D-Link

Wi-Fi 6

EAGLE PRO AI

AX3200 SMART ROUTER R32

works with Ok Google

JUST ASK amazon alexa

Preface

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

Manual Revisions

Hardware	Revision	Date	Description
A1	v1.00	2021/11/26	Initial release

Trademarks

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

Apple®, Apple logo®, Safari®, iPhone®, and Macintosh® are trademarks of Apple Inc., registered in the U.S. and other countries. App Store℠ is a service mark of Apple Inc.

Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Copyright © 2021 by D-Link Corporation, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Corporation, Inc.

ErP Power Usage

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted.

R32	Network Standby:

Table of Contents

Product Overview 1
Package Contents 1
System Requirements 2
Introduction 3
Features 3
Hardware Overview 4
LED Indicators 4
Back Panel 5

Installation 6
Before you Begin 6
Wireless Installation Considerations 7
Setup 8
EAGLE PRO AI Setup 9
Hardware Setup 10
Setup Wizard 13

Configuration 20
Home 21
Internet 22
R32 23
Connected Clients 24
Settings 26
Wizard 26
Internet - IPv4 27
IPv4 - Dynamic IP (DHCP) 28
IPv4 - Static IP 29
IPv4 - PPPoE 30
IPv4 - PPTP 32
IPv4 - L2TP 34
IPv4 - DS-Lite 36
Internet - IPv6 37
IPv6 - Auto Detection 38
IPv6 - Static IPv6 40
IPv6 - Auto Configuration (SLAAC/DHCPv6) 42
IPv6 - PPPoE 45
IPv6 - 6rd 49
IPv6 - Local Connectivity Only 51
Internet - VLAN 52
Wireless 54
Guest Zone 60
Network 62
D-Link Cloud 64
Operation Mode 65
Features 66
Parental Control 66
QoS Engine 69
Firewall 71
Firewall Settings - IPv4/IPv6 Rules 73
Port Forwarding 75
Port Forwarding - Virtual Server 77
Static Routes - IPv4 79
Static Routes - IPv6 80
Dynamic DNS 81
Quick VPN 83

Management....84
Time & Schedule - Time....84
Time & Schedule - Schedule....85
System Log....86
System Admin - Admin....88
System Admin - System....89
User....90
Upgrade....91
Statistics....92

EAGLE PRO AI....93

Voice Control....97
Link D-Link Cloud Service to Other Services....98
Google Home Setup....98
Amazon Alexa Setup....103
Amazon Alexa Voice Commands....106
The Google Assistant Setup....107
Google Assistant Voice Commands....109

Quick VPN....110
Important Information....111
iOS Devices....112
VPN Setup Instructions....112
Connect or Disconnect....114
Mac OS X....115
VPN Setup Instructions....115
Connect or Disconnect....117
Windows 7....118
VPN Setup Instructions....118
Connect or Disconnect....121
Windows 8.1/8....122
VPN Setup Instructions....122
Connect or Disconnect....127
Windows 10....128
VPN Setup Instructions....128
Connect or Disconnect....130
Android....131
VPN Setup Instructions....131
Connect or Disconnect....133

Connect a Wireless Client to your Router....134
WPS Button....134
Windows® 10....135
Windows® 8....136
Windows® 7....138

Troubleshooting....140

Wireless Basics....142

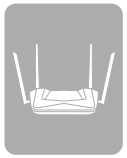
Networking Basics....146

Wireless Security....148

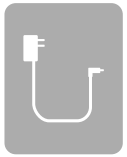
Technical Specifications....149

Regulatory Statements....151

Product Overview
Package Contents

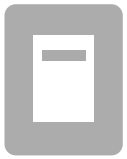


R32 AX3200 Smart Router



Power Adapter (12V, 2A)

Ethernet Cable (RJ45, 1m)



Quick Installation Guide

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

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

System Requirements

Network Requirements	• An Ethernet-based cable, DSL or fiber modem • IEEE 802.11ax/ac/n/g/b/a wireless clients • 10/100/1000 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 11 or later • Firefox 28 or later • Safari 6 or later • Chrome 28 or later
EAGLE PRO AI APP Requirements	• iOS® or Android™ device (Please refer to the description of the app's page to check whether your device is compatible.)

Introduction

With a powerful network processor, the AX3200 Smart Router packs in strong processing power to help you manage your home or office network. It's a powerful, intelligent home router with AI-assisted traffic control, Wi-Fi utilization and mesh optimization, and parental controls. It also has integrated voice assistant compatibility for Amazon Alexa and Google Assistant so you can control your network with voice commands.

Features

Smooth Wireless Connectivity with Maximized Bandwidth
The innovative AI Traffic Optimizer provides weekly usage report to inform administrators about the consumption of network bandwidth along with heavy users. It also rates the overall condition of the wireless network and states the number of times the engine has optimized the network automatically based on the network conditions and usage data.

Handle More with a High-Power Processor
With the R32, you're not only enjoying buffer-free gaming and lightning-fast surfing, but also features such as optimized QoS, controlled Internet access with website filtering, and compatibility with voice assistants. All this is possible with the router's 1.4 GHz dual-core high-power processor, 128 MB of flash memory and 256 MB of RAM.

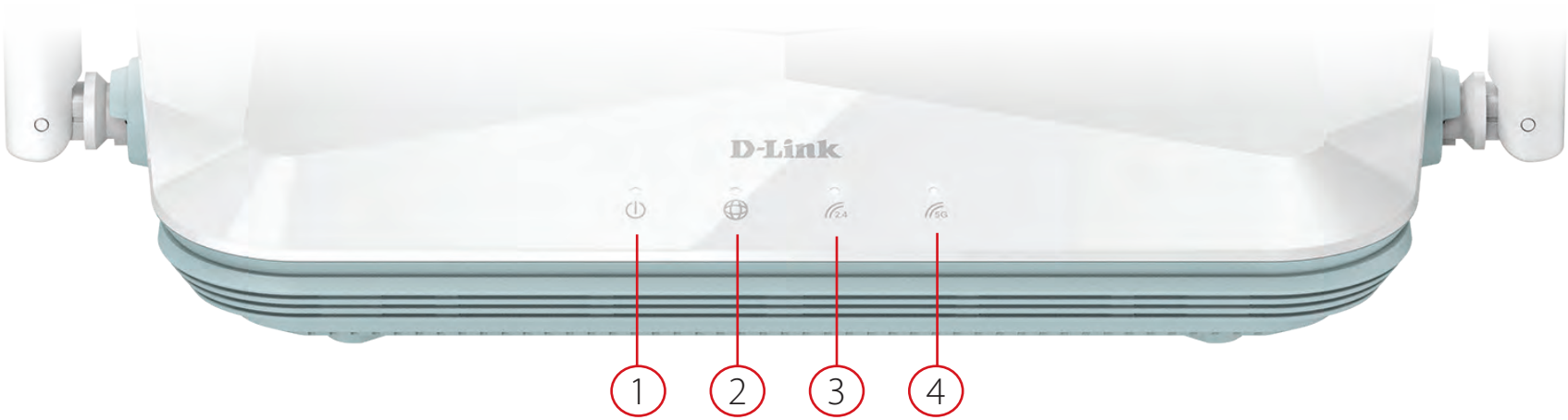
Intelligent Quality of Service Features
The Quality of Service (QoS) allows you to prioritize important traffic to ensure that real-time applications are receiving optimal bandwidth. Moreover, the inbuilt AI engine collects and analyzes traffic data and notifies administrators of clients that consume high bandwidth so that they can take prompt action.

Always Up-to-Date with the Latest Features
The R32 will automatically check daily for updates to make sure that the device always has the latest security upgrades and new features, which will install silently in the background. For extra peace of mind, in the event of failure during the firmware update, the router will store a backup system image in the memory before proceeding with the update.

Easy Setup and Flexible Management
Managing your Internet utilization has never been easier; just download the free EAGLE PRO AI for your mobile device and follow the on-screen step-by-step instructions to add your device. You also have the option to use a web browser to access the setup wizard for basic configuration and advanced features. Support for industry-standard Wi-Fi Protected Setup (WPS) lets you create encrypted connections to new devices by pressing a button.

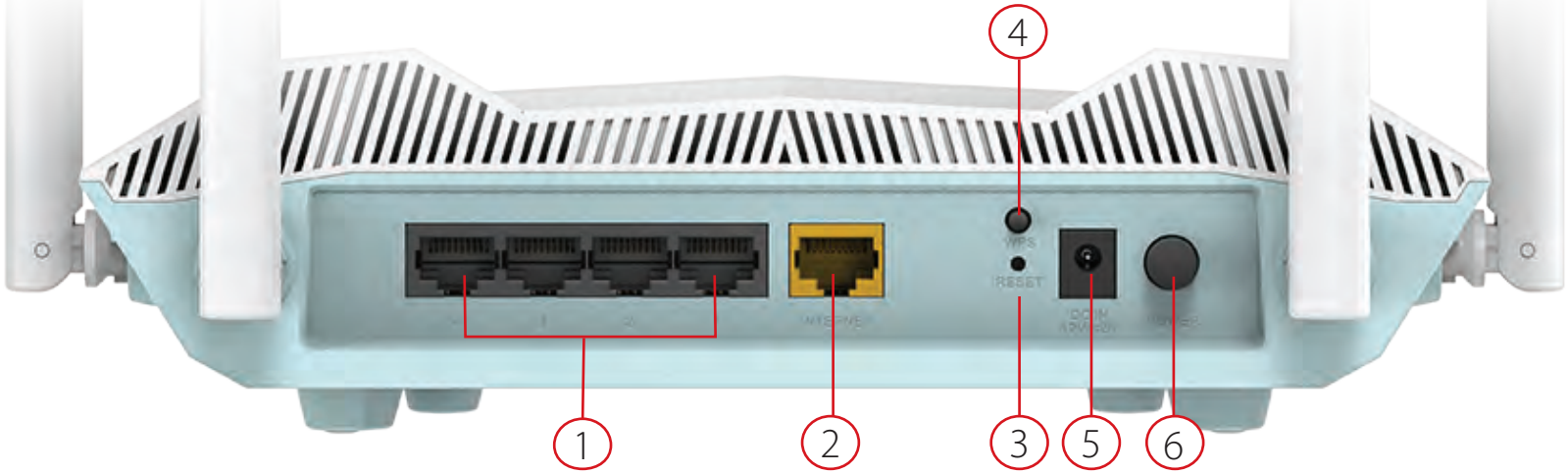
Hardware Overview

LED Indicators



1	**Power**	Solid White	The device is on and the system is healthy.
		Solid Orange	The device is booting up or performing the factory reset process.
		Blinking Orange	The device is under recovery mode.
2	**Internet**	Solid White	The Internet connection is established.
		Solid Orange	The device cannot connect to the Internet.
		Blinking Orange & White Alternately	The device is undergoing the firmware upgrade process.
		Blinking Orange	Internet access has been paused.
3	**Wireless (2.4 GHz)**	Solid White	The 2.4 GHz wireless band is enabled.
		Blinking White	The device is transmitting data. It is processing WPS if the below 5 GHz LED is blinking at the same time.
4	**Wireless (5 GHz)**	Solid White	The 5 GHz wireless band is enabled.
		Blinking White	The device is transmitting data. It is processing WPS if the above 2.4 GHz LED is blinking at the same time.

Back Panel



1	**Gigabit LAN Ports (1- 4)**	Connect Ethernet devices such as computers, switches, storage (NAS) devices, and game consoles.
2	**Gigabit WAN Port**	Use an Ethernet cable to connect your broadband modem to this port.
3	**Reset Button**	Insert a paperclip in the hole, wait for the power LED turns orange (all other LEDs should be off), then release to reset the router to default settings.
4	**WPS Button**	Press to start the WPS process and automatically create an encrypted connection to a WPS client.
5	**Power Connector**	Connector for the supplied power adapter.
6	**Power Button**	Press the power button to power the device on or off.

Installation

This section will walk you through the installation of your R32.

Before you Begin

- Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, attic, or garage.
- Configure the router with the computer that was last connected directly to your Internet connection. Verify that it is connected to the Internet before connecting additional devices.
- If your ISP provides you with a modem/router combo, you will need to set it to bridge or router mode depending on your usage requirements. Please contact your ISP or refer to the user manual for your modem/router device.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, then turn the modem back on. In some cases, you may need to call your Internet Service Provider (ISP) to change connection types (USB to Ethernet).
- If connecting to a DSL modem, make sure to have your DSL service information provided by your Internet Service Provider handy. This information is likely to include your DSL account's username and password. Your ISP may also supply you with additional WAN configuration settings which might be necessary to establish a connection.
- If you are connecting a considerable amount of networking equipment, it may be a good idea to take the time to label each cable or take a picture of your existing setup before making any changes.
- 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 router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind 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 router 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 (0.5 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 routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete 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 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Setup

There are several ways you can configure your router to connect to the Internet

- **EAGLE PRO AI** - Use your compatible iOS or Android device to install and configure your router. Refer to **EAGLE PRO AI Setup** on page **9.**
- **Hardware Setup** - This section explains how to set up your R32. Refer to **Hardware Setup** on page **10.**
- **D-Link Setup Wizard** - This wizard will launch when you log in to the router using your browser for the first time. Refer to **Setup Wizard** on page **13**.
- **Manual Setup** - Log in to the router to manually configure your router. Refer to **Configuration** on page **20**

EAGLE PRO AI Setup

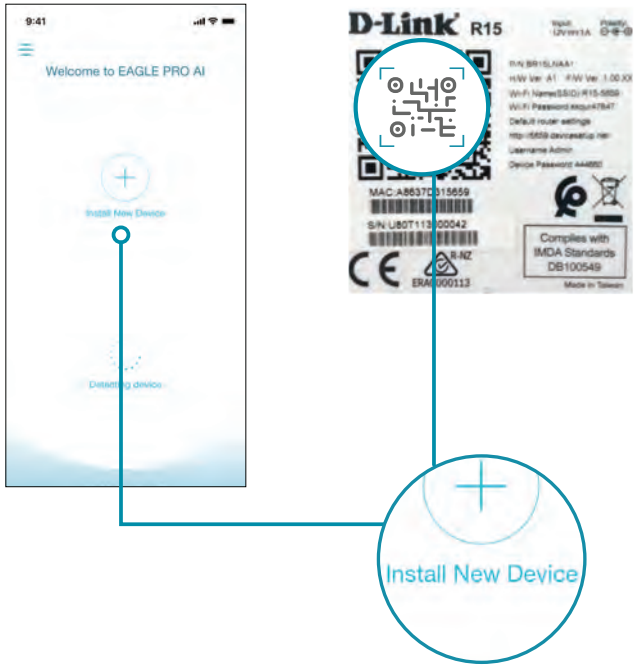
The EAGLE PRO AI allows you to install and configure your R32 from your compatible Android or iOS device.

Note: *The screenshots may be different depending on your mobile device's OS version. However, the process is the same.*

Step 1
Search and install the free **EAGLE PRO AI** available on the App Store or on Google Play.

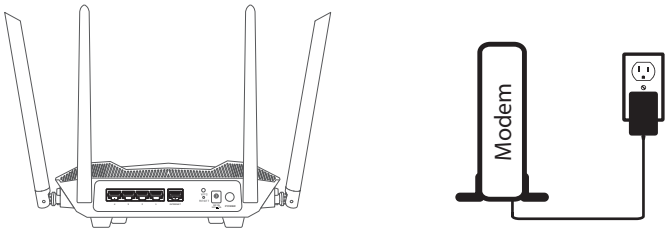
Step 2
Launch the EAGLE PRO AI from the home screen of your device.

Step 3
Tap **Install New Device**. Scan the setup code on the device label on the bottom of the router. Follow the on-screen instructions to complete the setup.

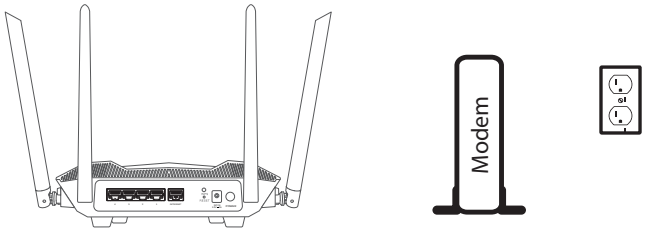


Hardware Setup

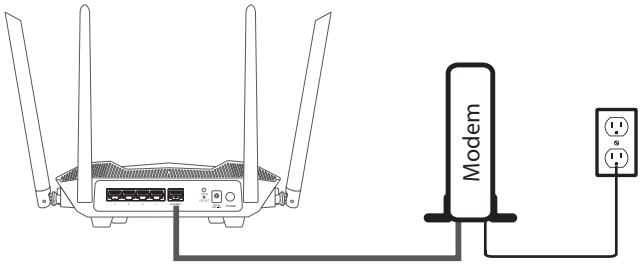
Step 1
Position your R32 near your Internet-connected modem. Place it in an open area for better wireless coverage.



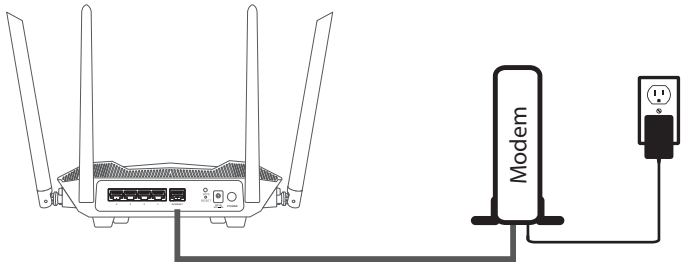
Step 2
Turn off and unplug the power to your cable or DSL broadband modem. This is required. In some cases, you may need to turn it off for up to five minutes.



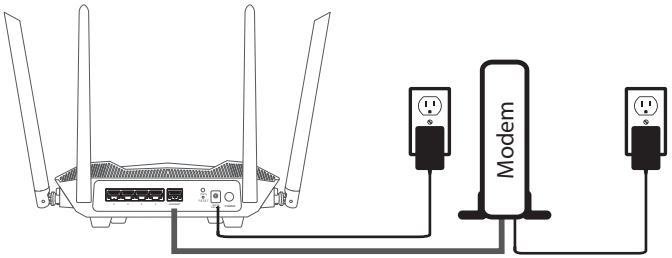
Step 3
Use the Ethernet cable to connect your modem to the port labelled **INTERNET** on the router.



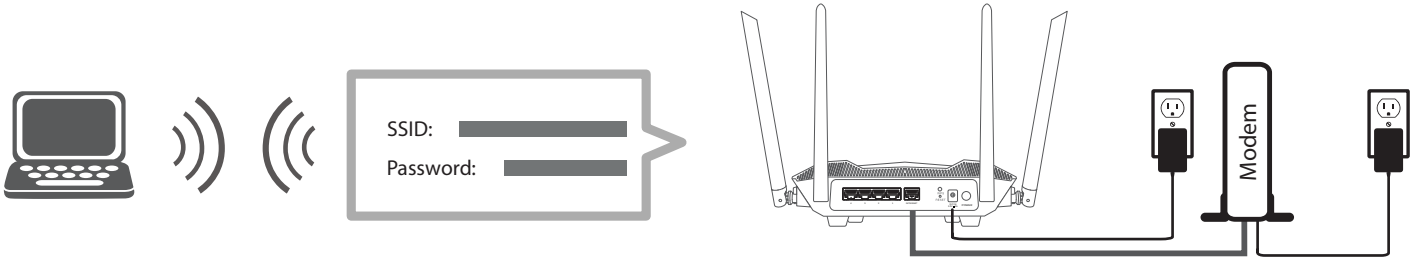
Step 4
Plug in the power and turn your modem back on and wait approximately one minute before proceeding with the procedure.



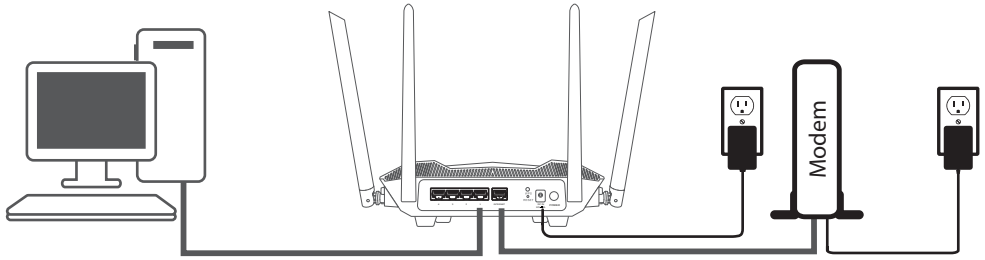
Step 5
Connect the supplied power adapter to the router and a power outlet, and wait approximately one minute until the LED indicator on the front of the device changes from orange to solid white.



Step 6
If you are configuring the router wirelessly from a PC, connect to the Wi-Fi network name printed on the label attached to the bottom of your router. **Note:** The Wi-Fi name (SSID), Wi-Fi password, and device password are printed on the device label on the bottom of the device.



If you are configuring the router from a PC with a wired Ethernet connection, plug one end of an Ethernet cable into the port labelled 1 on the back of the router, and the other end into the Ethernet port on your computer.



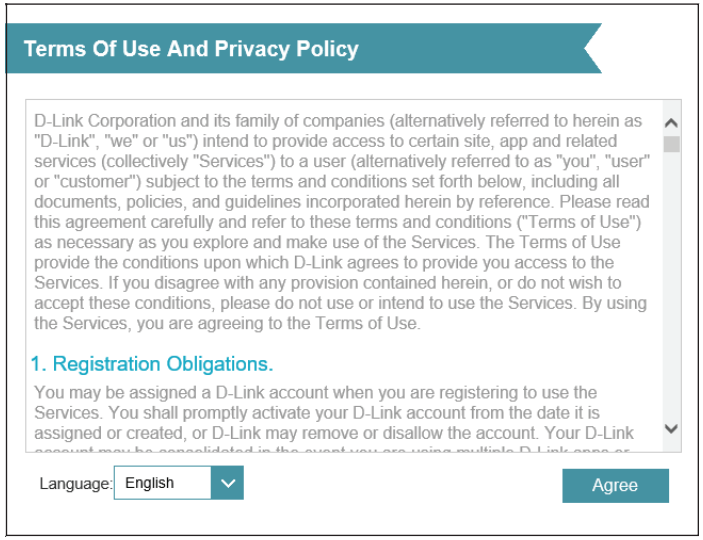
Step 7
If you are connecting to a broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and connecting to a website. If the website does not load, proceed to **Setup Wizard** on page **13**.

Setup Wizard

The setup wizard is designed to guide you through a step-by-step process of configuring your new R32 for Internet connection.

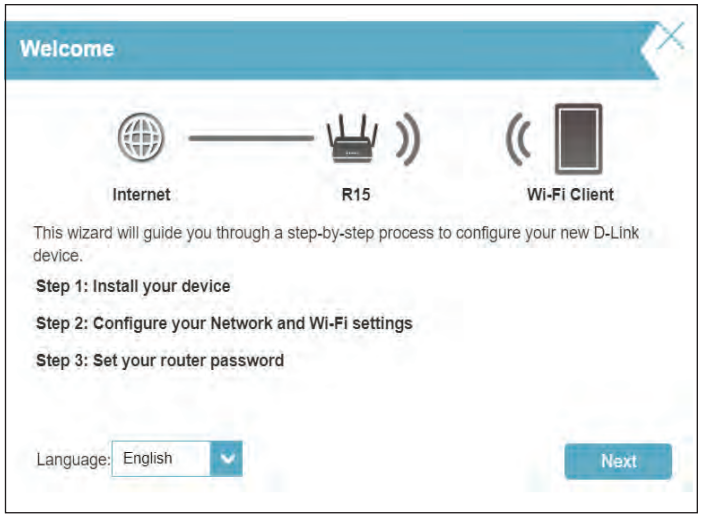
If this is your first time installing the router, open your web browser and enter **http://*XXXX*.devicesetup.net/** into the browser (XXXX represents the last 4 digits of the MAC address). Enter the **Admin Password** and click **Log In** to start the configuration process. The web address and device password are printed on the device label on the bottom of the device.

Agree to the **Terms of Use and Privacy Policy** before proceeding.

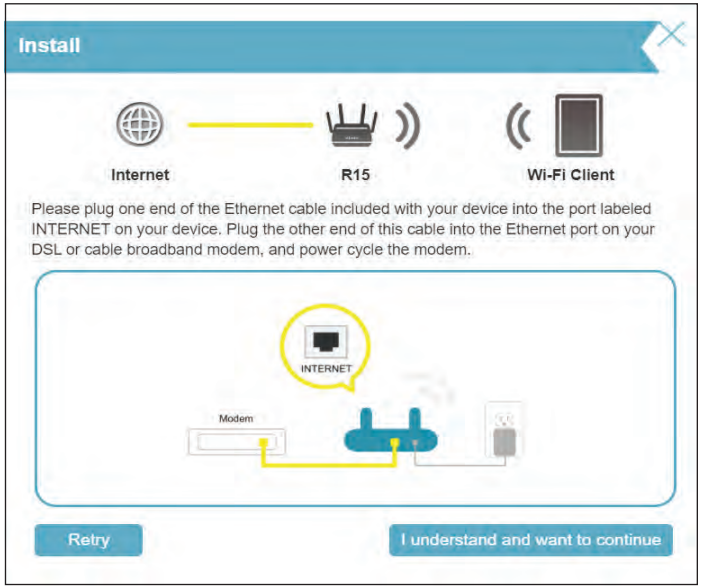


Follow the on-screen instructions to configure your new D-Link router and connect to the Internet.

Click **Next** to continue.

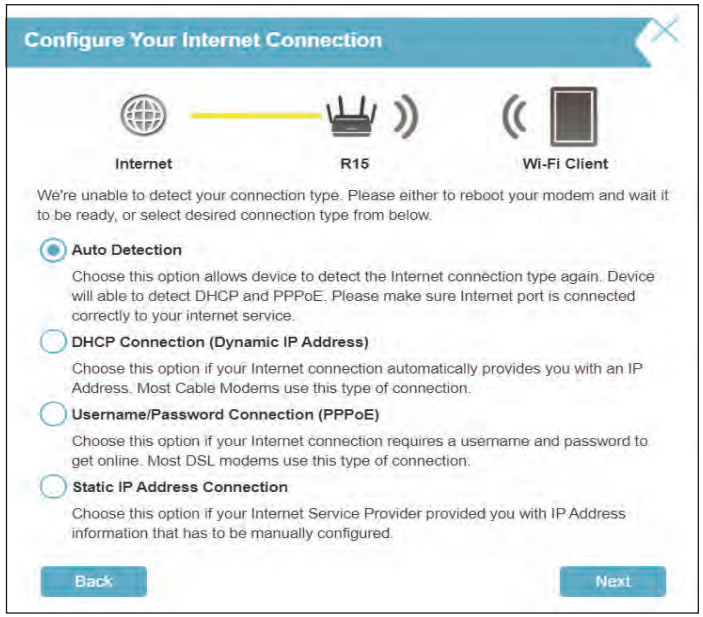


Connect the router and the modem with an Ethernet cable.



If the router does not detect a valid Internet connection, a list of connection types will be displayed. Select your Internet connection type (this information can be obtained from your Internet Service Provider).

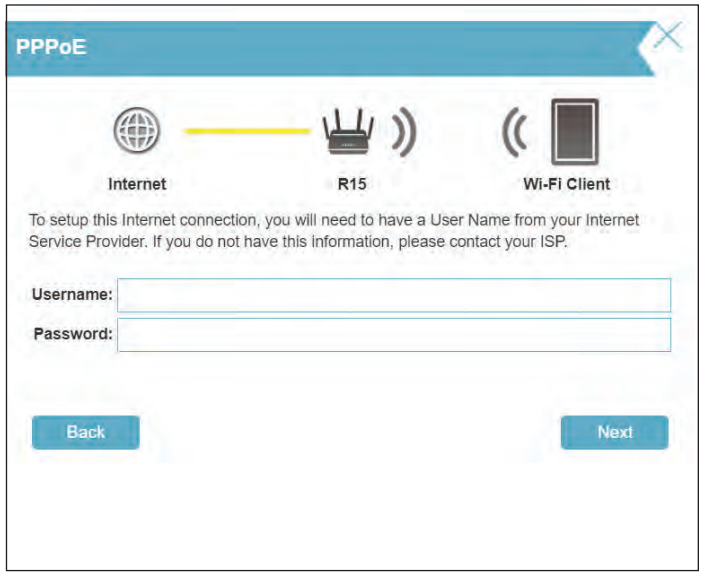
Click **Next** to continue.



If the router detects or you select **PPPoE**, enter your PPPoE username and password. If you do not have this information, please contact your ISP.

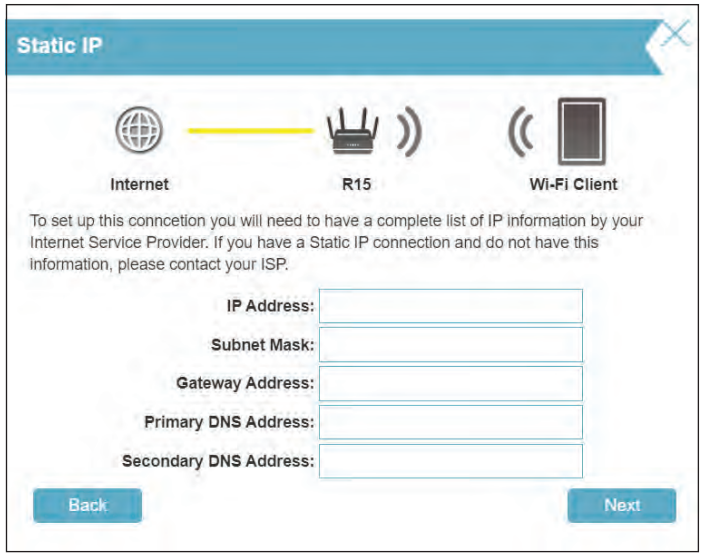
Click **Next** to continue.

Note: *Be sure to remove all other existing PPPoE software from your computer. The software is no longer needed and will not work through a router.*



If the router detects or you select **Static**, enter the IP and DNS settings supplied by your ISP. If you do not have this information, please contact your ISP.

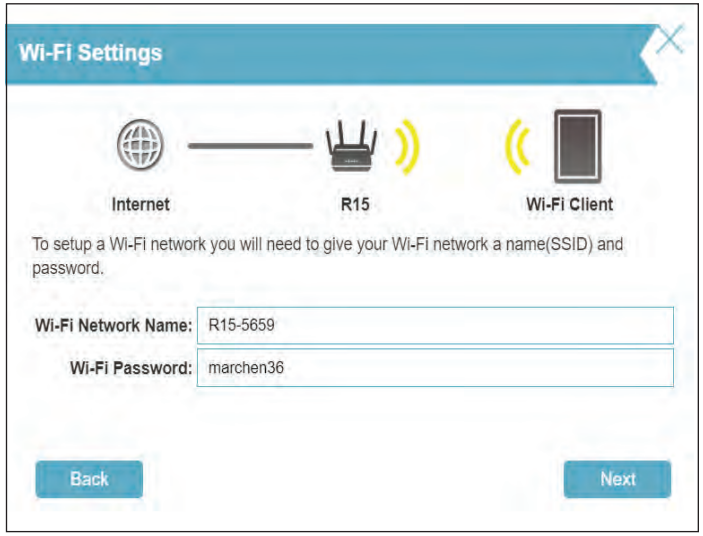
Click **Next** to continue.



Type in a **Wi-Fi Network Name** and **Wi-Fi Password** to set up your Wi-Fi network. Your wireless clients will need this network password to be able to connect to your wireless network.

Click **Next** to continue.

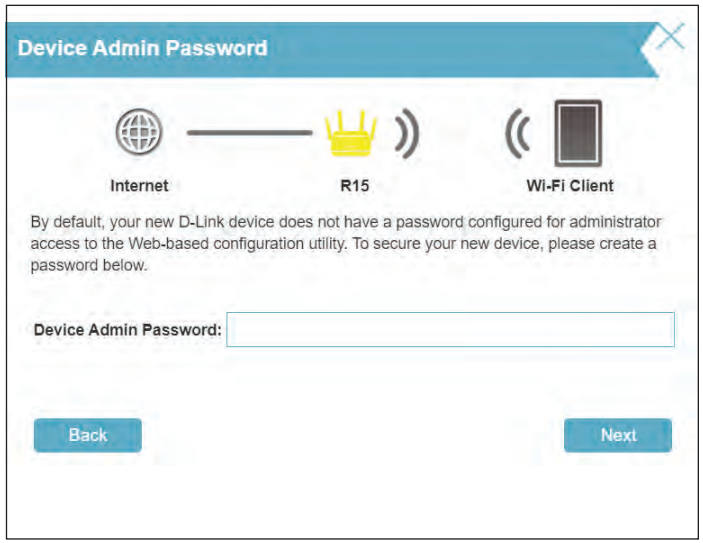
Note: *The router's Smart Connect feature presents a single wireless network. When connecting clients to an extended network, they will be automatically added to the best band, either 2.4 GHz or 5 GHz. To disable the Smart Connect feature and individually configure 2.4 GHz and 5 GHz networks, refer to* ***Wireless*** *on page* ***54.***



In order to better protect the router's configuration page, please enter a password. You will be prompted for this password every time you log in to the router's web configuration utility. Password must be 8-15 characters and contains both numbers and letters.

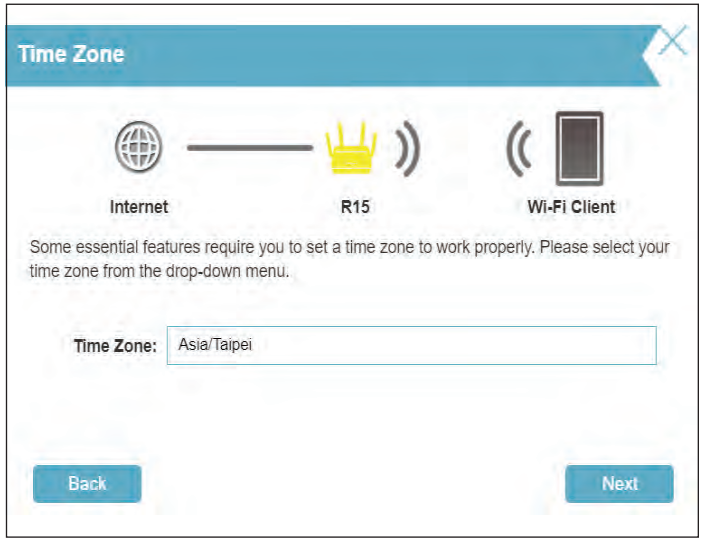
Note: It is strongly recommended that you change the default device password for accessing the router's configuration page.

Click **Next** to continue.



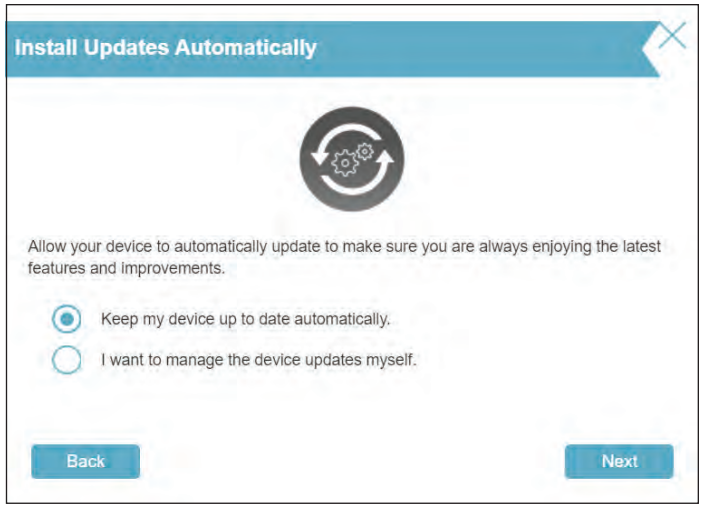
Select your time zone from the drop-down menu.

Click **Next** to continue.



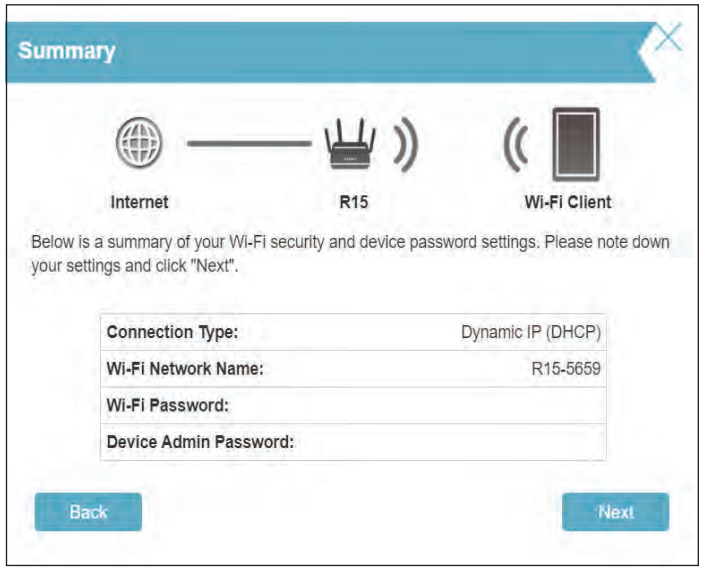
Keeping your router's firmware up-to-date provides you with the latest security upgrades and new features over the air. Choose whether to keep your device up-to-date automatically or to manage the device updates by yourself.

