



User Manual

5G NR AX3000 Wi-Fi 6 Router

G530

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
A3	v1.00	2024/08/08	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.

Amazon, Alexa and all related logos are trademarks of Amazon.com, Inc. or its affiliates.

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

ChromeTM browser, Google PlayTM and AndroidTM are trademarks of Google Inc.

Google, Nest Hub, and Google Home are trademarks of Google LLC.

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

Copyright © 2023 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 inactivity.

G530	Network Standby: TBD Switched Off: TBD
-------------	---

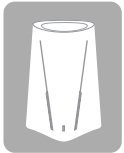
Table of Contents

Product Overview.....	1	IPv4 - Dynamic IP (DHCP).....	28
Package Contents.....	1	IPv4 - Static IP	29
System Requirements	2	IPv4 - PPPoE	30
Introduction	3	Internet - IPv6.....	32
Features.....	3	IPv6 - Auto Detection	33
Hardware Overview	4	IPv6 - Static IPv6	35
Front View: LED Indicator	4	IPv6 - Auto Configuration (SLAAC/DHCPv6)	37
Rear View: Back Panel and LED Indicators	5	IPv6 - PPPoE	39
Bottom View: Reset Button	6	IPv6 - 6rd	43
Rear View:	6	IPv6 - Local Connectivity Only	45
Installation	7	Wireless.....	46
Before you Begin.....	7	Guest Zone.....	52
Wireless Installation Considerations.....	8	Network.....	54
Setup.....	9	D-Link Cloud.....	56
D-Link FALCON Setup.....	10	Operation Mode.....	57
Setup Wizard	11	Features.....	58
Configuration.....	18	Parental Control	58
Home	19	Data Cap.....	61
Internet.....	20	SMS	62
G530	21	PIN.....	64
Connected Clients	22	USSD.....	65
Settings	24	Firewall	66
Wizard	24	Firewall Settings - IPv4/IPv6 Rules.....	68
Cellular.....	25	Port Forwarding	70
Failover	26	Port Forwarding - Virtual Server.....	72
Internet - IPv4.....	27	Static Routes - IPv4.....	74
		Static Routes - IPv6.....	75

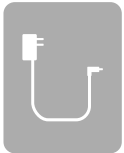
Dynamic DNS	76	Connect or Disconnect	110
Quick VPN	78	Android	111
Management	79	VPN Setup Instructions	111
Time & Schedule - Time	79	Connect or Disconnect	113
Time & Schedule - Schedule	80	Connect a Wireless Client to Your Router	114
System Log	81	WPS Button	114
System Admin - Admin	83	Windows® 10	115
System Admin - System	84	Windows® 8 - WPA/WPA2	116
User	85	Windows® 7	118
Upgrade	86	Troubleshooting	120
Statistics	87	Wireless Basics	122
D-Link FALCON	88	Networking Basics	126
Quick VPN	90	Wireless Security	128
Important Information	91	Technical Specifications	129
iOS Devices	92	Regulatory Statements	130
VPN Setup Instructions	92		
Connect or Disconnect	94		
Mac OS X	95		
VPN Setup Instructions	95		
Connect or Disconnect	97		
Windows 7	98		
VPN Setup Instructions	98		
Connect or Disconnect	101		
Windows 8.1/8	102		
VPN Setup Instructions	102		
Connect or Disconnect	107		
Windows 10	108		
VPN Setup Instructions	108		

Product Overview

Package Contents



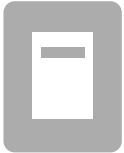
G530 5G NR AX3000 Wi-Fi 6 Router



Power Adapter (12V, 2.5A)



CAT5e Ethernet Cable (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 & k/v 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 10 or later • Firefox 28 or later • Safari 6 or later • Chrome 28 or later
D-Link FALCON 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, G530 5G NR AX3000 Wi-Fi 6 Router packs in strong processing power to help you manage your home or office network. The powerful and intelligent home router is designed with Wi-Fi utilization, mesh optimization, and parental control features.

Features

Handling More with a High-Power Processor

With G530, you could not only enjoy buffer-free gaming and lightning-fast surfing but also management-convenient features with the router's embedded dual-core ARM Cortex-A53 MPCore processor, 128 MB of flash memory and 512 MB of RAM.

