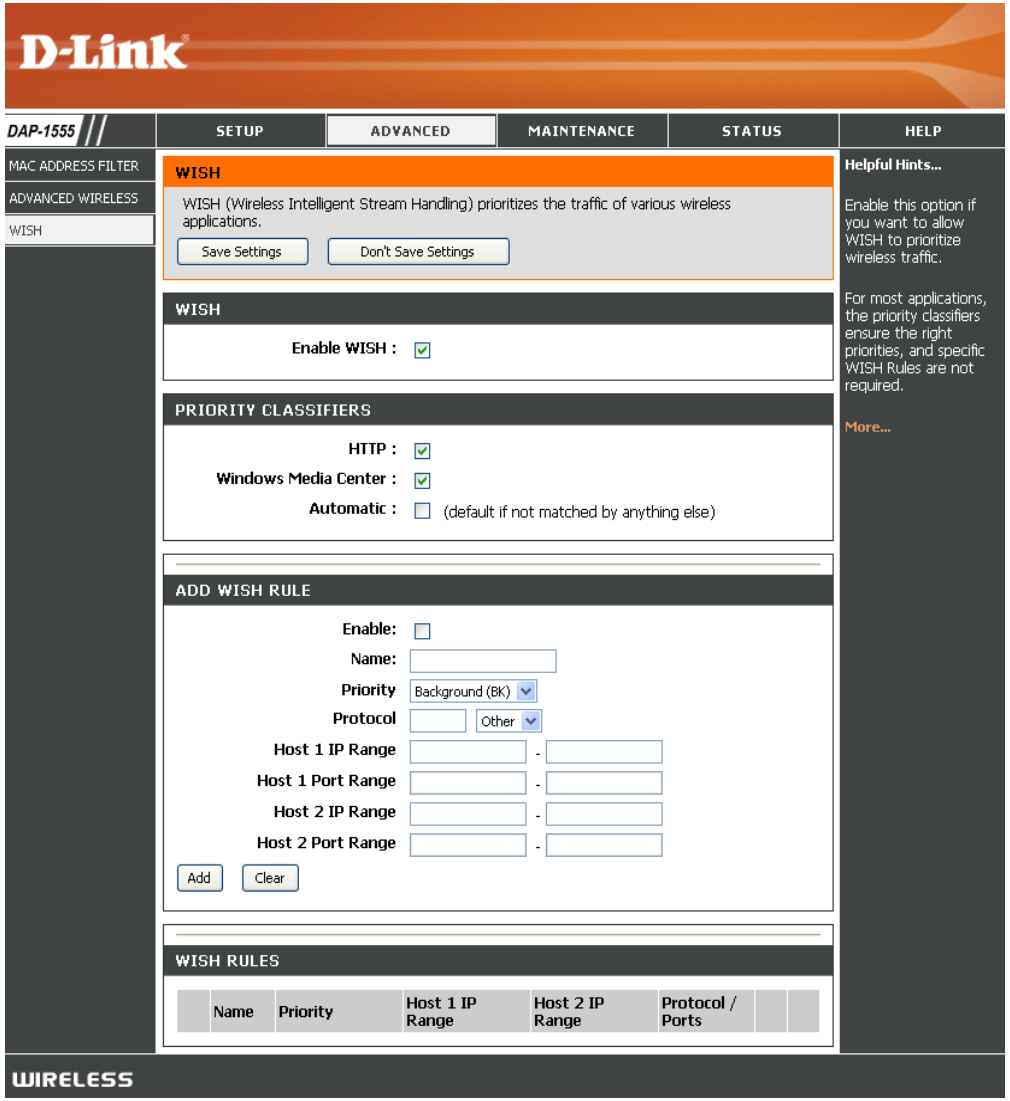
Enable WISH: Enable this option if you want to allow WISH to prioritize your traffic.

HTTP: Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center: Enables the access point to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic: When enabled, this option allows the access point to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to de-prioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

WISH Rule: A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.
WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.



Enable: Enable this option if you want to allow WISH to prioritize your traffic.

Name: Create a name for the rule that is meaningful to you.

Priority: The priority of the message flow is entered here. The four priorities are defined as:

BK: Background (least urgent)
BE: Best Effort
VI: Video
VO: Voice (most urgent)

Protocol: The protocol used by the messages.

Host 1 IP Range: The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host 1 Port Range: The rule applies to a flow of messages for which host 1's port number is within the range set here.

Host 2 IP Range: The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

Host 2 Port Range: The rule applies to a flow of messages for which host 2's port number is within the range set here.

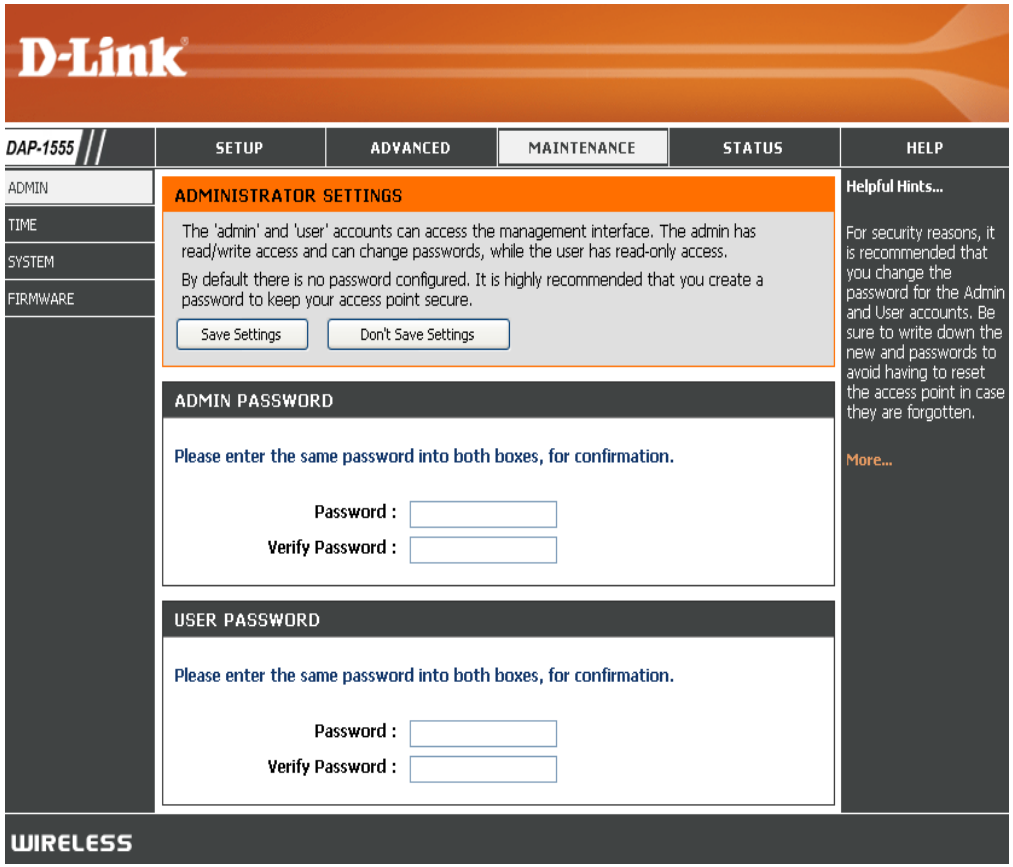
WISH Rules: This section is where you define WISH Rules. Enable or disable defined rules with the check boxes at the left.

Tools
Admin

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

Admin Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.



Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

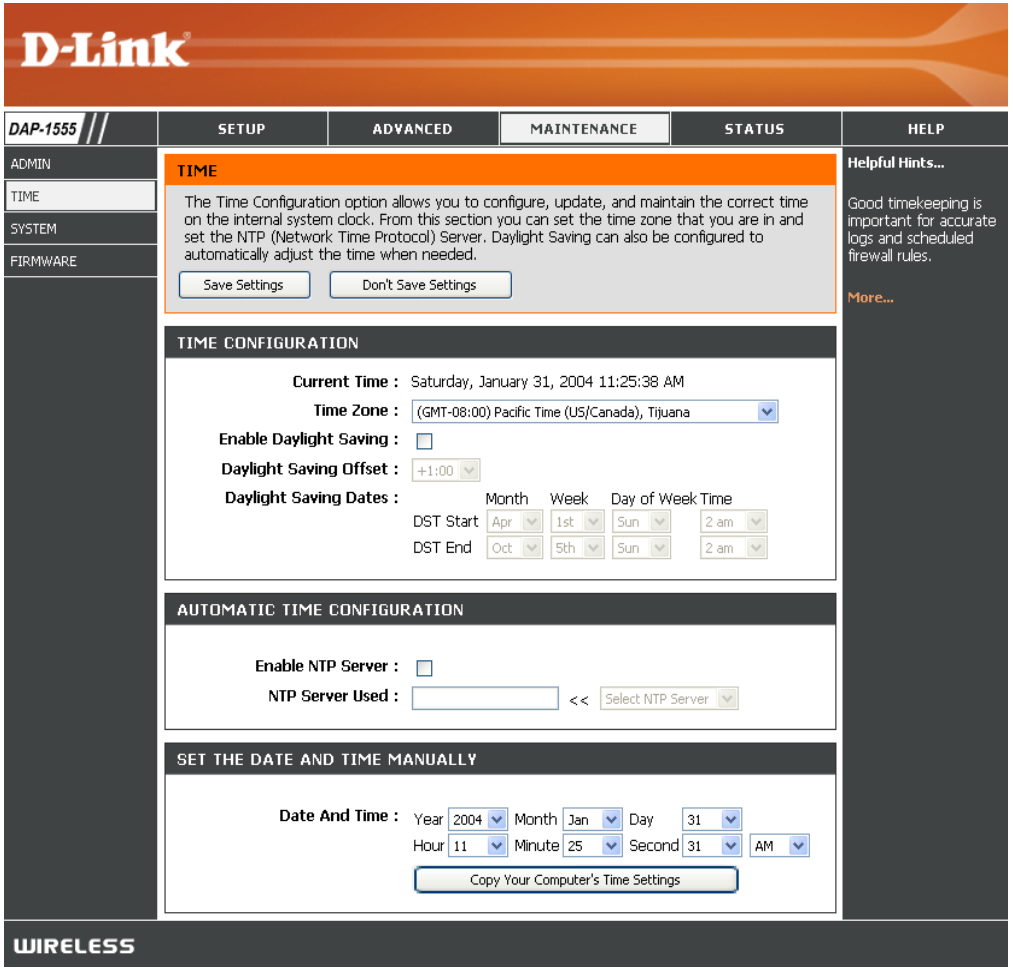
Time Zone: Select the Time Zone from the drop-down menu.

Daylight Saving: To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

Enable NTP Server: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

NTP Server Used: Enter the NTP server or select one from the drop-down menu.

Manual: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Save Settings**. You can also click **Copy Your Computer's Time Settings**.



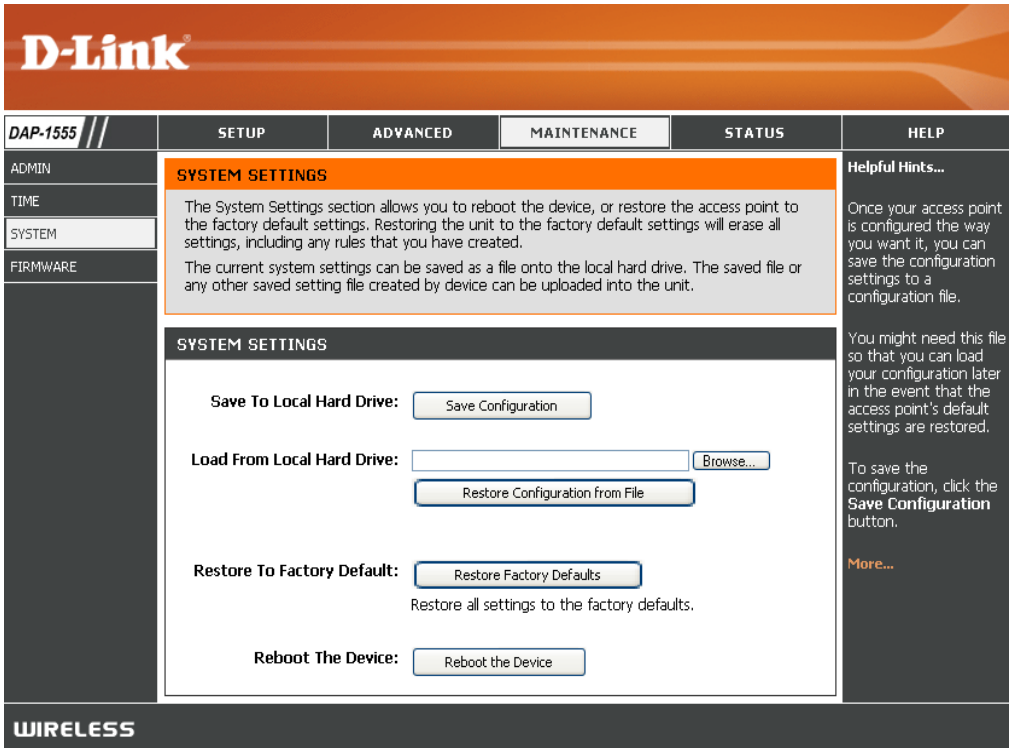
System

Save Settings to Local Hard Drive: Use this option to save the current access point configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved access point configuration settings. First, use the Browse control to find a previously save file of configuration settings. Then, click the Load button to transfer those settings to the access point.

Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the access point was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current access point configuration settings, use the Save button above.
Note: Restoring the factory default settings will not reset the Wi-Fi Protected Status to Not Configured.

Reboot Device: Click to reboot the access point.

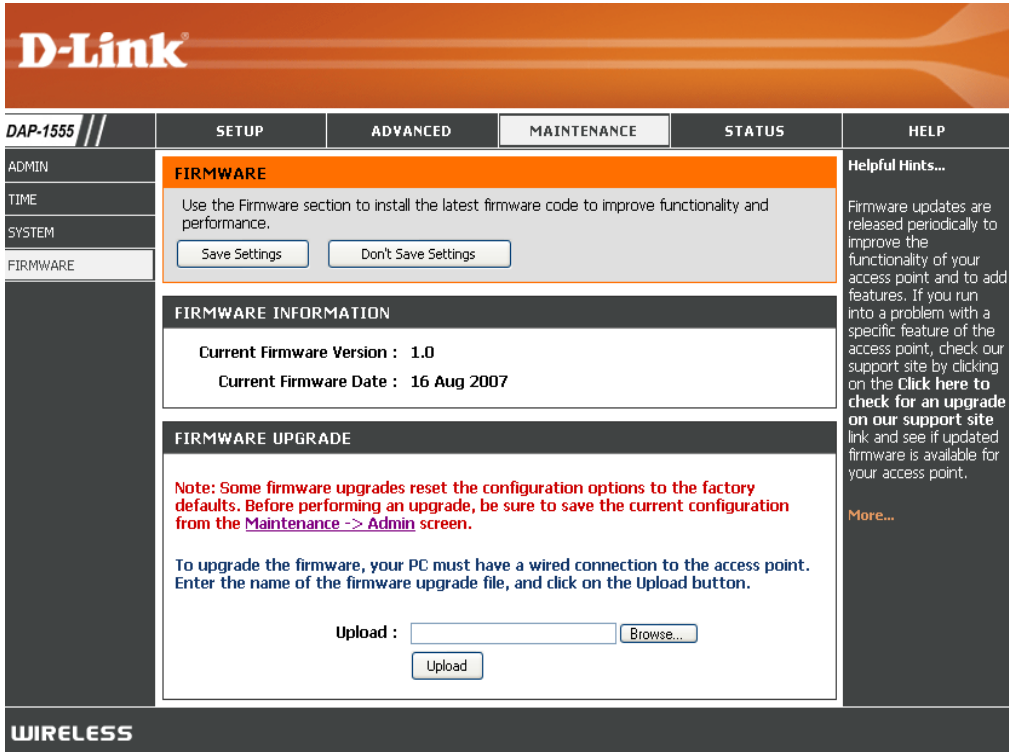


Firmware

You can upgrade the firmware of the access point here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to locate the firmware file to be used for the update. Please check the D-Link support website for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from this site.