Click **Next** to continue.



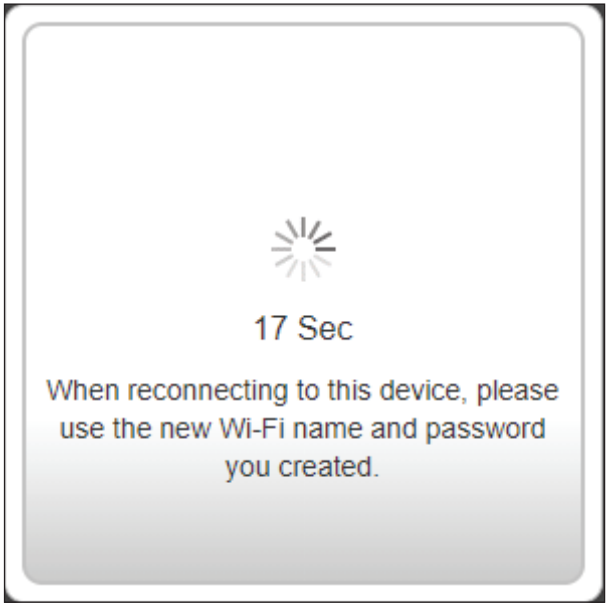
You will be presented with a summary of your settings.

Click **Next** to apply the settings or **Back** to make changes.



Please wait while the device settings are saved.

Do not turn off or unplug your router during this time.

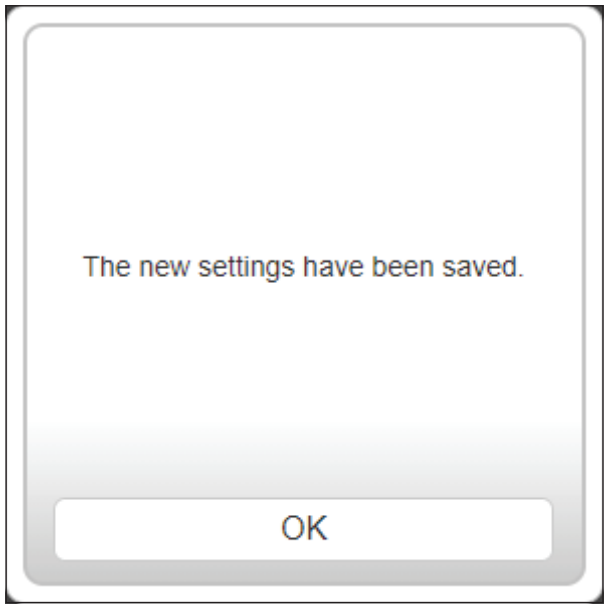


Your new settings have been saved and your router is now configured.

Click **OK** to close the Setup Wizard.

Congratulations, your device has been successfully configured!

You can log in to the web configuration interface with the Admin Password.



Configuration

If this is your first time installing the router, open your web browser and enter the default management address at **http://*XXXX*.devicesetup.net/**. (where XXXX represents the last 4 digits of the MAC address).

Note: *If you cannot remember your password for login, use a paperclip to press the recessed **Reset** button on the back of the device to restore the router to its default settings.*

The router's home page will open displaying its current connection status.

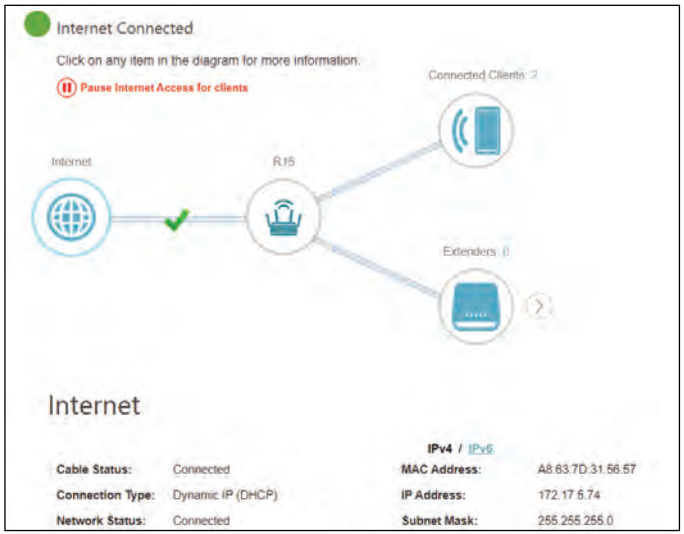
The left pane has quick access to **Settings**, **Features,** and **Management** functions. You can access **AI Assistant** (an AI-assisted message center for reports on Wi-Fi conditions and bandwidth utilization at the top right). Note that you need to turn on AI-assisted functions to receive messages.

Note: *The system will automatically log out after a period (180 seconds) of inactivity.*

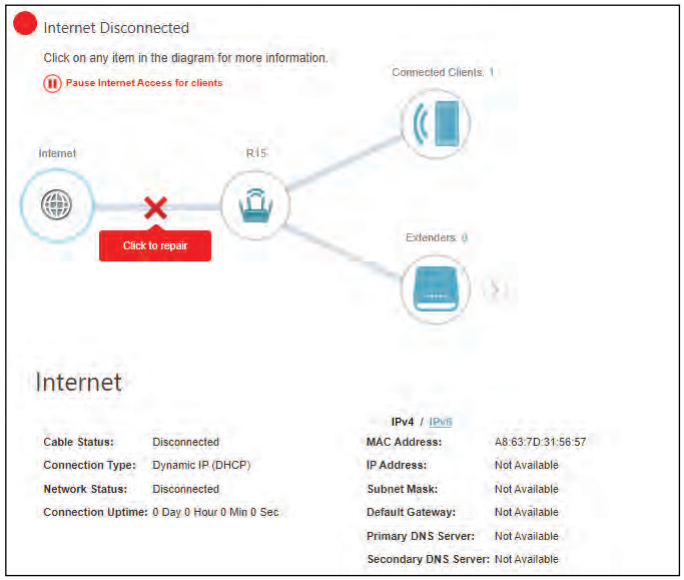
Home

The Home page displays the status of the router in the form of an interactive diagram. You can click each icon to display information about the components of the network at the bottom of the screen. The left pane allows you to quickly navigate to other pages.

The Home page displays whether the router is currently connected to the Internet.



If it is disconnected, click **Click to repair** to bring up the setup wizard, refer to the **Setup Wizard** on page **13** for more information.



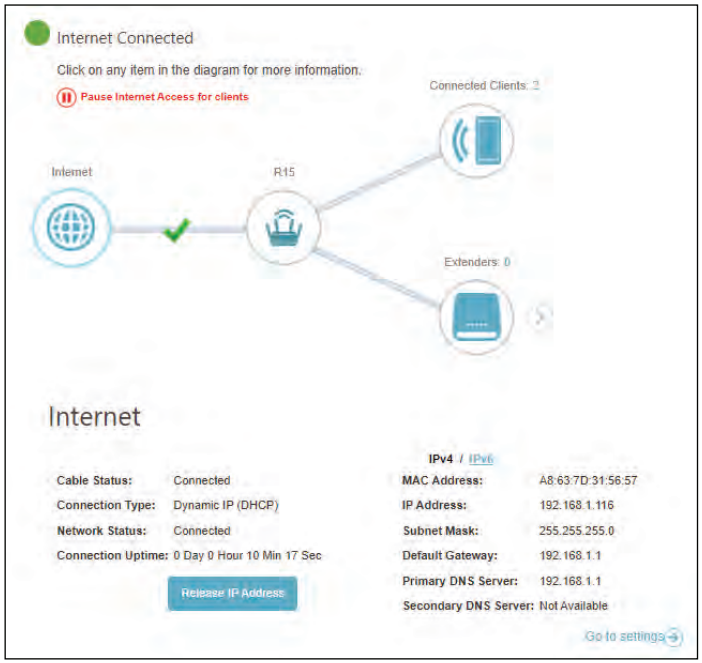
Internet

To bring up more details about your Internet connection, click on the **Internet** icon.

Click **IPv4** or **IPv6** to see details of the IPv4 connection and IPv6 connection respectively.

Click **Release IP Address** to disconnect from the Internet. To reconnect, click **Renew IP Address**.

To reconfigure the Internet settings, refer to **Internet - IPv4** on page **27**.



R32

Click on the **R32** icon to view details about the router and its wireless settings.

Here you can see the router's current Wi-Fi network name and password, as well as the router's MAC address, IPv4 address, and IPv6 address.

To reconfigure network settings, either click **Go to settings** at the bottom of the page, or click **Settings > Network** (in the left pane). Refer to **Network** on page **62** for more information.

To reconfigure wireless settings, either click **Go to settings**, on the lower right, or click **Settings > Wireless** menu (in the left pane). Refer to **Wireless** on page **54** for more information.

Connected Clients

Click on the **Connected Clients** icon to obtain information about the connected clients of the router.

On this page you can see all the clients currently connected to the router along with their IP addresses and device manufacturers.

To view more information about a client or edit a client's settings such as IP reservation and parental control, click on the client you want to edit.

Edit Rule

Name Enter a custom name for this client.

Vendor Displays the vendor of the client.

MAC Address Displays the MAC address of the client.

IP Address Displays the current IP address of the client.

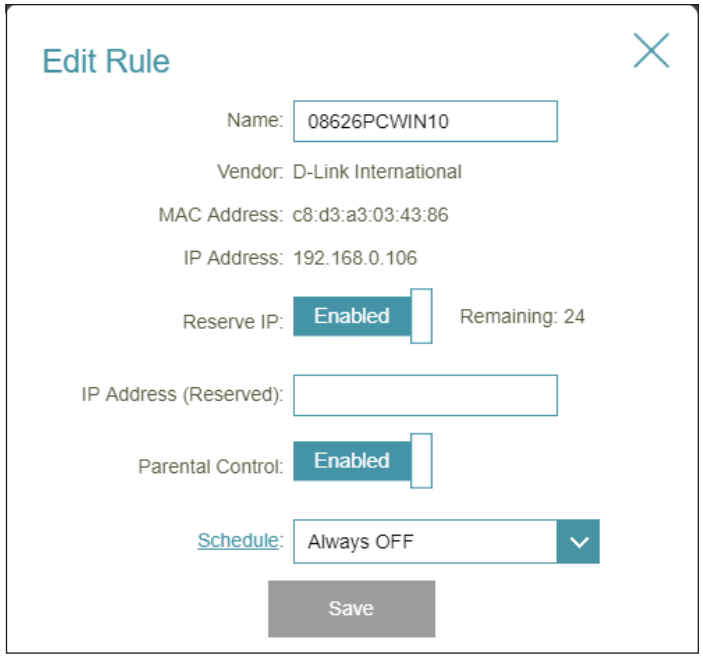
Reserve IP Click **Enable** to reserve an IP address for the client.

IP Address (Reserved) Specify an IP address for the router's DHCP server to assign.

Parental Control Enable Parental Control and select a profile to control the client's Internet access. Make sure that this device is also on the device list of the selected profile.

Profile Use the drop-down menu to select a profile to be used for Parental Control. The profile can be set to **Always Block** to have this client blocked from accessing the Internet, or you can create your own profiles to specify the times that the client can access the network. You can also block access to unwanted websites. Refer to **Features > Parental Control** on page **66** for more information.

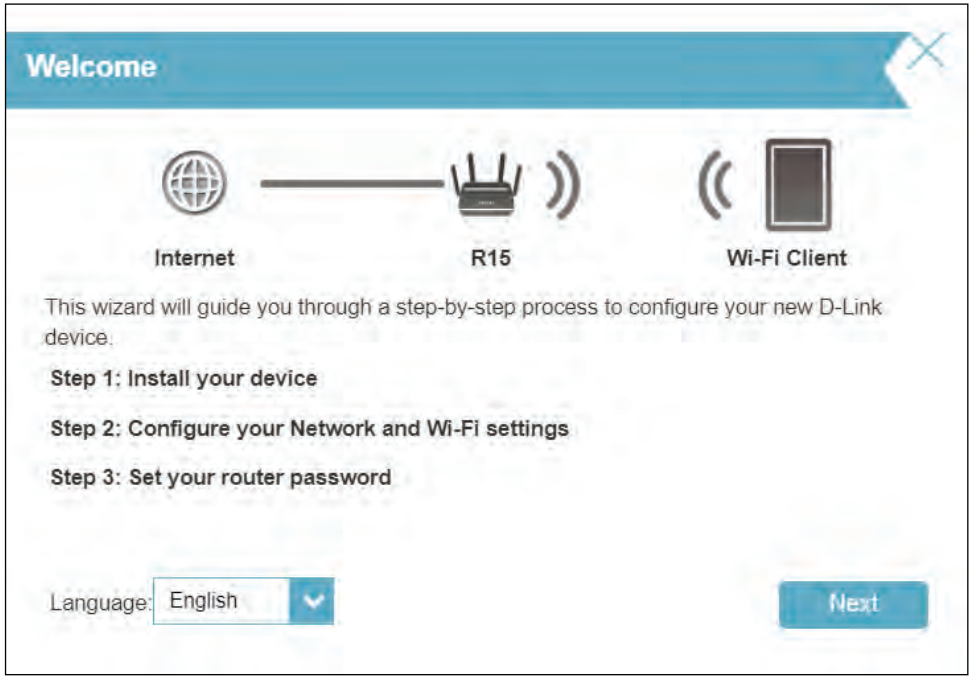
Click **Save** when you are done.



Settings
Wizard

Go to **Settings > Wizard** to open the setup wizard. This is the same wizard that appears when you start the router for the first time. Refer to **Setup Wizard** on page **13** for details.

Note: *When the Wizard is opened, the router will disconnect from the Internet.*

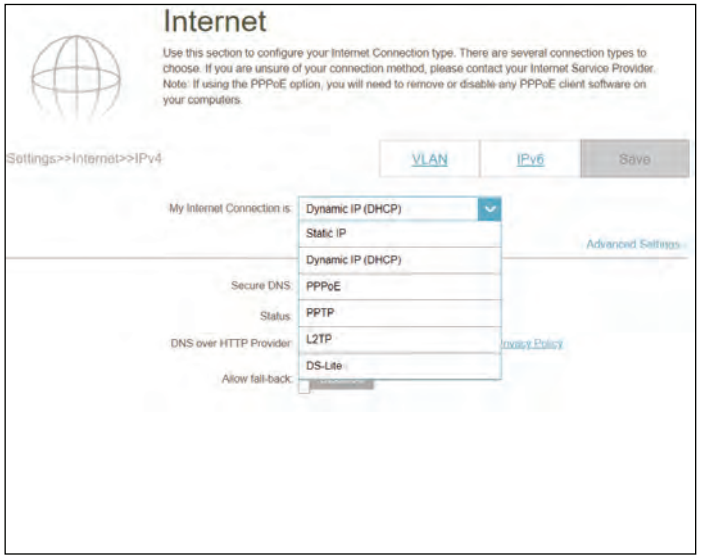


Internet - IPv4

Go to **Settings > Internet** to see the Internet configuration options for IPv4 connection.

To configure IPv6 Internet and network connection details, click the **IPv6** tab. Refer to **Internet - IPv6** on page **37**.
To configure VLAN connection details, click the **VLAN** link. Refer to **Internet - VLAN** on page **52**.

Click **Save** at any time to save the changes you have made on this page.



My Internet Connection is Choose your Internet connection type from the drop-down menu. You will be presented with more options for your connection type.

For **IPv4 - Dynamic IP (DHCP)** refer to page **28**

For **IPv4 - Static IP** refer to page **29**

For **IPv4 - PPPoE** refer to page **30**

For **IPv4 - PPTP** refer to page **32**

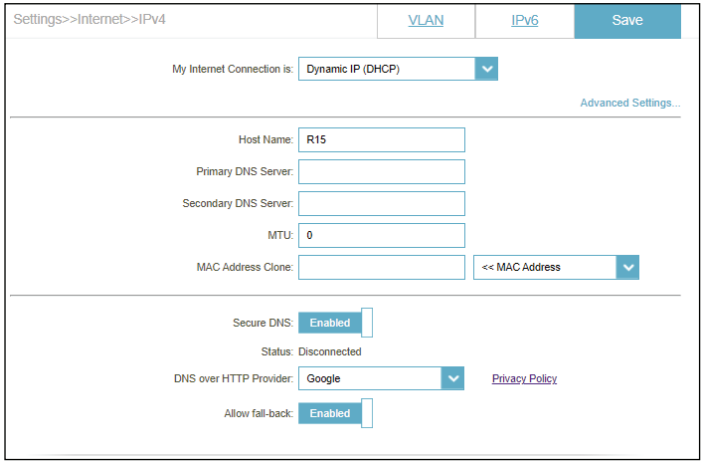
For **IPv4 - L2TP** refer to page **34**

For **IPv4 - DS-Lite** refer to page **36**

IPv4 - Dynamic IP (DHCP)

Select **Dynamic IP (DHCP)** to obtain IP address information automatically from your Internet Service Provider (ISP). Select this option if your ISP does not specify an IP address to use. Click **Save** at any time to save the changes you have made on this page.

Advanced Settings...	
Host Name	The host name is optional but may be required by some ISPs. Leave it blank if you are not sure.
Primary DNS Server	Enter the primary DNS server IP address assigned by your ISP. This address is usually filled in automatically.
Secondary DNS Server	Enter the secondary DNS server IP address assigned by your ISP. This address is usually filled in automatically.
MTU	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP. The default is 1500.
MAC Address Clone	The default MAC address is set to the Internet port's physical interface MAC address on the router. You can replace the Internet port's MAC address with the MAC address of a connected client.
Secure DNS	Enable this option to use public DNS with encryption via DNS-over-HTTPS (DoH).
DNS over HTTP Provider	Select the public DNS service provider: Google or Cloudflare.
Allow Fall-back	Use your primary or secondary DNS server as an alternative if the configured provider is not working.



IPv4 - Static IP

Select **Static IP** if your IP information is provided by your Internet Service Provider (ISP). Click **Save** at any time to save the changes you have made on this page.

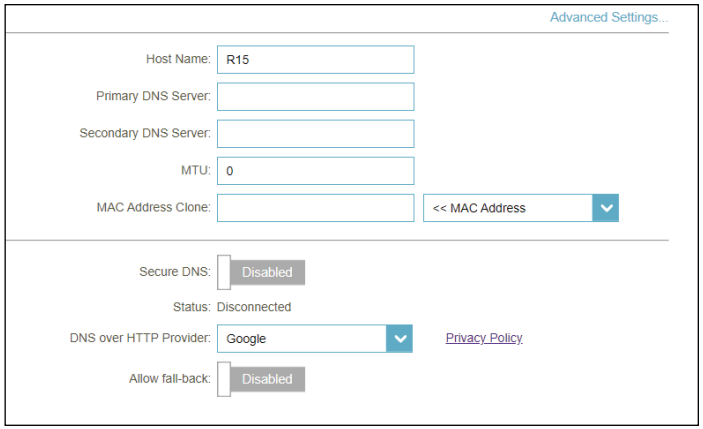
IP Address Enter the IP address provided by your ISP.

Subnet Mask Enter the subnet mask provided by your ISP.

Default Gateway Enter the default gateway address provided by your ISP.

Primary DNS Server Enter the primary DNS server IP address provided by your ISP.

Advanced Settings...



Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

MTU Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP.

MAC Address Clone The default MAC address is set to the Internet port's physical interface MAC address on the router. You can replace the Internet port's MAC address with the MAC address of a connected client.

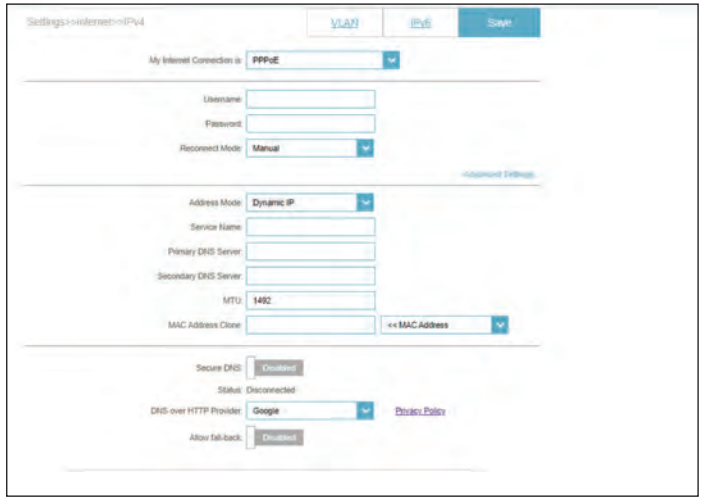
Secure DNS Enable this option to use public DNS with encryption via DNS-over-HTTPS (DoH).

DNS over HTTP Provider Select the DNS-over-HTTPS (DoH) service provider: Google or Cloudflare.

Allow Fall-back Use your primary or secondary DNS server as an alternative if the configured provider is not working.

IPv4 - PPPoE

Select **PPPoE** (Point-to-Point Protocol over Ethernet) if your ISP requires you to enter a PPPoE username and password in order to connect to the Internet. Click **Save** at any time to save the changes you have made on this page.



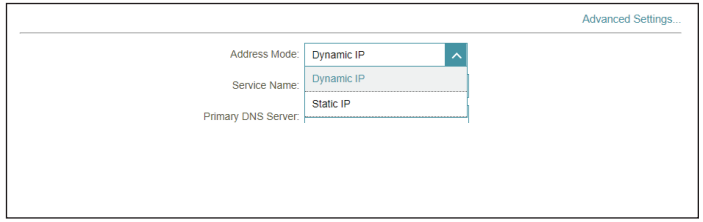
Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

Reconnect Mode Select either **Always on**, **On Demand**, or **Manual**.

Maximum Idle Time Configurable when **On Demand** is selected. Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, select **Always on** or **Manual** as the reconnect mode. The default is 5 minutes.

Advanced Settings...



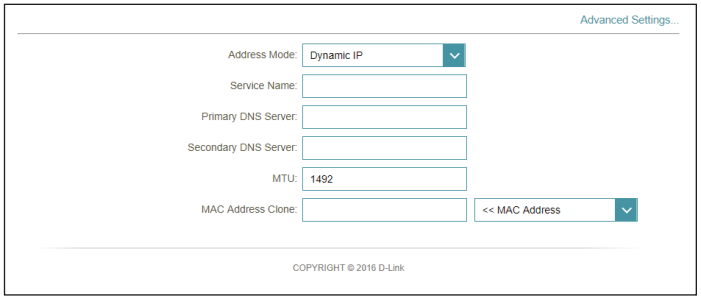
Address Mode Select **Static IP** if the following information has been provided by your ISP: IP address, MTU, and DNS server addresses. In most cases, select **Dynamic IP**.

Advanced Settings... - Dynamic IP

Address Mode Shows your chosen address mode.

Service Name Enter the ISP service name (optional)

Primary DNS Server Enter the primary DNS server IP address assigned by your ISP.

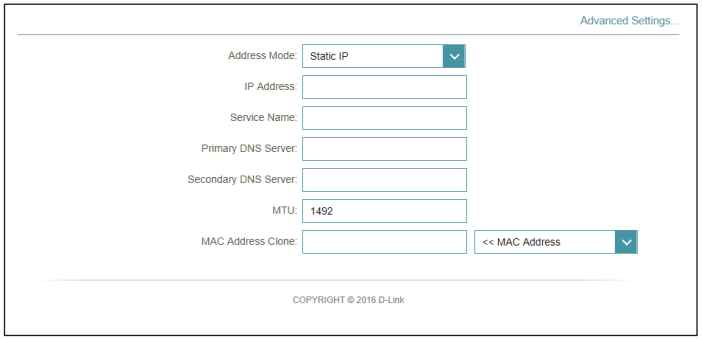


Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

MTU Maximum Transmission Unit (1280~1500)- you may need to change the MTU for optimal performance with your ISP. The default is 1500.

MAC Address Clone The default MAC address is set to the Internet port's physical interface MAC address on the router. You can replace the Internet port's MAC address with the MAC address of a connected client.

Advanced Settings... - Static IP



Address Mode Displays your chosen address mode.

IP Address Enter the IP address provided by your ISP.

Service Name Enter the ISP service name (optional)

Primary DNS Server Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

MTU Maximum Transmission Unit (1280~1492)- you may need to change the MTU for optimal performance with your ISP. The default is 1492.

MAC Address Clone The default MAC address is set to the Internet port's physical interface MAC address on the router. You can replace the Internet port's MAC address with the MAC address of a connected client.

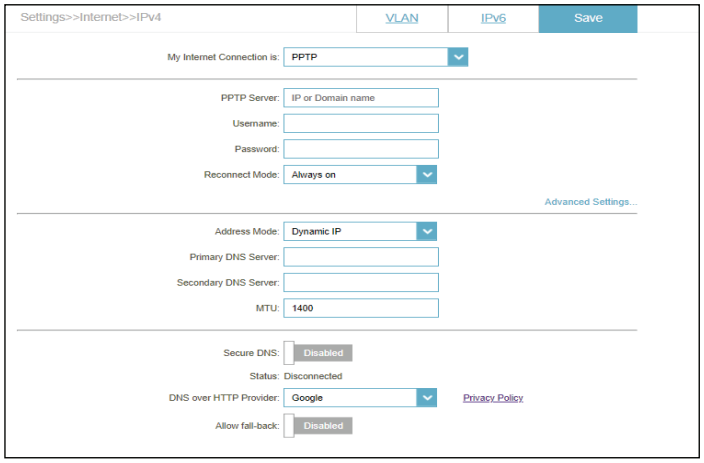
Secure DNS Enable this option to use public DNS with encryption via DNS-over-HTTPS (DoH).

DNS over HTTP Provider Select the DNS-over-HTTPS (DoH) service provider: Google or Cloudflare.

Allow Fall-back Use your primary or secondary DNS server as an alternative if the configured provider is not working.

IPv4 - PPTP

Choose **PPTP** (Point-to-Point-Tunneling Protocol) if your Internet Service Provider (ISP) uses a PPTP connection. Your ISP will provide you with a username and password. Click **Save** at any time to save the changes you have made on this page.



PPTP Server Enter the PPTP server's IP address or name provided by your ISP.

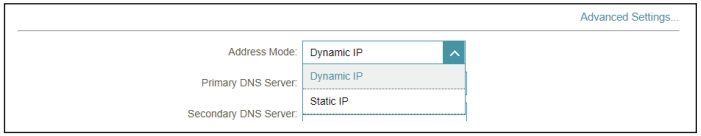
Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

Reconnect Mode Select **Always on**, **On Demand**, or **Manual**.

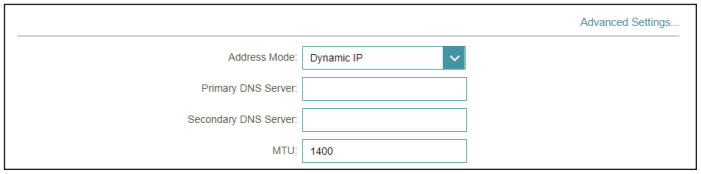
Maximum Idle Time Configurable when **On Demand** is selected. Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, select **Always on** as the reconnect mode.

Advanced Settings...



Address Mode Select **Static IP** if the following information is given by your ISP: IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

Advanced Settings... - Dynamic IP



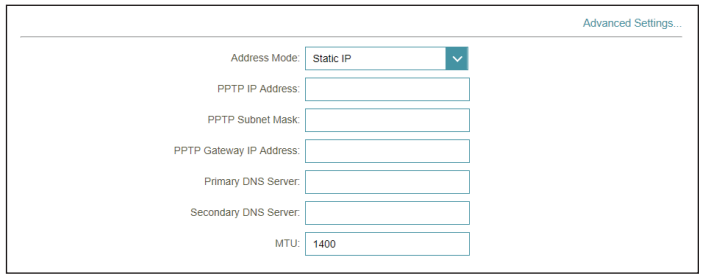
Address Mode Shows your chosen address mode.

Primary DNS Server Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

MTU Maximum Transmission Unit (1280~1460) - you may need to change the MTU for optimal performance with your ISP. The default is 1400.

Advanced Settings... - Static IP



Address Mode Displays your chosen address mode.

PPTP IP Address Enter the IP address provided by your ISP.

PPTP Subnet Mask Enter the subnet mask provided by your ISP.

PPTP Gateway IP Address Enter the gateway IP address provided by your ISP.

Primary DNS Server Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

MTU Maximum Transmission Unit (1280~1460) - you may need to change the MTU for optimal performance with your ISP. The default is 1400.

Secure DNS Enable this option to use public DNS with encryption via DNS-over-HTTPS (DoH).

DNS over HTTP Provider Select the DNS-over-HTTPS (DoH) service provider: Google or Cloudflare.

Allow Fall-back Use your primary or secondary DNS server as an alternative if the configured provider is not working.

IPv4 - L2TP

Choose **L2TP** (Layer 2 Tunneling Protocol) if your Internet Service Provider (ISP) uses an L2TP connection. Your ISP will provide you with a username and password. Click **Save** at any time to save the changes you have made on this page.

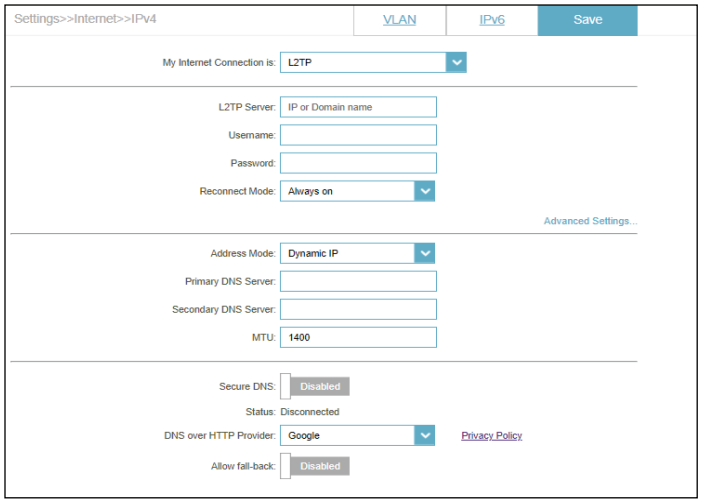
L2TP Server Enter the L2TP server IP address provided by your ISP.

Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

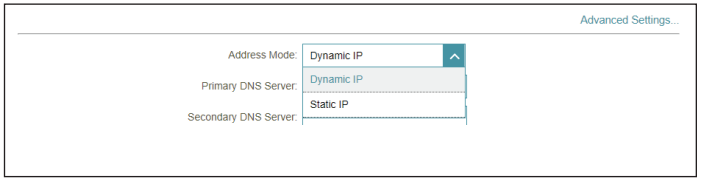
Reconnect Mode Select **Always on**, **On Demand**, or **Manual**.

Maximum Idle Time Configurable when **On Demand** is selected. Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, select **Always on** or **Manual** as the reconnect mode. The default is 5 minutes.



Advanced Settings...

Address Mode Select **Static IP** if the following information is given by your ISP: IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

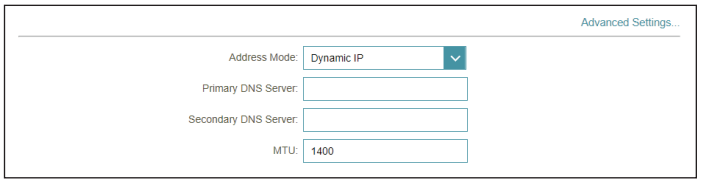


Advanced Settings... - Dynamic IP

Address Mode Shows your chosen address mode.

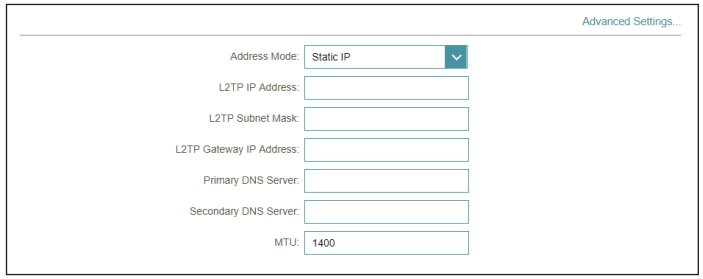
Primary DNS Server Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.



MTU Maximum Transmission Unit (1280~1460) - you may need to change the MTU for optimal performance with your ISP. The default is 1400

Advanced Settings... - Static IP



Address Mode Shows your chosen address mode.

L2TP IP Address Enter the IP address provided by your ISP.

L2TP Subnet Mask Enter the subnet mask provided by your ISP.

L2TP Gateway IP Address Enter the gateway IP address provided by your ISP.

Primary DNS Server Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

MTU Maximum Transmission Unit (1280~1460) - you may need to change the MTU for optimal performance with your ISP. The default is 1400.

Secure DNS Enable this option to use public DNS with encryption via DNS-over-HTTPS (DoH).

DNS over HTTP Provider Select the DNS-over-HTTPS (DoH) service provider: Google or Cloudflare.

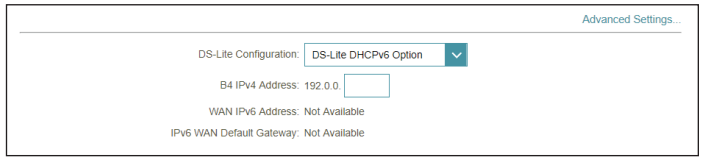
Allow Fall-back Use your primary or secondary DNS server as an alternative if the configured provider is not working.

IPv4 - DS-Lite

DS-Lite allows local IPv4 packets to travel through an IPv6 network. After selecting DS-Lite, the following parameters will be available for configuration. Click **Save** at any time to save the changes you have made on this page.

Advanced Settings...

DS-Lite Configuration — Select **DS-Lite DHCPv6 Option** to let the router allocate the AFTR IPv6 (Address Family Transition Router) address automatically. Select **Manual Configuration** to enter the AFTR IPv6 address manually.

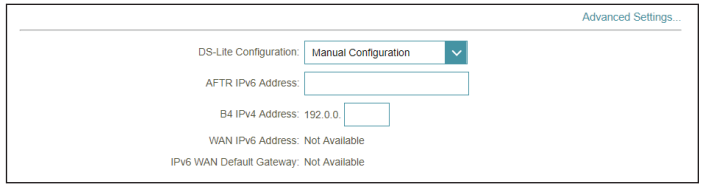


Advanced Settings... - DS-Lite DHCPv6 Option

B4 IPv4 Address — Enter the B4 (Basic Bridging Broadband) IPv4 address that will be encapsulated into IPv6 packets to transmit over an IPv6 network.

WAN IPv6 Address — Once connected, the WAN IPv6 address will be displayed here.

IPv6 WAN Default Gateway — Once connected, the IPv6 WAN default gateway address will be displayed here.



Advanced Settings... - Manual Configuration Option

AFTR IPv6 Address — Enter the Address Family Transition Router (AFTR) IPv6 address. This is where an IPv6 packet will be decapsulated.

B4 IPv4 Address — Enter the B4 IPv4 address.

WAN IPv6 Address — Once connected, the WAN IPv6 address will be displayed here.

IPv6 WAN Default Gateway — Once connected, the IPv6 WAN default gateway address will be displayed here.

Secure DNS — Enable this option to use public DNS with encryption via DNS-over-HTTPS (DoH).

DNS over HTTP Provider — Select the DNS-over-HTTPS (DoH) service provider: Google or Cloudflare.

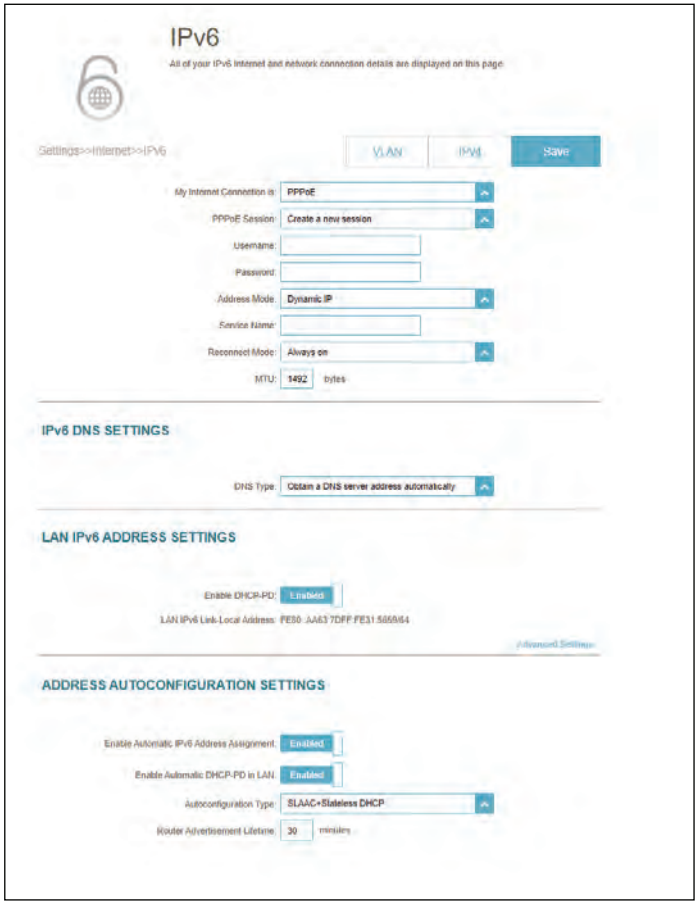
Allow Fall-back — Use your primary or secondary DNS server as an alternative if the configured provider is not working.