Always Up-to-Date with the Latest Features

G530 will automatically check for daily updates and silently finish the install in the background to ensure that the device is always equipped with the latest features and the most secure firmware. For extra peace of mind, in the event of any failure during a firmware update, the router will automatically store a system image in the memory for backup before proceeding with any update.

Easy Setup and Flexible Management

Managing your Internet utilization has never been easier; just download the free D-Link FALCON app 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. Supporting industry-standard Wi-Fi Protected Setup (WPS), G530 lets you create encrypted connections to new devices by easily pressing on the WPS button.

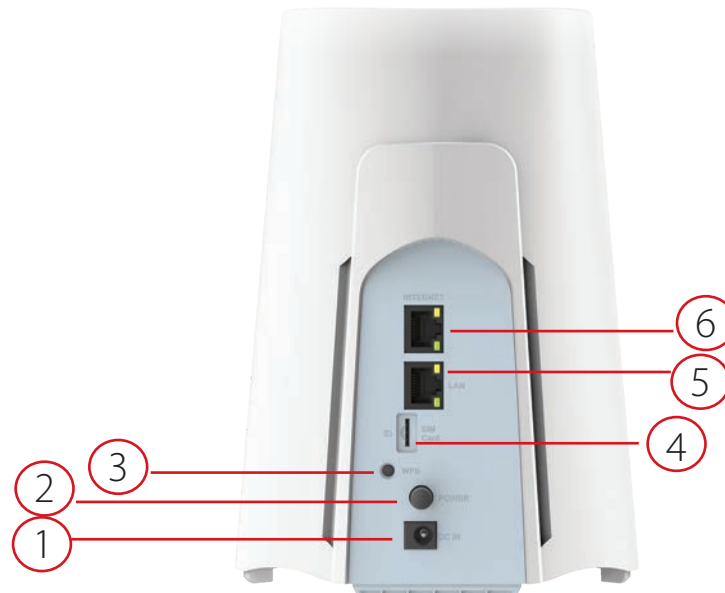
Hardware Overview

Front View: LED Indicator



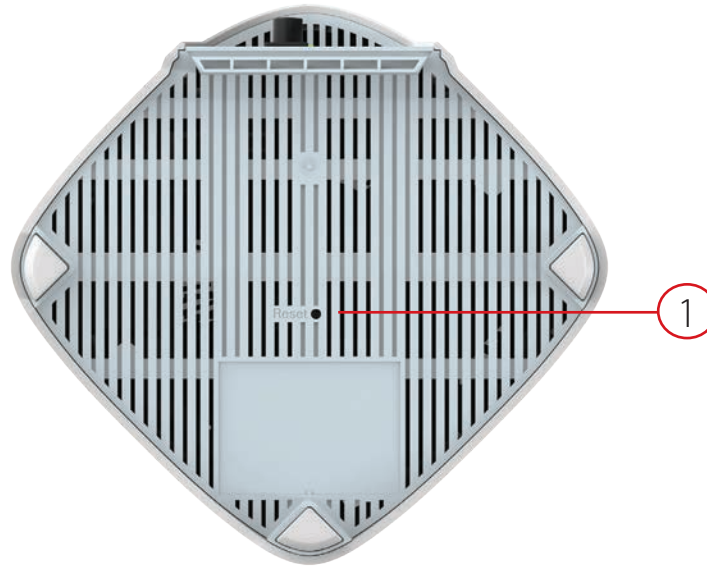
1	Power/ Status	Solid White	The device is on and ready for 5G/4G/3G or Wi-Fi connection.
		Blinking White	The device is in WPS process.
		Blinking Orange	The device is not inserted with a SIM card, inserted with a locked SIM card, or there is no cellular signal.
		Solid Red	The device has system errors.
		Blinking Red	The device is powering on, restoring to default factory setting, or undergoing reboot process.
		Off	The device is off.