Browse: After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

Upload: Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the access point.



Status

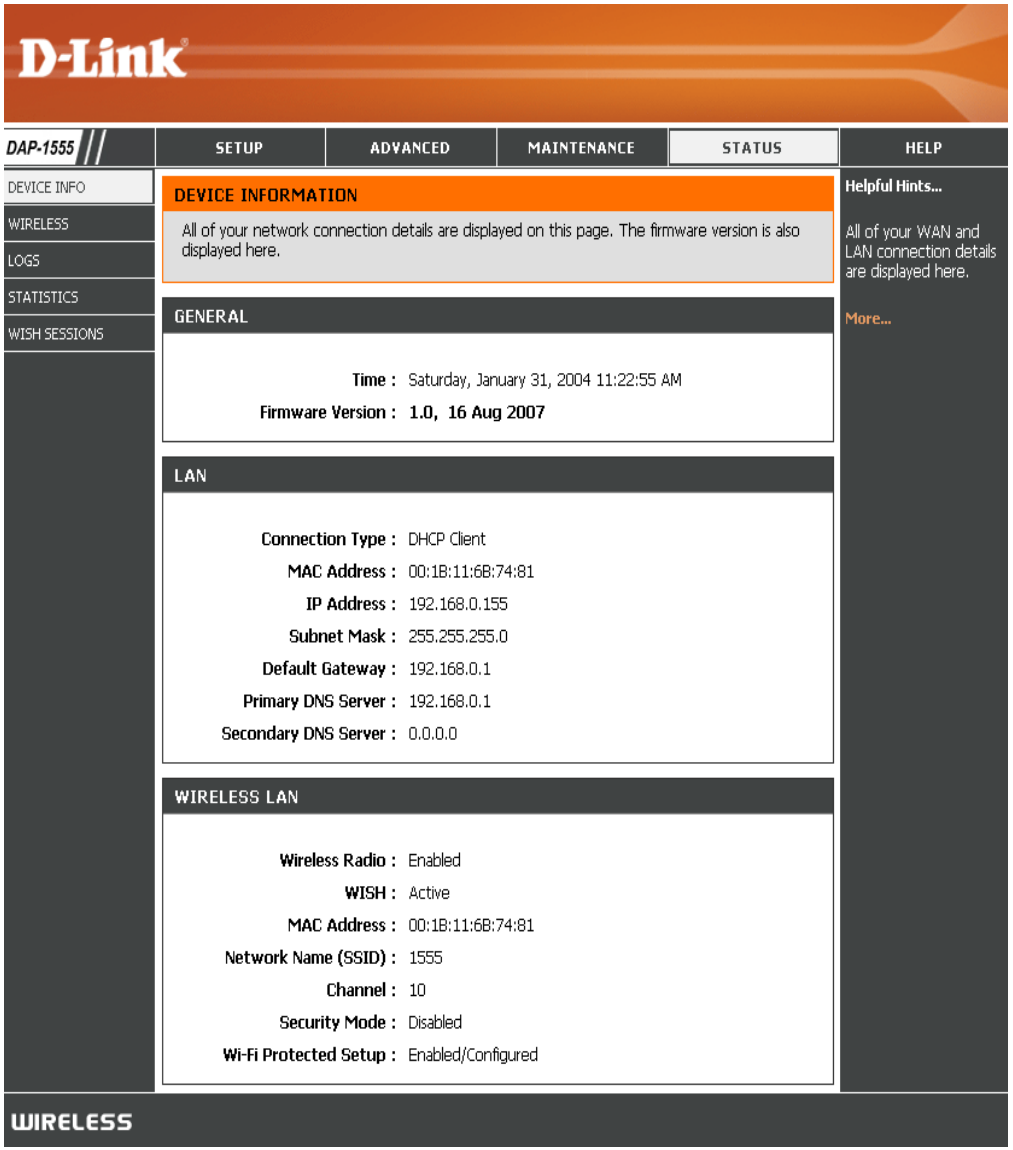
Device Info

This page displays the current information for the DAP-1555. It will display the LAN and Wireless information.

General: Displays the access point's time and firmware version.

LAN: Displays the MAC address and the private (local) IP settings for the access point.

Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID and Channel.



Wireless

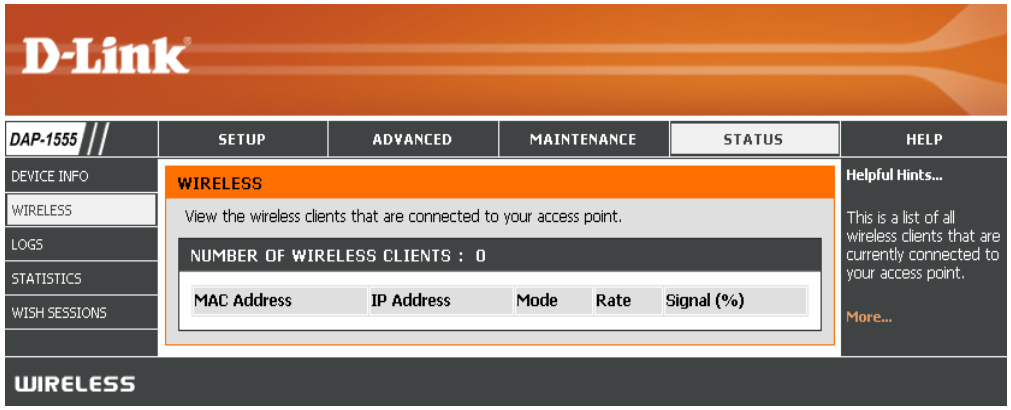
The wireless section allows you to view the wireless clients that are connected to your wireless access point.

MAC Address: The Ethernet ID (MAC address) of the wireless client.

IP Address: The LAN-side IP address of the client.

Mode: The transmission standard being used by the client. Values are 11a, 11b, 11g, 11ng or 11na for 802.11a, 802.11b, 802.11g or 802.11n respectively.

Rate: Displays the actual transmission rate of the client in megabits per second.



Signal: This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the access point and the wireless device.

Logs

The access point automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the access point logs. You can define what types of events you want to view and the level of the events to view. This access point also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility

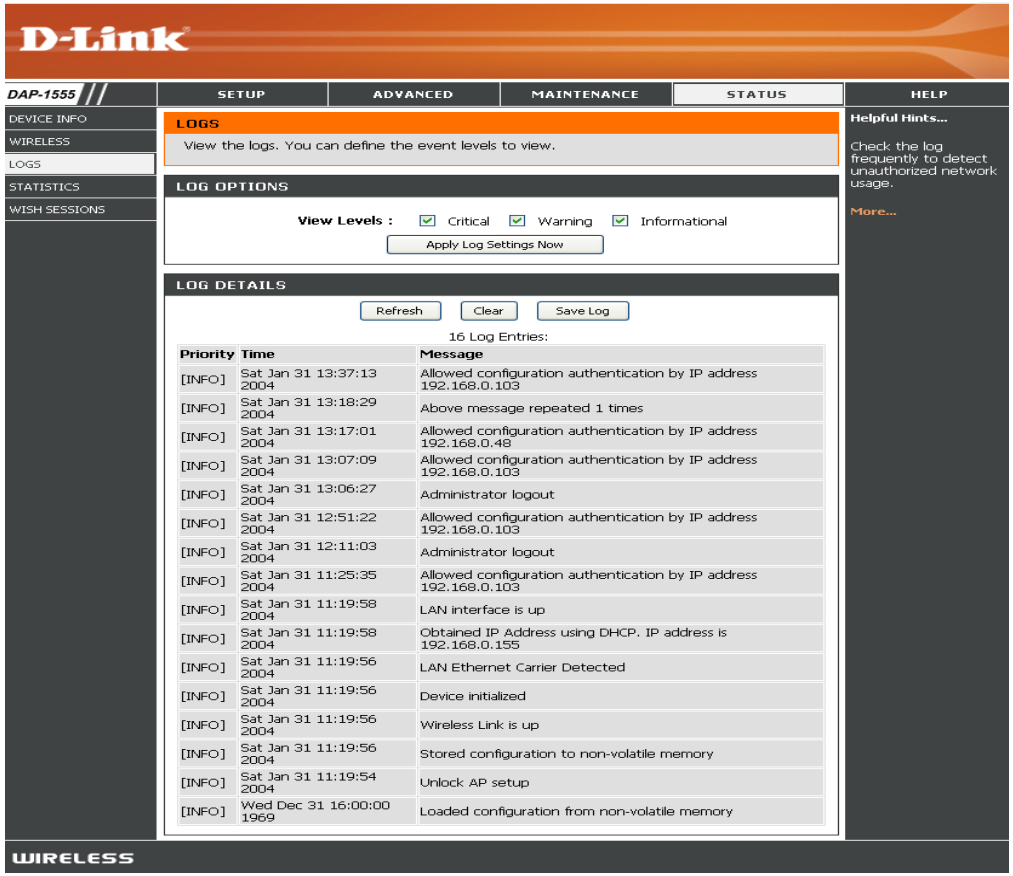
View Levels: There are three levels of message importance: Informational, Warning, and Critical. Select the levels that you want displayed in the log.

Apply Log Settings: Will filter the log results so that only the selected options appear.

Refresh: Updates the log details on the screen so it displays any recent activity.

Clear: Clears all of the log contents.

Save Log: This option will save the access point to a log file on your computer.



Statistics

The Statistics page displays all of the LAN, WAN, and Wireless packets transmit and receive statistics.

Sent: The number of packets sent from the access point.

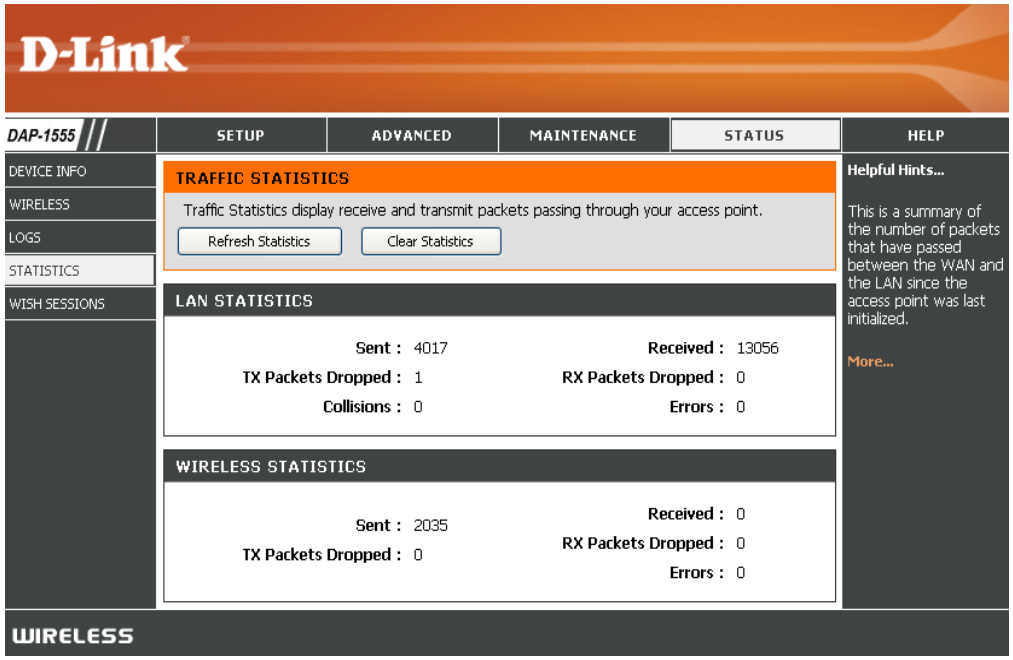
Received: The number of packets received by the access point.

TX Packets Dropped: Displays the number of packets that were dropped while sending, due to errors, collisions, or access point resource limitations.

RX Packets Dropped: Displays the number of packets that were dropped while receiving, due to errors, collisions, or access point resource limitations.

Collisions: Displays the number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).

Errors: The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.



Wish Sessions

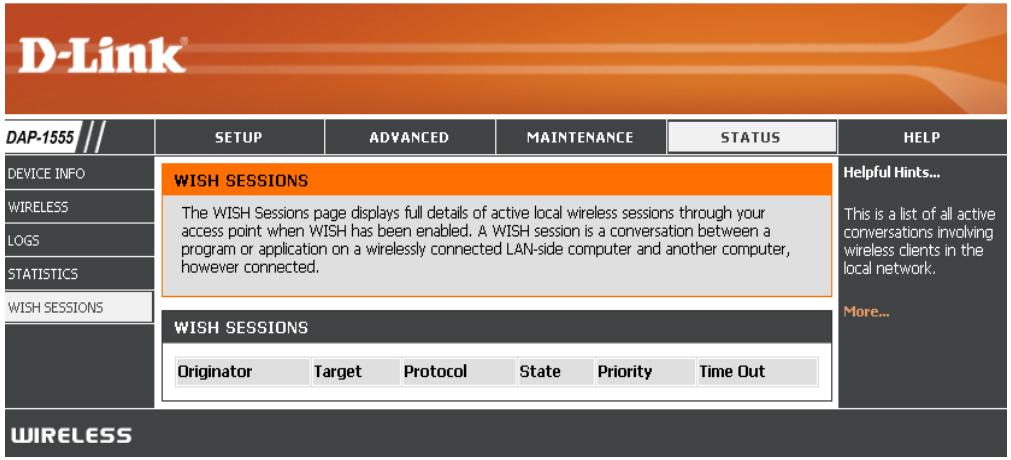
The WISH Sessions page displays full details of active local wireless sessions through your access point when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

Originator: The IP address and, where appropriate, port number of the computer that originated a network connection.

Target: The IP address and, where appropriate, port number of the computer to which a network connection has been made.

Protocol: The communications protocol used for the conversation.

State: State for sessions that use the TCP protocol.



- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- CW: Close Wait -- the server system has requested that the connection be stopped.
- TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Priority: The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:

- BK: Background (least urgent)
- BE: Best Effort
- VI: Video
- VO: Voice (most urgent)

Time out: The number of seconds of idle time until the access point considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

300 seconds

UDP connections.

240 seconds

Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.

7800 seconds

Established or closing TCP connections.

Help

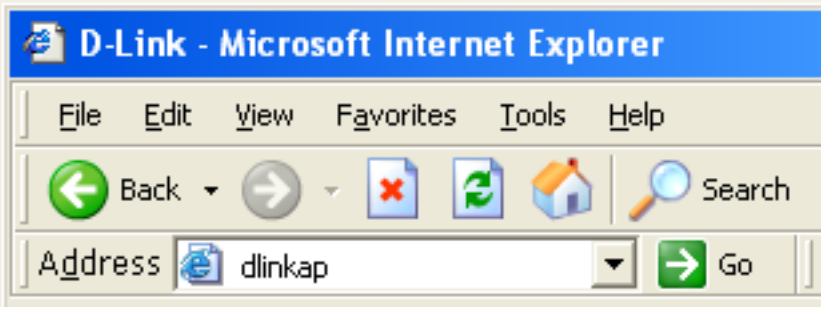
D-Link
DAP-1555
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
MENU
SETUP
ADVANCED
MAINTENANCE
STATUS
GLOSSARY
SUPPORT MENU
Setup
Advanced
Maintenance
Status
Glossary
SETUP HELP
Wizard
Network Settings
Wireless
ADVANCED HELP
Advanced Wireless
MAINTENANCE HELP
Admin
System
Firmware
STATUS HELP
Device Info
Logs
WIRELESS

Configuration for Bridge Mode

This section will show you how to configure your new D-Link wireless MediaBridge using the web-based configuration utility.