Internet - IPv6

Go to **Settings > Internet** to see the Internet configuration options for IPv4 , then click the **IPv6** tab to access the configuration options for IPv6.

To configure the IPv4 Internet and network connection details, click the **IPv4** tab. Refer to **Internet - IPv4** on page **27**
To configure the VLAN connection details, click the **VLAN** tab. Refer to **Internet - VLAN** on page **52**

Click **Save** at any time to save the changes you have made on this page.



My Internet Connection is Choose your Internet connection type from the drop-down menu. You will be presented with the appropriate options for your connection type.

For **IPv6 - Auto Detection** refer to page **38**

For **IPv6 - Static IPv6** refer to page **40**

For **IPv6 - Auto Configuration (SLAAC/DHCPv6)** refer to page **42**

For **IPv6 - PPPoE** refer to page **45**

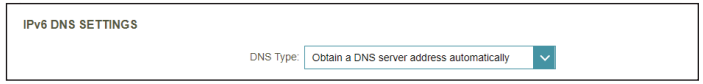
For **IPv6 - 6rd** refer to page **49**

For **IPv6 - Local Connectivity Only** refer to page **51**

IPv6 - Auto Detection

Select **Auto Detection** to automatically detect the IPv6 connection method used by your Internet Service Provider (ISP). If Auto Detection fails, you can manually select another IPv6 connection type. Click **Save** at any time to save the changes you have made on this page.

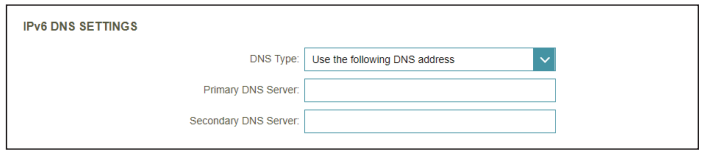
IPv6 DNS Settings



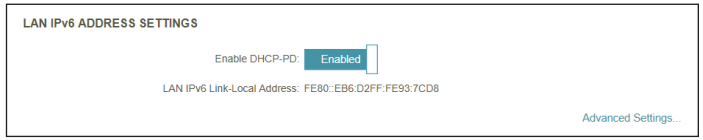
DNS Type Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

Primary DNS Server If you select **Use the following DNS address**, enter the primary DNS server address.

Secondary DNS Server Enter the secondary DNS server address as a backup.



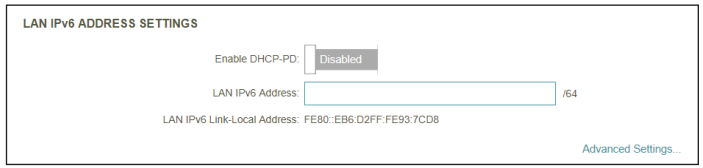
LAN IPv6 Address Settings



Enable DHCP-PD Enable or disable DHCP prefix delegation.

LAN IPv6 Link-Local Address Displays the router's LAN link-local address, which is used only within the local network.

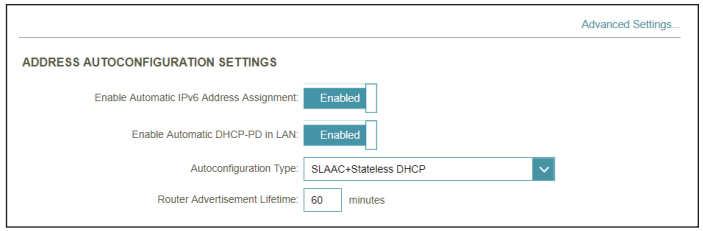
*If **Enable DHCP-PD** is disabled, enter the following:*



LAN IPv6 Address Enter a valid LAN IPv6 address.

LAN IPv6 Link-Local Address Displays the router's LAN link-local address.

Advanced Settings... - Address Autoconfiguration Settings

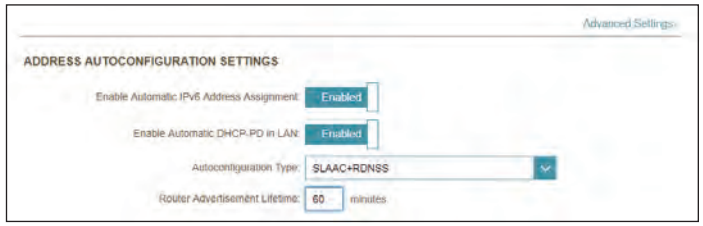


Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

Enable Automatic DHCP-PD in LAN Enable or disable DHCP-PD for other IPv6 routers connected to the LAN interface.

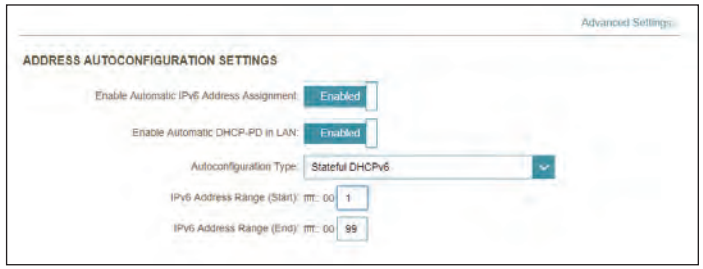
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes). The default is 30 minutes.

*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*



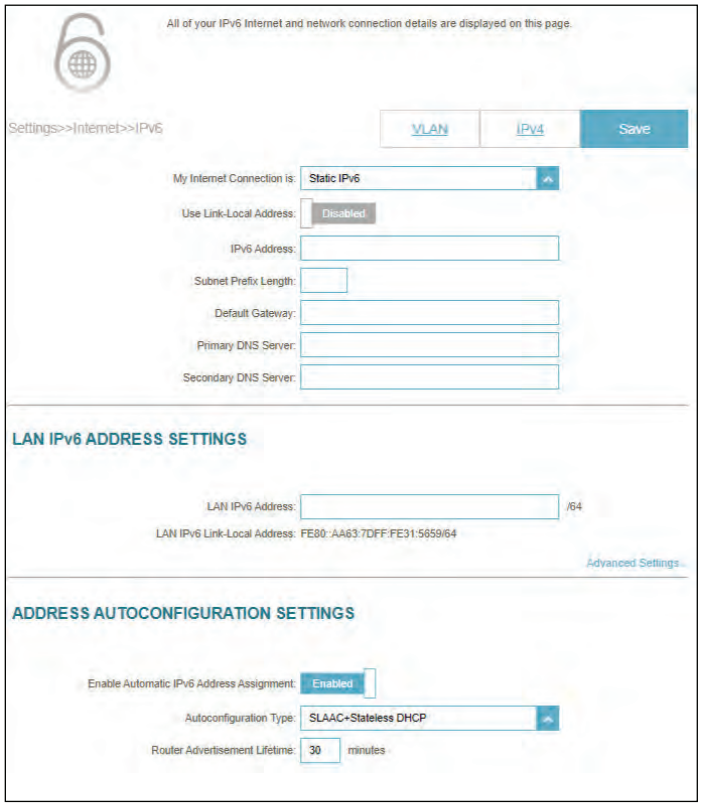
IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Lifetime Enter the dynamic IP's retention time. The default is 10080 minutes.

IPv6 - Static IPv6

Select **Static IP** if your IPv6 information is provided by your Internet Service Provider (ISP). Click **Save** at any time to save the changes you have made on this page.



Use Link-Local Address Enable or disable link-local address.

IPv6 Address Configurable when **Use Link-Local Address** is disabled. Enter the address supplied by your ISP.

Subnet Prefix Length Configurable when **Use Link-Local Address** is disabled. Enter the subnet prefix length (1~128) supplied by your ISP.

Default Gateway Enter the default gateway for your IPv6 connection.

Primary DNS Server Enter the primary DNS server address.

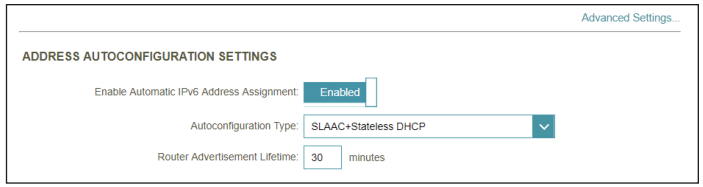
Secondary DNS Server Enter the secondary DNS server address.

LAN IPv6 Address Settings

LAN IPv6 Address Enter the LAN (local) IPv6 address for the router.

LAN IPv6 Link-Local Address Displays the router's LAN link-local address.

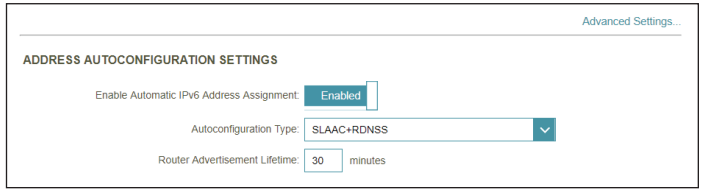
Advanced Settings... - Address Autoconfiguration Settings



Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

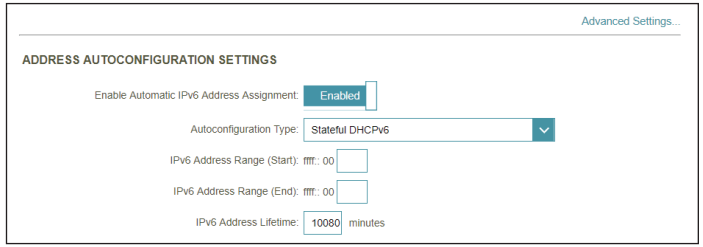
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes). The default is 30 minutes.

*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*



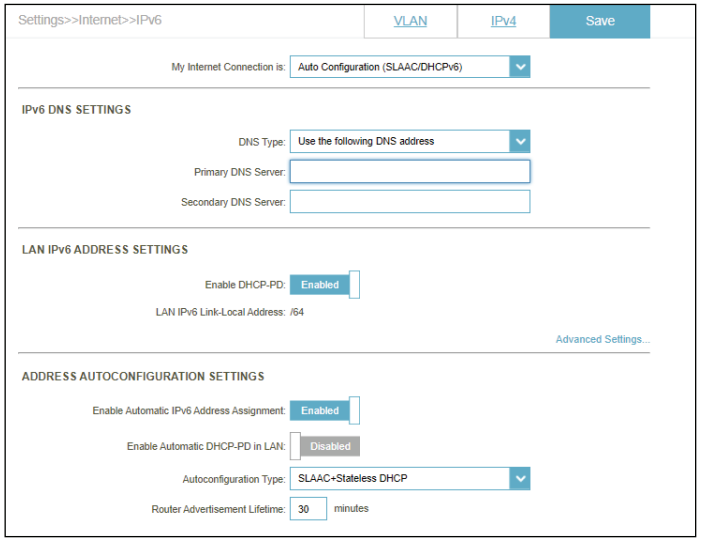
IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Lifetime Enter the dynamic IP's retention time. The default is 10080 minutes.

IPv6 - Auto Configuration (SLAAC/DHCPv6)

Select **Auto Configuration** if your ISP assigns an IPv6 address when your router requests one from the ISP's server. Some ISPs require you to configure relevant settings in advance before your router can connect to the IPv6 Internet. Click **Save** at any time to save the changes you have made on this page.



IPv6 DNS Settings

DNS Type Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

Primary DNS Server If you select **Use the following DNS address**, enter the primary DNS server address.

Secondary DNS Server If you select **Use the following DNS address**, enter the secondary DNS server address.

LAN IPv6 Address Settings

Enable DHCP-PD Enable or disable prefix delegation.

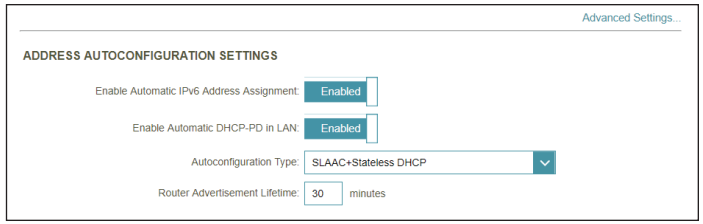
LAN IPv6 Link-Local Address Displays the router's LAN link-local address.

*If **Enable DHCP-PD** is disabled, configure the following:*

LAN IPv6 Address Enter a valid LAN IPv6 address.

LAN IPv6 Link-Local Address Displays the router's LAN link-local address for the local network only.

Advanced Settings... - Address Autoconfiguration Settings



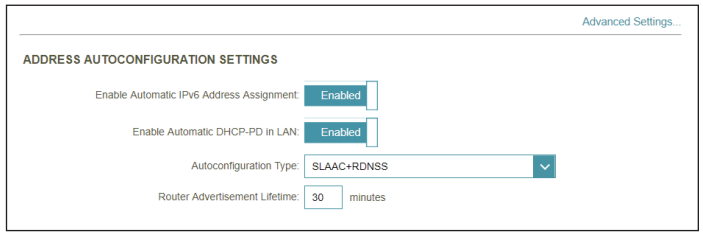
Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

*If **Enable DHCP-PD** is enabled in the previous LAN IPv6 Address Settings:*

Enable Automatic DHCP-PD in LAN Enable or disable DHCP-PD for other IPv6 routers connected to the LAN interface.

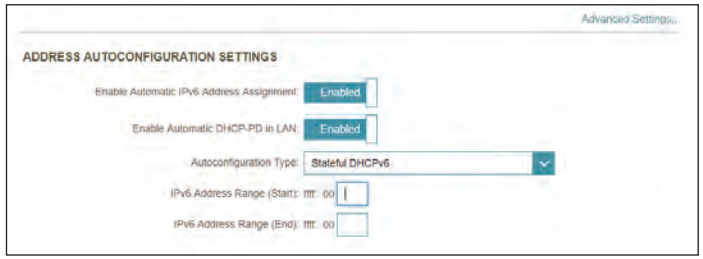
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes). The default is 30 minutes.

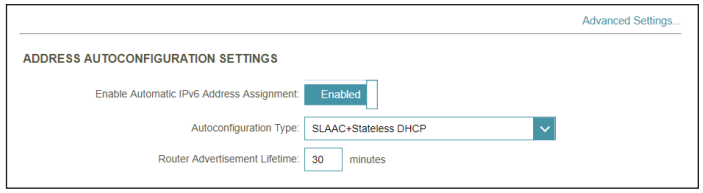
*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*



IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

Advanced Settings... - Address Autoconfiguration Settings

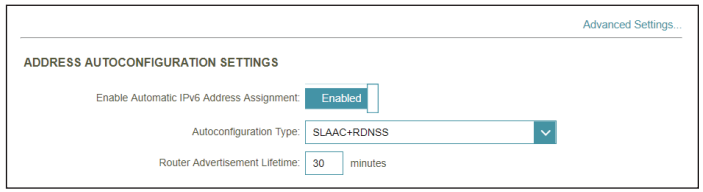


Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

*If **Enable DHCP-PD** is disabled in the previous LAN IPv6 Address Settings:*

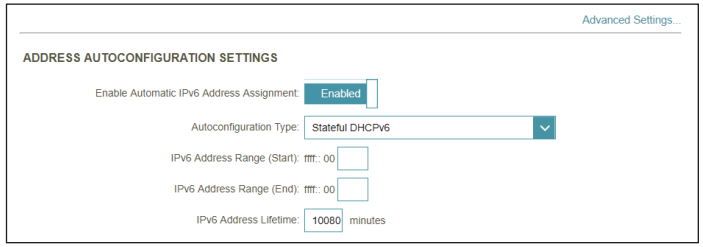
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes). The default is 30 minutes.

*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*



IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Lifetime Enter the IP address retention period in minutes. The default is 10080 minutes.

IPv6 - PPPoE

Select **PPPoE** if your ISP requires you to enter a PPPoE username and password to connect to the Internet. Click **Save** at any time to save the changes you have made on this page.

PPPoE Session Create a new PPPoE session.

Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

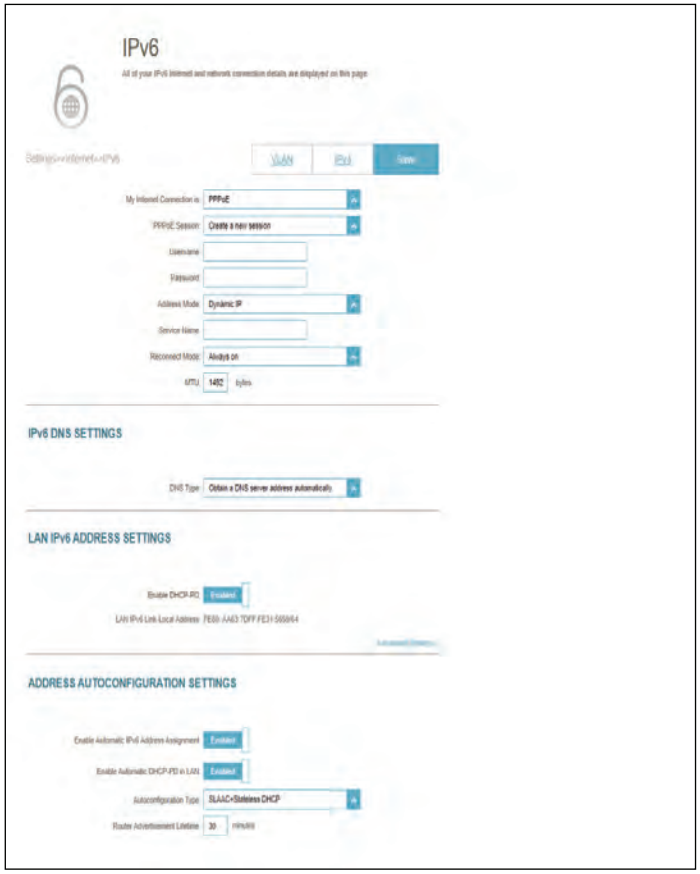
Address Mode Select either **Dynamic IP** or **Static IP**.

IP Address Configurable if Static IP is chosen. Enter the IP address provided by your ISP.

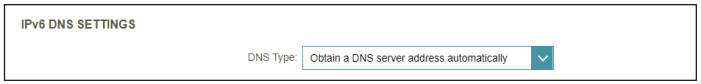
Service Name Enter the ISP service name (optional).

Reconnect Mode Select either **Always On** or **Manual**.

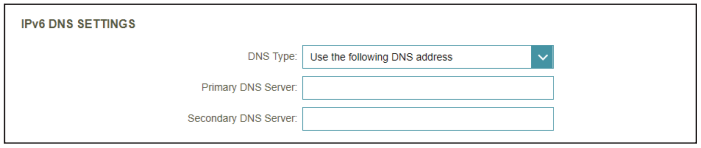
MTU Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP. The default is 1492 bytes.



IPv6 DNS Settings



DNS Type Select either **Obtain DNS server address automatically** or **Use the following DNS address**.



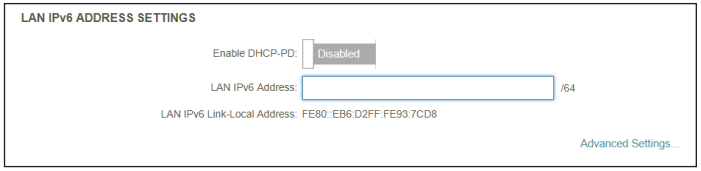
Primary DNS Server If you select **Use the following DNS address**, enter the primary DNS server address.

Secondary DNS Server If you select **Use the following DNS address**, enter the secondary DNS server address as a backup.

LAN IPv6 Address Settings

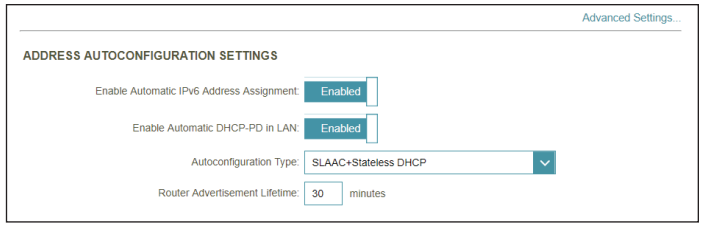
Enable DHCP-PD Enable or disable prefix delegation.

LAN IPv6 Address Configurable if the above DHCP-PD is disabled. Enter the IP address provided by your ISP.



LAN IPv6 Link-Local Address Displays the router's LAN link-local address for the local network only.

Advanced Settings... - Address Autoconfiguration Settings



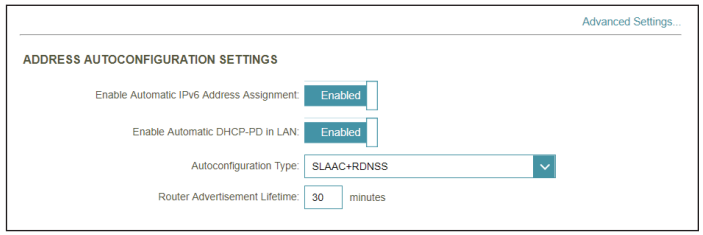
Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment.

*If **Enable DHCP-PD** is enabled in the previous LAN IPv6 Address Settings:*

Enable Automatic DHCP-PD in LAN Enable or disable DHCP-PD for other IPv6 routers connected to the LAN interface.

Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



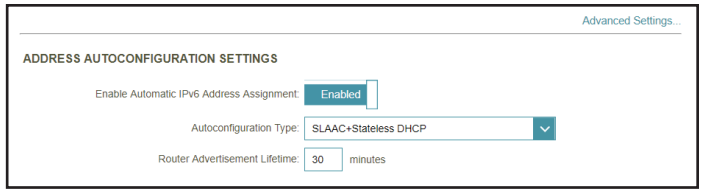
Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes).

*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*

IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

Advanced Settings... - Address Autoconfiguration Settings

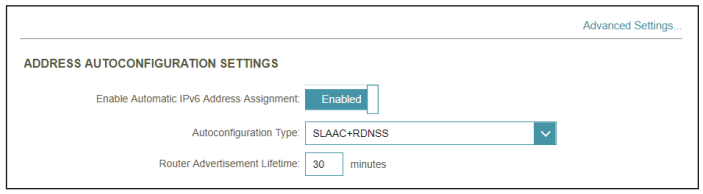


Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

*If **Enable DHCP-PD** is disabled in the previous LAN IPv6 Address Settings:*

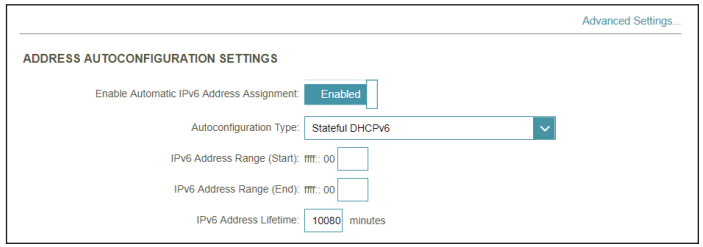
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes). The default is 30 minutes.

*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*



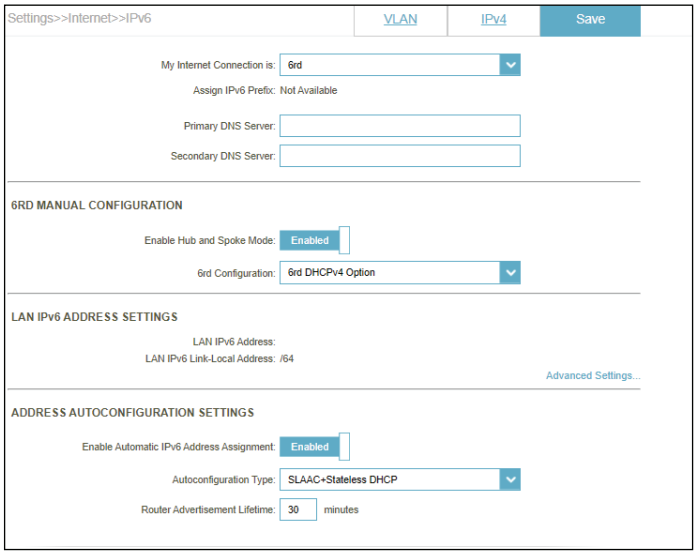
IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Lifetime Enter the IPv6 address lifetime (in minutes). The default is 10080 minutes.

IPv6 - 6rd

IPv6 **6rd** (rapid deployment) allows IPv6 packets to be transmitted over an IPv4 network. Click **Save** at any time to save the changes you have made on this page.



Assign IPv6 Prefix Currently unsupported.

Primary DNS Server Enter the primary DNS server address.

Secondary DNS Server Enter the secondary DNS server address as a backup.

6rd Manual Configuration

Enable Hub and Spoke Mode Enable this option if you want to minimize the number of routes to the destination by using a hub and spoke method of networking.

6rd Configuration Choose the **6rd DHCPv4 Option** to automatically discover and populate the data values, or **Manual Configuration** to enter the settings yourself.

*If you select **Manual Configuration** as the 6rd Configuration:*

6rd IPv6 Prefix Enter the 6rd IPv6 network address and prefix length (1~128) supplied by your ISP.

WAN IPv4 Address Enter the IPv4 network prefix.

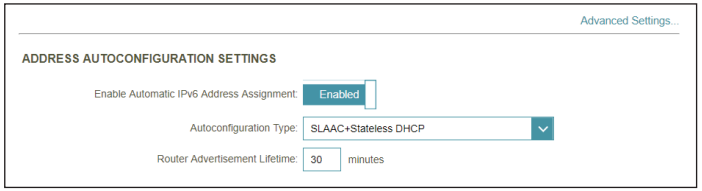
6rd Border Relay IPv4 Address Enter the 6rd border relay IPv4 address settings supplied by your ISP.

LAN IPv6 Address Settings

LAN IPv6 Address Displays the router's LAN IPv6 address.

LAN IPv6 Link-Local Address Displays the router's LAN link-local address.

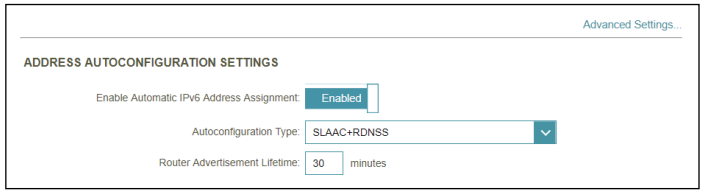
Advanced Settings... - Address Autoconfiguration Settings



Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

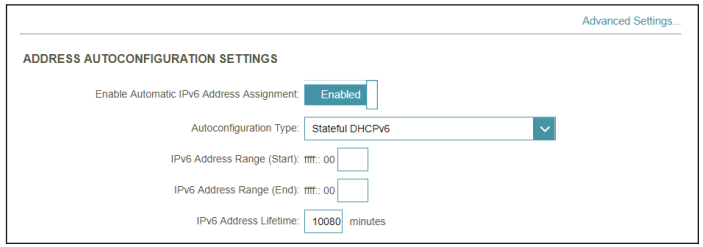
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:*



Router Advertisement Lifetime Enter the router advertisement lifetime (in minutes). The default is 30 minutes.

*If you select **Stateful DHCPv6** as the Autoconfiguration Type:*



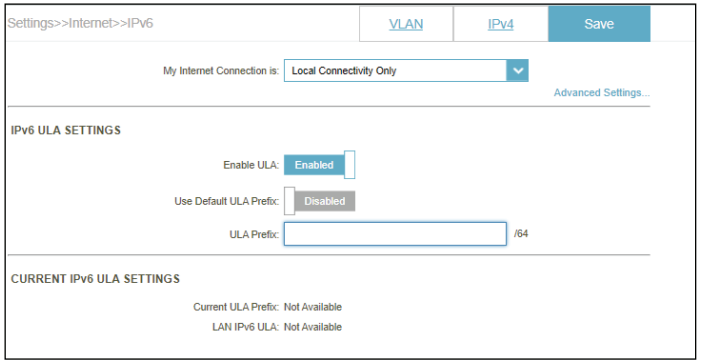
IPv6 Address Range (Start) Enter the start IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the end IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Lifetime Enter the IPv6 address lifetime (in minutes). The default is 10080 minutes.

IPv6 - Local Connectivity Only

Local Connectivity Only allows you to set up an IPv6 connection that will not connect to the Internet. Click **Save** at any time to save the changes you have made on this page.



Advanced Settings... - IPv6 ULA Settings

Enable ULA	Click here to enable Unique Local IPv6 Unicast Addresses settings.
Use Default ULA Prefix	Enable this option to use the default ULA prefix.
ULA Prefix	If you disable Use Default ULA Prefix, enter your own ULA prefix.

Advanced Settings... - Current IPv6 ULA Settings

Current ULA Prefix	Displays the current ULA prefix.
LAN IPv6 ULA	Displays the LAN's IPv6 ULA.

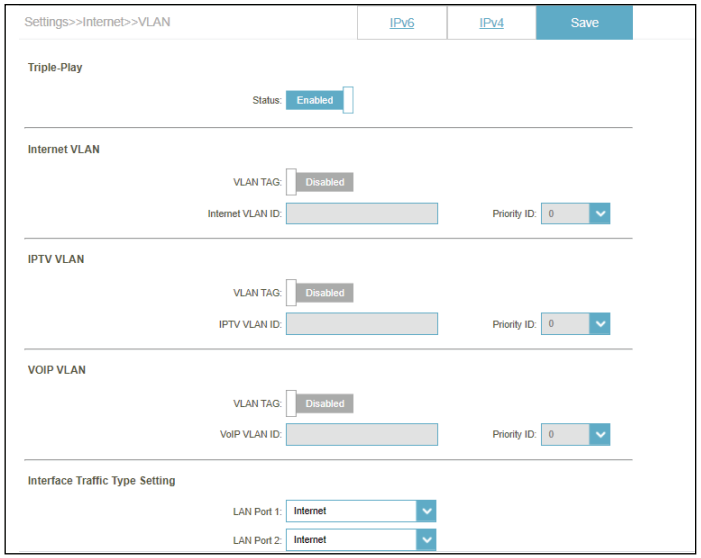
Internet - VLAN

Go to **Settings > Internet**, then click the **VLAN** link to access the configuration options for the VLAN.

VLAN allows Triple-Play services to be differentiated by dividing a network into segments and allowing access to these services by devices only in the assigned segment.

To configure the IPv4 Internet and network connection details, click the **IPv4** link. Refer to **Internet - IPv4** on page **27**
To configure the IPv6 Internet and network connection details, click the **IPv6** link. Refer to **Internet - IPv6** on page **37**

Click **Save** at any time to save the changes you have made on this page.



Status Click to enable or disable the Triple-Play VLAN feature. More configuration options will be available if the Status is enabled.

*If Triple-Play is **Enabled**:*

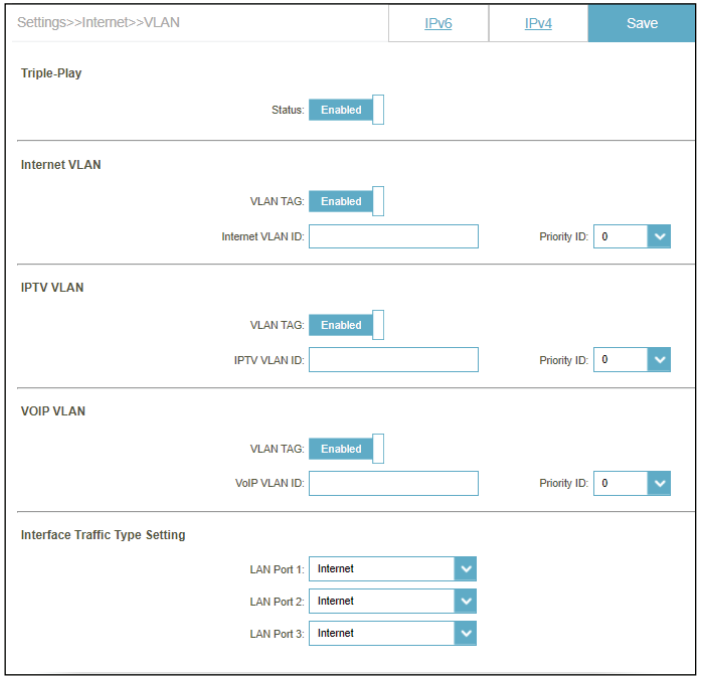
VLAN TAG Enable VLAN TAG to enter VLAN ID, as provided by your ISP

Internet VLAN ID Enter the VLAN ID for your Internet connection, as provided by your ISP.

IPTV VLAN ID Enter the VLAN ID for your IPTV service, as provided by your ISP.

VOIP VLAN ID Enter the VLAN ID for your VoIP network, as provided by your ISP.

Priority ID Enable or disable traffic priority ID for the Internet, IPTV, and VoIP VLANs. Select a priority ID from the drop-down menus to assign to the corresponding VLAN (0-7). Higher priority ID traffic takes precedence over traffic with a low priority ID tag.



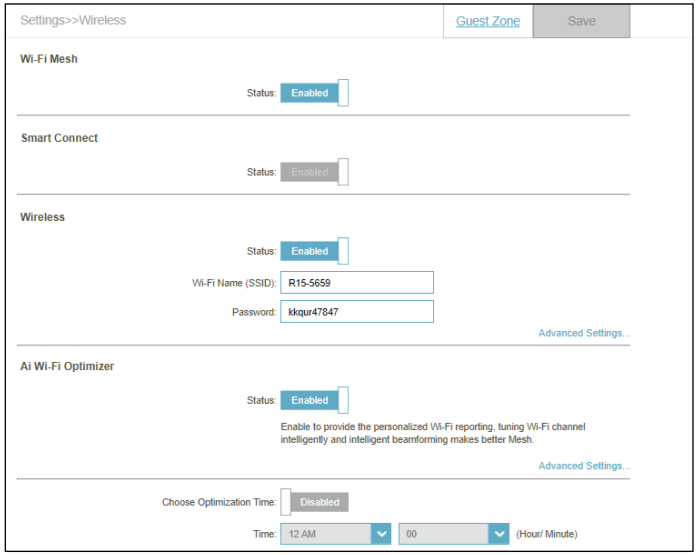
Interface Traffic Type Setting

LAN Port 1-3 Select the type of connection (Internet, IPTV, or Voice over IP) coming from the WAN connection to each interface on the router.

Wireless

Go to **Settings** > **Wireless** to see your wireless network settings for your router.

Click **Save** at any time to save the changes you have made on this page.



Wi-Fi Mesh

Status Enable or disable Wi-Fi mesh if you plan to build a mesh network in your environment. The mesh network is able to find the shortest and fasted path to your gateway/router in a mesh network topology. Hence, it enhances efficiency and reliability.

Smart Connect

Status Enable or disable the Smart Connect Feature. The Smart Connect feature presents a single wireless network. When connecting clients to the extended network, the clients will be automatically added to the best band, either 2.4 GHz or 5 GHz.

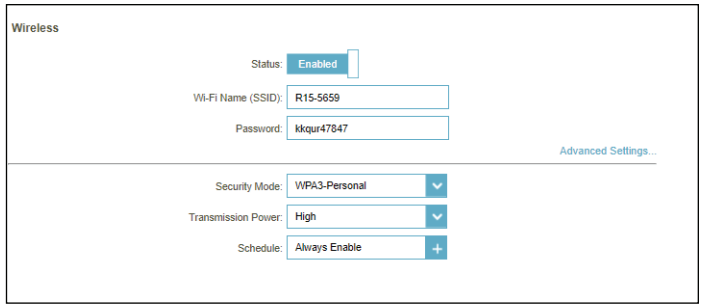
*If Smart Connect is **Enabled**:*

Wireless

Wi-Fi Name (SSID) Create a name for your wireless network. Up to 32 characters are allowed.

Password Create a Wi-Fi password. Wireless clients will need to enter this password to successfully connect to the network.

Wireless - Advanced Settings...



Security Mode Choose **None, WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these. Note that WPS will be disabled if WPA3 is used.

Transmission Power Select the desired wireless transmission power: High, Medium, or Low.

Schedule Select the time during which the wireless network will be available. The schedule may be set to Always Enable or you can add your own schedule.

To add a schedule:
Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule.

Smart Connect

Status Enable or disable the Smart Connect Feature. When disabled, 2.4GHz and 5GHz configuration options become available.

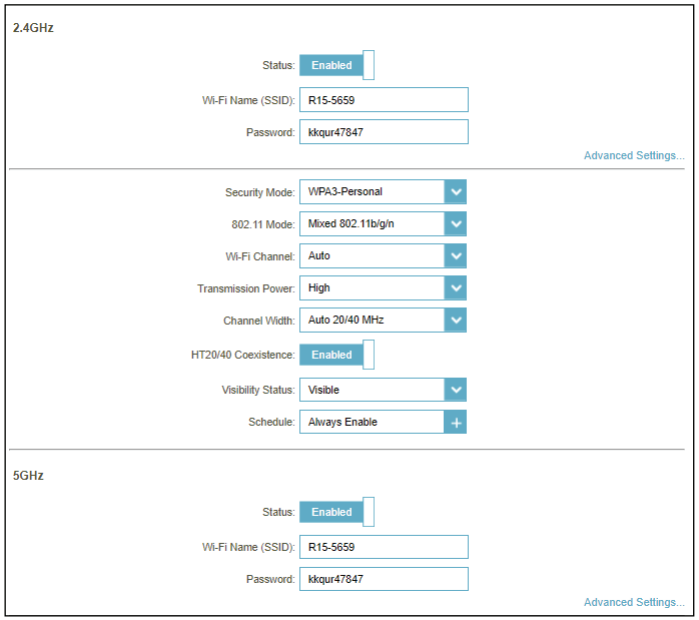
*If Smart Connect is **Disabled**:*

2.4GHz / 5GHz

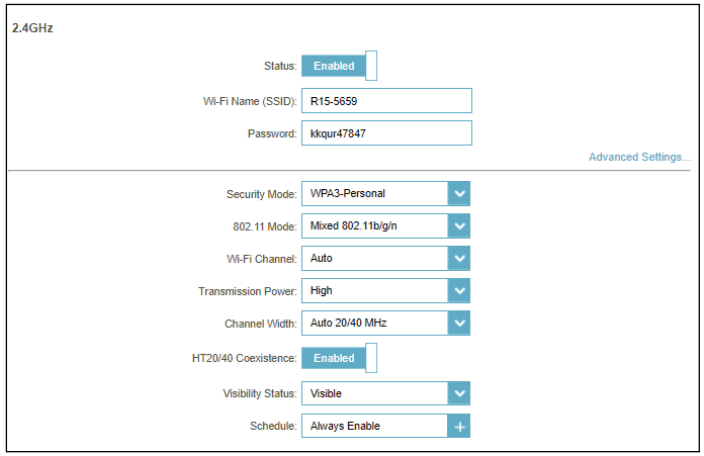
Status Enable or disable the 2.4GHz / 5GHz wireless network.