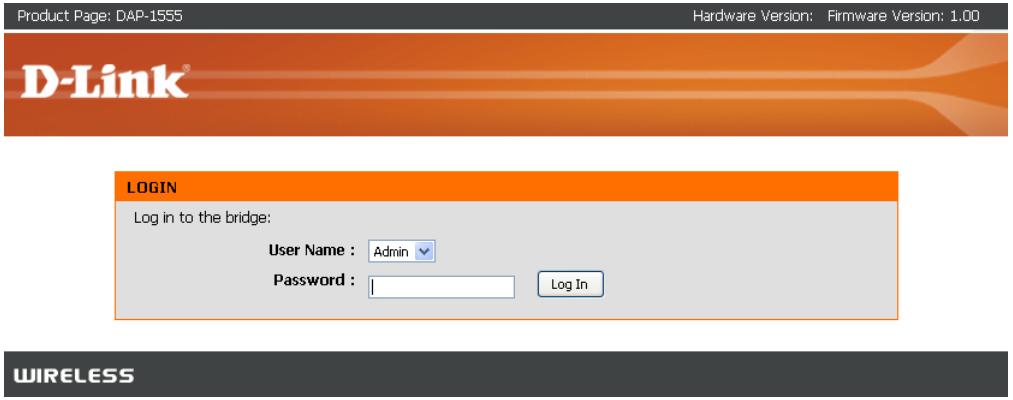
Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter the friendly address for Bridge mode (dlinkap).



Select **Admin** from the drop-down menu and then enter your password. Leave the password blank by default.

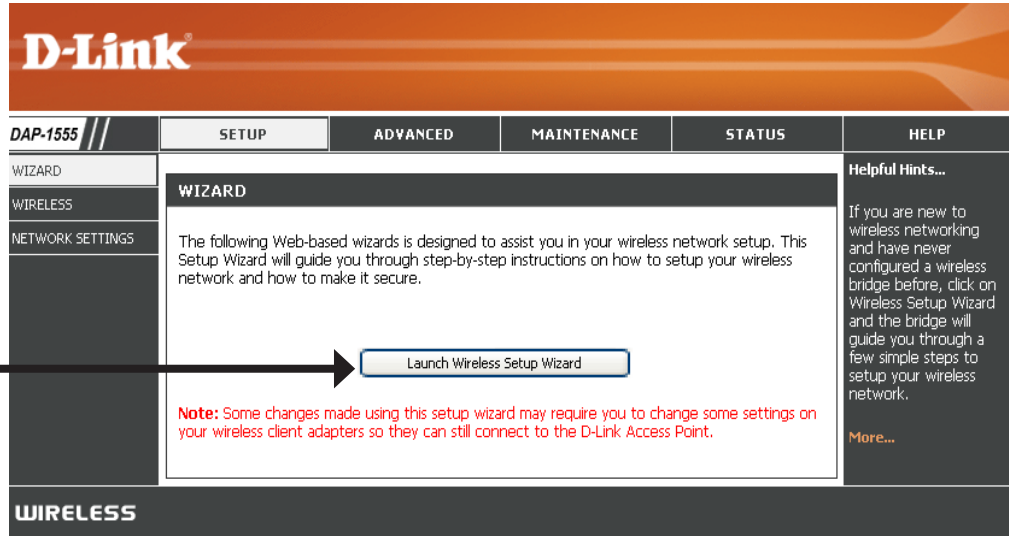
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



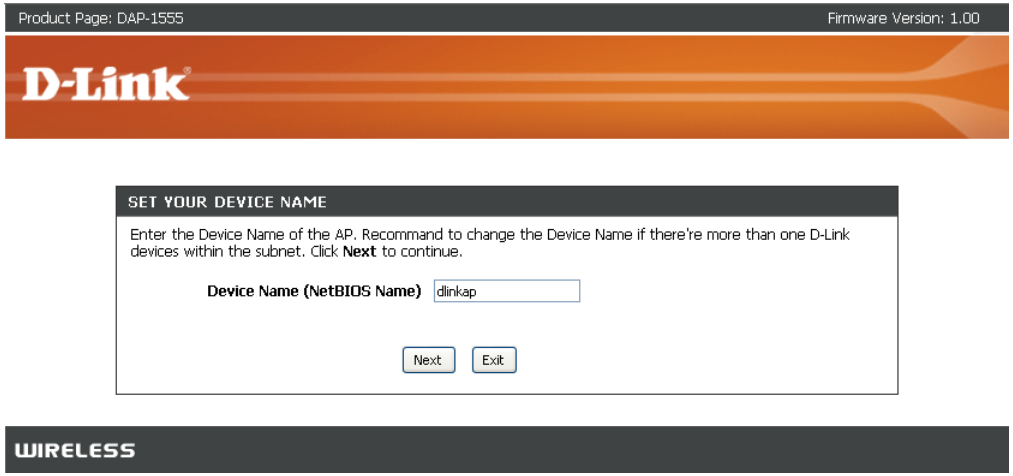
Setup Wizard

This wizard is designed to assist you in configuring the wireless settings for your bridge. It will guide you through step-by-step instructions on how to setup your wireless network.

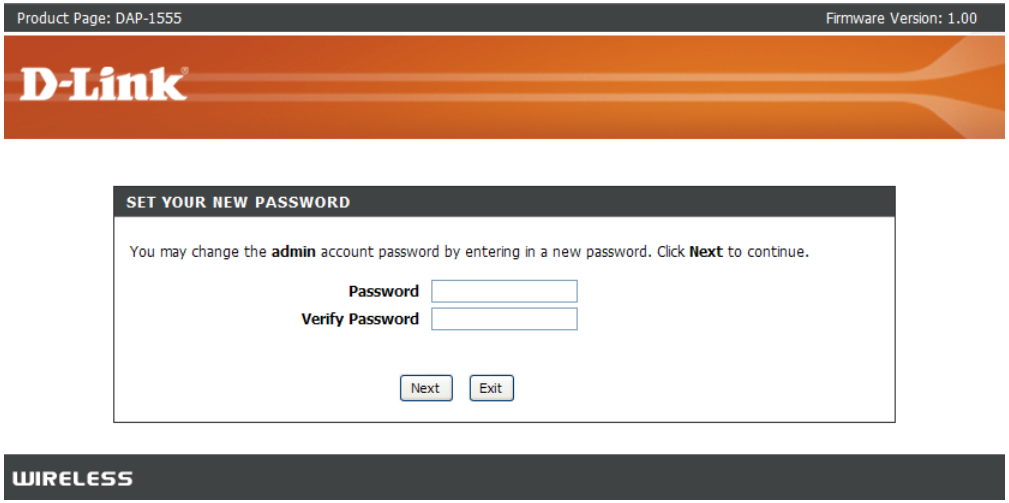
Click **Launch Wireless Setup Wizard** to begin.



Enter the Device Name of the AP and click **Next** to continue. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.



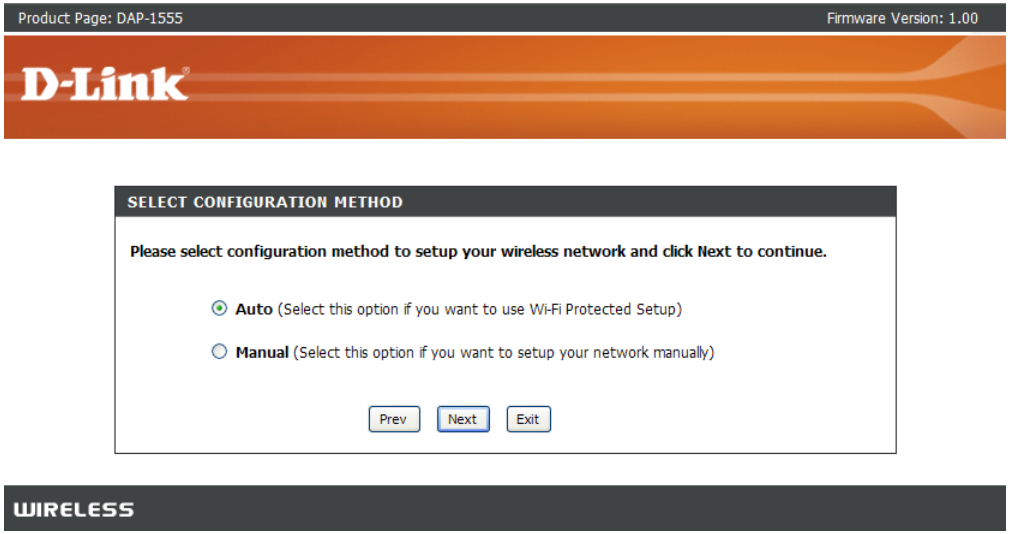
If you want to change the admin account password, enter a new password and click **Next**.



Select **Auto** configuration if you want to use Wi-Fi Protected Setup.

If you want to setup your network manually, skip to page 50.

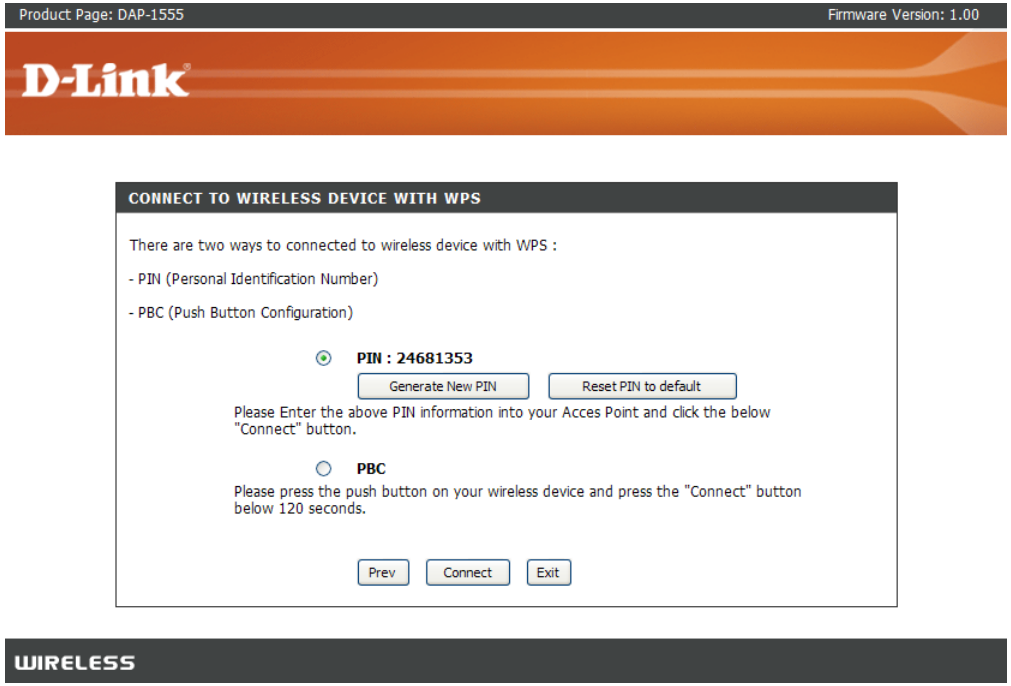
Click **Next** to continue.



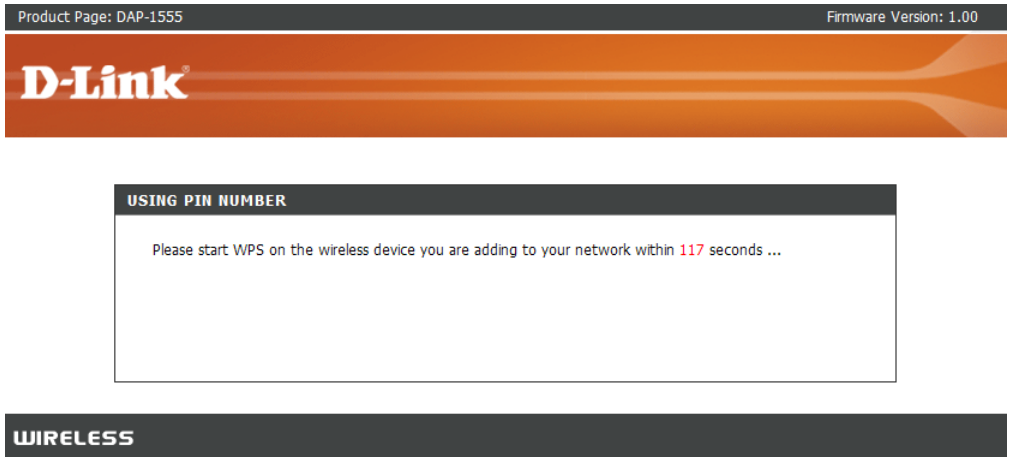
Select **PIN** to connect your wireless device with WPS.

For **PBC** configuration, skip to page 49.

Enter the PIN number used into you access point and click **Connect**.

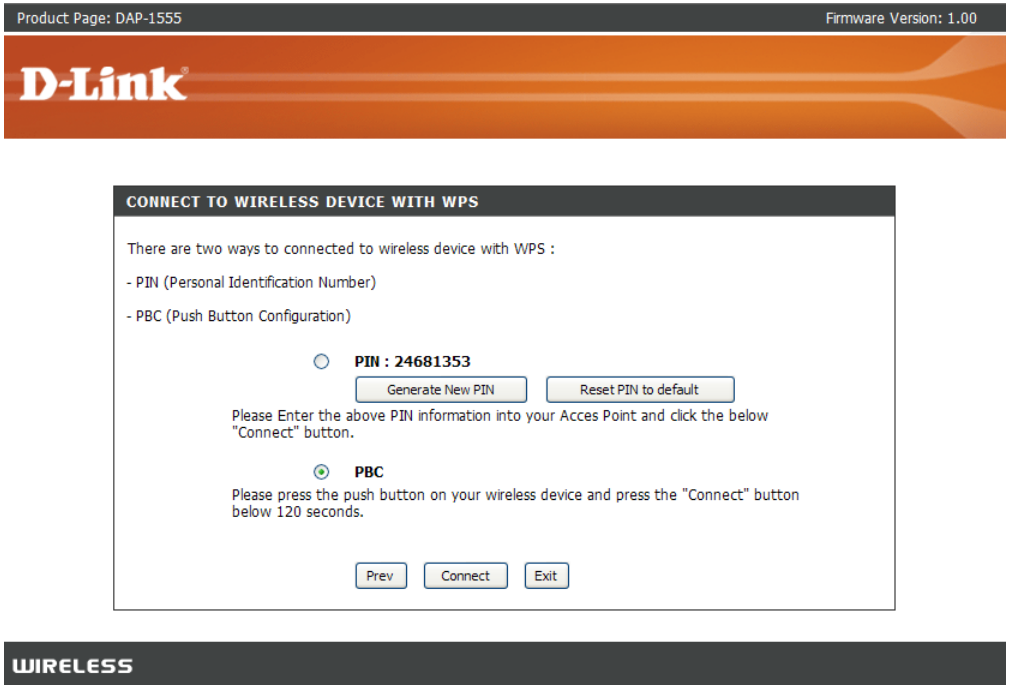


Start WPS on the wireless device you are adding to you wireless network to complete the setup.