Wi-Fi Name (SSID) Create a name for your wireless network. Up to 32 characters are allowed.

Password Create a Wi-Fi password. Wireless clients will need to enter this password to connect to the network.



2.4GHz - Advanced Settings...



Security Mode

Choose **None, WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these. Note that WPS will be disabled if WPA3 is used.

802.11 Mode (2.4GHz)

Select the desired wireless networking standards to use in your environment.
The available options for the 2.4 GHz wireless network are **Mixed 802.11b/g/n, Mixed 802.11b/g, Mixed 802.11g/n**, **802.11b only, 802.11g only,** and **802.11n only**.

Wi-Fi Channel

Select the desired channel:1-11. The default is **Auto** (recommended).

Transmission Power

Select the desired wireless transmission power: High, Medium, or Low.

Channel Width (2.4GHz)

Select **Auto 20/40 MHz** if you are using both 802.11n and non-802.11n (802.11b/g) devices, or select **20 MHz** if you are using a mix of 802.11b/g devices.

HT20/40 Coexistence (2.4GHz)

Enable or disable the existence of both 20 MHz and 40 MHz channel width. Keep it enabled to achieve the maximum operability of wireless products using different standards in your environment. However, it might prevent your 802.11n devices from reaching the maximum performance.

Visibility Status

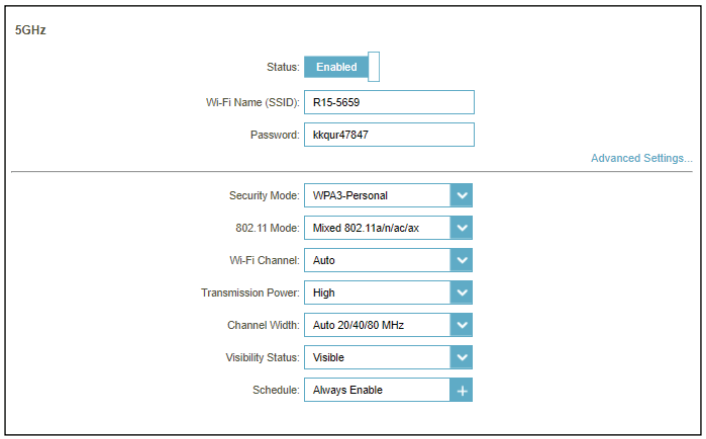
The default setting is **Visible**. Select **Invisible** if you do not want to broadcast the SSID of your wireless network.

Schedule

Select the time during which the wireless network will be available. The schedule may be set to Always Enable or you can add your own schedule.

To add a schedule:
Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule.

5GHz - Advanced Settings...



Security Mode

Choose **None, WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these. Note that WPS will be disabled if WPA3 is used.

802.11 Mode (5GHz)

Select the desired wireless networking standards to use. The available options for the 5 GHz wireless network are **Mixed 802.11a/n/ac/ax, Mixed 802.11a/n/ac, Mixed 802.11a/n, 802.11ac only, 802.11a only,** and **802.11n only**.

Wi-Fi Channel

Select the desired channel: 36, 40, 44, 48, 149, 153, 157, 161, or 165. The default is **Auto** (recommended).

Transmission Power

Select the desired wireless transmission power: High, Medium, or Low.

Channel Width (5GHz)

Select **Auto 20/40/80 MHz** if you are using 802.11ax, 802.11ac, 802.11n, and 802.11a devices, select **Auto 20/40** if you are using 802.11n and 802.11a devices, or select **20 MHz** if you are using 802.11a devices.

Visibility Status

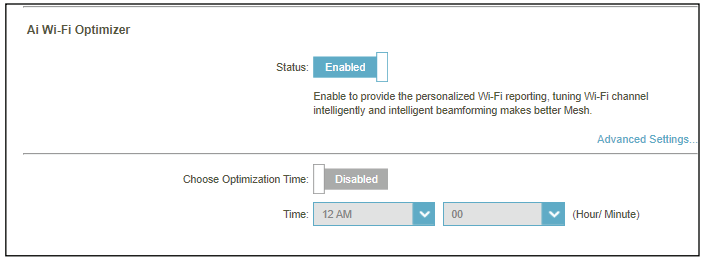
The default setting is **Visible**. Select **Invisible** if you do not want to broadcast the SSID of your wireless network.

Schedule

Select the time during which the wireless network will be available. The schedule may be set to Always Enable or you can add your own schedule.

To add a schedule:
Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule.

AI Wi-Fi Optimizer



AI-assisted Wi-Fi Optimizer intelligently assists in bandwidth optimization in your home or office network. It automatically adopts the "cleanest" channel and utilizes beamforming technology to improve signal efficiency and reduce interference. It also provides push notifications about weekly network bandwidth utilization and network management advice on prioritizing clients to maintain the overall Internet quality. Refer to **EAGLE PRO AI** on page **93** for more information.

AI Wi-Fi Optimizer Enable or disable AI Wi-Fi Optimizer functionality.

Choose Optimization Time Enable or disable scheduled optimization. Select the time at which the AI Wi-Fi Optimizer will start.

Once this is turned on, you will start receiving weekly reports on Wi-Fi conditions through AI Assistant.

Wi-Fi Protected Setup

The easiest way to connect your wireless devices to the router is with Wi-Fi Protected Setup (WPS).

WPS-PBC Status Enable or disable WPS-PBC (Push Button Configuration) functionality. Press to establish a connection with another WPS compatible device.

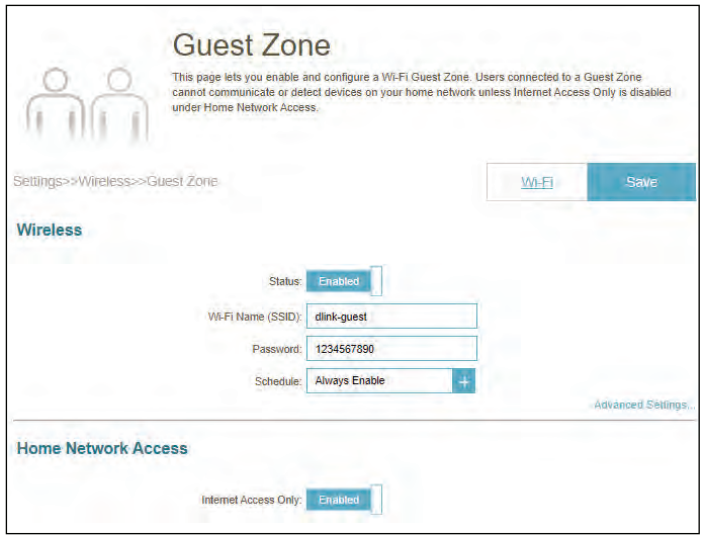
Guest Zone

Go to **Settings > Wireless**, then click the **Guest Zone** tab to configure your guest Wi-Fi.

The **Guest Zone** feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. You may configure different zones for the 2.4 GHz and 5 GHz wireless bands.

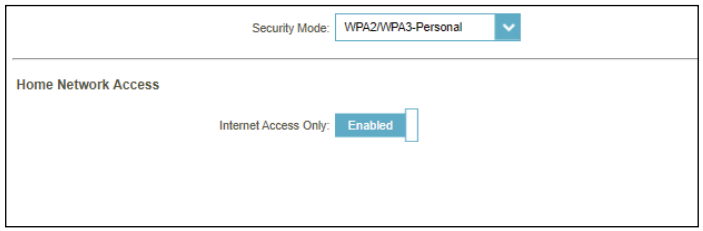
Click **Save** at any time to save the changes you have made on this page.

*If Smart Connect is **Enabled** in the previous Wireless settings, configure the following for both radio frequencies. If it is **Disabled**, configure the following for 2.4GHz and 5GHz individually.*



Wireless	
Status	Enable or disable the Guest Zone feature. The status is disabled by default.
Wireless Name (SSID)	Create a name for your wireless network using up to 32 characters.
Password	Create a Wi-Fi password. Your password must be between 8-63 characters in length.
Schedule	Select the time during which the wireless network will be available. The schedule may be set to Always Enable or you can add your own schedule. To add a schedule: Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule.

Advanced Settings



Security Mode Choose **None, WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these. Note that WPS will be disabled if WPA3 is used.

Home Network Access

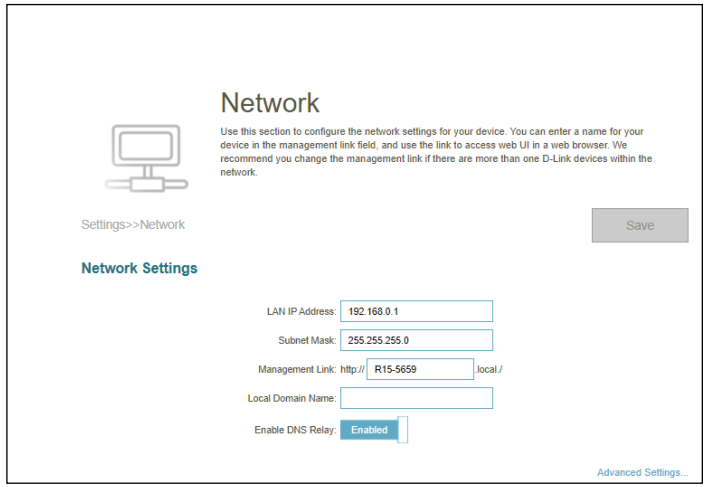
Internet Access Only Enabling this option will confine connectivity to the Internet and prevent guests from accessing other local network devices.

Network

Go to **Settings > Network** to change the local network settings of the router and configure the DHCP settings.

Click **Save** at any time to save the changes you have made on this page.

Network Settings	
LAN IP Address	Enter the IP address of the router. The default IP address is **192.168.0.1**. If you change the IP address, you will need to enter the new IP address in your browser to log in to the web configuration.
Subnet Mask	Enter the subnet mask of the router. The default subnet mask is **255.255.255.0.**
Management Link	The default address to access the router's configuration is **http://R32-*XXXX*.local./** (where XXXX represents the last 4 digits of your router's MAC address). You can replace **R32-XXXX** with a name of your choice.
Local Domain Name	Enter the domain name (optional).
Enable DNS Relay	Disable this option to transfer the DNS server information from your ISP to network clients for setting DNS server. If enabled, network clients will instead set the router's IP address as the DNS server.



DHCP Server

Status Enable or disable the DHCP server.

DHCP IP Address Range Enter the start and end IP addresses for the DHCP server's IP assignment. **Note**: *If you statically assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.*

DHCP Lease Time Enter the length of time for the IP address lease in minutes. The default is 10080 minutes.

Always Broadcast Enable this feature to broadcast your network's DHCP server to LAN/WLAN clients.

Advanced Settings...

WAN Port Speed You may set the link speed of the Internet port to **10 Mbps, 100 Mbps, 1000 Mbps**, or **Auto** (recommended).

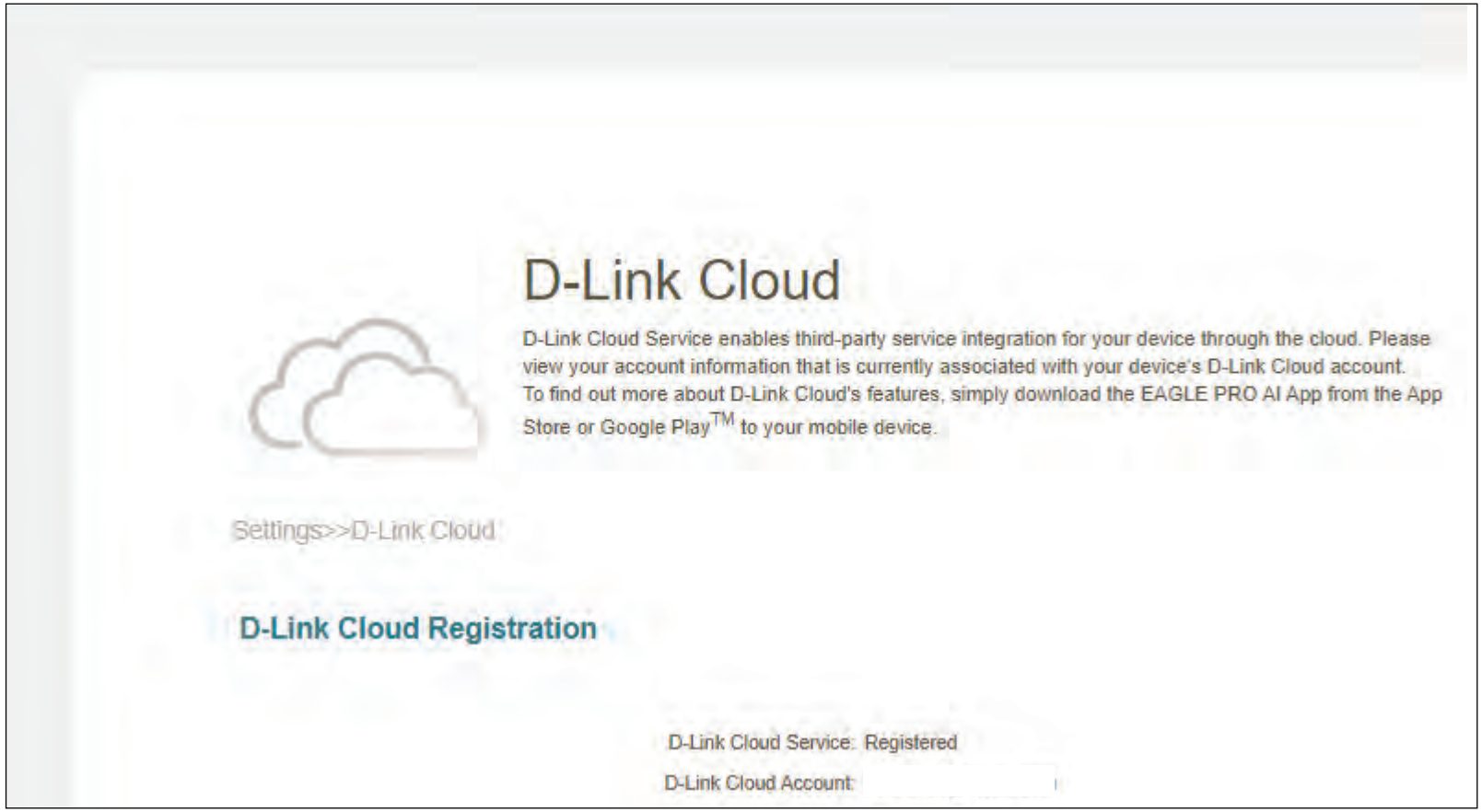
UPnP Enable or disable Universal Plug and Play (UPnP). UPnP provides compatibility with networking equipment, software, and peripherals. This is enabled by default.

IPv4 Multicast Streams Allow or disallow IPv4 multicast traffic to pass through the router from the Internet. This is enabled by default.

IPv6 Multicast Streams Allow or disallow IPv6 multicast traffic to pass through the router from the Internet. This is enabled by default.

D-Link Cloud

Go to **Settings > D-Link Cloud** to see your D-Link Cloud Service details. This page lists whether you are registered with D-Link Cloud Service and email address associated with the account. It enables you to manage your device anytime, anywhere and check the status of your router. Use the EAGLE PRO AI to find out more about D-Link Cloud's features.



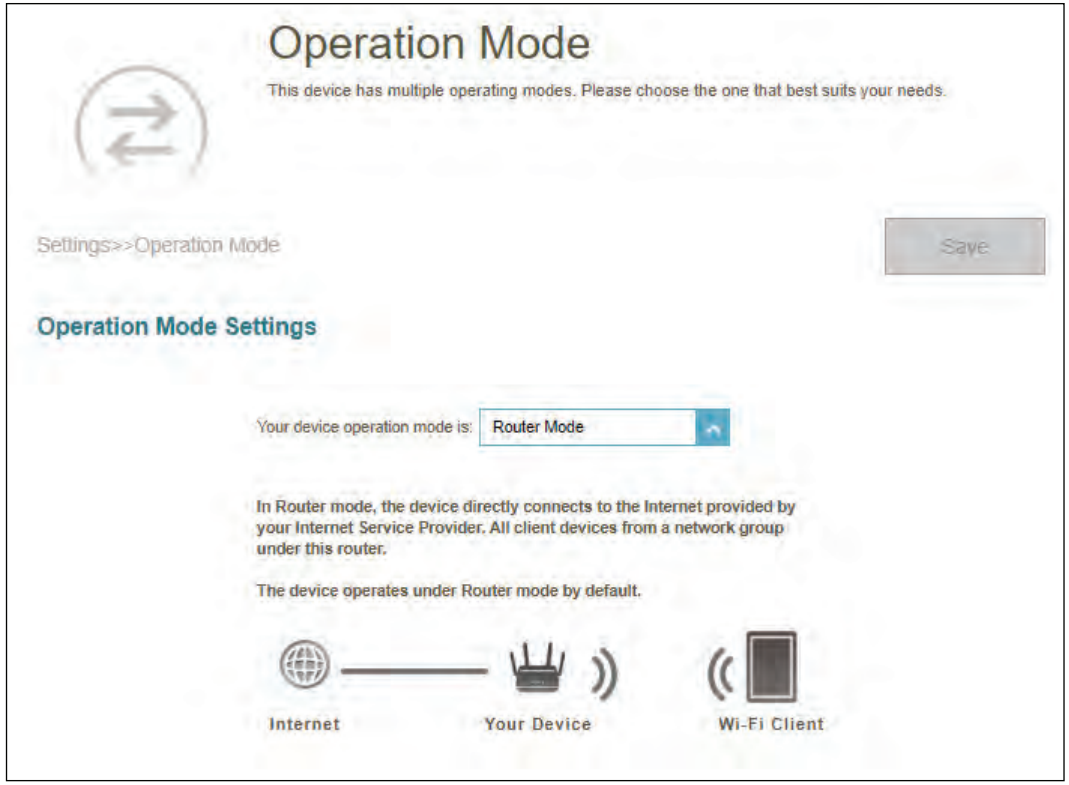
Operation Mode

Go to **Settings > Operation Mode** to select your operation mode. Depending on your network architecture, you can configure the router to function as one of the following types of network device: router, extender, or bridge.

Router Mode: In this mode, the R32 directly connects to the Internet provided by your ISP (Internet Service Provider). All client devices from a network group are connected and managed under this router. This is the default mode.

Bridge Mode: In this Mode, the R32 extends your existing network and improves overall Wi-Fi coverage, meaning that you already have a router on the premises. Under this mode, the DHCP Server, Parental Control, QoS, and Firewall settings rely on the existing router.

Extender Mode: In this mode, this device acts as an extender to connect your wireless devices, expanding Wi-Fi coverage. It provides connectivity between various wireless devices. This can be useful if you already have an existing wireless router. You can then manage the extender through the main router under this mode.



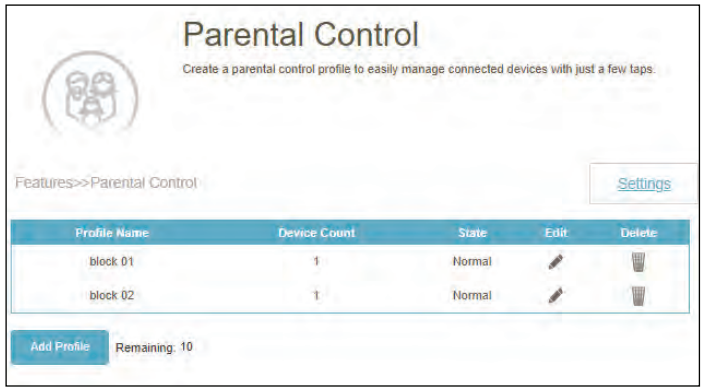
Features

Parental Control

Go to **Features** > **Parental Control** to configure parental control policies. You can configure schedules that set time limits for Internet access and prevent access to certain websites.

Click **Save** at any time to save the changes you have made on this page.

This page displays a list of profiles with the following information:

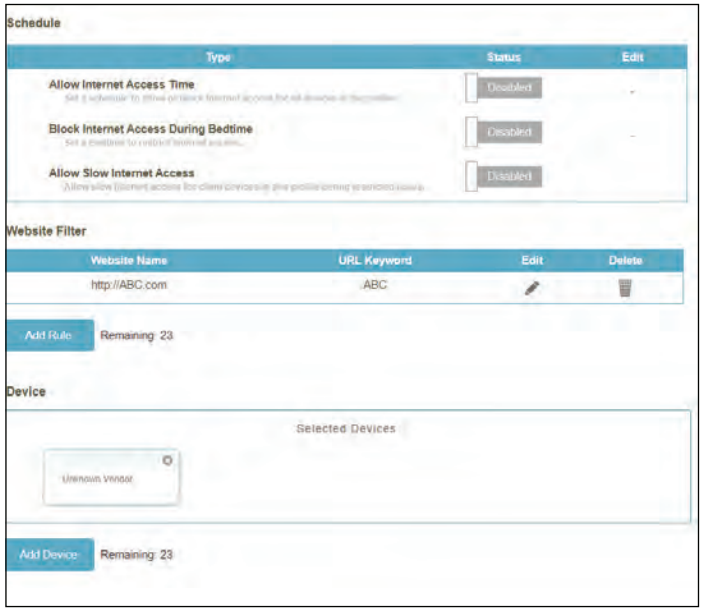


Profile Name	The name describes this profile.
Device Count	The number of devices that this policy will be applied to.
State	Displays the current status of Internet accessibility, i.e. Normal, Schedule Paused, or Paused on Demand.
Edit	Edit this access profile.
Delete	Remove this access profile.

A maximum of 12 profiles can be defined.

To add a profile, configure the following:

Schedule	
Profile Name	Enter a name for this profile.
Allow Internet Access Time	Click **Enabled** and define the schedule to allow Internet access. Select the time during which the Internet will be available. To add a schedule: Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule. If no time periods are selected, all devices in this profile will be denied Internet access.



Block Internet Access During Bedtime Click **Enabled** and define the schedule to block Internet access during bedtime.
To add a bedtime schedule:
Select the time during which bedtime schedule will be active. Select the days of the week, then select the pause time and the resume time for the period during which Internet access will be blocked. To specify different time periods for days of the week, click **Add another Bedtime schedule...** A maximum of 2 schedules can be defined.

Allow Slow Internet Access Enable this option to allow slow Internet access with reduced speed during restricted hours set above.

You can also modify an existing schedule by clicking **Edit**.

Website Filter

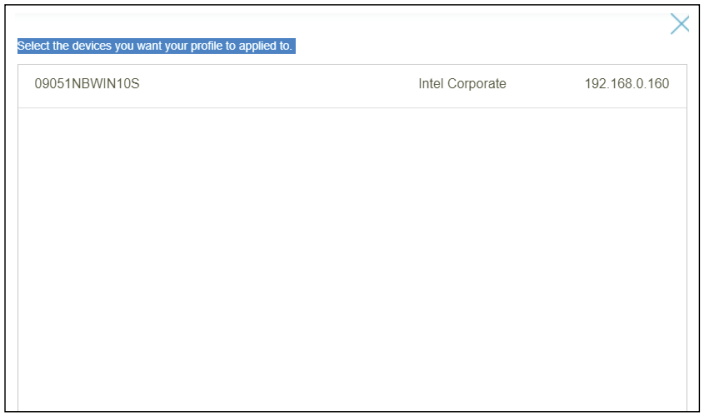
Click **Add Rule** to add a new website to be blocked:

Website Name Enter the name for the website. This blocks access to websites based on a website's address. For example, enter "ABC.com" or "www.ABC.com."

URL Keyword This blocks access to websites based on the keywords with matching URLs. For example, use "ABC" to block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC. Enter the same website name as the above in this field to block only the specific URL.

You can also modify or delete an existing rule by clicking **Edit** or **Delete** respectively.

Device



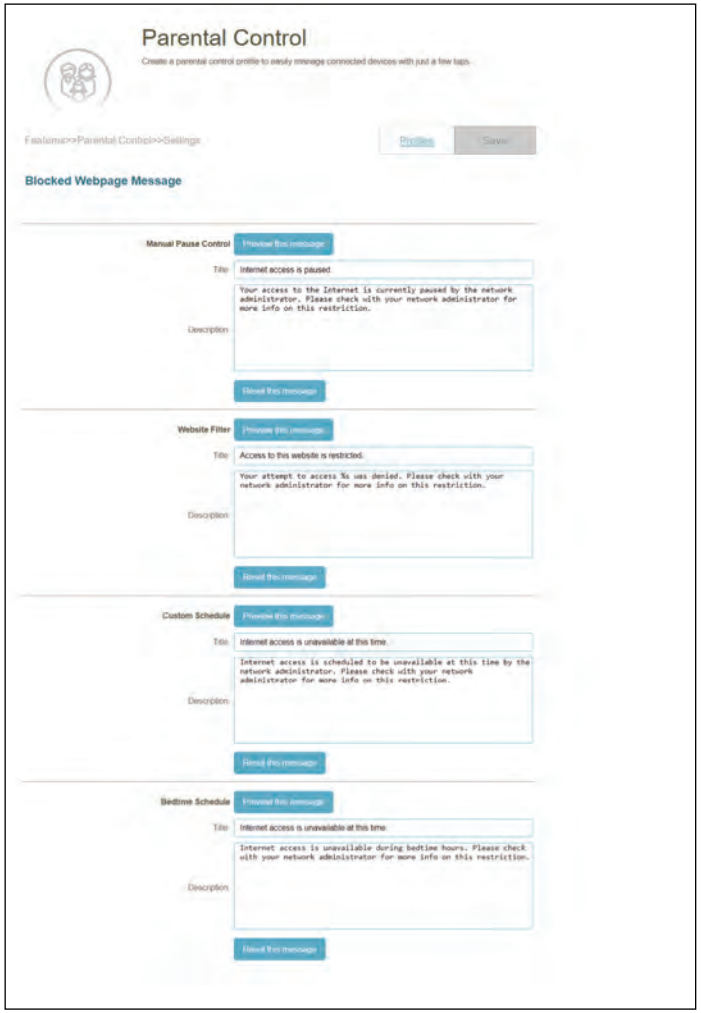
Click **Add Device** to add devices to be in the defined profile. Select the devices from the list of connected devices to which the access policy should be applied, then click **Apply** to close the screen. Click **Save** to save your profile settings and the new profile will be added to the profile list. You can also modify or delete an existing profile by clicking **Edit** or **Delete** respectively.On the Edit page for a selected profile, you can click to pause Internet access to specified devices of the profile immediately.

Click **Settings** to view the messages displayed to the device users whose Internet access has been restricted.

Blocked Webpage Message

For these access controls: **Manual Pause Control, Website Filter, Custom Schedule,** and **Bedtime Schedule**, you can view and customize the messages as well as the titles:

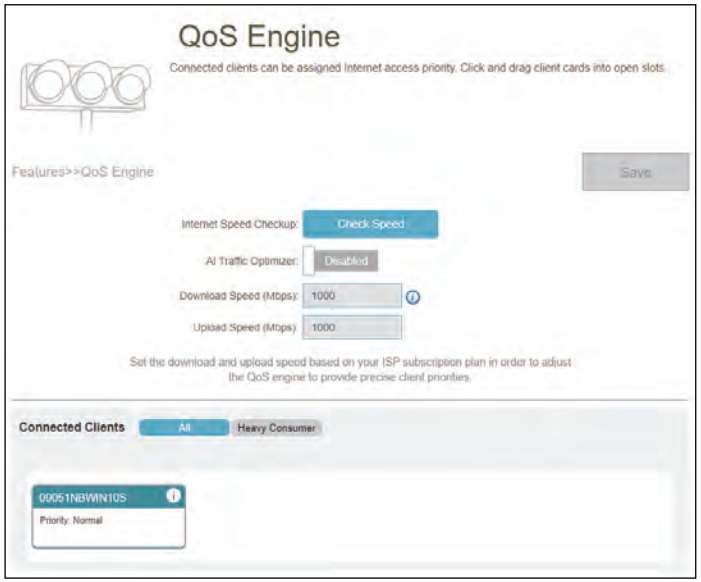
Title	Enter the title of the message in the text box.
Description	State the message to inform the user about the restricted access.
Reset this message	Click this button to reset the modified message to its factory default.
Preview this message	Display the presentation of the message on a new webpage.



QoS Engine

Go to **Features** > **QoS Engine** to configure clients' Internet access priorities. It aims to optimize Internet traffic to enhance the overall user experience.

Click **Save** at any time to save the changes you have made on this page.



Click **Check Speed** to run a speed check to determine how to distribute Wi-Fi bandwidth to prioritized devices. The speed test helps the QoS engine to distribute Wi-Fi bandwidth to prioritized devices (configured in the device cards below).

AI Traffic Optimizer The intelligent QoS Engine lists devices consuming comparatively large resources and will intelligently adjust bandwidth to these devices by assigning a low priority. It will also allocate appropriate bandwidth to connected devices based on their priorities to maintain quality online experience.

Once this is turned on, you will start receiving weekly reports on bandwidth usage through AI Assistant.

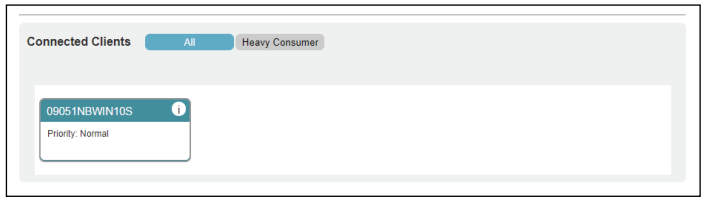
Upload Speed The rate at which the content is being transferred to the Internet.

Download Speed The rate at which the content is being transferred to the router.

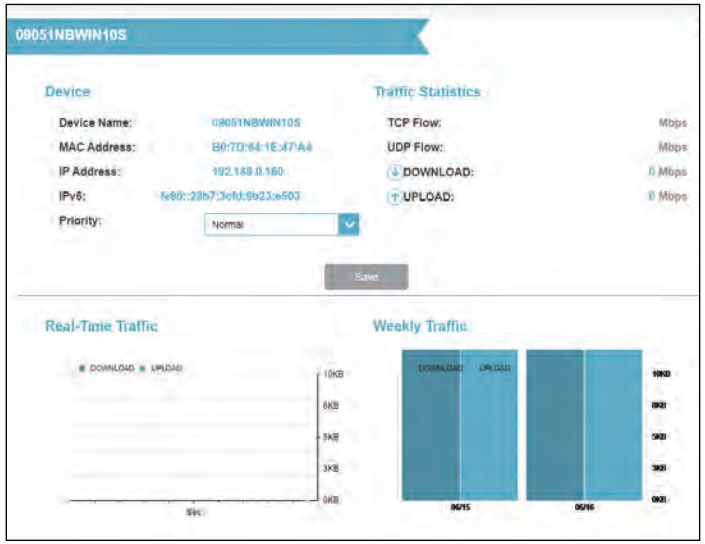
Click **Apply to QoS** after the Speed Test to automatically fill in the above information.

This **Quality of Service (QoS) Engine** allows you to prioritize particular clients over others, so that these clients receive higher bandwidth. For example, if one client is streaming a movie and another is downloading a bulk of files, you might want to assign the former device a higher priority than the latter so that the movie streaming is not disrupted.

Under **Connected Clients**, you will see device cards representing each connected client. Click **All** to see all connected devices and **Heavy Consumer** to see clients that are particularly active on the Internet.



To assign a priority level to a device, enable **AI Traffic Optimizer** first. Then click the client to open its information page. It shows the following information:



Device Name: The name that describes the client device
MAC Address: The MAC address of the client device
IPv4/IP v6 Address: The IP address in IPv4 and IPv6 addressing mechanism of the client device.
Priority: Select the priority for the client device with the following categories:

Normal; **High: Always Enable**, for **1 Day**, for **4 Hours**, for **2 Hours**, or for **1 Hour**; **Low: Always Enable**, for **1 Day**, for **4 Hours**, for **2 Hours**, or for **1 Hour**.

Traffic Statistics

It shows traffic statistics for these activities: TCP flow, UDP flow, and Download and Upload speeds in megabit per second.

Real-Time & Weekly Traffic

Two graphs: Real-time Traffic represents real-time data speeds in megabyte per second or kilobyte per second. Weekly Traffic represents daily download and upload data volume for the past week in kilobyte or megabyte.

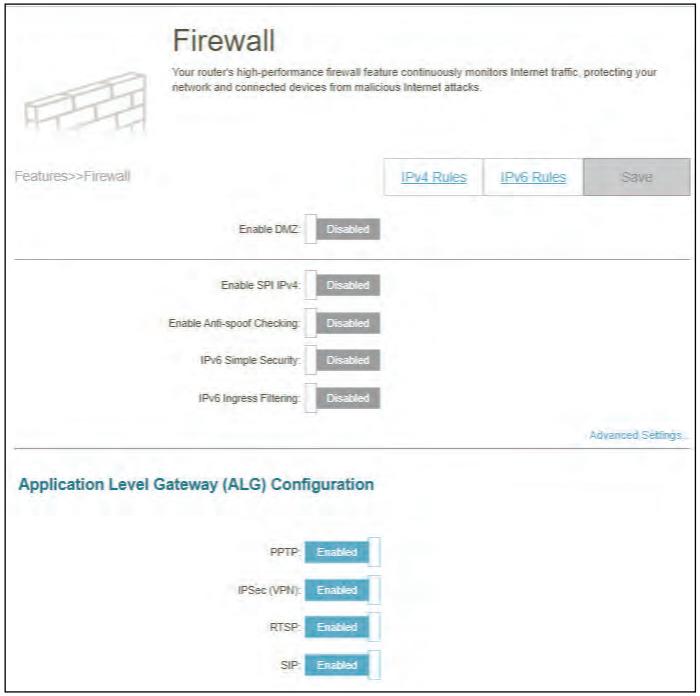
If no devices are explicitly assigned a priority, they will all be treated with equal priority.

Firewall

Go to **Features > Firewall** to configure the router's firewall settings. The firewall feature helps protect your network from malicious attacks over the Internet.

To configure the IPv4 firewall rules, click the **IPv4 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on page **73**
To configure the IPv6 firewall rules, click the **IPv6 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on page **73**

Click **Save** at any time to save the changes you have made on this page.



Enable DMZ Enable or disable Demilitarized Zone (DMZ). Devices in this zone are completely exposed to threats over the Internet. This is not recommended unless they are servers that must be exposed to the WAN.

DMZ IP Address If you enable DMZ, enter the IP address of the client to be placed in this zone, or use the drop-down menu to quickly select one of the clients.

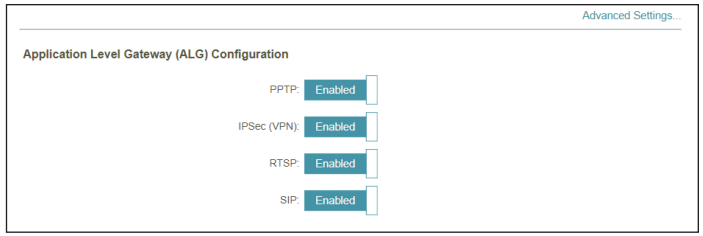
Enable SPI IPv4 Enabling Stateful Packet Inspection (SPI) or dynamic packet filtering helps prevent cyber attacks by tracking more states per session to validate that the traffic passing through the session conforms to the protocol.

Enable Anti-spoof Checking Enable this feature to help protect your network from certain kinds of "spoofing" attacks.

IPv6 Simple Security Enable or disable IPv6 simple security. A simple firewall configuration that denies access directly to computers behind the router.

IPv6 Ingress Filtering Enable or disable IPv6 ingress filtering for incoming packets to prevent suspicious senders.

Advanced Settings... - Application Level Gateway (ALG) Configuration



Different ALGs provide special handling for specific protocols or applications. A number of ALGs for common applications are enabled by default as stated below.

PPTP Allows multiple machines on the LAN to connect to their corporate network using the PPTP protocol.

IPSec (VPN) Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through NAT. This Application Level Gateway (ALG) may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

RTSP Allows applications that uses Real Time Streaming Protocol (RTSP) to receive streaming media from the Internet.

SIP Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

Firewall Settings - IPv4/IPv6 Rules

Go to **Features** > **Firewall**, then click the **IPv4 Rules** tab or the **IPv6 Rules** tab to configure rules for traffic filtering.