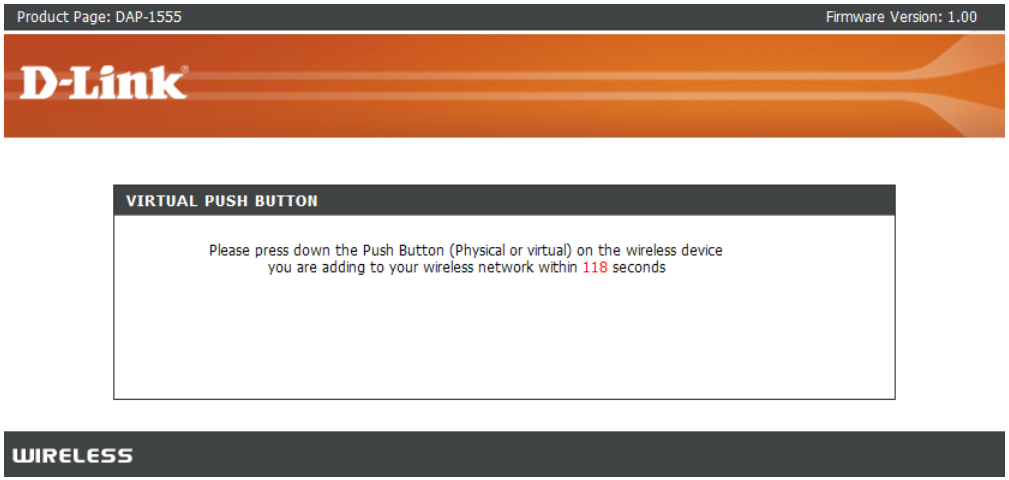


Select **PBC** to use the Push Button Configuration to connect to your network.

Click **Connect** to continue.

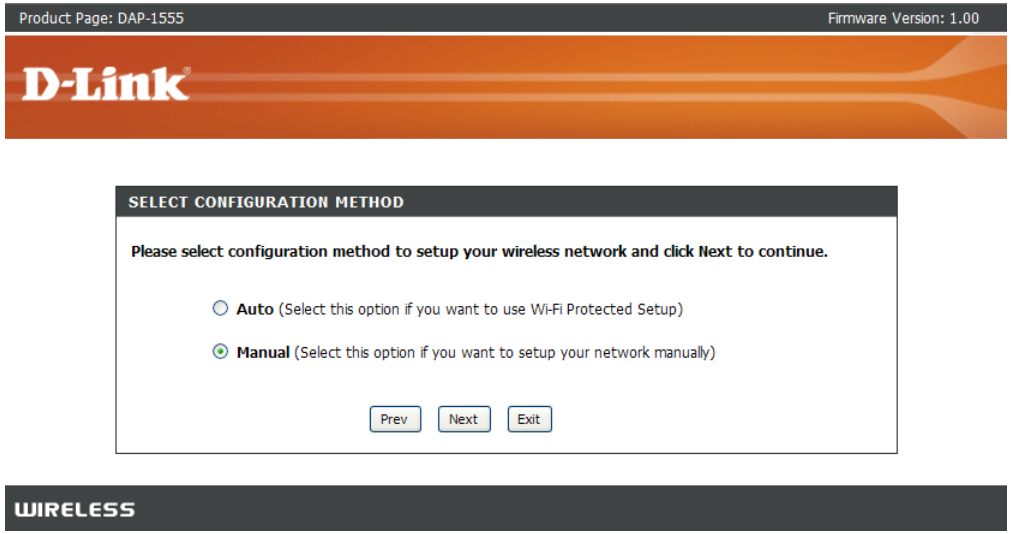


Press down the Push Button on the wireless device you are adding to your network to complete the setup.



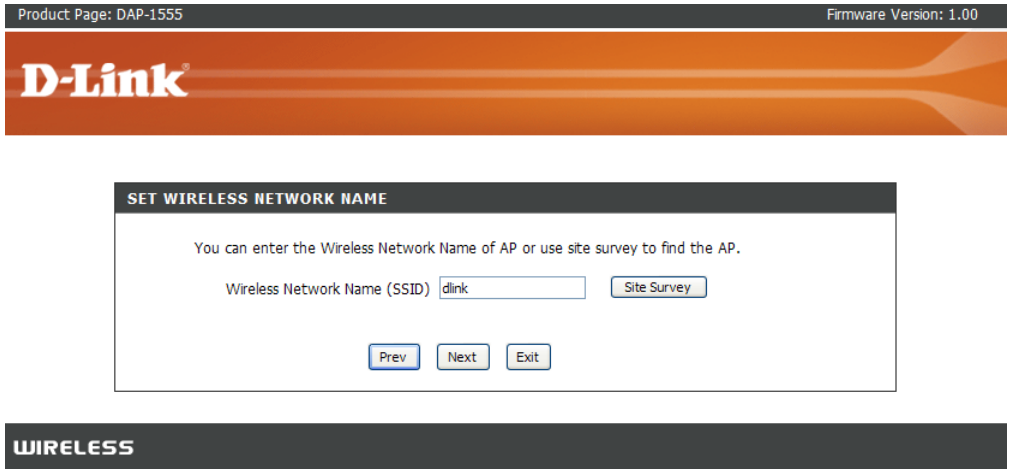
Select **Manual** configuration to setup your network manually.

Click **Next** to continue.



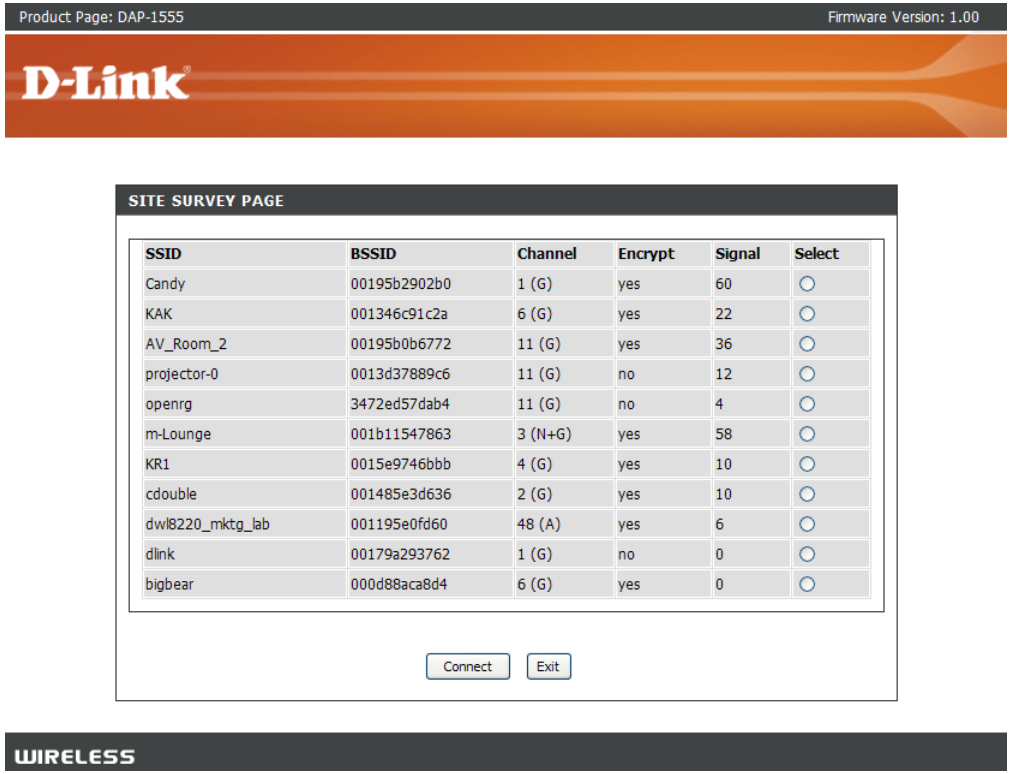
Enter the Wireless Network Name of the AP or use site survey to find the AP.

Click **Next** to continue on to page 52.

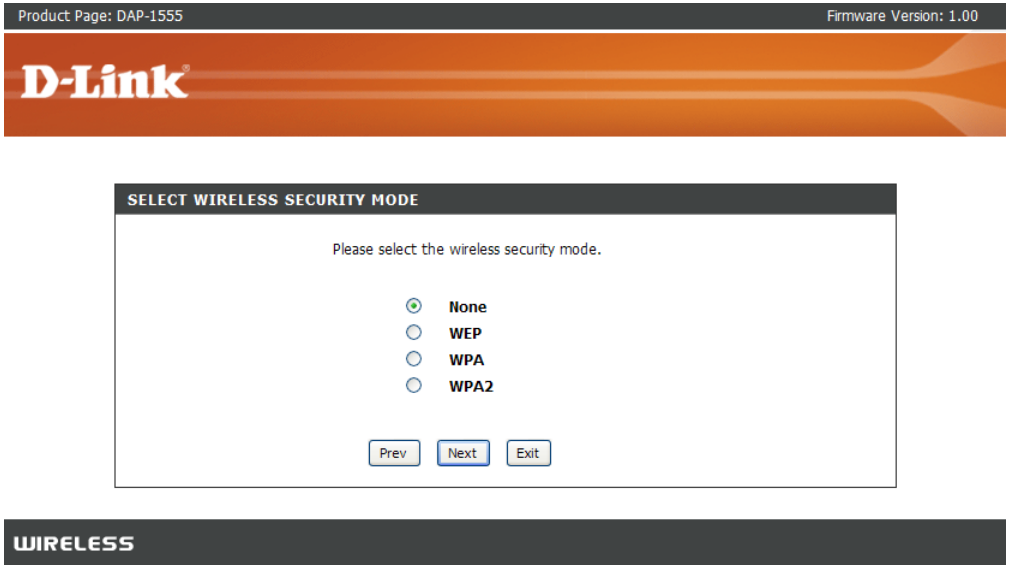


If you clicked on **Site Survey** to following screen will be displayed.

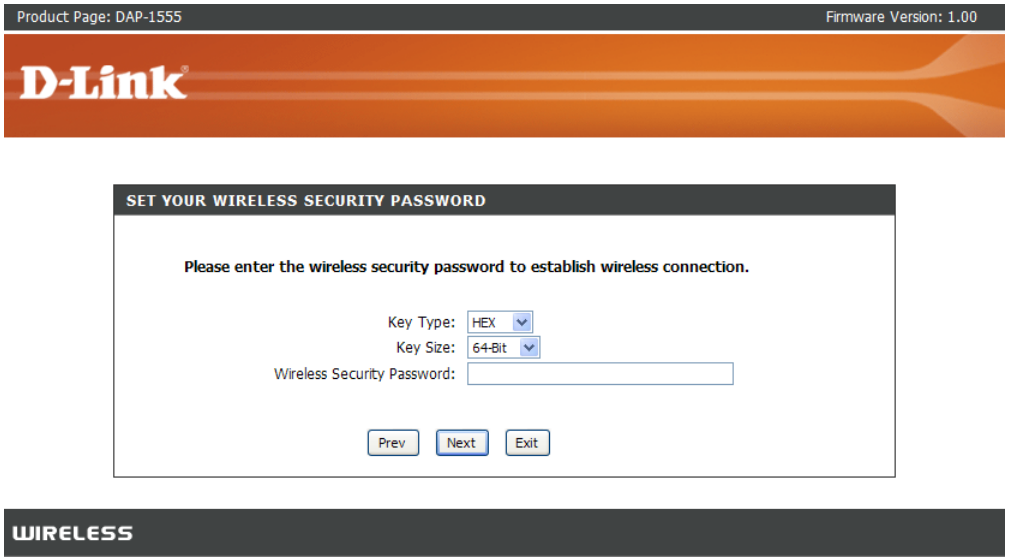
Find your access point from the list and click **Connect** to complete the Setup Wizard.



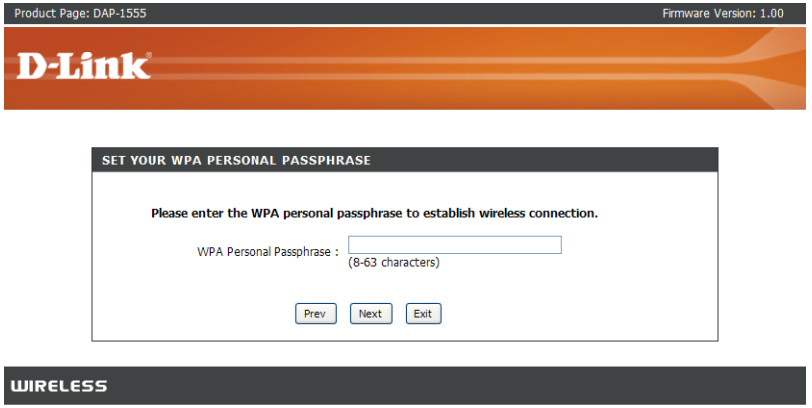
Choose which Security Mode you want to use and click **Next** to continue.



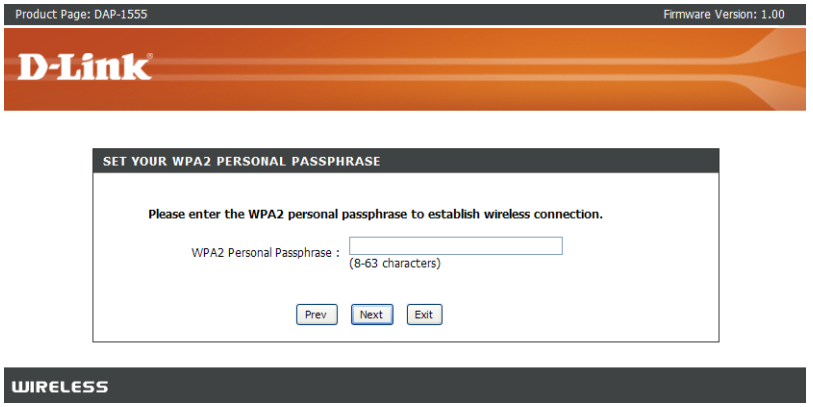
If you choose **WEP**, enter the wireless security password and click **Next** to complete the Setup Wizard.



If you choose **WPA**, enter the WPA Personal Passphrase and click **Next** to complete the Setup Wizard.

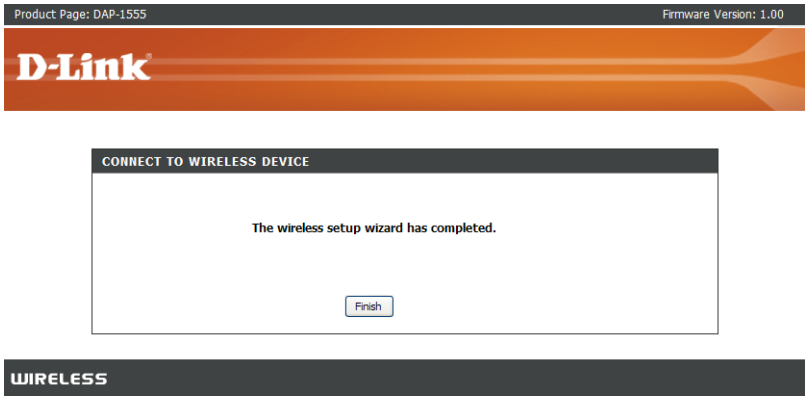


If you choose **WPA2**, enter the WPA2 Personal Passphrase and click **Next** to complete the Setup Wizard.



The Wireless Setup Wizard is complete.

Click **Finish** to reboot the device.



Wireless

Wireless Mode: Select Infrastructure to connect to a wireless (AP) Access Point, select Ad-hoc to connect to another bridge or wireless station.

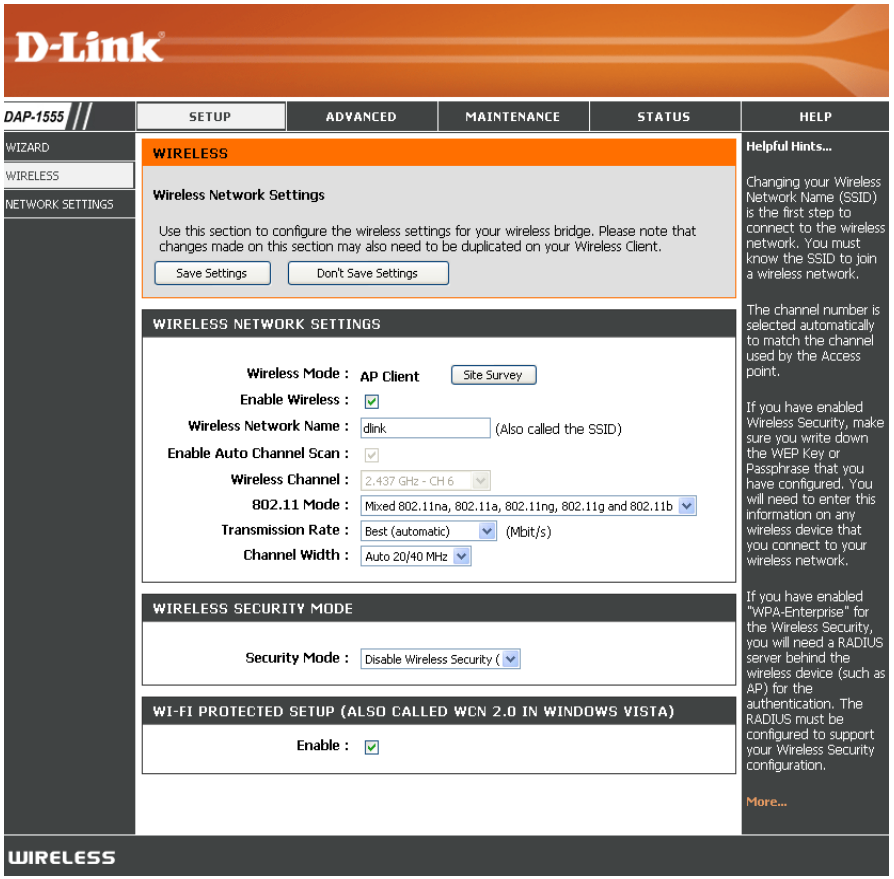
Site Survey: A function that looks for available wireless networks.

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-1555 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DAP-1555. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.



802.11 Mode: If all of the wireless devices in your wireless network can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Mixed 802.11a and 802.11g - Select this so the bridge can site survey to 802.11a and 802.11g networks.

Mixed 802.11a, 802.11g and 802.11b - Select this so the bridge can site survey to 802.11a, 802.11g and 802.11b networks.

Mixed 802.11a, 802.11g and 802.11ng - Select this so the bridge can site survey to 802.11a, 802.11g and 802.11ng networks. 802.11ng means it's 802.11n operated in 2.4GHz band.

Mixed 802.11a, 802.11g, 802.11ng and 802.11b - Select this so the bridge can site survey to 802.11a, 802.11g, 802.11ng and 802.11b networks.

Mixed 802.11na, 802.11a, 802.11g - Select this so the bridge can site survey to 802.11na, 802.11a and 802.11g networks. 802.11na means it's 802.11n operated in 5GHz band.

Mixed 802.11na, 802.11a, 802.11g and 802.11b - Select this so the bridge can site survey to 802.11na, 802.11a, 802.11g, and 802.11b networks.
Mixed 802.11na, 802.11a, 802.11ng and 802.11g - Select this so the bridge can site survey to 802.11na, 802.11a, 802.11ng and 802.11g networks.
Mixed 802.11na, 802.11a, 802.11ng, 802.11g and 802.11b - Select this so the bridge can site survey to 802.11na, 802.11a, 802.11ng, 802.11g and 802.11b networks.

Transmission Rate: Select the transmit rate. It is strongly suggested to select **Best (Auto)** for best performance.

Channel Width: Select the Channel Width:
Auto 20/40 - Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients.

Security Mode: Refer to page 65 for more information regarding wireless security.

Enable: Enable the Wi-Fi Protected Setup feature.

Network Settings
Static

This section will allow you to change the local network settings of the bridge and to configure the Static settings.

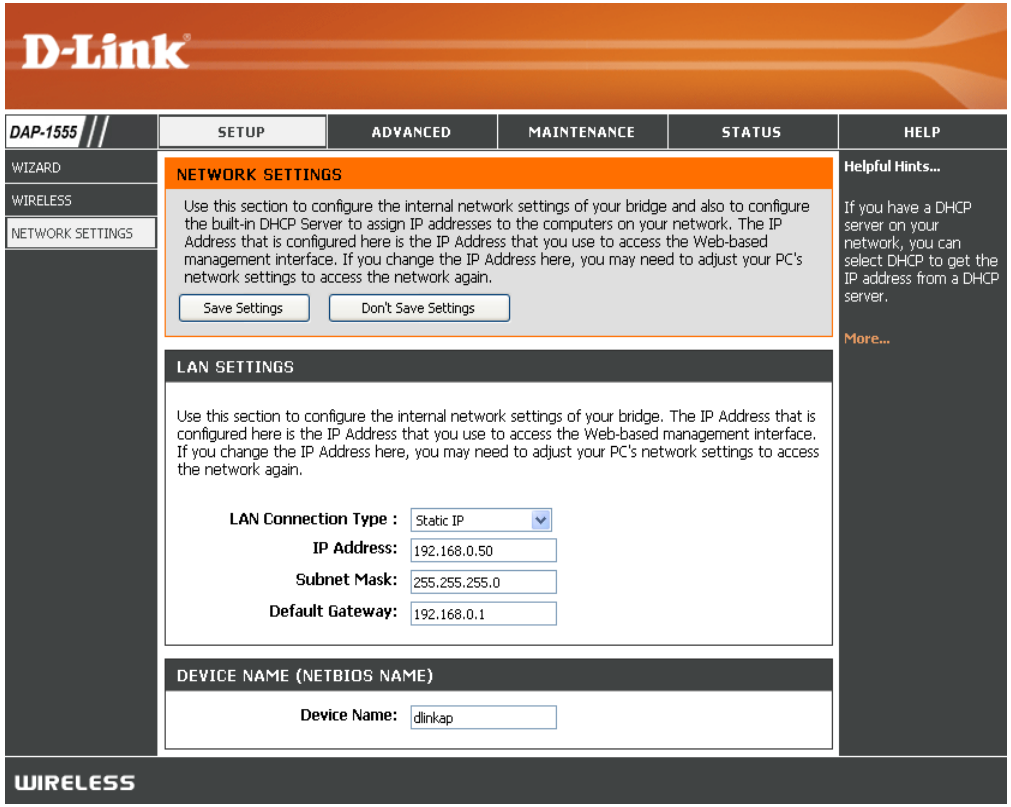
IP Address Mode: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. Select DHCP to automatically assign an IP address to the computers on the LAN/private network.

IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

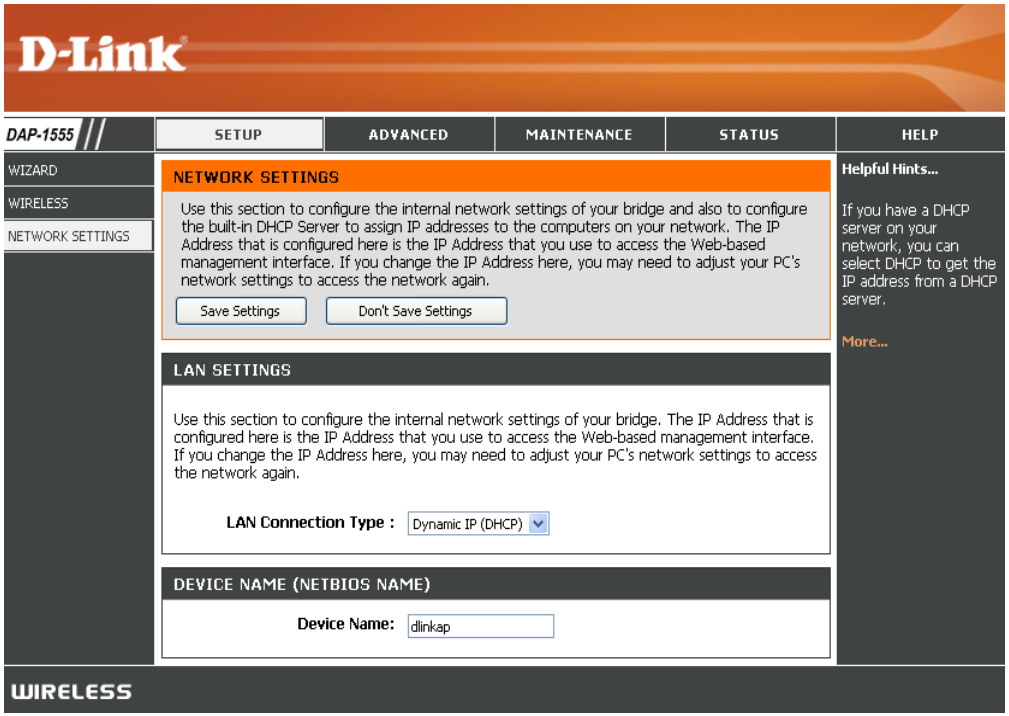
Device Name: Enter the Device Name of the AP and click **Next** to continue. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.



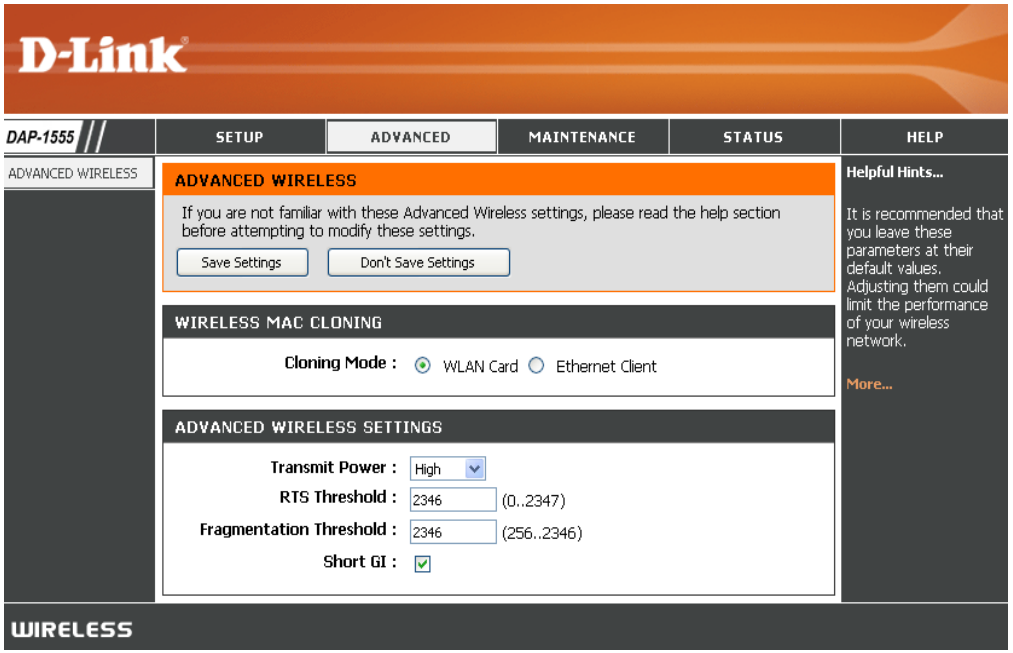
DHCP

LAN Connection Type: Select DHCP to automatically obtain an IP address on the LAN/private network.

Device Name: Enter the Device Name of the AP and click **Next** to continue. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.



Advanced
Advanced Wireless



MAC Cloning Mode: This feature controls the MAC Address of the Bridge as seen by other devices (wired or wireless).

WLAN Card: If set to **Ethernet Client**, the MAC Address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC Address is being used.

Ethernet Client: If set to **WLAN** Card, the MAC Address of the WLAN Card (typically written on the back of the card) will be used. When multiple Ethernet devices are connected to the Bridge, the MAC Address of the Bridge will not change.

Transmit Power: Set the transmit power of the antennas.

RTS Threshold: This value should remain at its default setting of 2436. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

Tools
Admin

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

Admin Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.

Web Idle Timeout: Enter a maximum idle time in which the internet connection is maintained during inactivity.

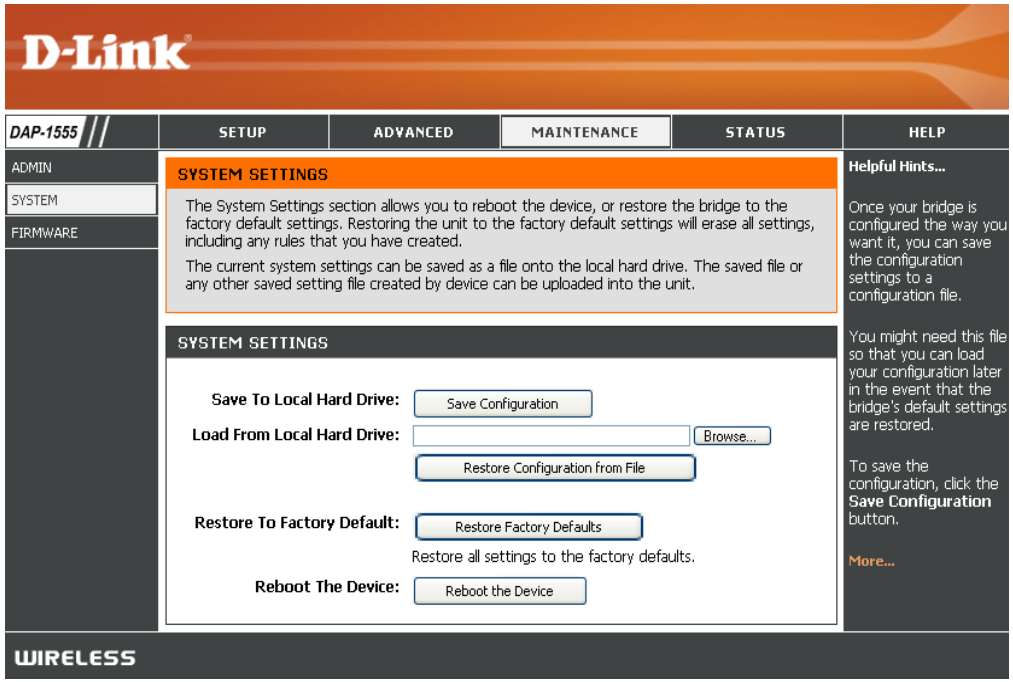
System

Save To Local Hard Drive: Use this option to save the current access point configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. You will then see a file dialog, where you can select a location and file name for the settings.

Load From Local Hard Drive: Use this option to load previously saved access point configuration settings. First, use the Browse control to find a previously save file of configuration settings. Then, click the Load button to transfer those settings to the access point.

Restore To Factory Default: This option will restore all configuration settings back to the settings that were in effect at the time the access point was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current access point configuration settings, use the Save button above.

Reboot The Device: Click to reboot the bridge.