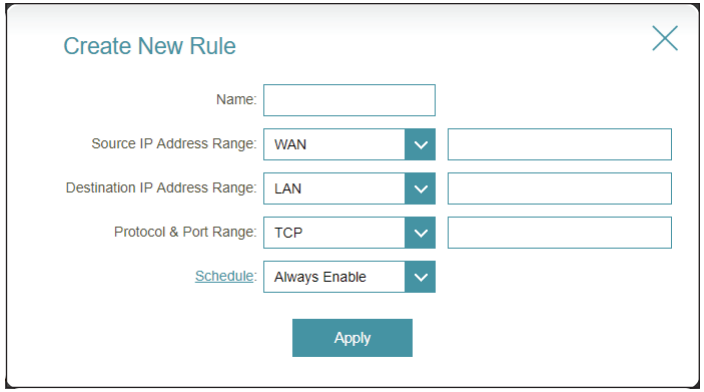
To configure the Firewall Advanced settings, click the **Advanced** link. Refer to **Firewall** on page **71**

Click **Save** at any time to save the changes you have made on this page.

To begin, use the drop-down menu to select whether it is an **ALLOW** or **DENY** rule. You can also choose to turn filtering **OFF**.

If you want to remove a rule, click in the Delete column. If you wish to edit a rule, click in the Edit column. If you wish to create a new rule, click the **Add Rule** button.

*If you click **Edit** or **Add Rule**, the following options will appear:*



Name Enter a name for the rule.

Source IP Address Range Enter the source IP address range (e.g. 1.1.1.1-1.1.1.2 for IPv4 or 2001::1-2001::2 for IPv6) that the rule will apply to. Using the drop-down menu, specify whether it is a **WAN** or **LAN** IP address. Both a single IP address and a range of IP addresses can be entered.

Destination IP Address Range Enter the destination IP address range (e.g. 1.1.1.1-1.1.1.2 for IPv4 or 2001::1-2001::2 for IPv6) that the rule will apply to. Using the drop-down menu, specify whether it is a **WAN** or **LAN** IP address. Both a single IP address and a range of IP addresses can be entered.

Protocol & Port Range Select the protocol of the traffic to allow or deny (**Any, TCP, or UDP**) and then enter the range of ports (e.g. 21-23) that the rule will apply to. Select **Any** to allow/deny all types of traffic regardless of the port number.

Schedule Use the drop-down menu to select the time schedule for the rule. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to **Management > Time & Schedule - Schedule** on page **85** for more information.

A maximum of 24 rules can be defined.

Port Forwarding

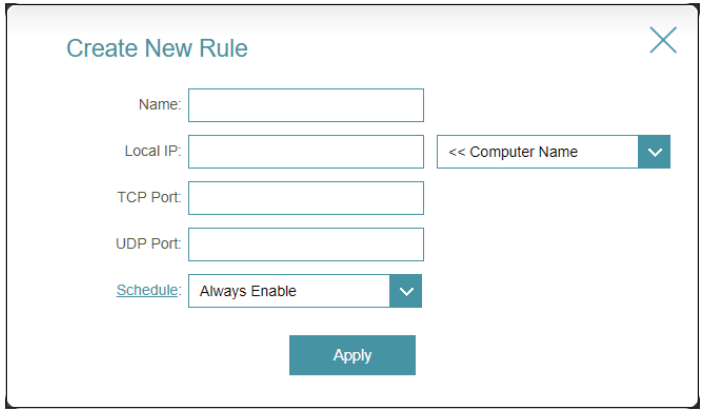
Go to **Features > Port Forwarding** to specify a port or range of ports to open for specific devices on the network. This might be necessary for certain applications to connect through the router. For example, access from the Internet can be redirected to a DMZ host using Port Forwarding.

To configure the Virtual Server settings, click the **Virtual Server** link. Refer to **Port Forwarding - Virtual Server** on page **77**.

Click **Save** at any time to save the changes you have made on this page.

If you want to remove a rule, click in the Delete column. If you want to edit a rule, click in the Edit column. If you want to create a new rule, click the **Add Rule** button.

*If you click **Edit** or **Add Rule**, the following options will appear:*



Name Enter a name for the rule.

Local IP Enter the IP address of the computer on your local network to which you want to direct the incoming service. Alternatively, select the device from the drop-down menu.

TCP Port Enter the TCP ports that you want to open. You can enter a single port or a range of ports. Separate ports with a comma (for example: 24,1009,3000-4000).

UDP Port Enter the UDP ports that you want to open. You can enter a single port or a range of ports. Separate ports with a comma (for example: 24,1009,3000-4000).

Schedule Use the drop-down menu to select the time schedule for the rule. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to **Management > Time & Schedule - Schedule** on page **85** for more information.

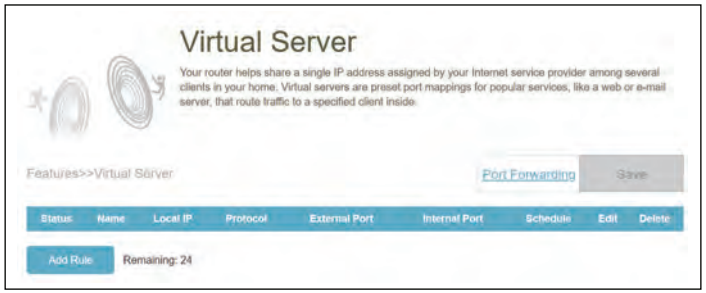
Port Forwarding - Virtual Server

Go to **Features** > **Port Forwarding** then click the **Virtual Server** tab to configure its settings and specify a public port on your router for redirection to an internal LAN IP with the mapped port. This might be necessary if you are hosting services behind the router.

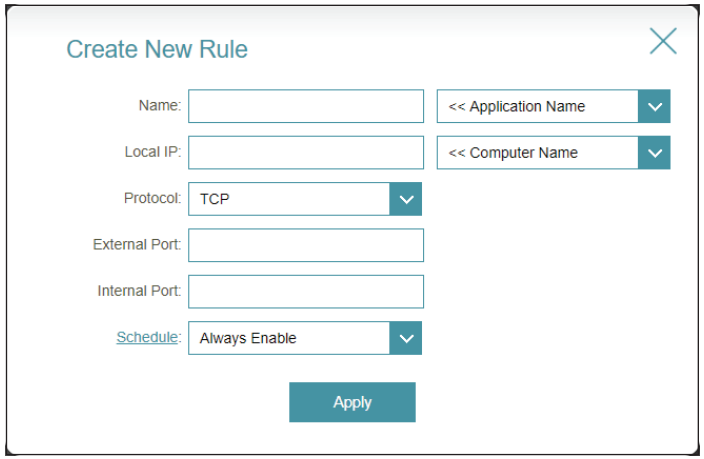
To configure the Port Forwarding settings, click the **Port Forwarding** link. Refer to **Port Forwarding** on page **75**

Click **Save** at any time to save the changes you have made on this page.

If you wish to remove a rule, click in the Delete column. If you wish to edit a rule, click in the Edit column. If you wish to create a new rule, click the **Add Rule** button.



*If you click on **Edit** or **Add Rule**, the following options will appear:*



Name Enter a name for the rule. Alternatively, select the protocol/ Application Name from the drop-down menu. Depending on the requested service, the router redirects the external service request to the appropriate internal host.

Local IP Enter the IP address of the computer on your local network that you want to direct the incoming service to. Alternatively, select the device from the drop-down menu.

Protocol Select the protocol of the traffic to allow or deny (**TCP, UDP, Both,** or **Other**).

Protocol Number If you entered **Other** above, enter the protocol number. Refer to https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml for Assigned Internet Protocol Numbers.

External Port Enter the public port you want to open.

Internal Port Enter the private port you want to open.

Schedule Use the drop-down menu to select the time schedule for the rule. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to **Time & Schedule - Schedule** on page **85** for more information.

Static Routes - IPv4

Go to **Features** > **Static Routes** to define custom routes to control how traffic moves around your network.

To configure the Static Route IPv6 settings, click the **IPv6** tab. Refer to **Static Routes - IPv6** on page **80**

Click **Save** at any time to save the changes you have made on this page.

If you wish to remove a rule, click in the Delete column. If you wish to edit a rule, click in the Edit column. If you wish to create a new rule, click the **Add Rule** button.

*If you click on **Edit** or **Add Route**, the following options will appear:*

Name Enter a name for the route.

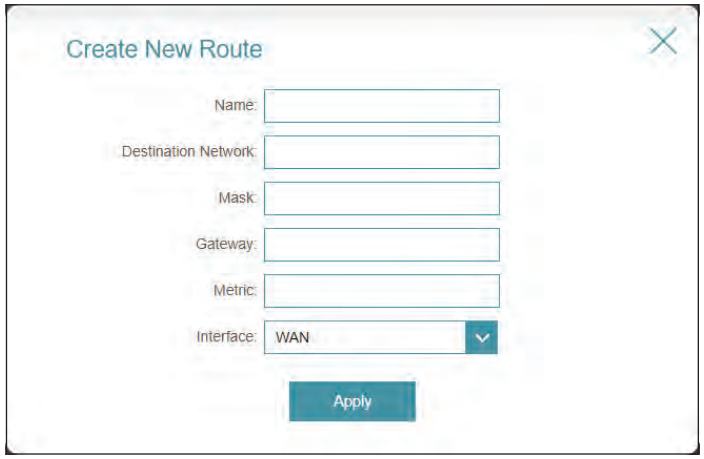
Destination Network Enter the destination IP address of the subnetwork.

Mask Enter the subnet mask of the destination address.

Gateway Enter the IP address of the next hop, which is the gateway to the remote network.

Metric Enter a route metric value between 1 and 16. This value indicates the cost of using this route.

Interface Select the interface that the IP packet will use to transit out of the router when this route is used.



Static Routes - IPv6

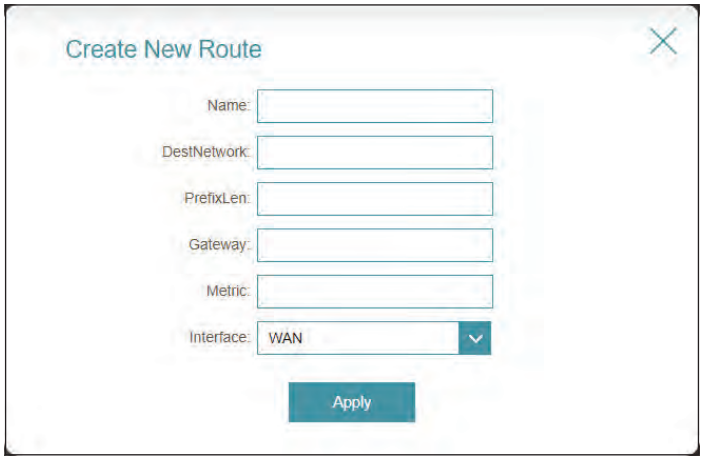
Go to **Features** > **Static Routes**, then click **IPv6** to configure the IPv6 Static Routes.

To configure the Static Route IPv4 settings, click the **IPv4** tab. Refer to **Static Routes - IPv4** on page **79**.

Click **Save** at any time to save the changes you have made on this page.

If you wish to remove a rule, click in the Delete column. If you wish to edit a rule, click in the Edit column. If you wish to create a new rule, click the **Add Rule** button.

*If you click on **Edit** or **Add Route**, the following options will appear:*



Name Enter a name for the route.

DestNetwork Enter the destination IPv6 address of the subnetwork or the prefix, for example, 2010:db9:abcd:1234::

PrefixLen Enter the prefix length, which is the number of prefix bits of the IPv6 address. Enter a value between 64 and 128.

Gateway Enter the IP address of the next hop, which is the gateway to the remote network.

Metric Enter a route metric value between 1 between 128. This value indicates the cost of using this route.

Interface Select the interface that the IP packet will use to transit out of the router when this route is used.

Dynamic DNS

Go to **Features > Dynamic DNS**. This page allows your router to associate an easy-to-remember domain name such as [YourDomainName].com with a regularly changing IP address assigned by your Internet Service provider. This feature is helpful when running a virtual server.

Click **Save** at any time to save the changes you have made on this page.

Enable Dynamic DNS Enable or disable dynamic DNS. Enable this feature to display more configuration options.

Status Displays the current dynamic DNS connection status.

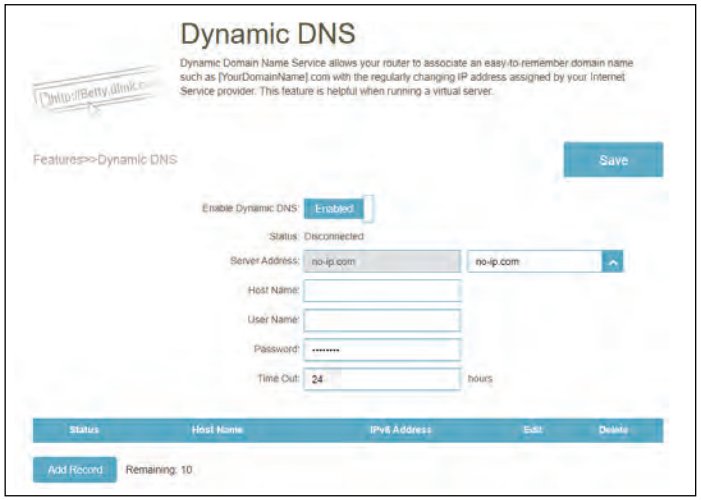
Server Address Select the DDNS service provider from the drop-down menu.

Host Name Enter the host name that you registered with your dynamic DNS service provider.

User Name Enter your dynamic DNS account name.

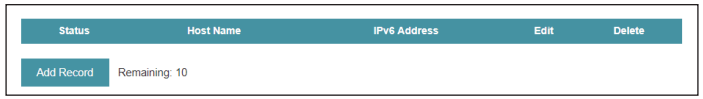
Password Enter your dynamic DNS account password.

Time Out Enter a time-out value (in hours) to indicate how often the router should update its Dynamic DNS settings.



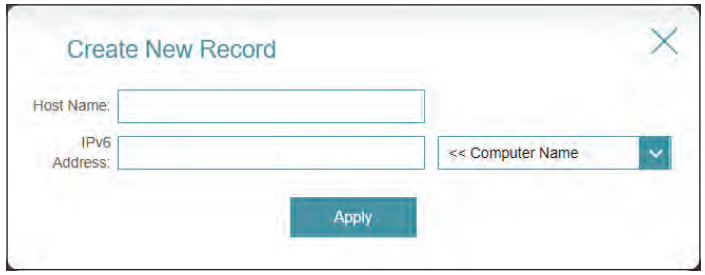
At the bottom of the page are the IPv6 host settings.

If you wish to remove a record, click in the Delete column. If you wish to edit a record, click in the Edit column. If you wish to create a new record, click the **Add Record** button.



Host Name Enter the host name that you registered with your dynamic DNS service provider.

IPv6 Address Enter the IPv6 address of your host or server for DDNS configuration. Alternatively, select the network interface for DDNS configuration.



A maximum of 10 records can be defined.

Quick VPN

Go to **Features > Quick VPN**. This page will help you configure the Quick VPN feature of your router. For more information, refer to **Quick VPN** on page **110**. Before proceeding, ensure that your Internet connection is working properly. We recommend configuring Dynamic DNS before proceeding with Quick VPN setup. If your router is assigned an IP address from your ISP using DHCP, it may frequently change, requiring connection parameters to be set accordingly and a DDNS address can avoid this hassle.

To configure the User settings and grant users with VPN permission, go to **Management > User**. Refer to **User** on page **90.**

Click **Save** at any time to save the changes you have made on this page.

L2TP over IPSec	Enable or disable the Quick VPN server. Quick VPN uses L2TP protocol.
Username	Enter a username.
Password	Enter a password containing both numbers and letters with 8 to 64 characters in length.
PSK	Enter a Pre-shared Key between 6 and 64 characters.
VPN Profile for iOS Device and MAC OS X	Click **Export** to save the VPN profile settings file for iOS devices and Mac OS X.
Advanced Settings...	
Authentication Protocol	Choose the authentication protocol type: **MSCHAPv2, PAP,** or **CHAP**. **MSCHAPv2** is the default.
MPPE	Select the encryption cipher strength for Microsoft Point-to-Point (MPPE) Encryption: **None, RC4-40,** or **RC4-128**. **None** is the default.

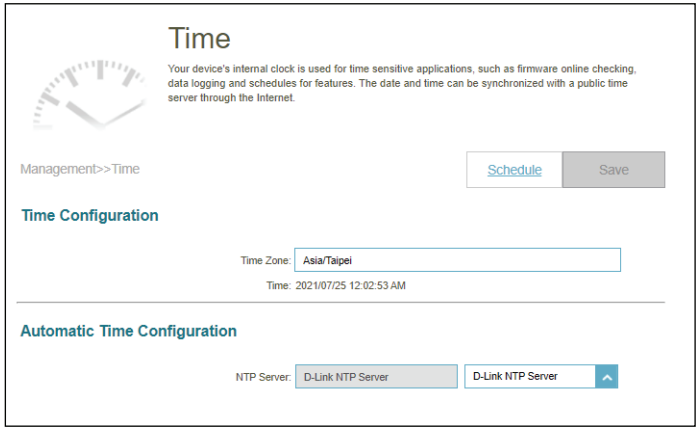
Management
Time & Schedule - Time

Go to **Management > Time & Schedule**. The **Time** page allows you to configure, update, and maintain the correct time on the internal system clock. From here you can set the time zone and the Network Time Protocol (NTP) server.

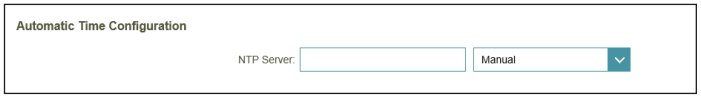
To configure the Schedule settings, click the **Schedule** tab. Refer to **Time & Schedule - Schedule** on page **85**

Click **Save** at any time to save the changes you have made on this page.

Time Configuration	
Time Zone	Select your time zone from the drop-down menu.
Time	Displays the current date and time of the router.



Automatic Time Configuration	
NTP Server	Select from the drop-down menu to use one of the following servers to synchronize the time and date for your router: D-Link NTP Server or Google NTP Server. Choose Manual to set the NTP server's IP address or server name.

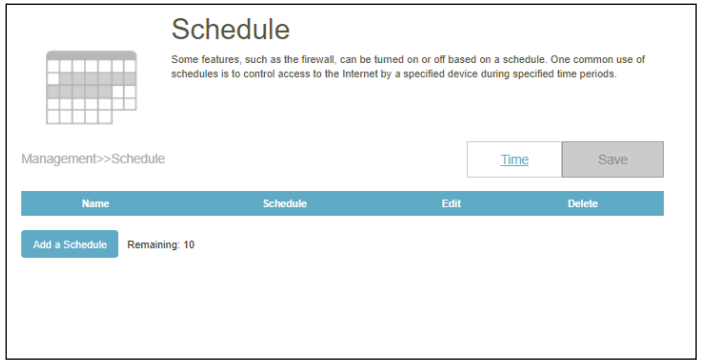


Time & Schedule - Schedule

Go to **Management > Time & Schedule**, then click the **Schedule** tab. The **Schedule** page allows you to control some of the functions based on a pre-configured schedule, for example, Port Forwarding in **Features > Port Forwarding** and Firewall Settings in **Features > Firewall** as well as sending Syslog via email in **Management > System Log**.

To configure the Time settings, click the **Time** tab. Refer to **Time & Schedule - Time** on page **84**

Click **Save** at any time to save the changes you have made on this page.



If you wish to remove a schedule, click in the Delete column. If you wish to edit a schedule, click in the Edit column. If you wish to create a new schedule, click the **Add a Schedule** button.

On the Schedule creation page, enter the name of your schedule in the **Name** field.

Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule.

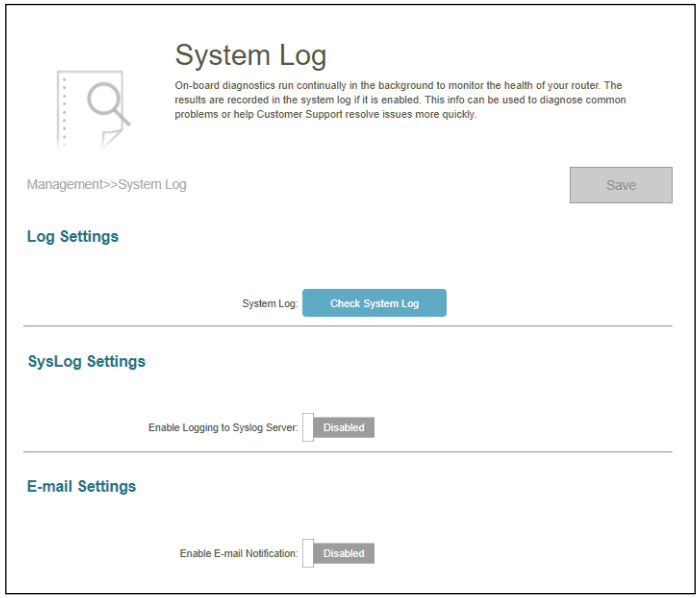
To remove a time period from the schedule, click on the cross icon.

Click **Apply** to save and close the page. Then click **Save** when you are done creating schedules.

System Log

Go to **Management > System Log**. The router keeps a running log of events. This log can be sent to a Syslog server or to your email address.

Click **Save** at any time to save the changes you have made on this page.



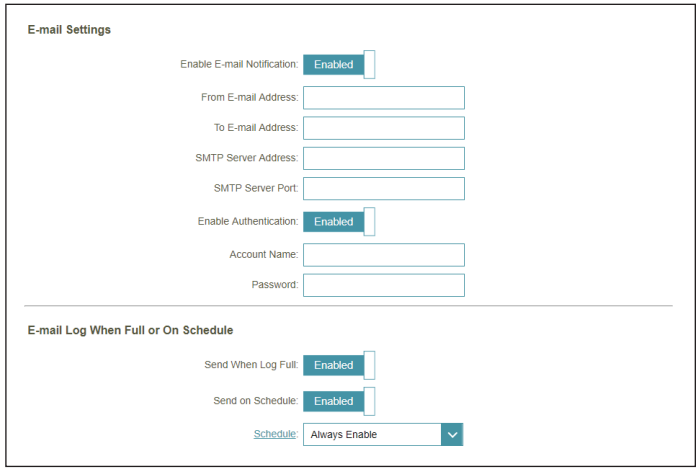
Log Settings

System Log	Click the **Check System Log** button to download a text file containing the system log. You can view the log entries by opening with any text editing applications such as WordPad on Windows.

SysLog Settings

Enable Logging to Syslog Server	Check this box to send the router logs to a SysLog Server.
SysLog Server IP Address	Configurable if **Enable Logging to Syslog Server** is enabled. Enter the IP address of the Syslog server. If the Syslog server is connected to the router, select it from the drop-down menu to automatically populate the field.

Email Settings



Enable E-mail Notification Enable this option if you want the logs to be automatically sent to an email address.

*If you enable **Enable E-mail Notification**, configure the following:*

From E-mail Address Enter the sender's email address of the SysLog messages.

To E-mail Address Enter the recipient's email address.

SMTP Server Address Enter the SMTP server address.

SMTP Server Port Enter the SMTP server port. The default is 25.

Enable Authentication Enable this if your SMTP server requires authentication.

Account Name Enter your SMTP account name.

Password Enter your SMTP account's password.

E-mail Log When Full or On Schedule

Send When Log Full If enabled, this option will set the router to send the log when the log buffer is full. The email account for sending logs is configured in the above section.

Send on Schedule If enabled, this option will set the router to send the log according to a set schedule periodically, so the administrator is always up to date on the operation of the router. The email account for sending logs is configured in the above section.

Schedule If you enable Send On Schedule, use the drop-down menu to select a schedule to apply. The schedule may be set to Always Enable, or you can create your own schedules in the Schedules section. Refer to **Time & Schedule - Schedule** on page **85** for more information.

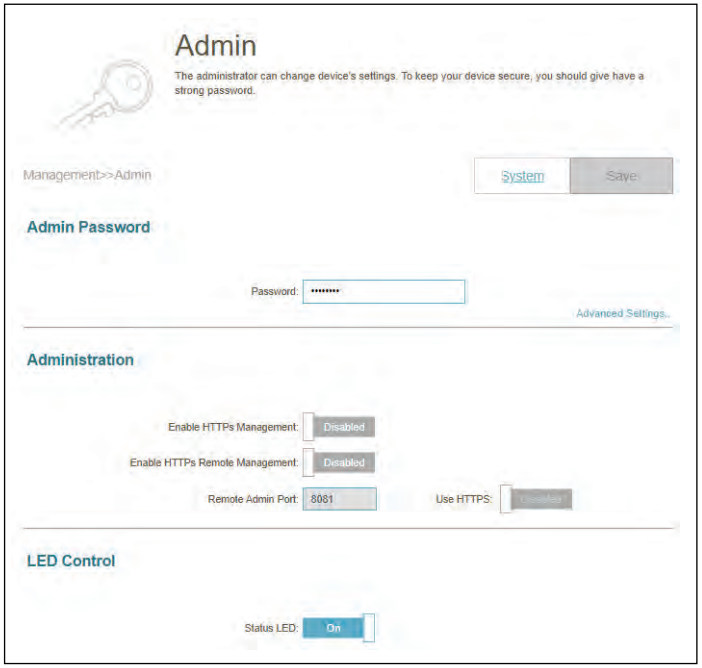
System Admin - Admin

Go to **Management > System Admin**. The Admin page will allow you to change the administrator (Admin) password.

To configure the System settings, click the **System** tab. Refer to **System Admin - System** on page **89**

Click **Save** at any time to save the changes you have made on this page.

Admin Password	
Password	Enter a new password for the administrator account. You will need to enter this password whenever you configure the router using a web browser or add the router to EAGLE PRO AI. It is recommended that you change the default device password printed on the device label on the bottom of the device.
Advanced Settings... - Administration	
Enable HTTPS Management	Enable router management using an encrypted HTTP connection.
Enable HTTPS Remote Management	Enable remote management over the Internet using an encrypted HTTP connection.
Remote Admin Port	Specify the port number for accessing the web configuration interface. The default is 8081.
LED Control	
Status LED	Turn the LED status lights on or off.



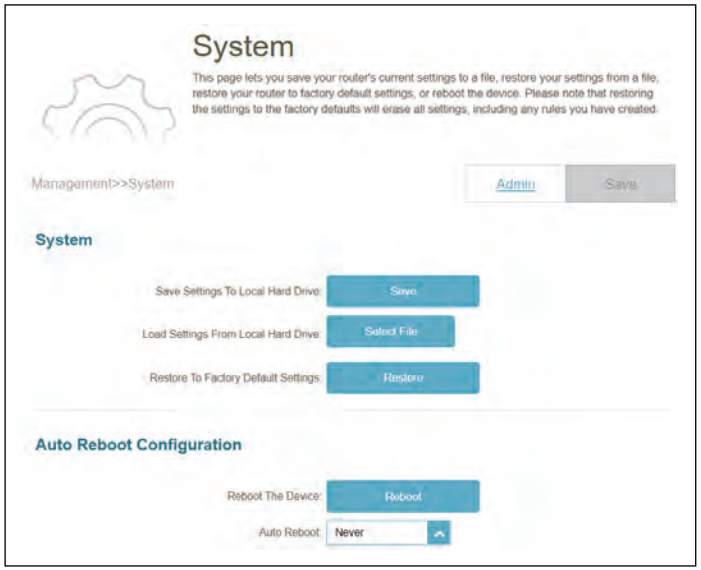
System Admin - System

Go to **Management > System Admin**, then click **System**. This page allows you to save the router's current configuration, load a previously saved configuration, reset the router to its factory default settings, or reboot the router.

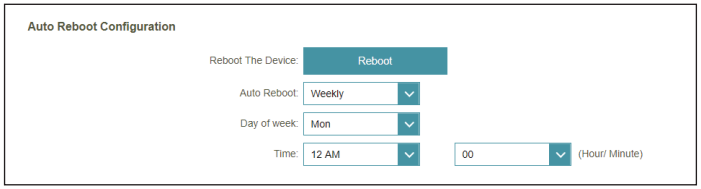
To configure the Admin settings, click the **Admin** tab. Refer to **System Admin - Admin** on page **88**

Click **Save** at any time to save the changes you have made on this page.

System	
Save Settings to Local Hard Drive	This option will save the current router configuration settings to a file (bin type) on your computer.
Load Settings from Local Hard Drive	This option will load a previously saved router configuration file. This will overwrite the router's current configuration.
Restore to Factory Default Settings	This option will restore the router back to the default configurations stored in the firmware. Any settings that have not been saved will be lost, including any rules that you have created. If you want to back up the current router configuration settings before restoring to factory defaults, use the **Save Settings to Local Hard Drive** function above.



Auto Reboot Configuration	
Reboot the Device	Click this button to reboot the router immediately.
Auto Reboot	You may set the router to automatically reboot at a set time. The options are **Never, Daily,** or **Weekly**. You may set the day, and hour and minute of the day for automatic reboot.

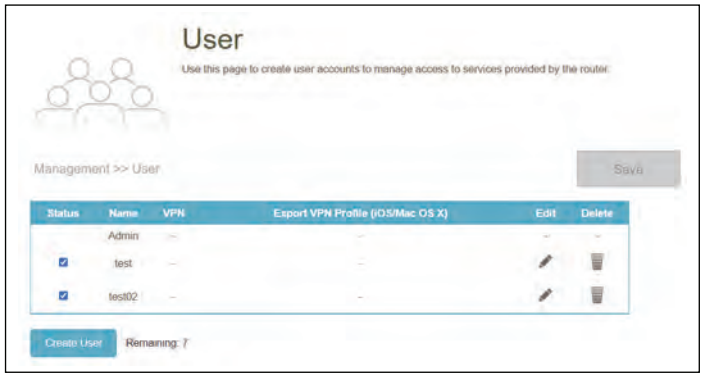


User

Go to **Management > User**. The User page is used to create, manage, and delete user accounts with VPN connection permission.

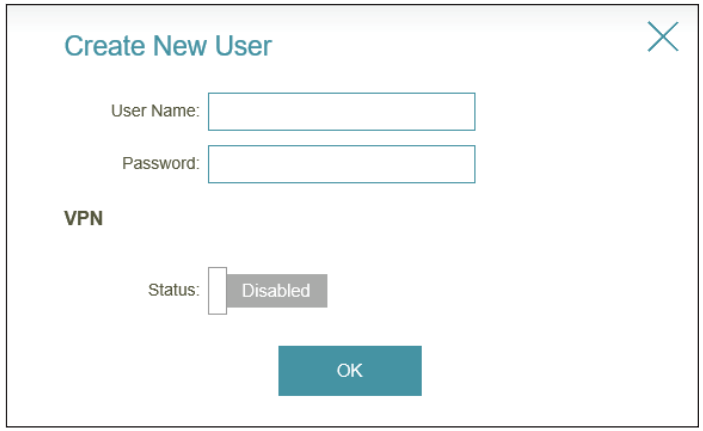
Click **Save** at any time to save the changes you have made on this page.

If you wish to remove a user, click in the Delete column. If you wish to edit a user, click in the Edit column. If you wish to create a new user, click the **Create User** button.



To create a user, click **Create User** and configure the following:

User Name	Enter a username for the new user account. Maximum length: 20 characters.
Password	Enter a password for the new user account. Maximum length: 32 characters.



VPN	
Status	Enable or disable Virtual Private Network (VPN) functionality for this user.

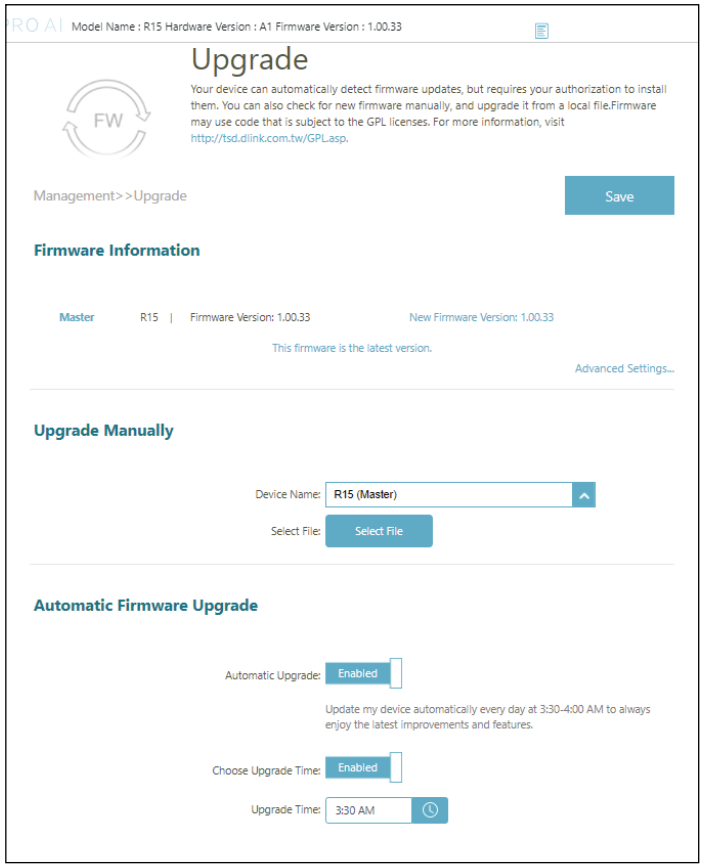
A maximum of 9 users (not including the Admin) can be created. Click **OK** to close the screen.

Upgrade

Go to **Management > Upgrade**. This page allows you to upgrade the router's firmware, either automatically or manually. To manually upgrade the firmware, you must first download the firmware file from **http://support.dlink.com**.

Click **Save** at any time to save the changes you have made on this page.

Firmware Information	
Current Firmware Version	Displays the current firmware version for both the main router as well as the extenders.
Check for New Firmware	Click this button to prompt the router to automatically check for a new firmware version. If a newer version is found, it will prompt you to install it.
Advanced Settings...Upgrade Manually	
Device Name	Select the device in the mesh network for manual update.
Select File	If you wish to upgrade manually, first download the firmware file. Then, click the **Select File** button and locate the file to install the new firmware.
Automatic Firmware Upgrade	
Automatic Upgrade	If enabled, the router will automatically upgrade to the newest firmware. The system will automatically upgrade to the latest firmware every day at 3:30-4:00 AM.
Choose Upgrade Time	Enable this function to set the router to automatically upgrade its firmware at a set time every day.
Upgrade Time	Configurable if **Choose Upgrade Time** is enabled. Set the hour and minute to automatically upgrade the router.



Statistics

Go to **Management > Statistics**. On the Statistics page you can view the amount of traffic that passes through the router on the Internet and LAN interfaces as well as the traffic from Wi-Fi 2.4 GHz and Wi-Fi 5GHz networks.

Router

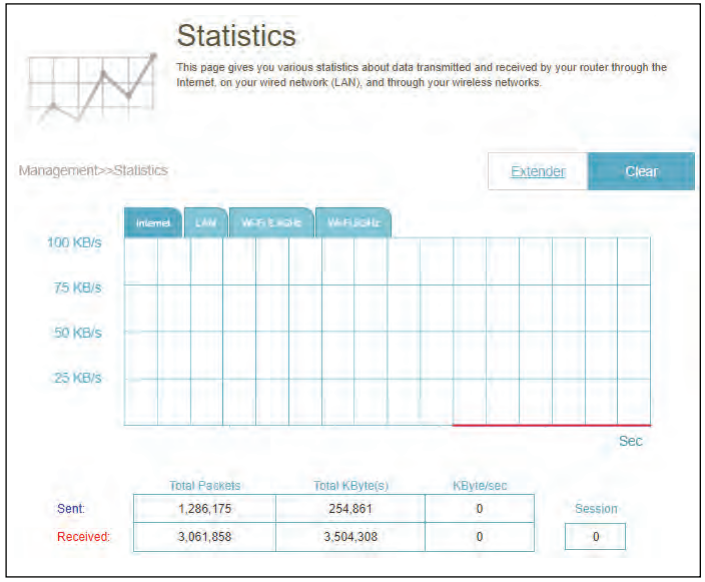
You can view the **Internet**, **LAN**, **Wi-Fi 2.4 GHz**, or **Wi-Fi 5 GHz** by clicking the respective tab at the top. The real-time graph of network traffic in kilobyte per second will be shown. To clear the information on the graph, click **Clear**.

The table below for each interface and radio frequency shows the total number of packets and data that are sent and received through the interface.

The traffic counter will reset if the device is rebooted.

Extender

Click the Extender tab to view the above information about the extender.



EAGLE PRO AI

With the EAGLE PRO AI on your smart devices, you can get the R32 up and running quickly. Just plug in the router, open the app and build your home network by following the easy instructions on the screen. The new EAGLE PRO AI is especially designed to ease your management work with the following features:

AI Wi-Fi Optimizer: Enable this feature to always connect to the cleanest Wi-Fi Channel using the breakthrough beamforming technology and receive information about automatic optimization for continuous improvement in the Wi-Fi environment.

AI Traffic Optimizer: The QoS engine controls the traffic flow intelligently by automatically assigning heavy traffic with a low priority to improve the overall user experience. It also generates information about bandwidth usage of individual devices and aggregate utilization data.

AI Assistant: The message center reports Internet traffic volume and provides usage notifications when clients are transmitting a large amount of data or overly active at night in the weekly bandwidth report. It also enables you to prioritize connected devices to reduce traffic congestion along with the report. Moreover, every improvement made by the Wi-Fi Optimizer will also be recorded to inform administrators about conditions of the wireless environment.