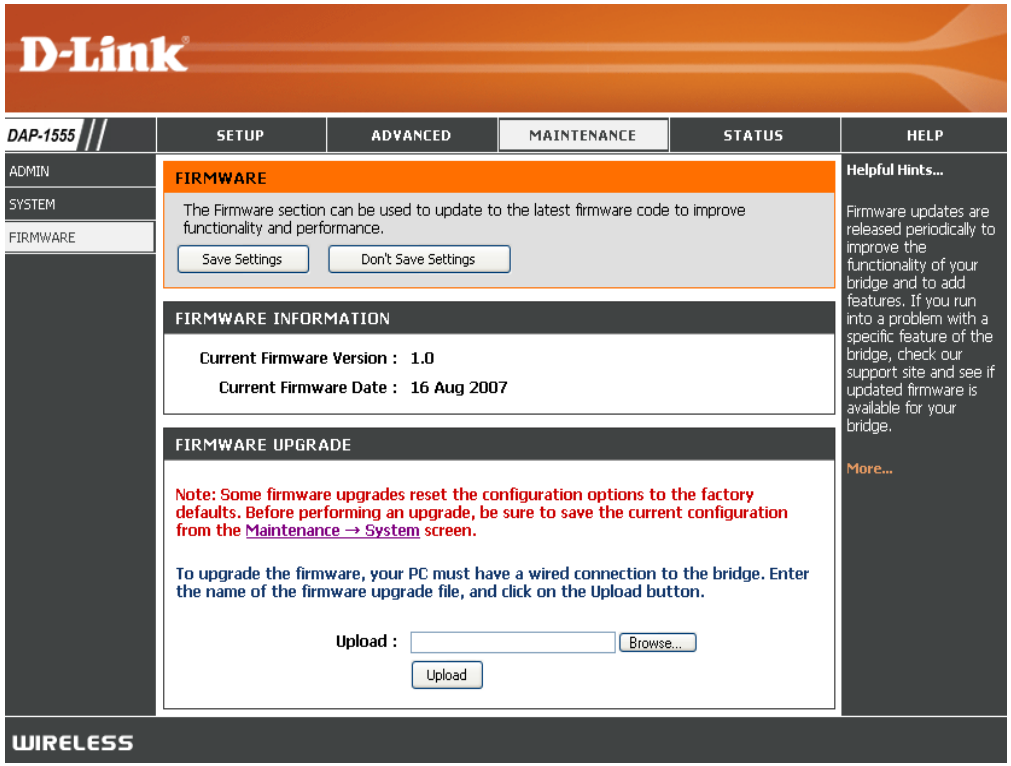


Firmware

You can upgrade the firmware of the Access point here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Browse: After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

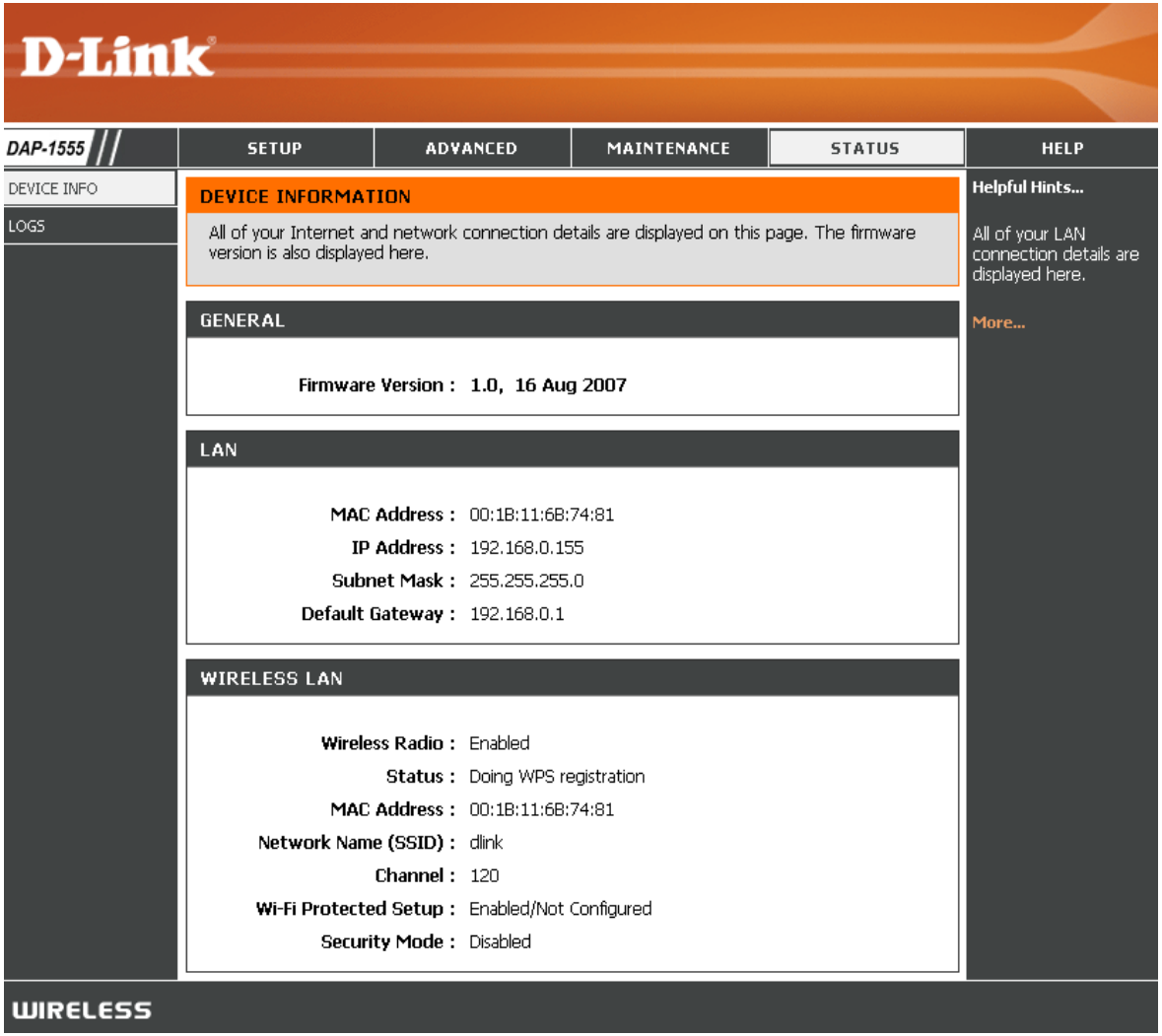
Upload: Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the bridge.



Status

Device Info

This page displays the current information for the DAP-1555. It will display the LAN and Wireless information.



Logs

The bridge automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the bridge logs. You can define what types of events you want to view and the level of events to view. This bridge also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

What to View: You can select the types of messages that you want to display from the log.

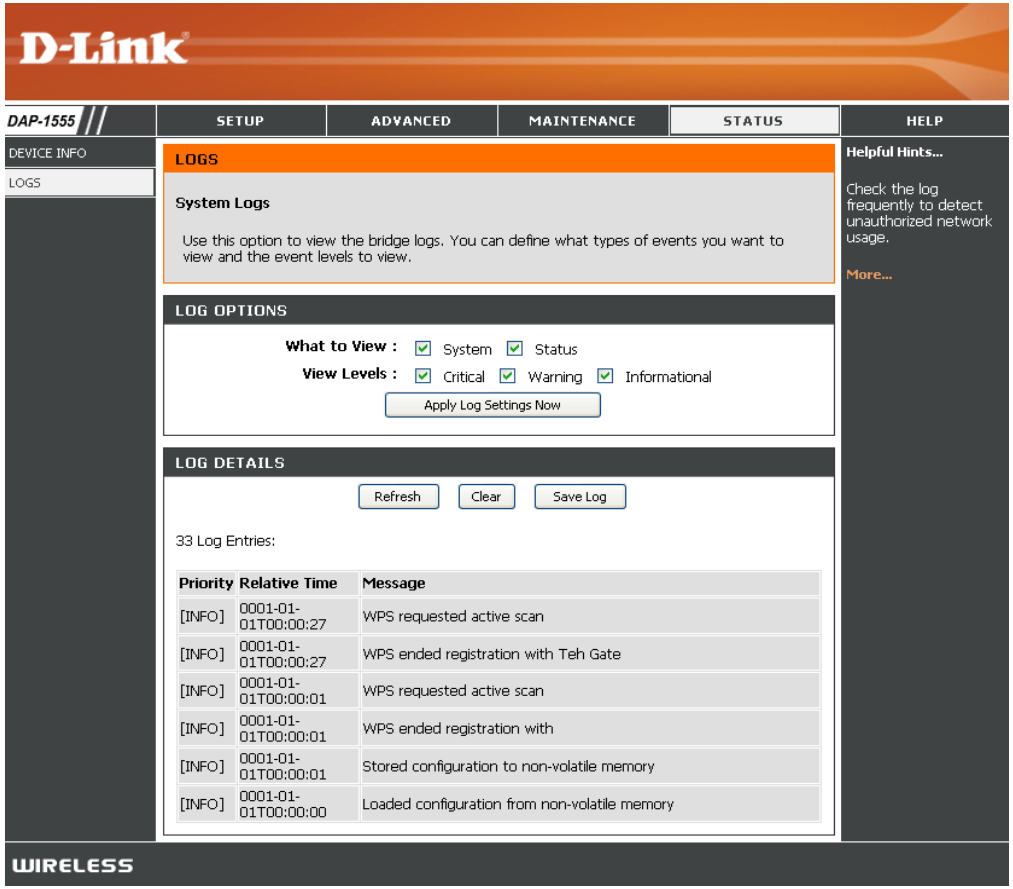
View Levels: There are three levels of message importance: Informational, Warning, and Critical. Select the levels that you want displayed in the log.

Apply Log Settings Now: Will filter the log results so that only the selected options appear.

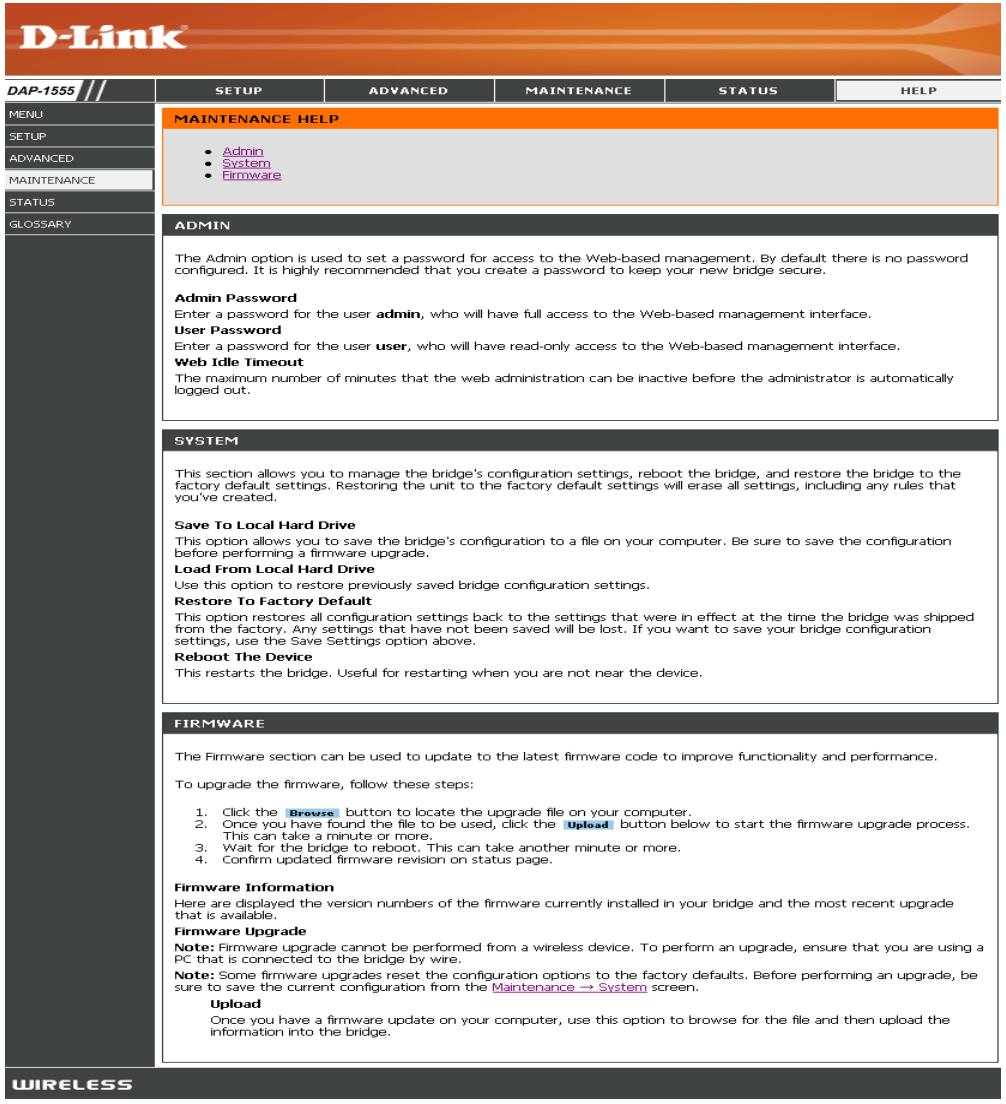
Refresh: Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

Clear: Clicking this button erases all log entries.

Save Log: Select this option to save the bridge log to a file on your computer.



Help


D-Link
DAP-1555
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
MENU
SETUP
ADVANCED
MAINTENANCE
STATUS
GLOSSARY
MAINTENANCE HELP
Admin
System
Firmware
ADMIN
The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new bridge secure.
Admin Password
Enter a password for the user admin, who will have full access to the Web-based management interface.
User Password
Enter a password for the user user, who will have read-only access to the Web-based management interface.
Web Idle Timeout
The maximum number of minutes that the web administration can be inactive before the administrator is automatically logged out.
SYSTEM
This section allows you to manage the bridge's configuration settings, reboot the bridge, and restore the bridge to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.
Save To Local Hard Drive
This option allows you to save the bridge's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.
Load From Local Hard Drive
Use this option to restore previously saved bridge configuration settings.
Restore To Factory Default
This option restores all configuration settings back to the settings that were in effect at the time the bridge was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your bridge configuration settings, use the Save Settings option above.
Reboot The Device
This restarts the bridge. Useful for restarting when you are not near the device.
FIRMWARE
The Firmware section can be used to update to the latest firmware code to improve functionality and performance.
To upgrade the firmware, follow these steps:
1. Click the Browse button to locate the upgrade file on your computer.
2. Once you have found the file to be used, click the Upload button below to start the firmware upgrade process. This can take a minute or more.
3. Wait for the bridge to reboot. This can take another minute or more.
4. Confirm updated firmware revision on status page.
Firmware Information
Here are displayed the version numbers of the firmware currently installed in your bridge and the most recent upgrade that is available.
Firmware Upgrade
Note: Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the bridge by wire.
Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Maintenance → System screen.
Upload
Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the bridge.
WIRELESS

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-1555 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless bridge or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Configure WEP In AP Mode

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (192.168.0.50). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WEP**.

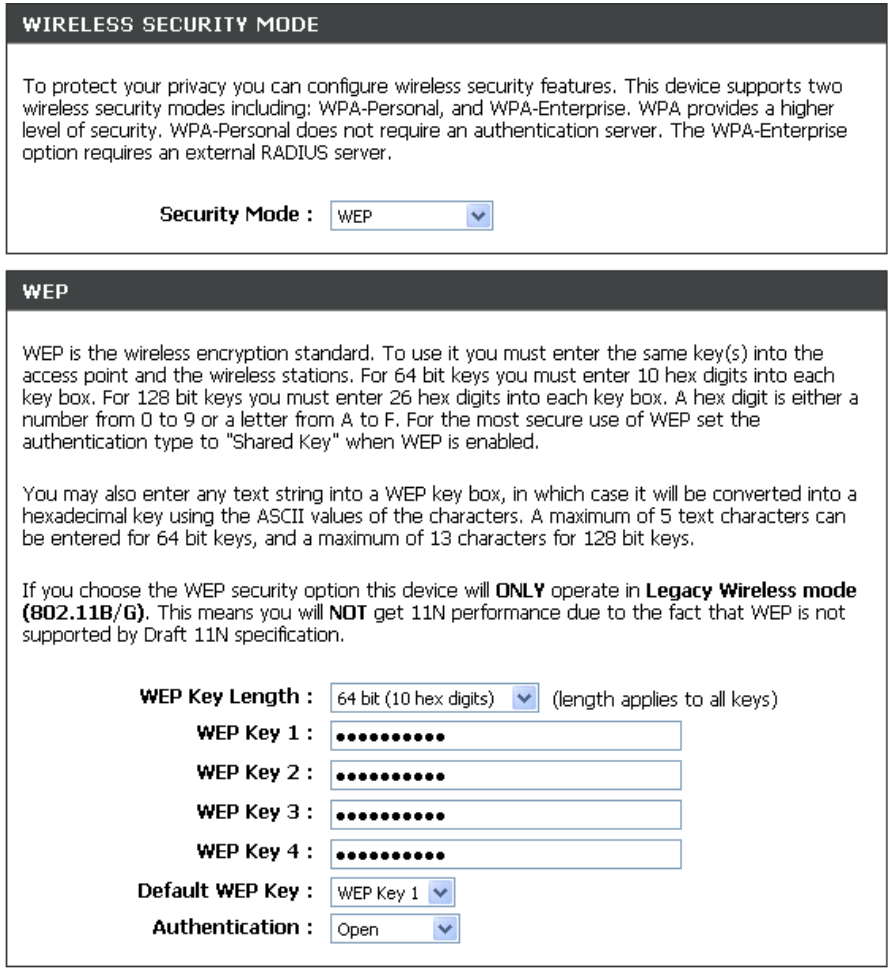
3. Next to *WEP Key Length*, select the level of encryption (64 or 128-bit).