AI Parental Control: The Parental Control provides the highest flexibility of Internet accessibility control and website filtering. It allows administrators to control the availability of Internet access and speed on individual devices during the designated time periods.

AI Wi-Fi Optimizer:

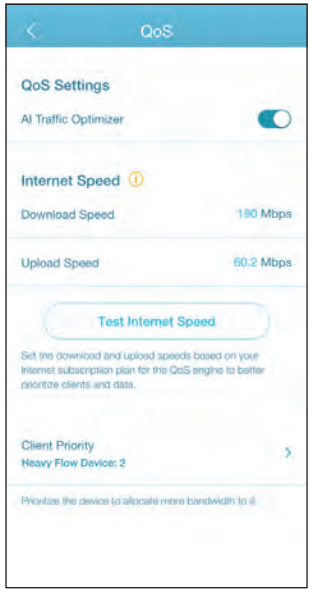
To enable this function, open the app. From the **Home** screen, tap **Wi-Fi** and tap . Then tap the slider for **AI Wi-Fi Optimizer**. Turn on Wi-Fi Optimizer to have your wireless connection adopting an interference-free channel automatically and receive weekly Wi-Fi environment report every Monday at 8 AM local time.

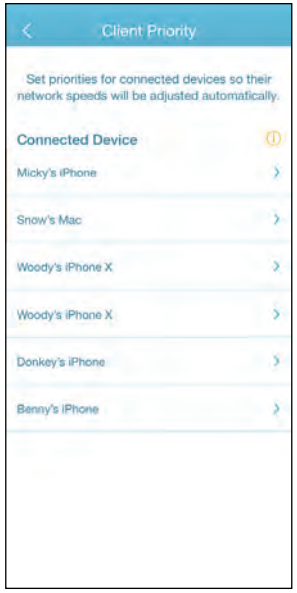
AI Traffic Optimizer:

To enable this function, open the app. From the **Home** screen, tap the main router, scroll down the **Device Info** screen to **Settings**, and tap **QoS**. Then tap the slider for **AI Traffic Optimizer**.

Before you start the AI Traffic Optimizer, run **Speed Test** from the **Home** screen (go to **Home> Internet Speed**) to set the download and upload speeds to assist the QoS engine in distributing the bandwidth to prioritized clients.

To prioritize clients, tap **Client Priority** from the **Home** screen. Tap a client device and assign a priority level with effective duration to this device. High priority devices running online games, video conferences, or other real-time programs will have the best access. The Red bar on the left indicates heavy users.





AI Parental Control:

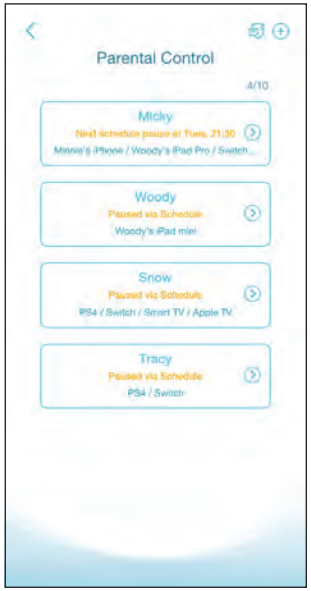
To enable this function, open the app. From the **Home** screen, tap **Parental Control**.

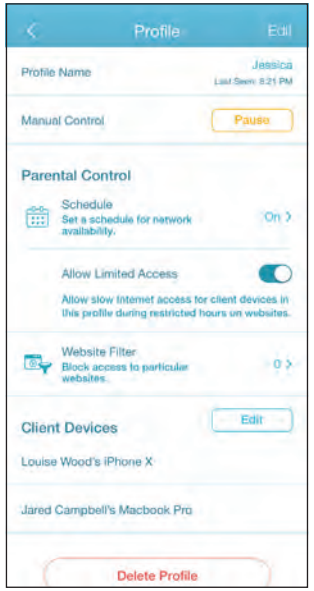
Then use the following procedure to add a new control profile:

1. Tap **Start**.
2. Name this profile. Then tap **Next** to continue.
3. Select client devices to which the profile will be applied.
4. Tap **Done** to proceed.
5. The profile summary will be displayed. On this page you can tap **Pause** to pause Internet immediately to the devices specified in the profile.

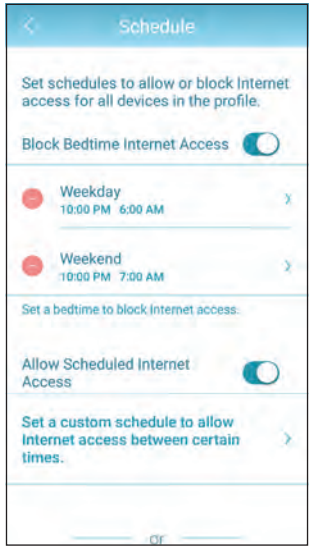
You can set schedules to restrict Internet access.

Use **Block Bedtime Internet Access** to block Internet access during the specified days with time periods. Up to two schedules can be defined. Use **Allow Scheduled Internet Access** to allow Internet access only during the specified days and times. Users cannot access the Internet except during the hours that you specify. Note that bedtime restriction takes precedence over the allowed schedules here.





You can also block specific websites on this page to prevent the specified devices from accessing certain websites. To do this, tap **Website Filter**, tap **Add Website**, then enter the website name and the domain keyword, for example, enter *violent.com* to block all access to this site and *violent* to block domain names that contain this keyword. Then tap **Add** at the top right.

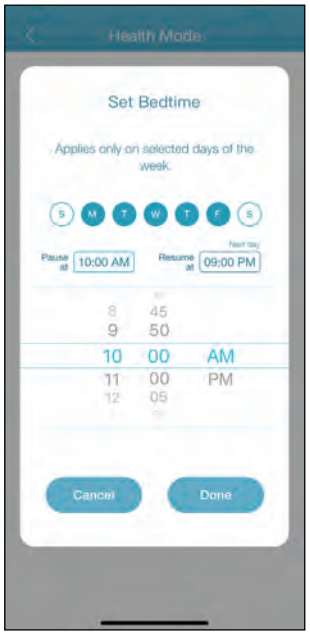


AI Assistant:

Tap **AI Assistant** to display the weekly reports on bandwidth consumption with information about heavy users. Weekly reports also give information on the number of times the system performs traffic management automatically when congestion occurs and provides qualitative rating on your Wi-Fi environment. Furthermore, the **Nighttime Internet Activity** informs you about the overly active Internet access during nighttime.

This app enables you to proactively improve sleep quality by restricting Internet access during nighttime. Tap **Health Mode** to set the bedtime during which Internet access will be blocked on *all* devices within the network.

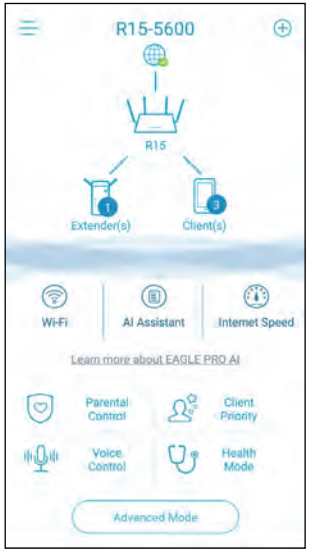
Note: The Bedtime scheduling also restricts local access by disabling Wi-Fi connectivity. However, remote management through the Internet is allowed.



Other Features

Advanced Mode

The advanced mode provides links to the web configuration interface of the device. Note that this feature is only available with local access (i.e. connected within the same Wi-Fi network). To access, go to **Home > Advanced Mode**.

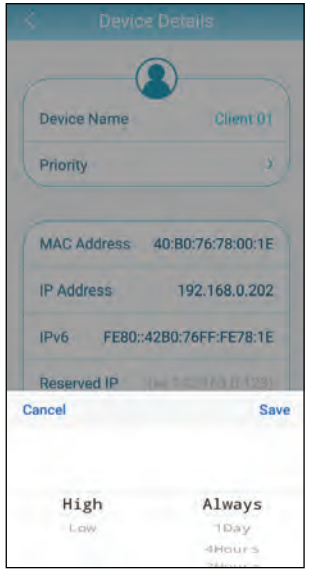


Device Information and Settings

From **Home**, tap the device **(main router)** of the mesh network topology to view its information and settings: name, IP and MAC address, hardware and firmware version, time zone, and model number. You can also configure the Internet connection method and change the device password on this page. It also provides basic device maintenance functions: reboot, LED indicator on/off, firmware update, and device identification with flashing LED.

Client Information and Statistics

From **Home**, tap the **device (Clients)** of the mesh network topology to view the clients currently online and blocked. Tap a device to obtain its information: name, IP and MAC address, and parental control profile. It also displays real-time traffic statistics as well as weekly traffic for the past days in a week for both download and upload data transmissions. The Priority function allows you to assign a High/Low priority for this device with effective duration: Always, 1 Day, 4 Hours, 2 Hours, or 1 Hour.

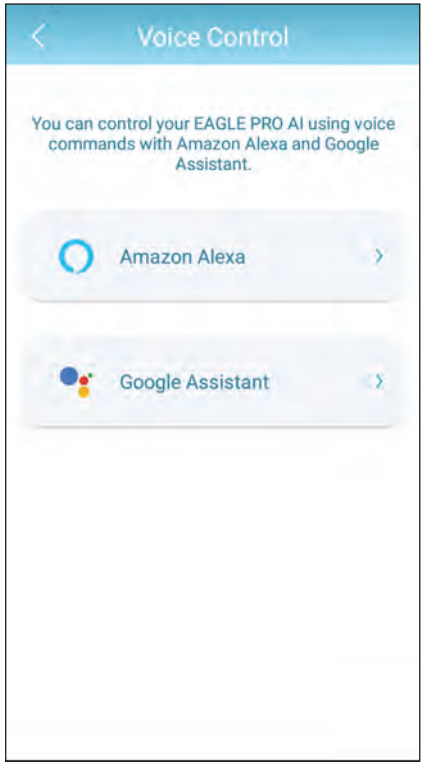


Extender Information

From **Home**, tap the **device (Extenders)** of the mesh network topology to view the extenders currently connected with the following information: name, IP and MAC address, and hardware and firmware version. Tap **Clients** to view its currently connected clients. You can also identify the device by flashing an LED indicator and restart the device on this screen.

Voice Control

With the R32, you can command your router's functionality with your voice through Amazon Alexa and the Google Assistant, enabling you to control your network with voice commands. Features include enabling and disabling your Wi-Fi guest zone without logging in to the web interface, rebooting the router, and checking your router for firmware upgrades. In order to use third-party services to control and manage your device, please register your device with D-Link Cloud Service first.



JUST ASK amazon alexa

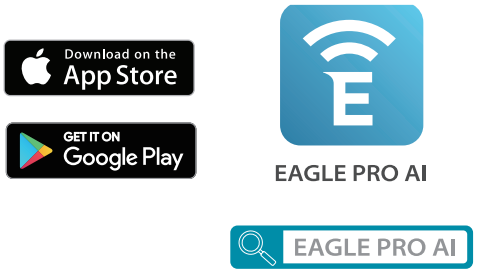
works with Ok Google

Link D-Link Cloud Service to Other Services

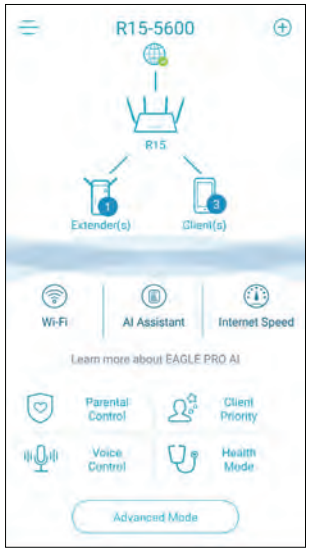
Google Home Setup

In order to use third-party apps to control and manage your device, you will first need to link your D-Link account with apps such as Google Assistant or Amazon Alexa.

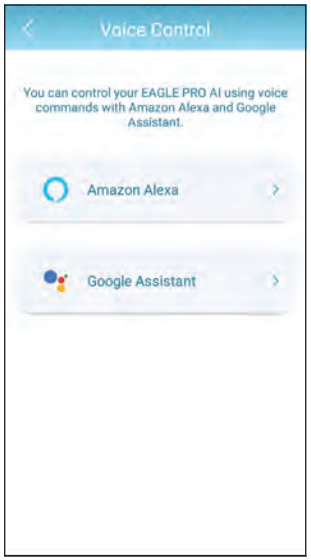
Step 1
Launch EAGLE PRO AI and go to the **Home** screen.



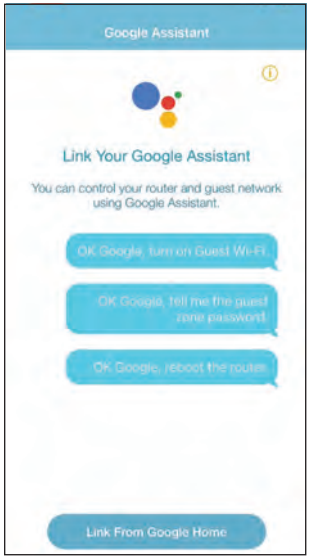
Step 2
Tap **Voice Control** from the **Home** screen.



Step 3
Choose the cloud service (e.g. Google Assistant).

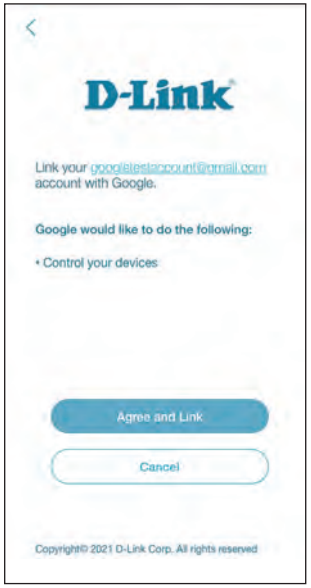


Step 4
Link with the Google Assistant.

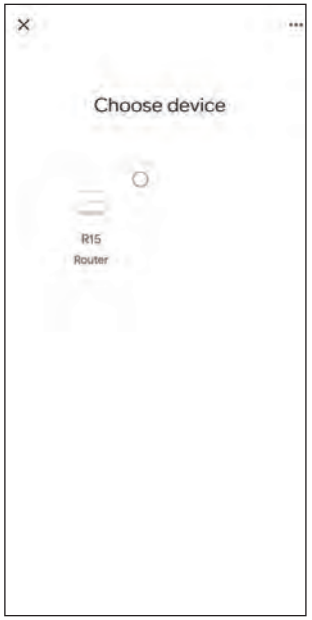


Step 5
The Google Home app will be launched.

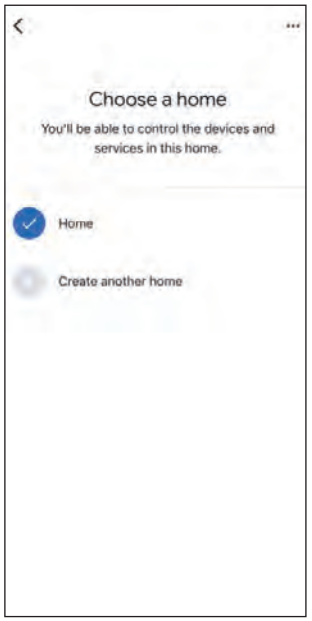
Step 6
Link your registered account with Google. Depending on your system, note that if the account link page does not display, please tap "+" on the top left from the above step to add the device manually:
Tap **+ Set up device**, choose **Works with Google**, and search for EAGLE PRO AI.
Then sign in using your registered D-Link account.



Step 7
Choose your device.



Step 8
Choose a home.



Step 9
Choose a location for your device.

Step 10
Device is now successfully set up with the Google Home.

Amazon Alexa Setup

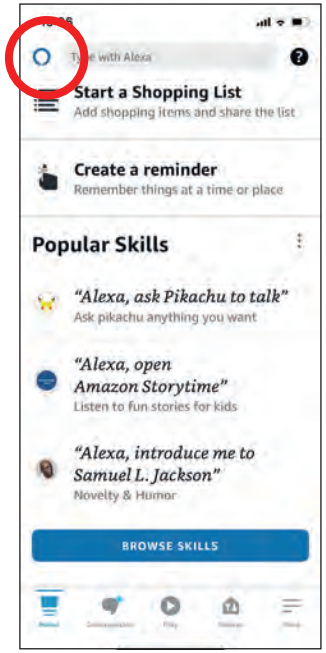
You will need the Amazon Alexa app, an Amazon account, and a D-Link account to use this feature.

Note: *The screenshots may be different depending on your mobile device's OS version. However, the process is the same.*

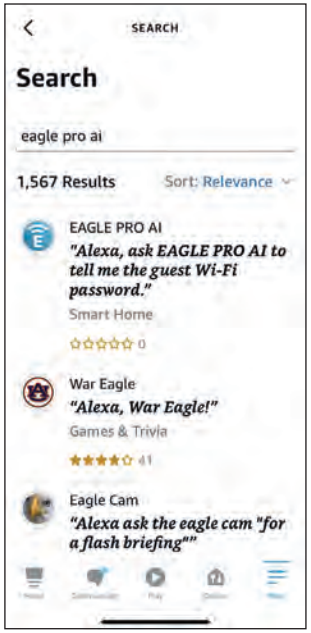
Step 1
Launch the **Amazon Alexa** app.

Amazon Alexa

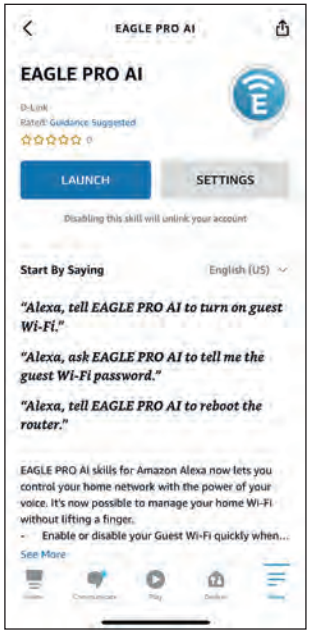
Step 2
Tap **Browse Skills**.



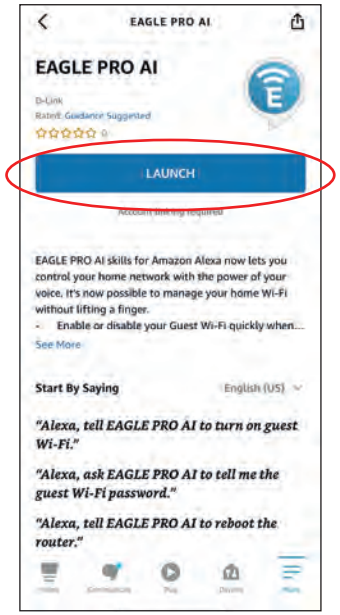
Step 3
Search EAGLE PRO AI for **Skills & Games**.



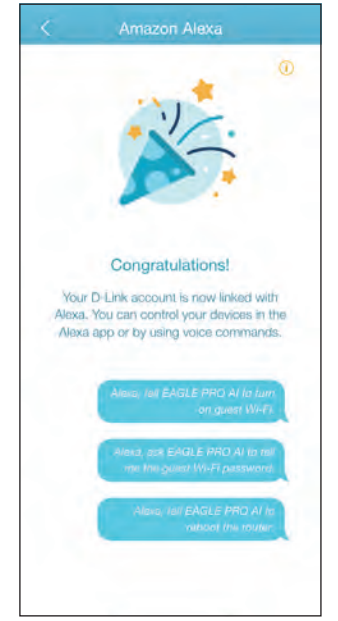
Step 4
The EAGLE PRO AI page.



Step 5
Tap **LAUNCH** to link the skill.



Step 6
Congratulations! **EAGLE PRO AI** has been successfully linked as a skill for your Amazon device. Refer to **Amazon Alexa Voice Commands** on the next page for tasks that you can ask your Amazon Alexa to perform.



Amazon Alexa Voice Commands

With **EAGLE PRO AI** enabled as a skill for Alexa, you can ask Alexa to do any of the following tasks. Before commanding Alexa, say "Open EAGLE PRO AI" and respond to Alexa's offering by saying "Help."

Task	Command
Enable the guest Wi-Fi	“Enable my guest Wi-Fi.”
Disable the guest Wi-Fi	“Disable my guest Wi-Fi.”
Find out your Wi-Fi SSID	"What is my Wi-Fi SSID?
Find out the guest Wi-Fi name and password	"What are my guest Wi-Fi credentials?"
Reboot the router	"Reboot my router."
Upgrade the router	"Upgrade my router.”
Obtain weekly report messages	"Read messages.”
Note: Network can be substituted for Wi-Fi.	

If using an Alexa speaker, start your command with one of the following:

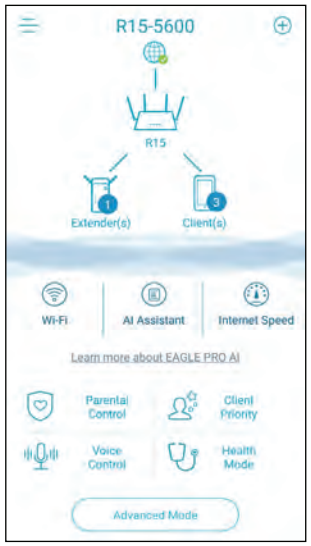
1. "Alex, ask EAGLE PRO AI to." For example, command Alexa by saying, " Alexa, ask EAGLE PRO AI to enable my guest Wi-Fi."
2. "Alex, talk to EAGLE PRO AI" and wait for Alexa to respond. Then say your command.

The Google Assistant Setup

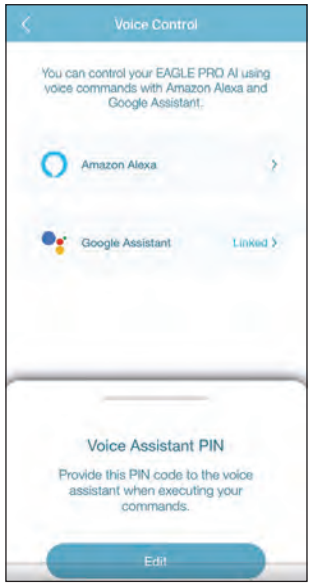
You will need the Google Assistant app, a Google account, and a D-Link Cloud Service account to use this feature.

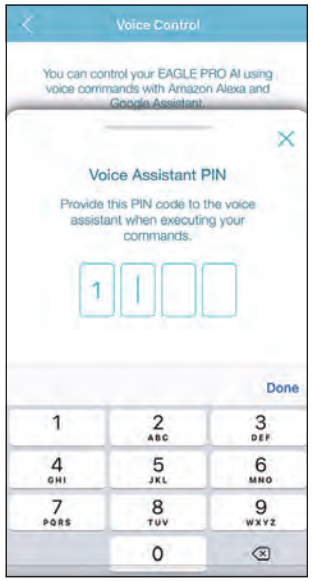
Note: *The screenshots may be different depending on your mobile device's OS version. However, the process is the same.*

Step 1
We will set up the pin code first for controls such as reboot and enable or disable guest Wi-Fi. Tap **Voice Control** from the **Home** screen of the EAGLE PRO AI app.



Step 2
Tap **Edit** to customize the pin code or use the randomly generated number.





Step 3
Launch the **Google Assistant** app.

Assistant

Step 4
Say or Type in your command and provide the pin code when being asked. Refer to **Google Assistant Voice Commands** on the next page for tasks that you can ask your Google Assistant to perform.

Google Assistant Voice Commands

With **EAGLE PRO AI** linked with the Google Assistant, you can ask your Google Assistant to do any of these tasks:

Task	Command
Check guest Wi-Fi status	"Is my guest Wi-Fi enabled?"
Check Wi-Fi status	"Is my Wi-Fi enabled?"
Check guest Wi-Fi SSID	"What is my guest Wi-Fi SSID?"
Check Wi-Fi SSID	"What is my Wi-Fi SSID?"
Enable the guest Wi-Fi	“Enable my guest Wi-Fi.”
Disable the guest Wi-Fi	“Disable my guest Wi-Fi.”
Find out the guest Wi-Fi password	"What is my guest Wi-Fi password?”[1]
Reboot the router	"Reboot my router."
Update the router	"Software update my router.”

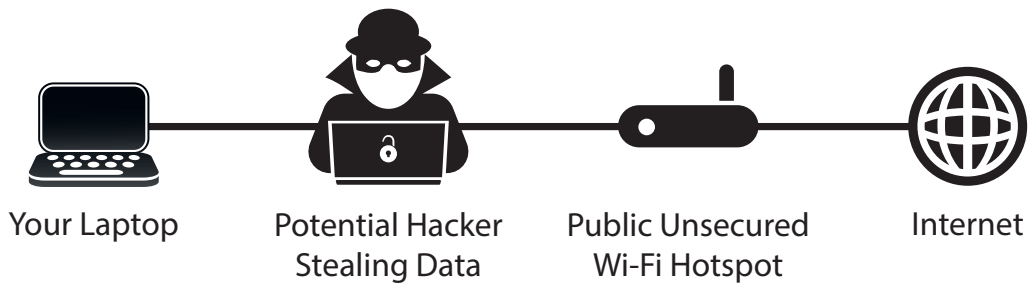
Notes:
1. Only supported on Nest Hub with screen display.
2. Network can be substituted for Wi-Fi.

If using a Google Home speaker, start your command by saying "Hey Google.”

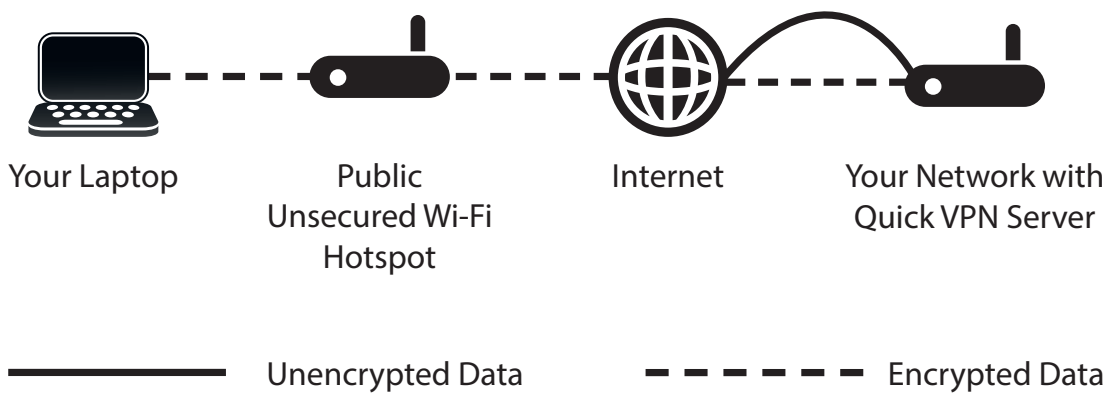
Quick VPN

This router is equipped with D-Link's Quick VPN technology. Virtual Private Networking (VPN) creates a connection between devices across the Internet. Using Quick VPN allows you to connect your computer or mobile device to places with free, untrusted Wi-Fi hotspots in places like coffee shops and hotels by encrypting and relaying it through your home Internet connection. This extra 'hop' reduces the chances of hackers stealing your information, such as logins, passwords, and credit card numbers. When traveling, Quick VPN lets you watch sports and use video streaming services without experiencing blackouts or filtering. You can surf the whole Internet just as you would at home.

Without Quick VPN



With Quick VPN



Important Information

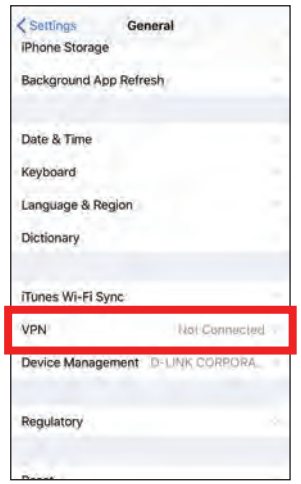
The following instructions explain and help you to configure your D-Link Quick VPN enabled router and devices to create a Virtual Private Network (VPN). This feature is provided for advanced users who wish to connect remotely and use their router's Internet connection to add a layer of security while using untrusted networks. Configure the Quick VPN Server on your router first and then set up client devices to connect through your router's WAN connection.

- Quick VPN only provides an added layer of security against specific types of snooping attacks and does not guarantee complete data integrity or protection. Only traffic in the tunnel between your router and device will be encrypted, WAN traffic will leave your D-Link Quick VPN enabled router unencrypted.
- Keep your Quick VPN Username, Password, and Passkey safe. Keep your Quick VPN Username, Password, and Passkey safe. It is recommended that you change these credentials periodically.
- A device connected via Quick VPN tunnel may experience lower data throughput and higher latency due to a number of factors including: Internet conditions, local and remote network Wi-Fi and WAN bandwidth limitations, and increased latency. This may negatively impact real time voice and video communication.
- Quick VPN supports up to five concurrent VPN client sessions using the same login and password are supported. Quick VPN uses L2TP/IPsec with MSCHAPv2, PAP, or CHAP authentication.
- You device may warn you that your information may be intercepted, since you control the Quick VPN server, you may ignore this.
- UDP Ports 500, 4500, 1701 and IP Port 50 must be open in order for Quick VPN to work.
- L2TP/IPsec VPN usage may be restricted in some countries and on some networks. If you have trouble using Quick VPN on some networks, but not others and are not violating network access rules, try contacting your ISP or network administrator.
- Devices connected via Quick VPN are assigned addresses on a separate subnet (ex. 192.168.1.x). Some network resources may be unavailable when connecting via Quick VPN.
- If your Internet connection uses DHCP, it is strongly recommended that you first set up Dynamic DNS (DDNS), such as D-Link DDNS, to eliminate the need to reconfigure client devices in the event your ISP assigns you a new WAN IP address.

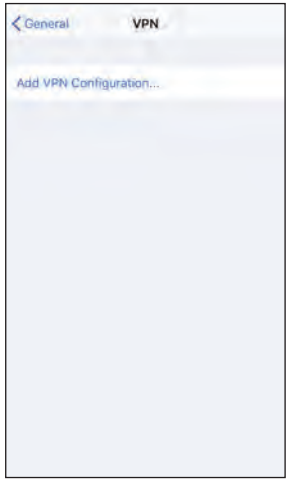
iOS Devices
VPN Setup Instructions

This section provides Quick VPN setup instructions for iOS devices. Refer to **Quick VPN** on page **83** for your router setup instructions.

Go into **Settings** on your compatible iOS device.
Scroll down and tap **General**.
Scroll down and tap **VPN**.



Tap **Add VPN Configuration...**



You should see a pop-up window asking you to fill out the details of your VPN connection.

Type: Choose **IPSec**. Tap **Back** to return to the Add Configuration page.

Description: For reference purposes only, used to differentiate between multiple VPN connections.

Server: Enter the IP/DDNS address of your Quick VPN server.

Account: Enter the Username used to authenticate login to VPN server

Password: Enter Password used to authenticate login to VPN server

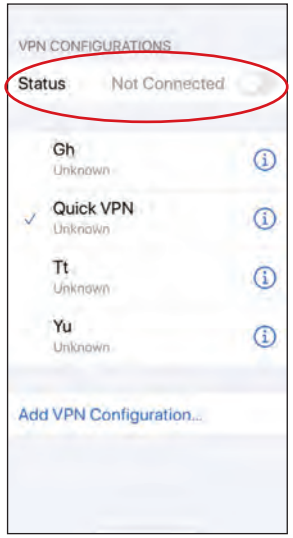
Secret: Enter your Pre-Shared Key (PSK).

Tap **Done** to close the configuration window.

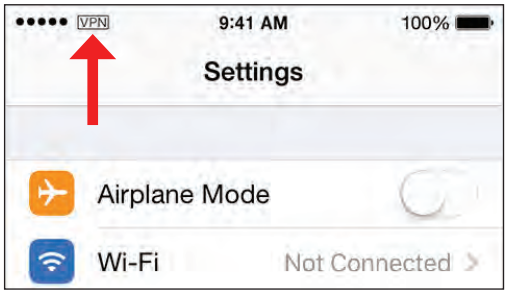
Your iOS device is now configured to connect to your Quick VPN server.

Connect or Disconnect

To connect or disconnect from to your Quick VPN server, go to **Settings** > **VPN** and tap the button next to **VPN Status**.



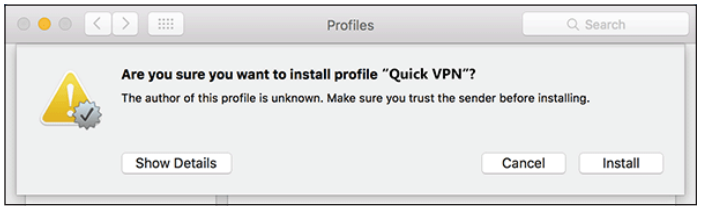
The VPN icon will appear in the notification area at the top of your screen indicating that your device is currently connected to the Quick VPN server.



Mac OS X
VPN Setup Instructions

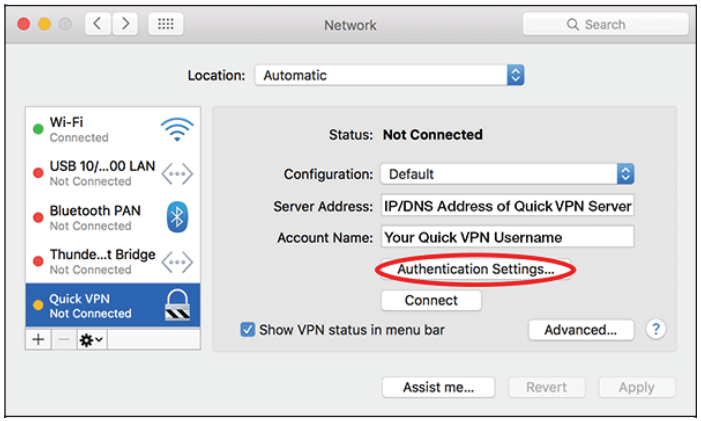
This section provides Quick VPN setup instructions for OS X using the **Export** Profile function. Refer to **Quick VPN** on page **83** for your router setup instructions.

Open the exported profile. The Install Profile dialogue will appear; click **Continue** and **Install**.

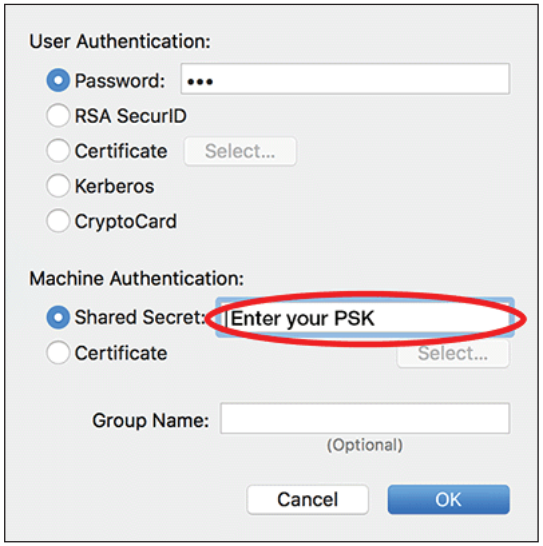


Enter your user account password when prompted. Close the **Profiles** dialogue.

Go to > **System Preferences**... > **Network** and select the Quick VPN connection and click **Authentication Settings**.



Enter your **Passkey** in the **Shared Secret** text box and click **OK, Apply,** then **OK**.

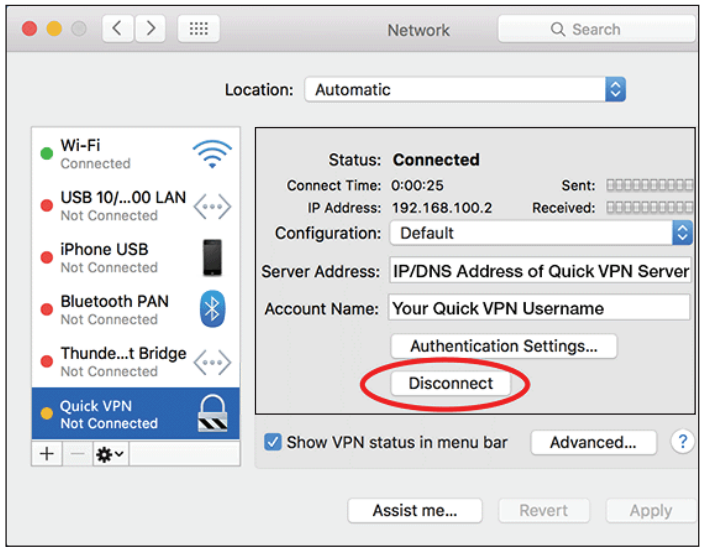


Your Mac is now configured to connect to your Quick VPN server.

Connect or Disconnect

To connect to or disconnect from your Quick VPN server, go to > **System Preferences**... > **Network**.

Select the Quick VPN connection and click on the **Connect** or **Disconnect** button.

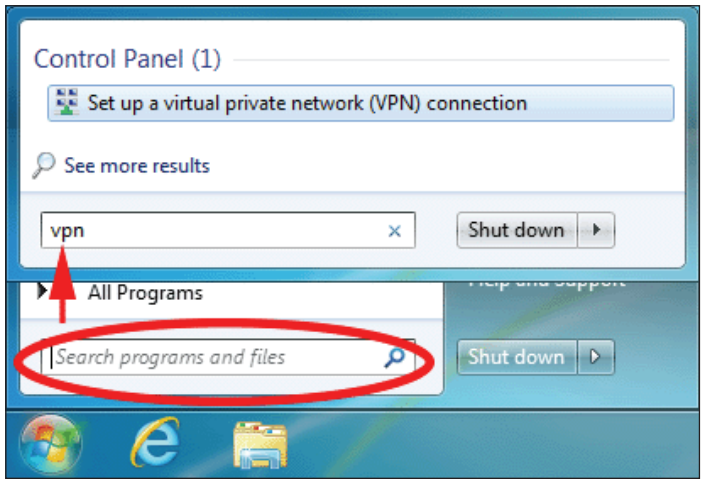


Windows 7
VPN Setup Instructions

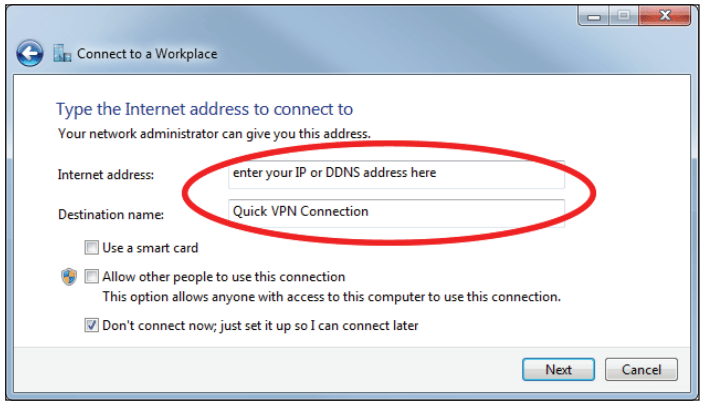
This section provides Quick VPN setup instructions for Windows 7. Refer to **Quick VPN** on page **83** for your router setup instructions.

Click the **Start** button and type **vpn** into the **Search programs and files** box.

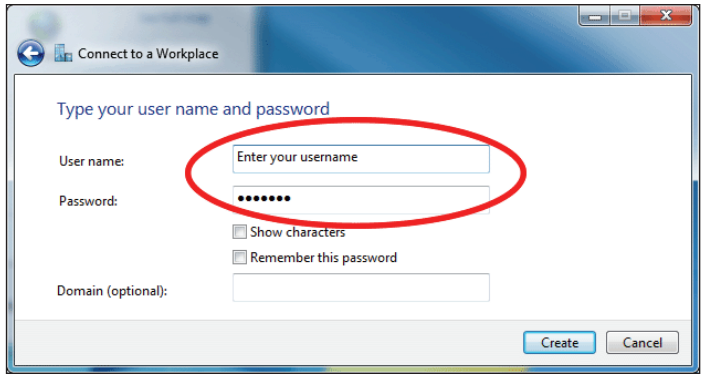
Select **Set up a virtual private network (VPN) connection.**



Enter the **IP/DDNS address** of your Quick VPN server in the **Internet address** box, create a name for your connection in the **Destination Name**, check **Don't Connect now; just set it up so I can connect later**, and click **Next**.

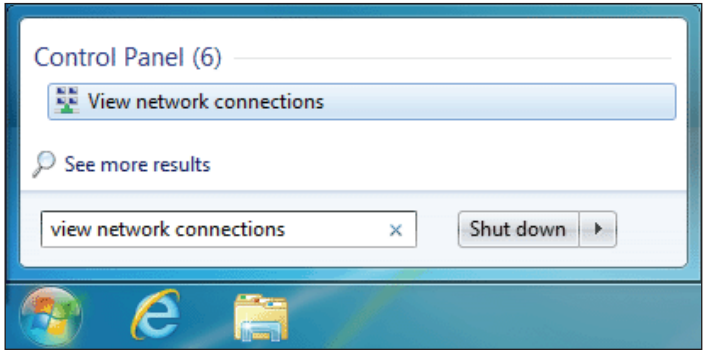


Enter your **Username**. If you would like windows to save your password, enter your **Password** and check **Remember this password**. Click **Create** to continue.



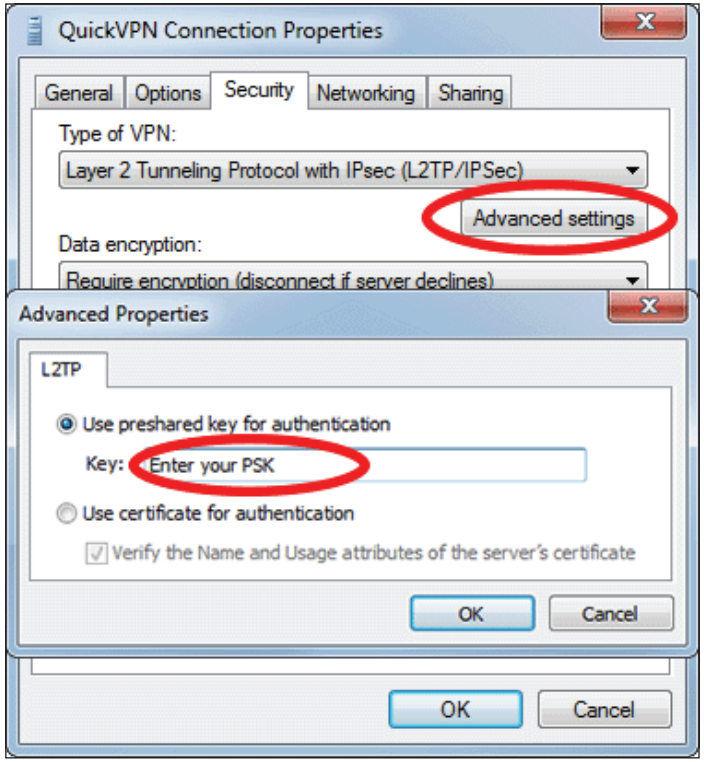
Do not click **Connect Now**.

Click **Close**. Click the **Start** button and type **view network connections** into the **Search programs and files** text box. Select **View network connections.**



Click **Advanced settings.** Enter your **Passkey** in the **Key** text box under **Use preshared key for authentication**. Click **OK** to close **Advanced Properties** and click **OK** to close **Quick VPN Connection Properties.**

Your Windows 7 system is now configured to connect to your Quick VPN server.



Connect or Disconnect

To connect to or disconnect from your Quick VPN server, click on the **Network Settings** icon in the notification area of the Windows taskbar and from the **Dial Up and VPN** section click on your Quick VPN connection and click on the **Connect** or **Disconnect** button.

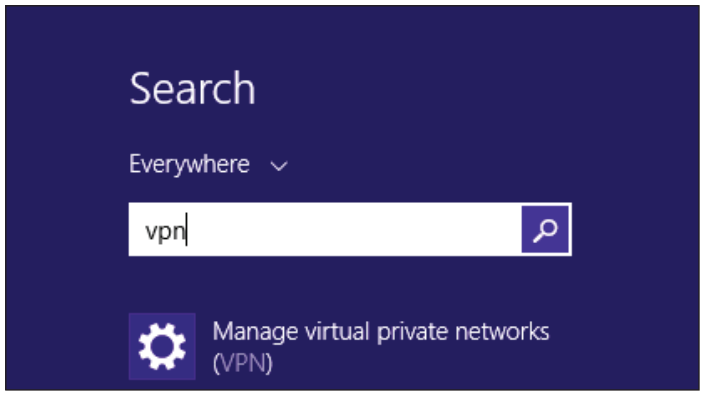
Windows 8.1/8
VPN Setup Instructions

This section provides Quick VPN setup instructions for Windows 8.1/8. Refer to **Quick VPN** on page **83** for your router setup instructions.

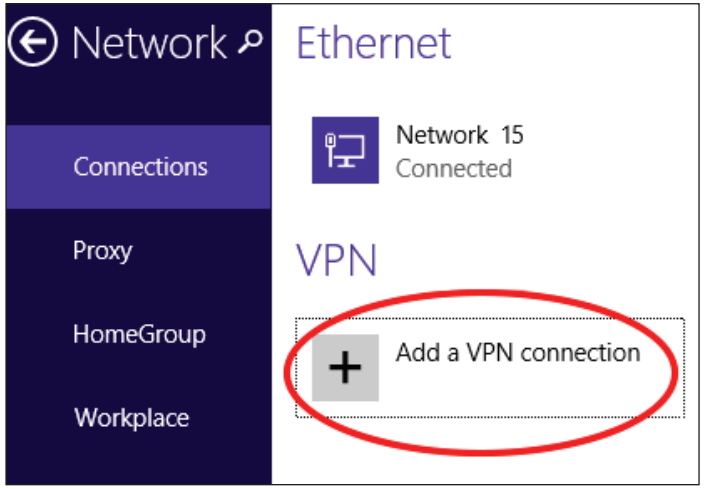
This section provides Quick VPN setup instructions for Windows 8.1/8.

Click the **Start** button and type **vpn**.

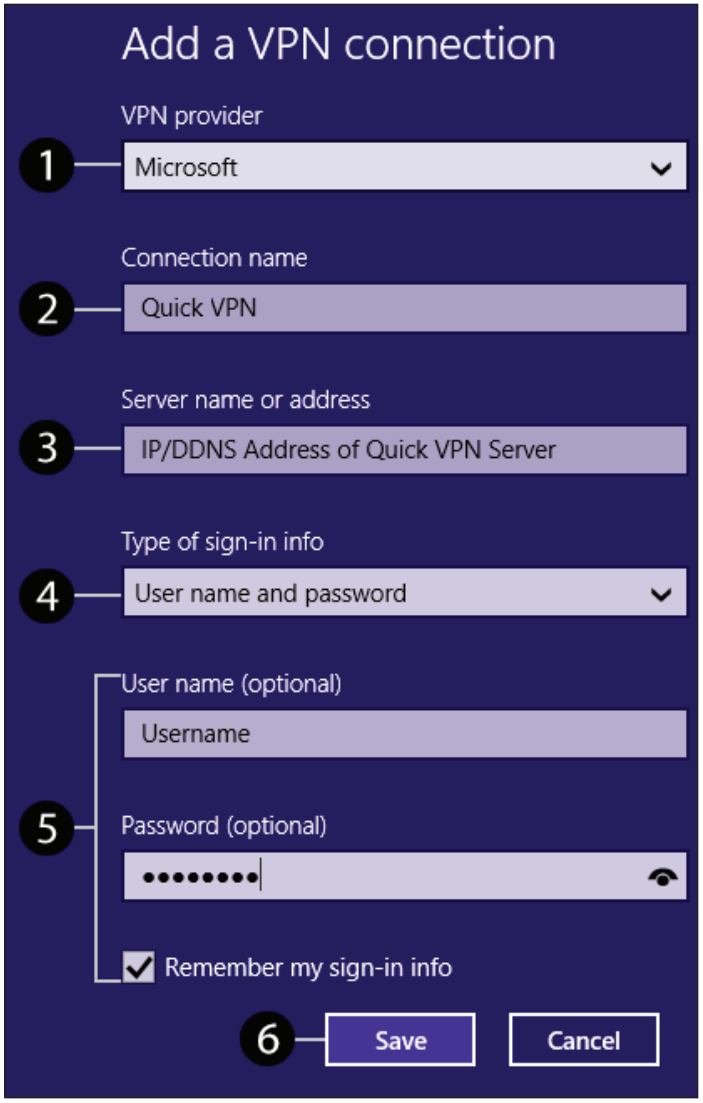
Select **Manage virtual private networks.**



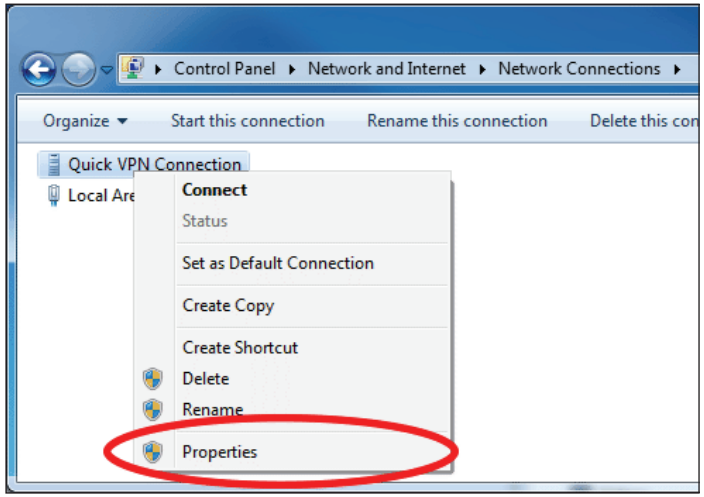
From the Network Settings page, click **Add a VPN Connection**.



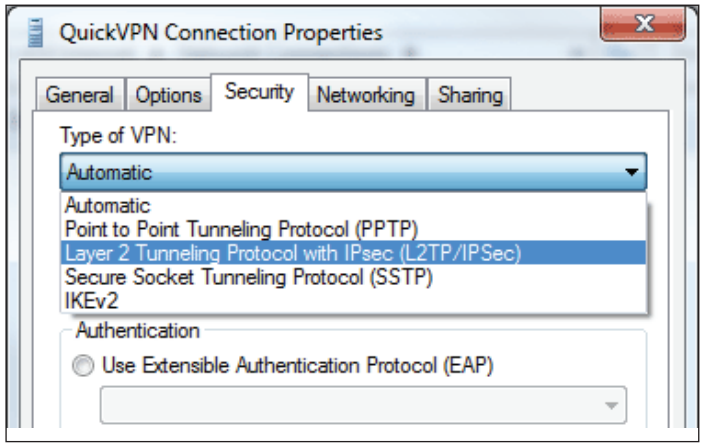
1. Select **Microsoft** from **VPN Provider**.
2. Create a name for your VPN connection.
3. Enter your **IP/DDNS address** of your Quick VPN server.
4. Select **User name and password** from **Type of sign-in info**.
5. If you would like windows to remember your sign-in information, enter your **User name, Password,** and select **Remember my sign-in info**
6. Choose **Save**.



Right-click on the Quick VPN Connection you just created and left-click on **Properties**.

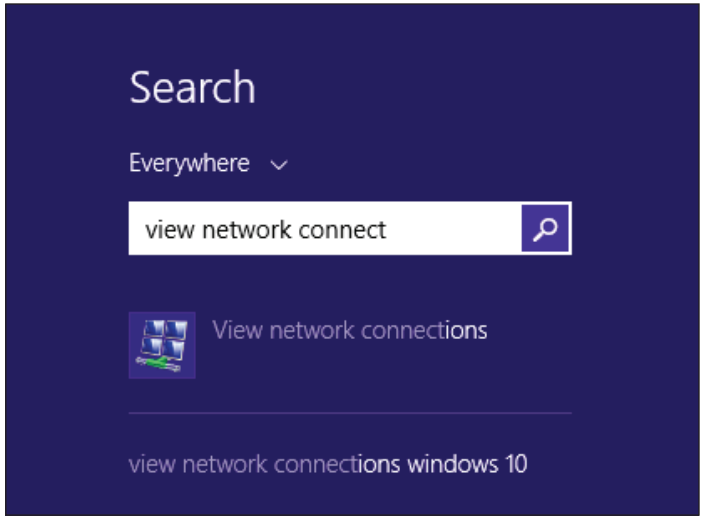


Select the **Security** tab. For the **Type of VPN**, select **Layer 2 Tunneling with IPsec (L2TP/IPSec).**



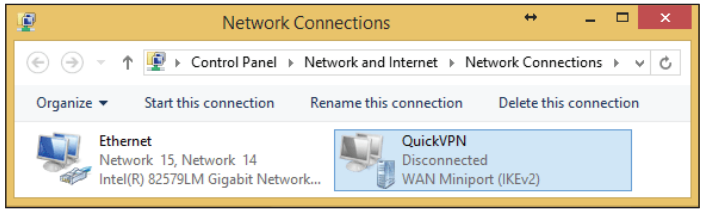
Click the **Start** button and type **view network connections**.

Select **View network connections.**



Right-click your **Quick VPN Connection** and left-click **Properties**.
Select the **Security** tab.

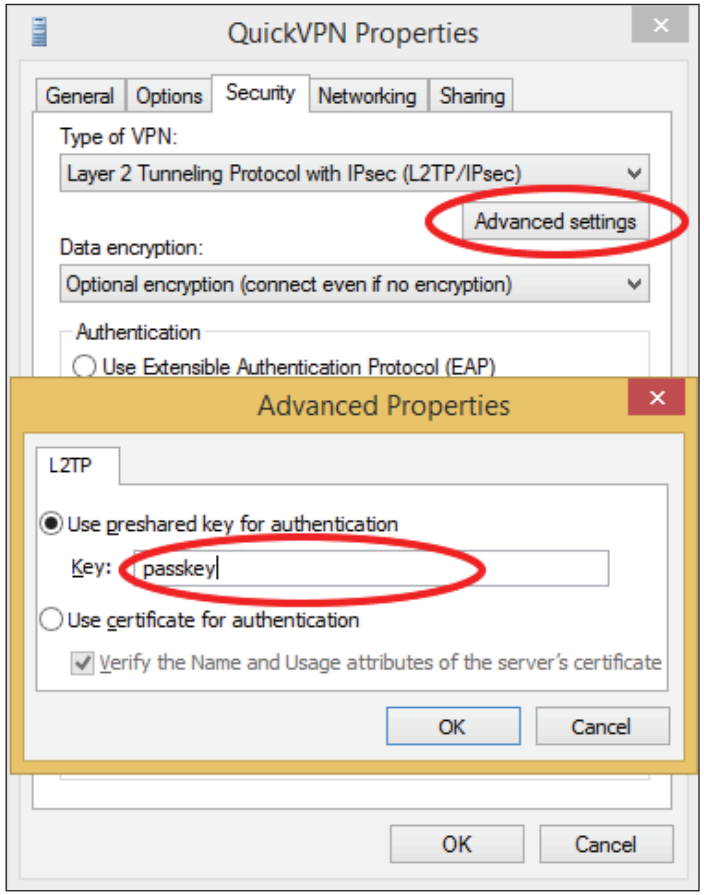
For the **Type of VPN**, select **Layer 2 Tunneling with IPsec (L2TP/IPSec).**



Click **Advanced settings.** Enter your **Passkey** in the **Key** text box under **Use preshared key for authentication**.

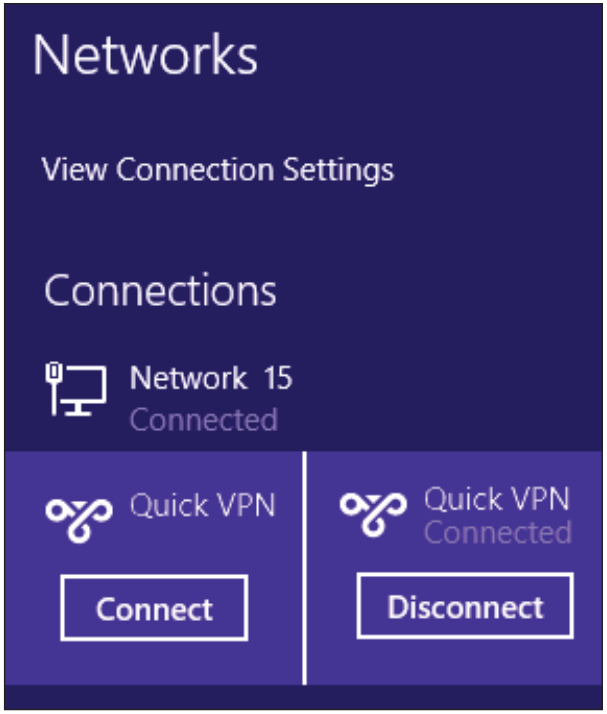
Click **OK** to close **Advanced Properties** and click **OK** to close **Quick VPN Properties.**

Your Windows 8.1/8 system is now configured to connect to your Quick VPN server.



Connect or Disconnect

To connect to or disconnect from your Quick VPN server, click on the **Network Settings** icon in the notification area of the Windows taskbar. Click on your Quick VPN connection and click on the **Connect** or **Disconnect** button.

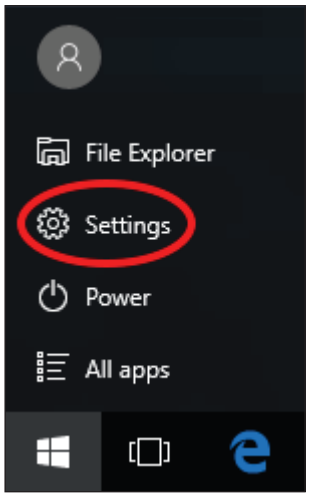


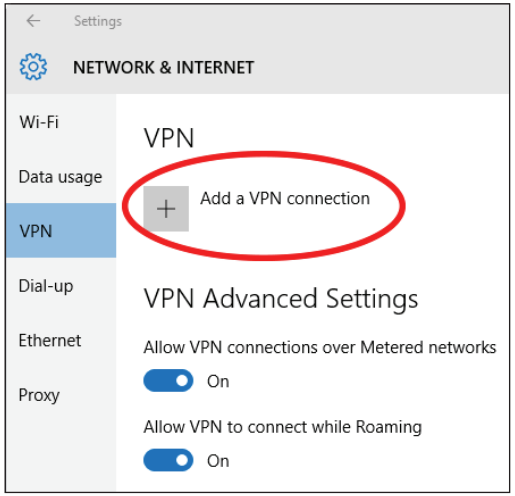
Windows 10
VPN Setup Instructions

This section provides Quick VPN setup instructions for Windows 10. Refer to **Quick VPN** on page **83** for your router setup instructions.

This section provides Quick VPN setup instructions for Windows 10.

Click **Start > Settings** > **Network & Internet** > **VPN > Add a VPN Connection**.



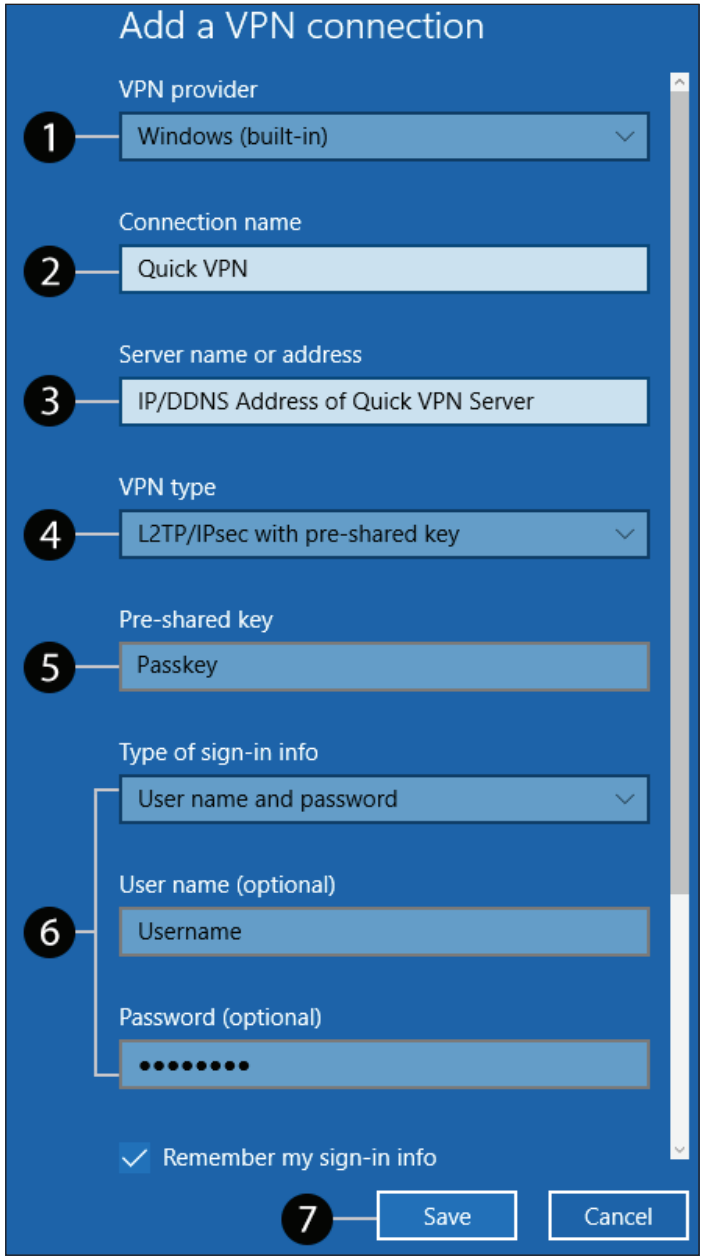


On the **Add a VPN connection** screen, do the following:

1. Select **Windows (built-in)** from the **VPN Provider** menu.
2. Create a name for your VPN connection.
3. Enter your **IP/DDNS address** of your Quick VPN server.
4. Select **L2TP/IPSec with pre-shared key** for **VPN type**.
5. Enter the **Passkey.**
6. Select **User name and password** from **Type of sign-in info**.

   If you would like windows to remember your sign-in information, enter your **User name, Password,** and select **Remember my sign-in info**
7. Choose **Save**.

Your Windows 10 system is now configured to connect to your Quick VPN server.

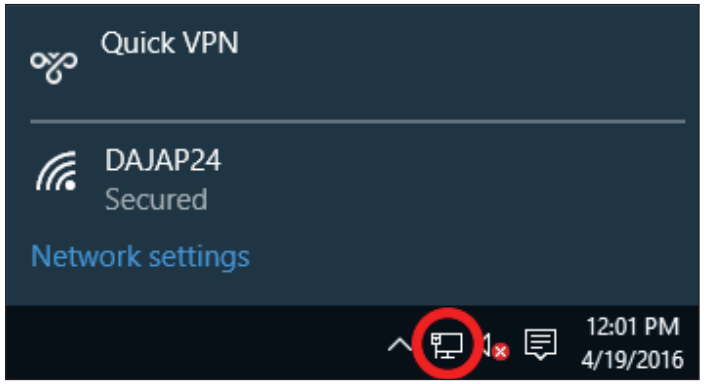


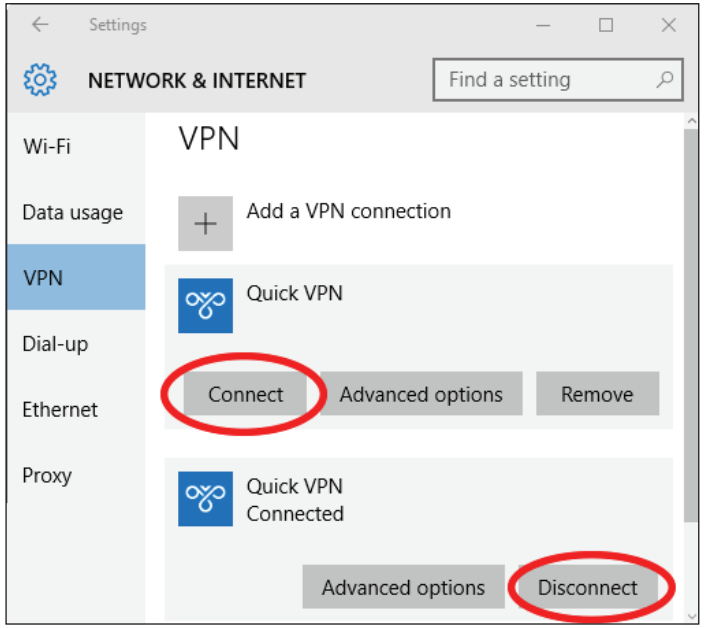
Connect or Disconnect

To connect to or disconnect from your Quick VPN server, click on the **Network Settings** icon (either or) in the notification area of the Windows taskbar and click on your Quick VPN connection.

The section of VPN in **Network & Internet Settings** page will open, select your Quick VPN, then select **Connect**. Or if the Connect button shows under the VPN connection, select **Connect**.

If connected, the VPN connection name will display **Connected** underneath it. You can click **Disconnect** to stop the connection.

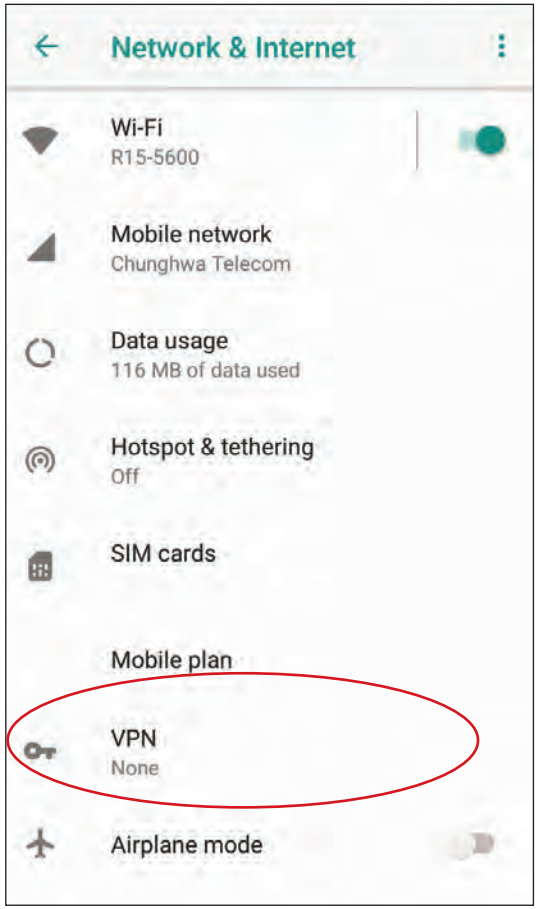




Android
VPN Setup Instructions

This section provides Quick VPN setup instructions for Android devices. Your device's screens may vary. Refer to **Quick VPN** on page **83** for your router setup instructions.

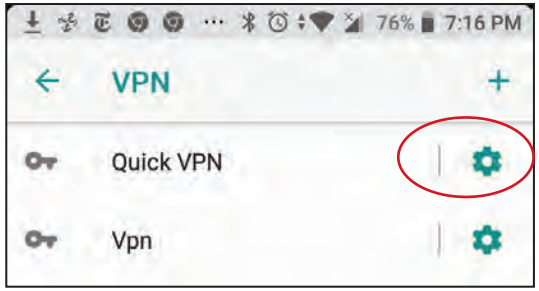
Go to **Settings** > **Network & Internet** > **VPN**

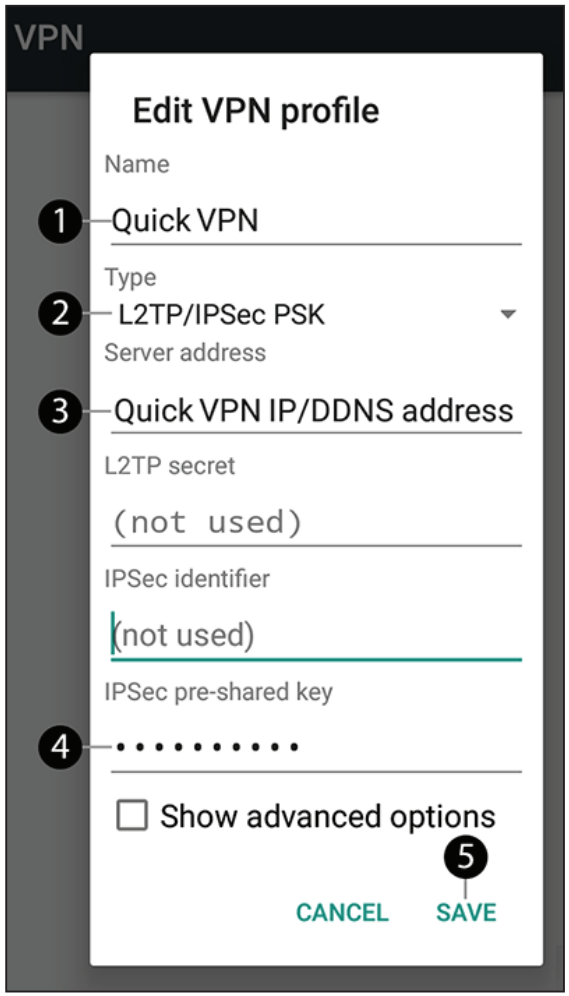


Tap **+** to create or **VPN Settings** to edit a VPN connection profile

1. Enter a name for your VPN connection.
2. Select **L2TP/IPSec** PSK for **Type.**
3. Enter the **IP/DDNS address** of your Quick VPN server.
4. Enter your **Passkey** in **IPSec pre-shared key** field.
5. Choose **Save**.

Your Android device is now configured to connect to your Quick VPN server.

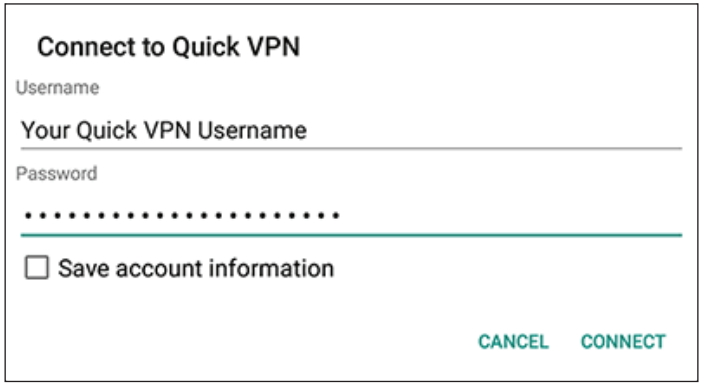




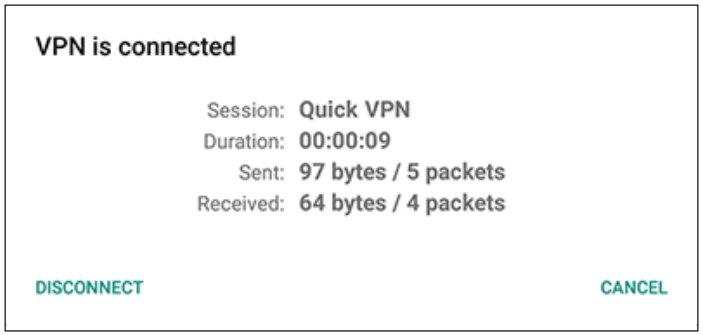
Connect or Disconnect

Tap the **Quick VPN** connection you created.

To connect, enter your **Username** and **Password,** then tap **CONNECT**.



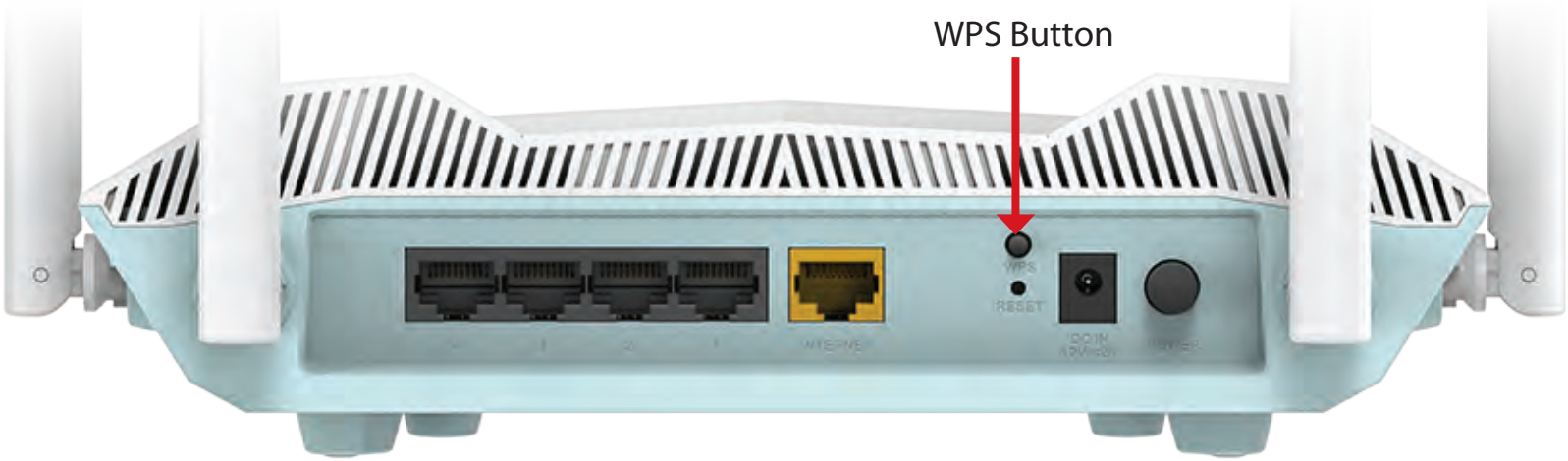
To disconnect, tap **DISCONNECT**.



Connect a Wireless Client to your Router
WPS Button

The easiest way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the router for about 1 second. The wireless LEDs will start to blink.



Step 2 - Within 2 minutes, press the WPS button on your wireless device (or launch the software utility and start the WPS process).

Step 3 - Allow up to 1 minute for your connection to be configured. Once the LEDs stop blinking, you will be connected using WPA2 encryption.

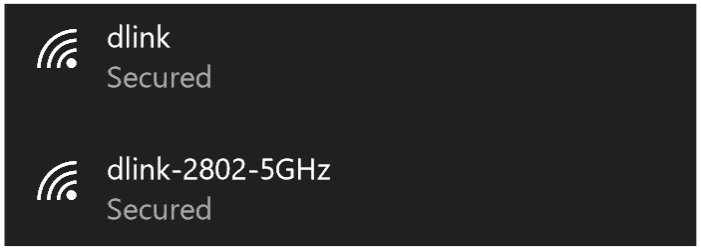
Windows® 10
WPA/WPA2/WPA3

Note: To enjoy the benefits offered by Wi-Fi 6 and WPA3, please make sure that your operating system and wireless network adapter support Wi-Fi 6.