   Hex - (recommended) Letters A-F and numbers 0-9 are valid.

4. Next to *WEP Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.

5. Next to *Authentication*, select **Open or Shared Key**.

6. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the access point.



Configure WPA-Personal (PSK) In AP Mode

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

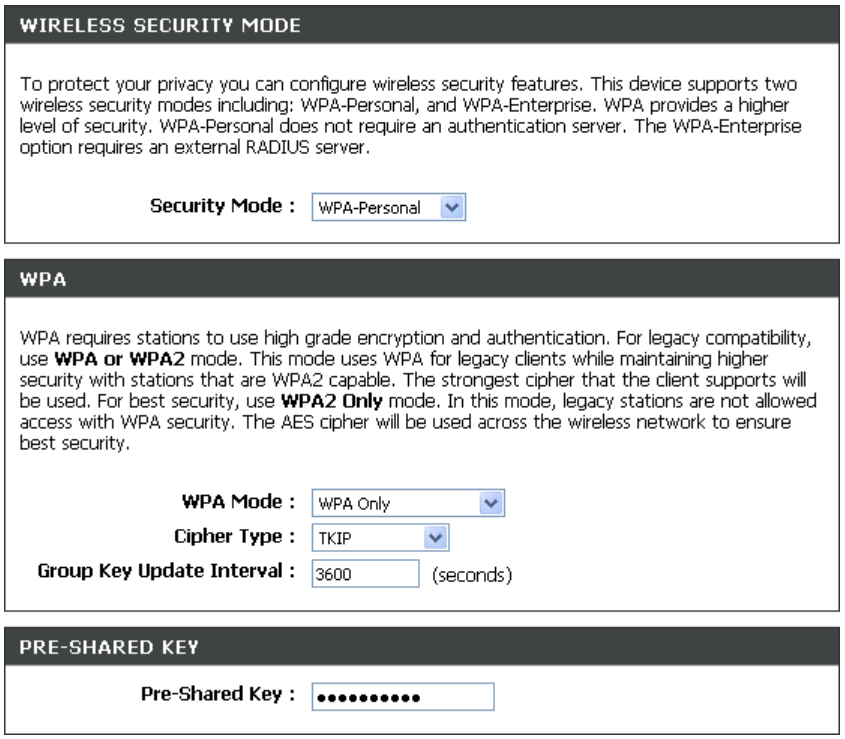
1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (192.168.0.50). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

4. Next to Cipher Type, select TKIP, AES, or TKIP and AES.

5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).



6. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.

7. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

Configure WPA-Enterprise (RADIUS) In AP Mode

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (192.168.0.50). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WPA-Enterprise**.

3. Next to *WPA Mode*, select **Auto WPA or WPA2**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

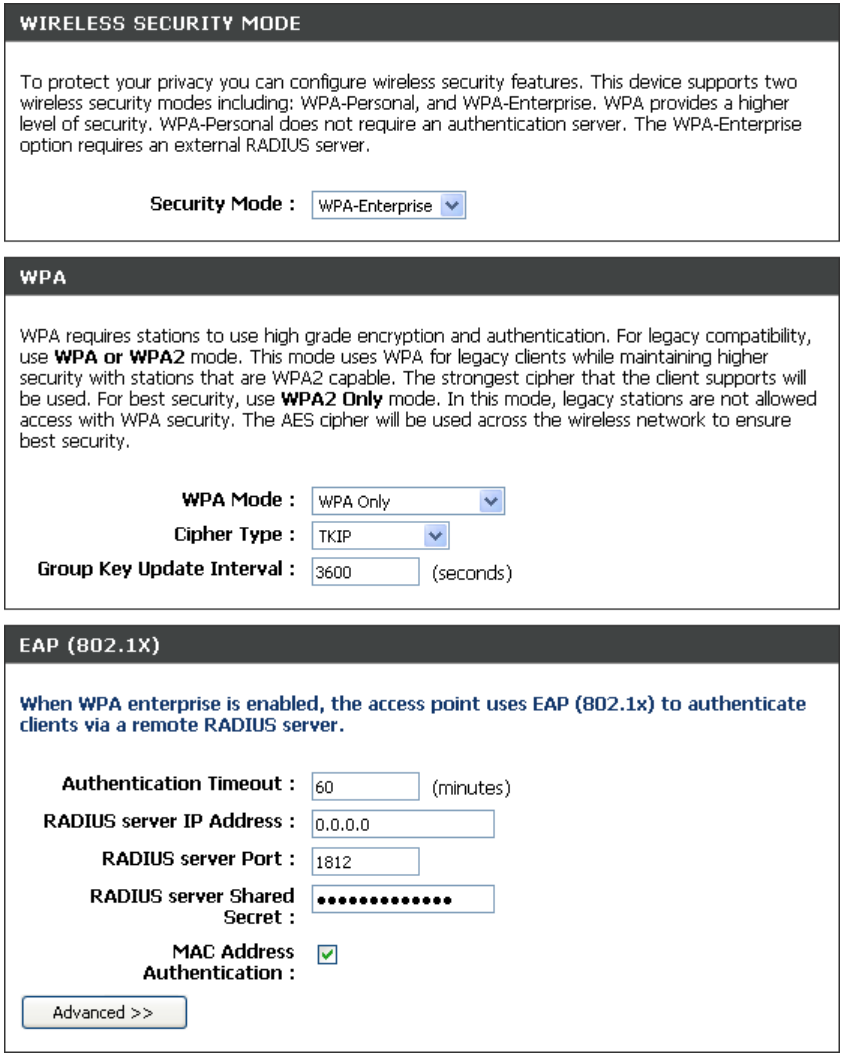
4. Next to Cipher Type, select TKIP, AES or TKIP and AES

5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

6. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).

7. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.

8. Next to *RADIUS Server Port*, enter the port you are using with



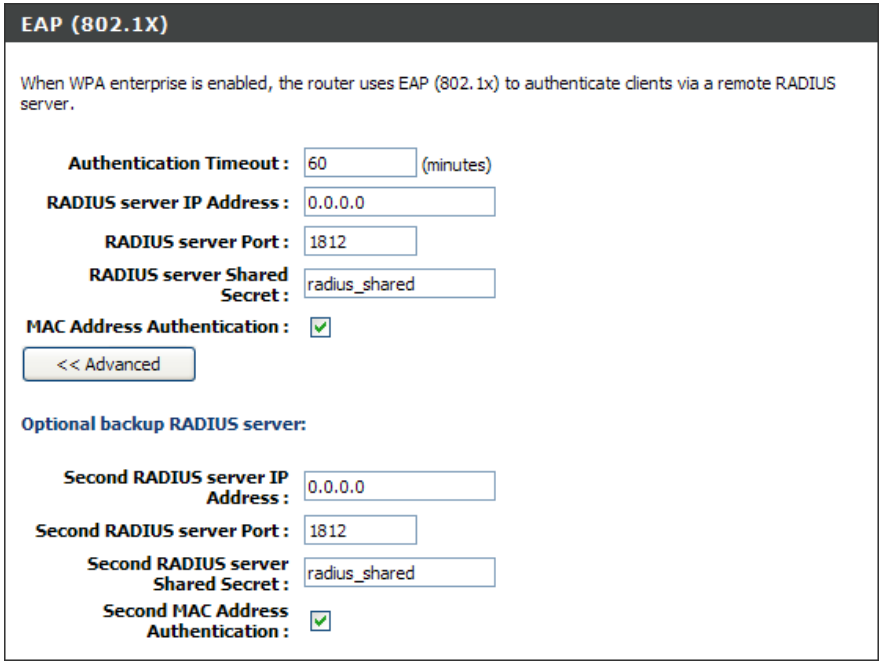
your RADIUS server. 1812 is the default port.

8. Next to *RADIUS Server Shared Secret*, enter the security key.

9. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.

10. Click **Advanced** to enter settings for a secondary RADIUS Server.

11. Click **Apply Settings** to save your settings.



Configure WEP In Bridge Mode

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the bridge (192.168.0.35). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WEP**.

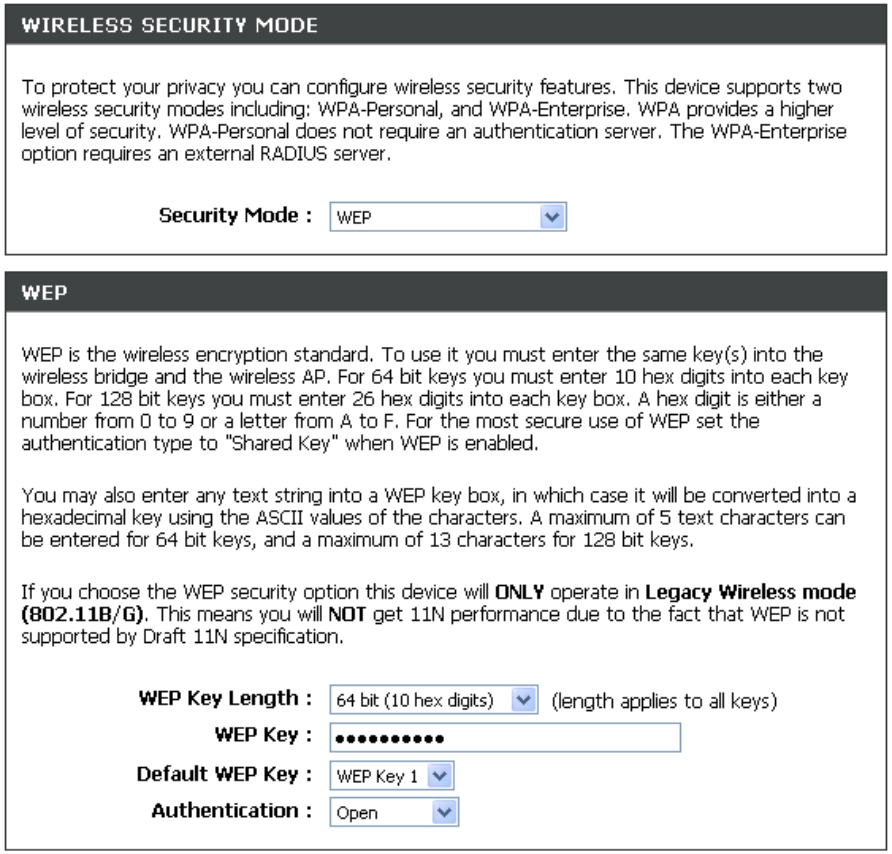
3. Next to *WEP Key Length*, select the level of encryption (64 or 128-bit).

   Hex - (recommended) Letters A-F and numbers 0-9 are valid.

4. Next to *WEP Key*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices.

5. Next to *Authentication*, select **Open or Shared Key**.

6. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the access point.



Configure WPA-Personal (PSK) In Bridge Mode

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

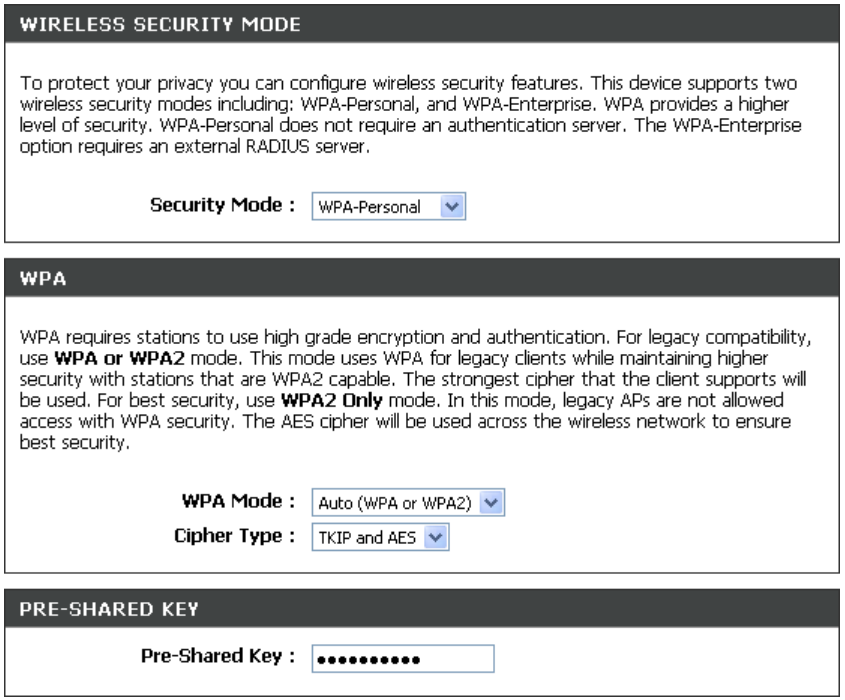
1. Log into the web-based configuration by opening a web browser and entering the IP address of the bridge (192.168.0.35). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **Auto WPA or WPA2, WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

4. Next to Cipher Type, select TKIP, AES, or TKIP and AES.

5. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.



6. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

Configure WPA-Enterprise (RADIUS) In Bridge Mode

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the bridge (192.168.0.35). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WPA-Enterprise**.

3. Next to *WPA Mode*, select **Auto WPA or WPA2**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

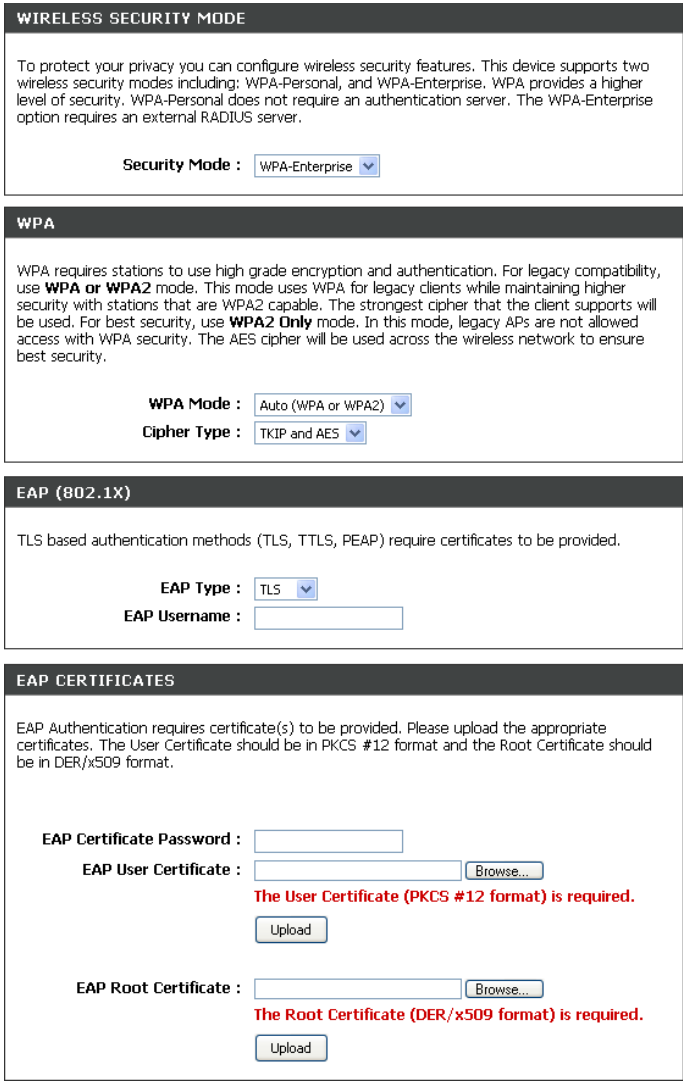
4. Next to Cipher Type, select **TKIP**, **AES** or **TKIP** and **AES**.

5. Next to EAP type, select **EAP-TLS**, **EAP-TTLS**, or **PEAP** that will be used for authentication.

6. Next to EAP Username, enter the username of the wireless client for the tunnel establishment and the inner authentication method.

7. Next to EAP Password, enter the password of the wireless client for **EAP-MD5** or the inner authentication methods of **PEAP** and **EAP-TTLS**.

8. Next to EAP Certificate Password, enter the password of the user certificate.



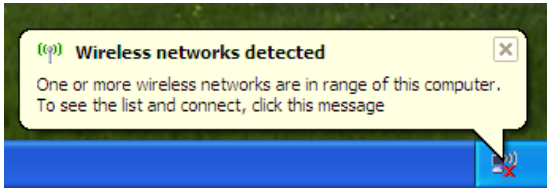
9. Next to EAP User Certificate, click Browse to locate the user certificate file. It is optional for **EAP-TLS**, but mandatory for **PEAP** and **EAP-TTLS**.

10. Next to EAP Root Certificate, click Browse to locate the Root Certificate file. It is mandatory to upload a root certificate to be able to authenticate the server certificate.

Connect to a Wireless Network Using Windows® XP

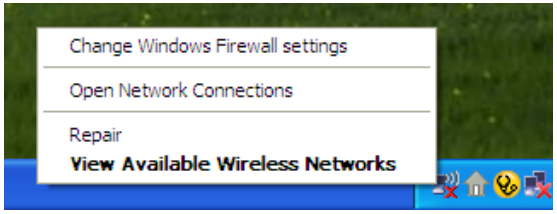
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

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



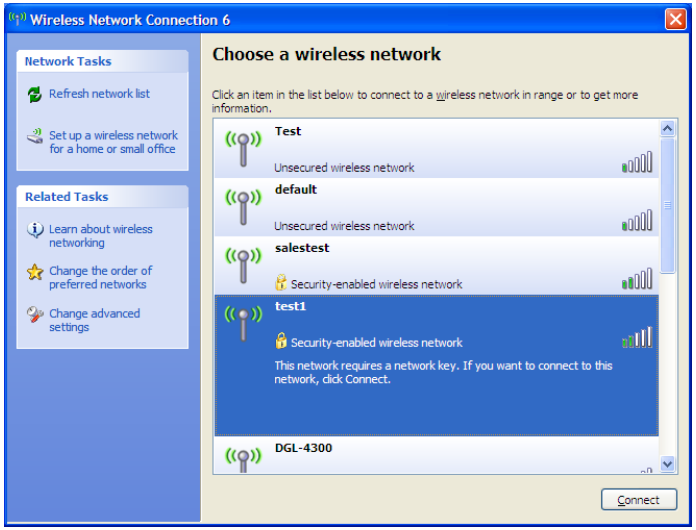
or

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.

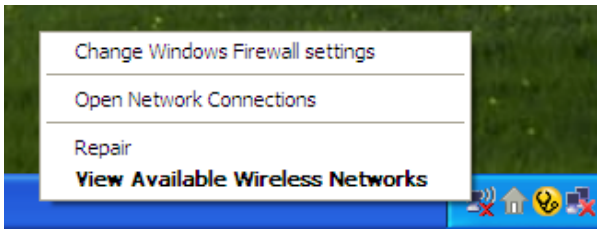
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



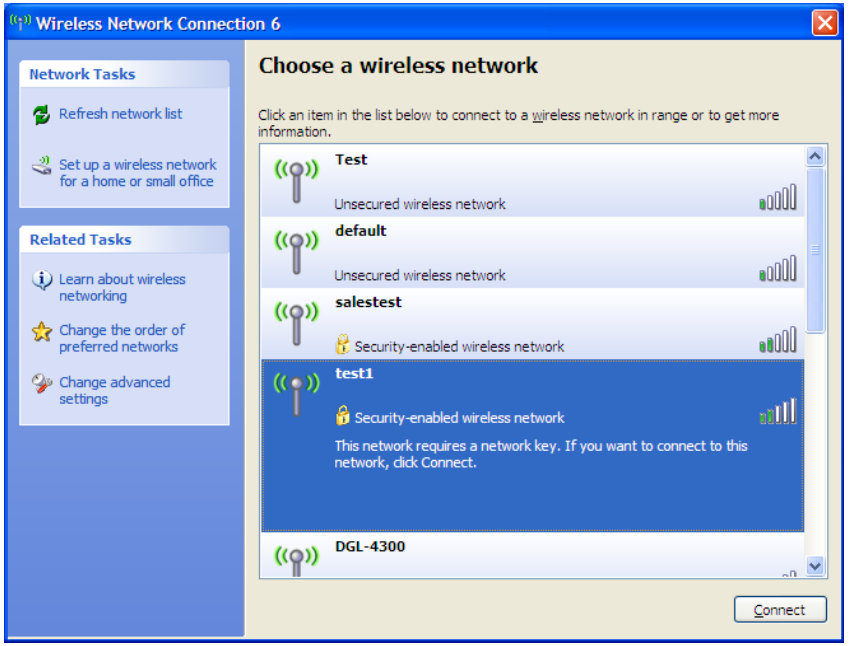
Configure WEP

It is recommended to enable WEP on your wireless bridge or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP 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**.

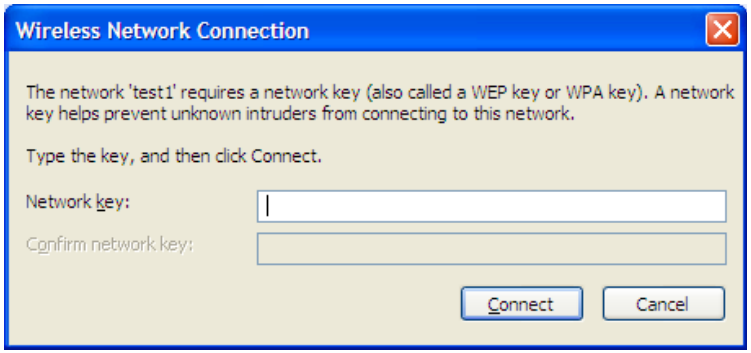


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the same WEP key that is on your access point and click **Connect**.

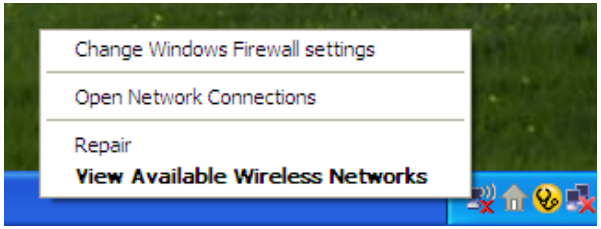
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless access point.



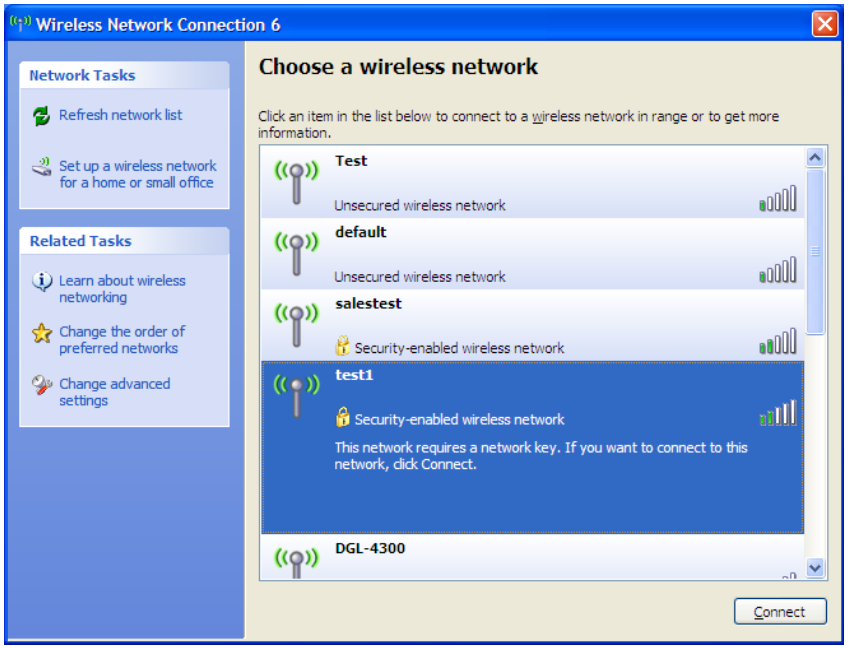
Configure WPA-PSK

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

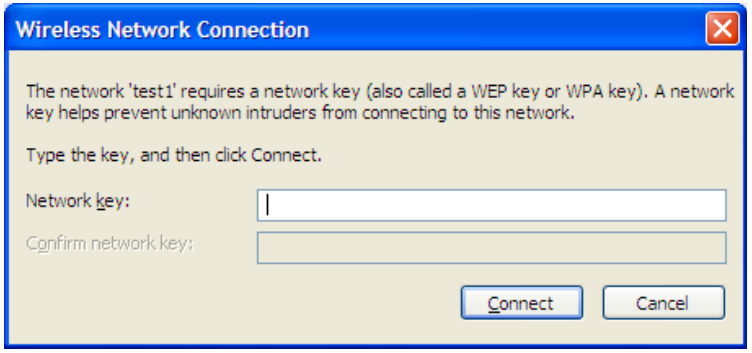
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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 access point.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-1555. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link access point (192.168.0.50 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device 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:

- Internet Explorer 6.0 or higher
- Netscape 8 or higher
- Mozilla 1.7.12 (5.0) or higher
- Opera 8.5 or higher
- Safari 1.2 or higher (with Java 1.3.1 or higher)
- Camino 0.8.4 or higher
- Firefox 1.5 or higher

• Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

• Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, 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:

    - 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 open it.

- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.

- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug 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 access point. Unfortunately this process will change all your settings back to the factory defaults.

To reset the access point, locate the reset button (hole) on the rear panel of the unit. With the access point powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the access point will go through its reboot process. Wait about 30 seconds to access the access point. The default IP address is 192.168.0.1. When logging in, the username is **admin** and leave the password box empty.

3. Why can't I connect to certain sites or send and receive emails when connecting through my access point?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, and XP users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

  ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your access point with the proper MTU size.

To change the MTU rate on your access point follow the steps below:

- Open your browser, enter the IP address of your access point (192.168.0.50) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

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 access the data you want, when and where you want it. 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 adapter cards 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 Access point is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your access point or Access Point

Make sure you place the bridge/access point in a centralized location within your network for the best performance. Try to place the bridge/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

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

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the access point. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless bridge.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DAP-1555 wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless bridge. All the wireless devices, or clients, will connect to the wireless bridge or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

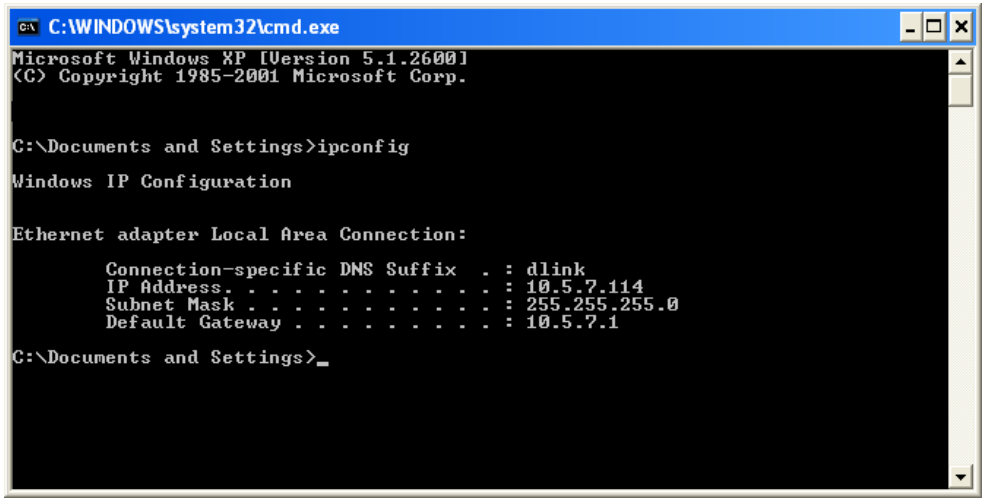
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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 access point. Some firewall software programs may block a DHCP request on newly installed adapters.



If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

Statically Assign an IP address

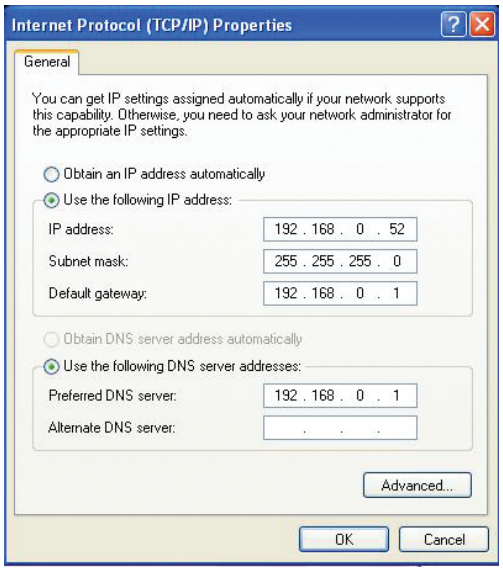
If you are not using a DHCP capable gateway/access point, or you need to assign a static IP address, please follow the steps below:

Step 1
Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

Step 3
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your access point.



Example: If the access point´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 access point (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your access point (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5
Click **OK** twice to save your settings.

Technical Specifications

Standards
- IEEE 802.11n (draft)
- IEEE 802.11a
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Security
- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise
- 64/128-bit WEP

Wireless Signal Rates[1]
- 300Mbps
- 108Mbps
- 54Mbps
- 48Mbps
- 36Mbps
- 24Mbps
- 18Mbps
- 12Mbps
- 11Mbps
- 9Mbps
- 6Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

Maximum Operating Voltage
3.3V

Maximum Power Consumption
1435 mA

Modulation
- 11b: DQPSK, DBPSK and CCK
- 11a/g: BPSK, QPSK, 16QAM, 64QAM, OFDM
- 11n: BPSK, QPSK, 16QAM, 64QAM, OFDM, MCS

Frequency Range[2]
- 2.4GHz to 2.483GHz
- 5.15GHz~5.825GHz[3]

External Antenna Type
Two (2) detachable reverse SMA Antennas

LEDs
- Power
- Bridge
- AP
- WLAN
- LAN (10/100)

Operating Temperature
32°F to 104°F (0°C to 40°C)

Humidity
90% maximum (non-condensing)

Safety & Emissions
- FCC
- CE
- IC
- C-Tick

Dimensions
- L = 7.75 inches
- W = 4.75 inches
- H = 1.25 inches

Warranty
1 Year

[1]Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and Draft 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 conditions will adversely affect wireless signal range.
[2]Range varies depending on country's regulation.
[3]The DAP-1555 doesn't include 5.25-5.35GHz & 5.47~5.725GHz.

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-1555)
- Hardware Revision (located on the label on the bottom of the access point (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the access point).

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.com

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 DLink 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:

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. DLink 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.

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.

Copyright ©2007 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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 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 communication. 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 or more 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 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.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment 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. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Industry Canada Notice:

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.

IMPORTANT NOTE:
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.

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Registration

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

Version 1.0
July 26, 2007