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

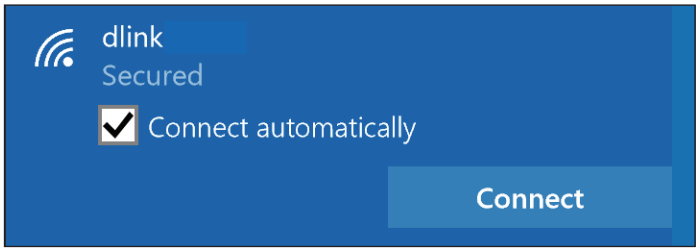
Wireless Icon

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

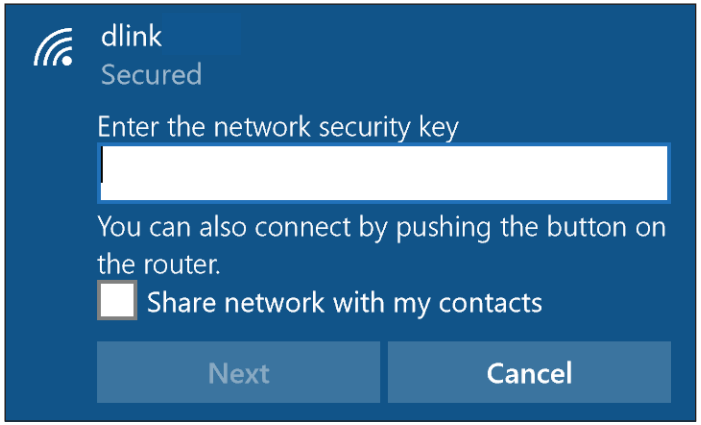


To connect to the SSID, click **Connect.**

To automatically connect with the router when your device next detects the SSID, check the **Connect Automatically** check box**.**



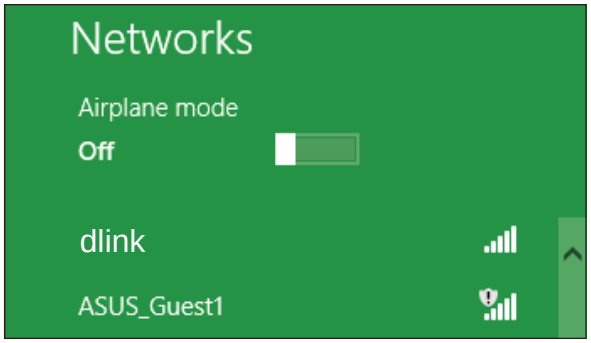
You will then be prompted to enter the Wi-Fi password (network security key) for the wireless network. Enter the password into the box and click **Next** to connect to the network. Your computer will now automatically connect to this wireless network when it is detected.



Windows® 8
WPA/WPA2

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

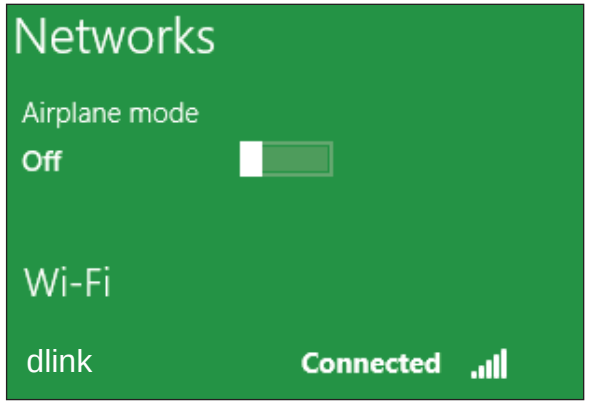
Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the extender's network by clicking on the network name.



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

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

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



Windows® 7
WPA/WPA2

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

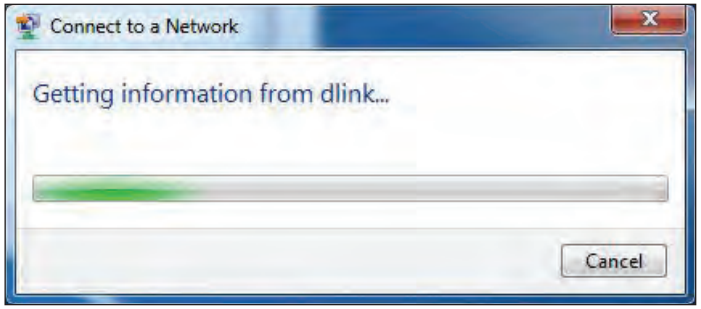
Click on the wireless icon in your system tray (lower-right corner).

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

Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page **146** for more information.

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



Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **OK**. You can also connect by pushing the WPS button on the router.

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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the router. Read the following descriptions if you are having problems.

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

When entering the IP address of the D-Link router (**192.168.0.1** for example), you are not connecting to a website, nor do you 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:

  - Microsoft Internet Explorer® 11 or higher
  - Mozilla Firefox 28 or higher
  - Google™ Chrome 28 or higher
  - Apple Safari 6 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 ZoneAlarm, BlackICE, Sygate and Norton Personal 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.

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

- If you still cannot access the configuration, unplug the power to the router 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 router. This process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the recessed button down until the power LED turns orange. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The address of the web configuration is printed on the device label on the bottom of the device. You may also enter the default IP address: **192.168.0.1**. When logging in, enter the default device password printed on the device label too.

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 allows you to 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 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 router 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.

How does wireless work?

Wireless works similarly to how cordless phones work, through radio signals that 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 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, university 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. This 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 has 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 Uses/Benefits

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

Small Office and Home Office Uses/Benefits

- 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 USB adapter with your laptop, you can access the hotspot to connect to the 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 router or access point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/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 or an extender to boost the signal to extend the range.

Extend and Strengthen Your Wireless Network with Wi-Fi Mesh

D-Link's Wi-Fi Mesh is a scalable solution that allows you to easily increase the coverage and eliminate weak spots of your wireless AX network. Setup is effortless; configuration of multiple routers and extenders can be done in minutes as settings can be passed on to other devices once the first is configured. And routing is more efficient and reliable since mesh network intelligently finds the shortest path and reroutes data traffic through working mesh points in the event of link or device failures.

Eliminate Interference

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

Wireless Encryption

Don't let your next-door neighbors or intruders connect to your wireless network. Encrypt your wireless network with the latest WPA3 security protocol. Refer to the product manual for detail information on how to set it up.

Networking Basics

Check your IP address

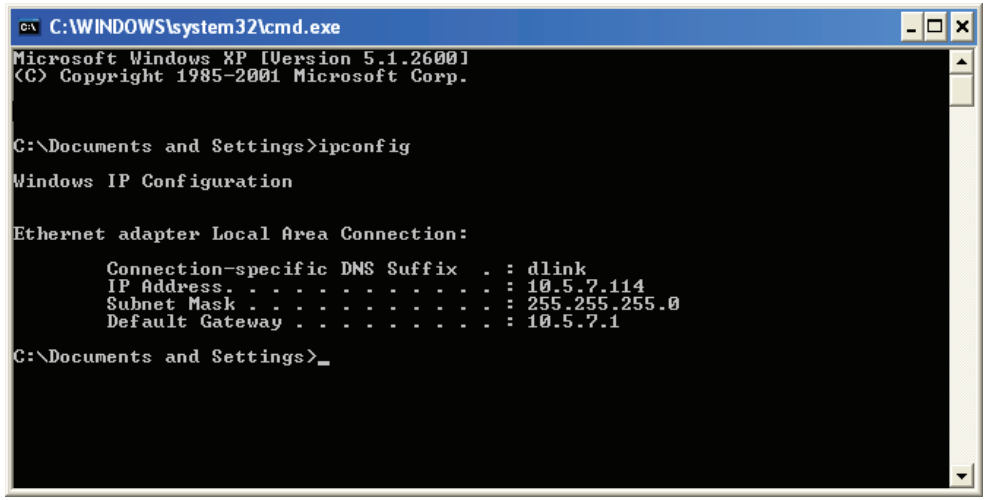
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start** and type *cmd* in the **Search** box.

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



Statically Assign an IP address

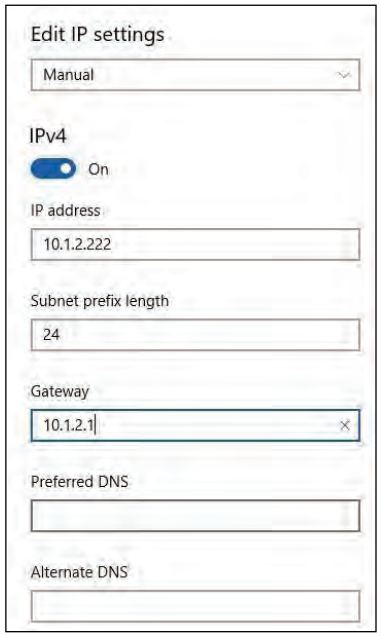
1. If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Windows® 10	Start> Settings > Network & Internet.
Windows® 7 /8	Start > Control Panel > Network and Internet > Network and Sharing Center
Windows® XP	Start > Control Panel > Network Connections

2. Select **Wi-Fi > Manage known networks**. For Windows 7/8/XP, click **Change adapter settings.** Choose the network you want to modify, right-click on it, then select **Properties.**

3. Under **IP assignment**, select **Edit**. For Windows 7/8/XP, select **Internet Protocol Version 4 (TCP/IPv4) Properties** or **Internet Protocol Version 6 Properties (TCP/IPv6)**. Then select **Use the Following IP Address**.

4. Under **Edit IP settings**, select **Manual**. If IPv4 is selected, type the IP address settings in **IP address, Subnet prefix length** (subnet mask), and **Gateway** fields. If IPv6 is selected, type the IP address settings in **IP address, Subnet prefix length,** and **Gateway** fields.



Example: Enter x.x.x.x for IPv4 addressing scheme (where x is between 0 and 255) and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx for IPv6 addressing scheme (where x is a hexadecimal digit).

Set Preferred DNS the same as the LAN IP address of your router.
The Alternate DNS is only optional or you may enter a DNS server from your ISP.

5. When you're done, click **Save**.

Wireless Security

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

- WPA3 (Wi-Fi Protected Access 3)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)
- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)

What is WPA?

WPA (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/WPA3-SAE 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 router or access point. Further, The Simultaneous Authentication of Equals (SAE) of WPA3 enhances the protection against dictionary attacks.

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.

WPA3 has the strongest encryption among these with the increased cryptographic capability and the requirements of the Protected Management Frames (PMFs) to help prevent snooping attacks.

Technical Specifications

Device Interfaces
- Wireless Interface (2.4 GHz): IEEE 802.11n/g/b
- Wireless Interface (5 GHz): IEEE 802.11ax/ac/n/a
- One 10/100/1000 Mbps WAN port
- Four 10/100/1000 Mbps LAN port

Standards
- IEEE 802.11ax[1,2,3]
- IEEE 802.11ac[1,2,3]
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.1p/q (WAN)
- IEEE802.3x
- IEEE 802.11h
- IEEE 802.11k/v
- IEEE 802.11n/g/b/a

Antenna Types
- Four external antennas

Security
- WPA3/WPA2/WPA-Personal
- Wi-Fi Protected Setup (WPS)

WAN Connection Type
- Static IP
- Dynamic IP
- PPPoE
- PPTP
- L2TP
- DS-Lite

Power
- Input: 100 to 240 V AC, 50 / 60 Hz
- Output: 12 V, 2A

Temperature
- Operating: 0 to 40 °C (32 to 104 °F)
- Storage: -20 to 65 °C (-4 to 149 °F)

Humidity
- Operating: 10% to 90% maximum, non-condensing
- Storage: 5% to 95% maximum, non-condensing

Certifications
- IC
- FCC
- CE

Dimensions
- L x W x H: 228.23 x 158.99 x 61.57 mm

The marking information is located at the bottom of the apparatus.

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

[2] Frequency Range varies depending on country's regulation.

[3] The router does not include 5.25-5.35 GHz & 5.47-5.725 GHz in some regions.

Regulatory Statements

Federal Communication Commission Interference 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 communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

Non-modifications Statement:

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

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

Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Note

The country code selection is for non-USA models only and is not available to all USA models. Per FCC regulations, all WiFi product marketed in the USA must be fixed to USA operational channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement

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

Innovation, Science and Economic Development Canada (ISED) Statement:

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Innovation, Science and Economic Development Canada (ISED) Statement:

This device complies with ISED licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

This radio transmitter FCC ID: KA2R32A1 has been approved by FCC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna List

No.	Manufacturer	Part No.	Antenna Type	Peak Gain
1	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz
2	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz
3	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz
4	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz

Caution :

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and

(iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;

(iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement

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

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This radio transmitter IC: 4216A-R32A1 has been approved by ISED Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Cet émetteur radio IC: 4216A-R32A1 a été approuvé par ISED Canada pour fonctionner avec les types d'antennes énumérés ci-dessous avec le gain maximal admissible et impédance d'antenne requise pour chaque type d'antenne indiqué. Types d'antennes n'est pas inclus dans cette liste, ayant un gain supérieur au gain maximal indiqué pour ce type, sont strictement interdits pour une utilisation avec cet appareil.

Antenna List

No.	Manufacturer	Part No.	Antenna Type	Peak Gain
1	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz
2	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz
3	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz
4	LYNwave	AOX21X-221051-00	Dipole	5.1dBi for 2.4GHz 5.3dBi for 5GHz

CE

	Frequency Band(s) **Frequenzband** **Fréquence bande(s)** **Bandas de Frecuencia** **Frequenza/e** **Frequentie(s)**	**Max. Output Power (EIRP)** **Max. Output Power** **Consommation d'énergie max.** **Potencia máxima de Salida** **Potenza max. Output** **Max. Output Power**
5 G	5.15 – 5.25 GHz	200 mW
	5.25 – 5.35 GHz	200 mW
	5.47 – 5.725 GHz	1 W
2.4 G	2.4 – 2.4835 GHz	100 mW

European Community Declaration of Conformity:

Česky [Czech]	Tímto D-Link Corporation prohlašuje, že tento produkt, jeho příslušenství a software jsou v souladu se směrnicí 2014/53/EU. Celý text ES prohlášení o shodě vydaného EU a o firmwaru produktu lze stáhnout na stránkách k produktu www.dlink.com.
Dansk [Danish]	D-Link Corporation erklærer herved, at dette produkt, tilbehør og software er i overensstemmelse med direktiv 2014/53/EU. Den fulde tekst i EU-overensstemmelseserklæringen og produktfirmware kan wnloades fra produktsiden hos www.dlink.com.
Deutsch [German]	Hiermit erklärt die D-Link Corporation, dass dieses Produkt, das Zubehör und die Software der Richtlinie 2014/53/EU entsprechen. Der vollständige Text der Konformitätserklärung der Europäischen Gemeinschaft sowie die Firmware zum Produkt stehen Ihnen zum Herunterladen von der Produktseite im Internet auf www.dlink.com zur Verfügung.
Eesti [Estonian]	Käesolevaga kinnitab D-Link Corporation, et see toode, tarvikud ja tarkvara on kooskõlas direktiiviga 2014/53/EL. Euroopa Liidu vastavusdeklaratsiooni täistekst ja toote püsivara on allalaadimiseks saadaval tootelehel www.dlink.com.
English	Hereby, D-Link Corporation, declares that this product, accessories, and software are in compliance with directive 2014/53/EU. The full text of the EU Declaration of Conformity and product firmware are available for download from the product page at www.dlink.com
Español [Spanish]	Por la presente, D-Link Corporation declara que este producto, accesorios y software cumplen con las directivas 2014/53/UE. El texto completo de la declaración de conformidad de la UE y el firmware del producto están disponibles y se pueden descargar desde la página del producto en www.dlink.com.
Ελληνική [Greek]	Με την παρούσα, η D-Link Corporation δηλώνει ότι αυτό το προϊόν, τα αξεσουάρ και το λογισμικό συμμορφώνονται με την Οδηγία 2014/53/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ και το υλικολογισμικό του προϊόντος είναι διαθέσιμα για λήψη από τη σελίδα του προϊόντος στην τοποθεσία www.dlink.com.
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit, ces accessoires et ce logiciel sont conformes aux directives 2014/53/UE.Le texte complet de la déclaration de conformité de l'UE et le icroprogramme du produit sont disponibles au téléchargement sur la page des produits à www.dlink.com.
Italiano [Italian]	Con la presente, D-Link Corporation dichiara che questo prodotto, i relativi accessori e il software sono conformi alla direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE e il firmware del prodotto sono disponibili per il download dalla pagina del prodotto su www.dlink.com.

Latviski [Latvian]	Ar šo uzņēmums D-Link Corporation apliecina, ka šis produkts, piederumi un programmatūra atbilst direktīvai 2014/53/ES. ES atbilstības deklarācijas pilno tekstu un produkta aparātprogrammatūru var lejupielādēt attiecīgā produkta lapā vietnē www.dlink.com.
Lietuvių [Lithuanian]	Šiuo dokumentu „D-Link Corporation“ pareiškia, kad šis gaminys, priedai ir programinė įranga atitinka direktyvą 2014/53/ES. Visą ES atitikties deklaracijos tekstą ir gaminio programinę aparatinę įrangą galima atsisiųsti iš gaminio puslapio adresu www.dlink.com.
Nederlands [Dutch]	Hierbij verklaart D-Link Corporation dat dit product, accessoires en software voldoen aan de richtlijnen 2014/53/EU. De volledige tekst van de EU conformiteitsverklaring en productfirmware is beschikbaar voor download van de productpagina op www.dlink.com.
Malti [Maltese]	Bil-preżenti, D-Link Corporation tiddikjara li dan il-prodott, l-aċċessorji, u s-software huma konformi mad-Direttiva 2014/53/UE. Tista' tniżżel it-test sħiħ tad-dikjarazzjoni ta' konformità tal-UE u l-firmware tal-prodott mill-paġna tal-prodott fuq www.dlink.com.
Magyar [Hungarian]	Ezennel a D-Link Corporation kijelenti, hogy a jelen termék, annak tartozékai és szoftvere megfelelnek a 2014/53/EU sz. rendeletek rendelkezéseinek. Az EU Megfelelőségi nyilatkozat teljes szövege és a termék firmware a termék oldaláról tölthető le a www.dlink.com cím en.
Polski [Polish]	D-Link Corporation niniejszym oświadcza, że ten produkt, akcesoria oraz oprogramowanie są zgodne z dyrektywami 2014/53/EU. Pełen tekst deklaracji zgodności UE oraz oprogramowanie sprzętowe do produktu można pobrać na stronie produktu w witrynie www.dlink.com.
Português [Portuguese]	Desta forma, a D-Link Corporation declara que este produto, os acessórios e o software estão em conformidade com a diretiva 2014/53/UE. O texto completo da declaração de conformidade da UE e do firmware
Slovensko[Slovenian]	Podjetje D-Link Corporation s tem izjavlja, da so ta izdelek, dodatna oprema in programnska oprema skladni z direktivami 2014/53/EU. Celotno besedilo izjave o skladnosti EU in vdelana programska oprema sta na voljo za prenos na strani izdelka na www.dlink.com.
Slovensky [Slovak]	Spoločnosť D-Link týmto vyhlasuje, že tento produkt, príslušenstvo a softvér sú v súlade so smernicou 214/53/EÚ. Úplné znenie vyhlásenia EÚ o zhode a firmvéri produktu sú k dispozícii na prevzatie zo stránky produktu www.dlink.com.
Suomi [Finnish]	D-Link Corporation täten vakuuttaa, että tämä tuote, lisävarusteet ja ohjelmisto ovat direktiivin 2014/53/EU vaatimusten mukaisia. Täydellinen EU-vaatimustenmukaisuusvakuutus samoin kuin tuotteen laiteohjelmisto ovat ladattavissa osoitteesta www.dlink.com.
Svenska[Swedish]	D-Link Corporation försäkrar härmed att denna produkt, tillbehör och programvara överensstämmer med direktiv 2014/53/EU. Hela texten med EU-försäkran om överensstämmelse och produkt-firmware kan hämtas från produktsidan på www.dlink.com.

Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisyfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á www.dlink.com.
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på www.dlink.com.

Warning Statement:

The equipment supplied by an approved external power adapter which is considered to be Pluggable Equipment Type A. The socket outlets shall be installed near the equipment and be easily accessible.

NCC :
「取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。」

5G產品
應避免影響附近雷達系統之操作。
高增益指向性天線只得應用於固定式點對點系統。

“電磁波曝露量MPE標準值1mW/cm^2，送測產品實測值為：0.6248 mW/cm^2”

NOTICE OF WIRELESS RADIO LAN USAGE IN THE EUROPEAN COMMUNITY (FOR WIRELESS PRODUCT ONLY):

- This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries. This equipment may be operated in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, and CY.

Usage Notes:

- To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
- This device is restricted from functioning in Ad-hoc mode while operating in 5 GHz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
- Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality as required when operating in 5 GHz band within the EU.
- Please refer to the product manual or datasheet to check whether your product uses 2.4 GHz and/or 5 GHz wireless.

HINWEIS ZUR VERWENDUNG VON DRAHTLOS-NETZWERK (WLAN) IN DER EUROPÄISCHEN GEMEINSCHAFT (NUR FÜR EIN DRAHTLOSES PRODUKT)

- Der Betrieb dieses Geräts in der Europäischen Gemeinschaft bei Nutzung von Kanälen im 5,15-5,35 GHz Frequenzband ist ausschließlich auf Innenräume beschränkt, um das Interferenzpotential zu reduzieren.
- Bei diesem Gerät handelt es sich um ein zum Einsatz in allen EU-Mitgliedsstaaten und in EFTA-Ländern - ausgenommen Frankreich. Der Betrieb dieses Geräts ist in den folgenden Ländern erlaubt: AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebrauchshinweise:

- Um den in Europa geltenden nationalen Vorschriften zum Nutzen des Funkspektrums weiterhin zu entsprechen, werden Frequenz und Kanalbeschränkungen, dem jeweiligen Land, in dem das Gerät zum Einsatz kommt, entsprechend, auf die Produkte angewandt.
- Die Funktionalität im Ad-hoc-Modus bei Betrieb auf 5 GHz ist für dieses Gerät eingeschränkt. Bei dem Ad-hoc-Modus handelt es sich um eine Peer-to-Peer-Kommunikation zwischen zwei Client-Geräten ohneeinen Access Point.
- Access Points unterstützen die Funktionen DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) wie erforderlich bei Betrieb auf 5 GHz innerhalb der EU.
- Bitte schlagen Sie im Handbuch oder Datenblatt nach nach, ob Ihr Gerät eine 2,4 GHz und / oder 5 GHz Verbindung nutzt.

AVIS CONCERNANT L'UTILISATION DE LA RADIO SANS FIL LAN DANS LA COMMUNAUTÉ EUROPÉENNE (UNIQUEMENT POUR LES PRODUITS SANS FIL)

- Cet appareil est limité à un usage intérieur lorsqu'il est utilisé dans la Communauté européenne sur les canaux de la bande de 5,15 à 5,35 GHz afin de réduire les risques d'interférences.
- Cet appareil est un système de transmission à large bande (émetteur-récepteur) de 2,4 GHz, destiné à être utilisé dans tous les États-membres de l'UE et les pays de l'AELE. Cet équipement peut être utilisé dans les pays suivants : AL, AD, BE , BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT , MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notes d'utilisation:

- Pour rester en conformité avec la réglementation nationale européenne en matière d'utilisation du spectre, des limites de fréquence et de canal seront appliquées aux produits selon le pays où l'équipement sera déployé.
- Cet appareil ne peut pas utiliser le mode Ad-hoc lorsqu'il fonctionne dans la bande de 5 GHz. Le mode Adhoc fournit une communication directe pair à pair entre deux périphériques clients sans point d'accès.
- Les points d'accès prendront en charge les fonctionnalités DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control) au besoin lors du fonctionnement dans la bande de 5 GHz au sein de l'UE.
- Merci de vous référer au guide d'utilisation ou de la fiche technique afin de vérifier si votre produit utilise 2.4 GHz et/ou 5 GHz sans fil.

AVISO DE USO DE LA LAN DE RADIO INALÁMBRICA EN LA COMUNIDAD EUROPEA (SOLO PARA EL PRODUCTO INALÁMBRICO)

- El uso de este dispositivo está restringido a interiores cuando funciona en la Comunidad Europea utilizando canales en la banda de 5,15-5,35 GHz, para reducir la posibilidad de interferencias.
- Este dispositivo es un sistema de transmisión (transceptor) de banda ancha de 2,4 GHz, pensado para su uso en todos los estados miembros de la UE y en los países de la AELC. Este equipo se puede utilizar en AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notas de uso:

- Para seguir cumpliendo las normas europeas de uso del espectro nacional, se aplicarán limitaciones de frecuencia y canal en los productos en función del país en el que se pondrá en funcionamiento el equipo.
- Este dispositivo tiene restringido el funcionamiento en modo Ad-hoc mientras funcione a 5 Ghz. El modo Ad-hoc es la comunicación directa de igual a igual entre dos dispositivos cliente sin un punto de acceso.
- Los puntos de acceso admitirán la funcionalidad DFS (Selección de frecuencia dinámica) y TPC (Control de la potencia de transmisión) si es necesario cuando funcionan a 5 Ghz dentro de la UE.
- Por favor compruebe el manual o la ficha de producto para comprobar si el producto utiliza las bandas inalámbricas de 2.4 GHz y/o la de 5 GHz.

AVVISO PER L'USO DI LAN RADIO WIRELESS NELLA COMUNITÀ EUROPEA (SOLO PER PRODOTTI WIRELESS)

- Nella Comunità europea, l'uso di questo dispositivo è limitato esclusivamente agli ambienti interni sui canali compresi nella banda da 5,15 a 5,35 GHz al fine di ridurre potenziali interferenze. Questo dispositivo è un sistema di trasmissione a banda larga a 2,4 GHz (ricetrasmittente), destinato all'uso in tutti gli stati membri dell'Unione europea e nei paesi EFTA.
- Questo dispositivo può essere utilizzato in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Note per l'uso

- Al fine di mantenere la conformità alle normative nazionali europee per l'uso dello spettro di frequenze, saranno applicate limitazioni sulle frequenze e sui canali per il prodotto in conformità alle normative del paese in cui il dispositivo viene utilizzato.
- Questo dispositivo non può essere attivato in modalità Ad-hoc durante il funzionamento a 5 Ghz. La modalità Ad-hoc è una comunicazione diretta peer-to-peer fra due dispositivi client senza un punto di accesso.
- I punti di accesso supportano le funzionalità DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) richieste per operare a 5 Ghz nell'Unione europea.
- Ti invitiamo a fare riferimento al manuale del prodotto o alla scheda tecnica per verificare se il tuo prodotto utilizza le frequenze 2,4 GHz e/o 5 GHz.

KENNISGEVING VAN DRAADLOOS RADIO LAN-GEBRUIK IN DE EUROPESE GEMEENSCHAP (ALLEEN VOOR DRAADLOOS PRODUCT)

- Dit toestel is beperkt tot gebruik binnenshuis wanneer het wordt gebruikt in de Europese Gemeenschap gebruik makend van kanalen in de 5.15-5.35 GHz band om de kans op interferentie te beperken.
- Dit toestel is een 2.4 GHz breedband transmissiesysteem (transceiver) dat bedoeld is voor gebruik in alle EU lidstaten en EFTA landen. Deze uitrusting mag gebruikt worden in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebruiksaanwijzingen:

- Om de gebruiksvoorschriften van het Europese Nationale spectrum na te leven, zullen frequentie- en kanaalbeperkingen worden toegepast op de producten volgens het land waar de uitrusting gebruikt zal worden.
- Dit toestel kan niet functioneren in Ad-hoc mode wanneer het gebruikt wordt in 5 GHz. Ad-hoc mode is directe peer-to-peer communicatie tussen twee klantenapparaten zonder een toegangspunt.
- Toegangspunten ondersteunen DFS (Dynamic Frequency Selection) en TPC (Transmit Power Control) functionaliteit zoals vereist bij gebruik in 5 GHz binnen de EU.
- Raadpleeg de handleiding of de datasheet om te controleren of uw product gebruik maakt van 2.4 GHz en/of 5 GHz.

SAFETY INSTRUCTIONS

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.
- Do not attempt to service the product and never disassemble the product. For some products with a user replaceable battery, please read and follow the instructions in the user manual.
- Do not spill food or liquid on your product and never push any objects into the openings of your product.
- Do not use this product near water, areas with high humidity, or condensation unless the product is specifically rated for outdoor application.
- Keep the product away from radiators and other heat sources.
- Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

SICHERHEITSVORSCHRIFTEN

Die folgenden allgemeinen Sicherheitsvorschriften dienen als Hilfe zur Gewährleistung Ihrer eigenen Sicherheit und zum Schutz Ihres Produkts. Weitere Details finden Sie in den Benutzeranleitungen zum Produkt.

- Statische Elektrizität kann elektronischen Komponenten schaden. Um Schäden durch statische Aufladung zu vermeiden, leiten Sie elektrostatische Ladungen von Ihrem Körper ab,
  (z. B. durch Berühren eines geerdeten blanken Metallteils), bevor Sie das Produkt berühren.
- Unterlassen Sie jeden Versuch, das Produkt zu warten, und versuchen Sie nicht, es in seine Bestandteile zu zerlegen. Für einige Produkte mit austauschbaren Akkus lesen Sie bitte das Benutzerhandbuch und befolgen Sie die dort beschriebenen Anleitungen.
- Vermeiden Sie, dass Speisen oder Flüssigkeiten auf Ihr Produkt gelangen, und stecken Sie keine Gegenstände in die Gehäuseschlitze oder -öffnungen Ihres Produkts.
- Verwenden Sie dieses Produkt nicht in unmittelbarer Nähe von Wasser und nicht in Bereichen mit hoher Luftfeuchtigkeit oder Kondensation, es sei denn, es ist speziell zur Nutzung in Außenbereichen vorgesehen und eingestuft.
- Halten Sie das Produkt von Heizkörpern und anderen Quellen fern, die Wärme erzeugen.
- Trennen Sie das Produkt immer von der Stromzufuhr, bevor Sie es reinigen und verwenden Sie dazu ausschließlich ein trockenes fusselfreies Tuch.

CONSIGNES DE SÉCURITÉ

Les consignes générales de sécurité ci-après sont fournies afin d'assurer votre sécurité personnelle et de protéger le produit d'éventuels dommages. Veuillez consulter les consignes d'utilisation du produit pour plus de détails.

- L'électricité statique peut endommager les composants électroniques. Déchargez l'électricité statique de votre corps (en touchant un objet en métal relié à la terre par exemple) avant de toucher le produit.
- N'essayez pas d'intervenir sur le produit et ne le démontez jamais. Pour certains produits contenant une batterie remplaçable par l'utilisateur, veuillez lire et suivre les consignes contenues dans le manuel d'utilisation.
- Ne renversez pas d'aliments ou de liquide sur le produit et n'insérez jamais d'objets dans les orifices.
- N'utilisez pas ce produit à proximité d'un point d'eau, de zones très humides ou de condensation sauf si le produit a été spécifiquement conçu pour une application extérieure.
- Éloignez le produit des radiateurs et autres sources de chaleur.
- Débranchez toujours le produit de l'alimentation avant de le nettoyer et utilisez uniquement un chiffon sec non pelucheux.

INSTRUCCIONES DE SEGURIDAD

Las siguientes directrices de seguridad general se facilitan para ayudarle a garantizar su propia seguridad personal y para proteger el producto frente a posibles daños. No olvide consultar las instrucciones del usuario del producto para obtener más información.

- La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej., tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.
- No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
- No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
- No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
- Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
- Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa.

ISTRUZIONI PER LA SICUREZZA

Le seguenti linee guida sulla sicurezza sono fornite per contribuire a garantire la sicurezza personale degli utenti e a proteggere il prodotto da potenziali danni. Per maggiori dettagli, consultare le istruzioni per l'utente del prodotto.

- L'elettricità statica può essere pericolosa per i componenti elettronici. Scaricare l'elettricità statica dal corpo (ad esempio toccando una parte metallica collegata a terra) prima di toccare il prodotto.
- Non cercare di riparare il prodotto e non smontarlo mai. Per alcuni prodotti dotati di batteria sostituibile dall'utente, leggere e seguire le istruzioni riportate nel manuale dell'utente.
- Non versare cibi o liquidi sul prodotto e non spingere mai alcun oggetto nelle aperture del prodotto.
- Non usare questo prodotto vicino all'acqua, in aree con elevato grado di umidità o soggette a condensa a meno che il prodotto non sia specificatamente approvato per uso in ambienti esterni.
- Tenere il prodotto lontano da caloriferi e altre fonti di calore.
- Scollegare sempre il prodotto dalla presa elettrica prima di pulirlo e usare solo un panno asciutto che non lasci filacce.

VEILIGHEIDSINFORMATIE

De volgende algemene veiligheidsinformatie werd verstrekt om uw eigen persoonlijke veiligheid te waarborgen en uw product te beschermen tegen mogelijke schade. Denk eraan om de gebruikersinstructies van het product te raadplegen voor meer informatie.

- Statische elektriciteit kan schadelijk zijn voor elektronische componenten. Ontlaad de statische elektriciteit van uw lichaam (d.w.z. het aanraken van geaard bloot metaal) voordat uhet product aanraakt.
- U mag nooit proberen het product te onderhouden en u mag het product nooit demonteren. Voor sommige producten met door de gebruiker te vervangen batterij, dient u de instructies in de gebruikershandleiding te lezen en te volgen.
- Mors geen voedsel of vloeistof op uw product en u mag nooit voorwerpen in de openingen van uw product duwen.
- Gebruik dit product niet in de buurt van water, gebieden met hoge vochtigheid of condensatie, tenzij het product specifiek geclassificeerd is voor gebruik buitenshuis.
- Houd het product uit de buurt van radiators en andere warmtebronnen.
- U dient het product steeds los te koppelen van de stroom voordat u het reinigt en gebruik uitsluitend een droge pluisvrije doek.

Disposing and Recycling Your Product

ENGLISH

EN

This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free. By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

D-Link and the Environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit **www.dlinkgreen.com**.

DEUTSCH

DE

Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

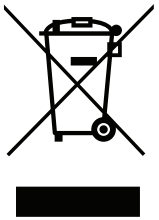
D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf diese Weise helfen Sie, Energie zu sparen und CO2-Emissionen zu reduzieren.

Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter **www.dlinkgreen.com**.

FRANÇAIS FR



Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et règlementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

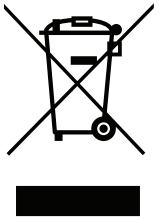
D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.

D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO2.

Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le **www.dlinkgreen.com**.

ESPAÑOL ES



Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

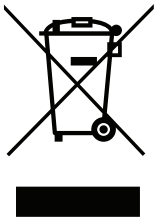
D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.

Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio **www.dlinkgreen.com**.

ITALIANO IT



La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

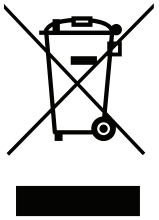
D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.

D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.

Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo **www.dlinkgreen.com**.

NEDERLANDS NL



Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen. Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

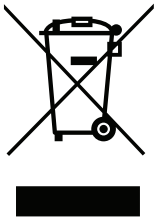
D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO2-emissies.

Breng een bezoek aan **www.dlinkgreen.com** voor meer informatie over onze milieuverantwoorde producten en verpakkingen.

POLSKI PL



Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze. Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

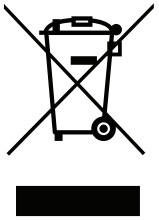
D-Link i środowisko

D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO2.

Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną Internetową **www.dlinkgreen.com**.

ČESKY CZ



Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

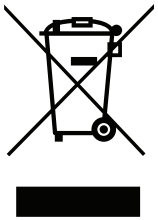
D-Link a životní prostředí

Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály.

Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO2.

Více informací o našich ekologických výrobcích a obalech najdete na adrese **www.dlinkgreen.com**.

MAGYAR HU



Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

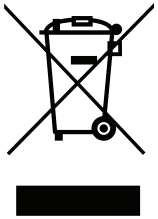
A D-Link és a környezet

A D-Linknél megértjük és elkötelezettek vagyunk a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azáltal, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat alkalmaz.

A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.

Környezetbarát termékeinkről és csomagolásainkról további információkat a **www.dlinkgreen.com** weboldalon tudhat meg.

NORSK NO



Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

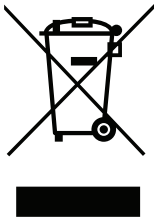
D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.

For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til **www.dlinkgreen.com**.

DANSK DK



Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

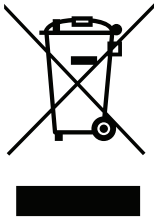
D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO2-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på **www.dlinkgreen.com**.

SUOMI FI



Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

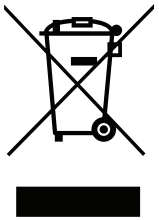
D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta **www.dlinkgreen.com**.

SVENSKA SE



Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

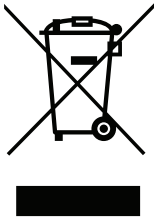
D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar **www.dlinkgreen.com**.

PORTUGUÊS PT



Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite **www.dlinkgreen.com**.