Rear View: Back Panel and LED Indicators



1	DC Power Connector	Connector for the supplied power adapter.
2	Power Button	Press power button to turn on/off the router.
3	WPS Button	Press WPS button to establish a secure Wi-Fi connection.
4	SIM Card Slot	Insert 4FF sim card to establish a cellular network.
5	LAN Port/Indicator	Solid Orange: Ready for 1Gbps data transmission with an Ethernet cable connected Blinking Orange: Data transmission in process at 1Gbps transfer rate Solid Green: Ready for 10/100Mbps data transmission with an Ethernet cable connected Blinking Green: Data transmission in process at 10/100Mbps transfer rate
6	Internet Port/Indicator	Solid Orange: Ready for 1Gbps data transmission with an Ethernet cable connected Blinking Orange: Data transmission in process at 1Gbps transfer rate Solid Green: Ready for 10/100Mbps data transmission with an Ethernet cable connected Blinking Green: Data transmission in process at 10/100Mbps transfer rate

Bottom View: Reset Button



1	Reset Button	Use a paperclip to press this button to reset the router to default factory settings.
---	---------------------	---

Installation

This section will walk you through the installation of your G530.

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 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 a 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.) Minimize the number of walls or ceilings your router and devices are positioned within.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters) appears to be almost 3 feet (1 meter) thick at a 45-degree angle . At a 2-degree angle, the wall appears to be over 42 feet (14 meters) thick. Position devices for their signals to travel straight through a wall or ceiling (instead of from a certain angle) for better signal reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position extenders, access points, wireless routers, and computers for their signal to directly pass 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

- **D-Link FALCON** - Use your compatible iOS or Android device to install and configure your router. Refer to **D-Link FALCON 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 **11**.
- **Manual Setup** - Log in to the router to manually configure your router. Refer to **Configuration** on page **19**

D-Link FALCON Setup

The D-Link FALCON app allows you to install and configure your G530 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 **D-Link FALCON** available on the App Store or on Google Play.

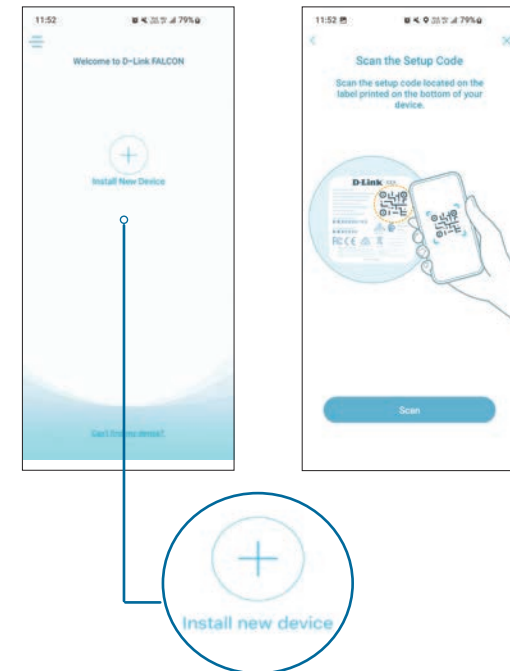


Step 2

Launch the D-Link FALCON from the home screen of your device.

Step 3

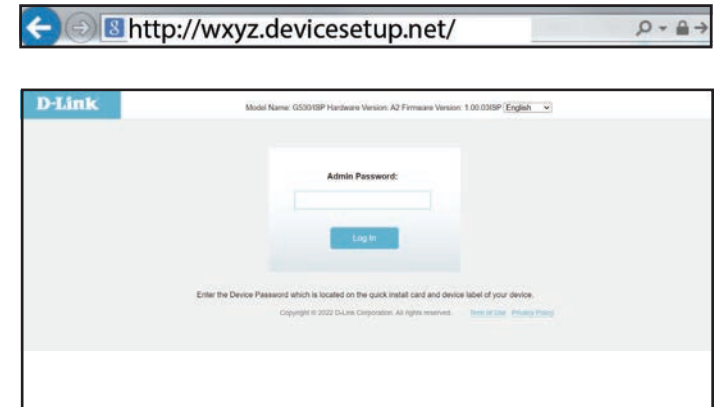
Tap **Install New Device**. Scan the setup code on the device label on the bottom of the router. Follow the on-screen instructions to complete the setup.



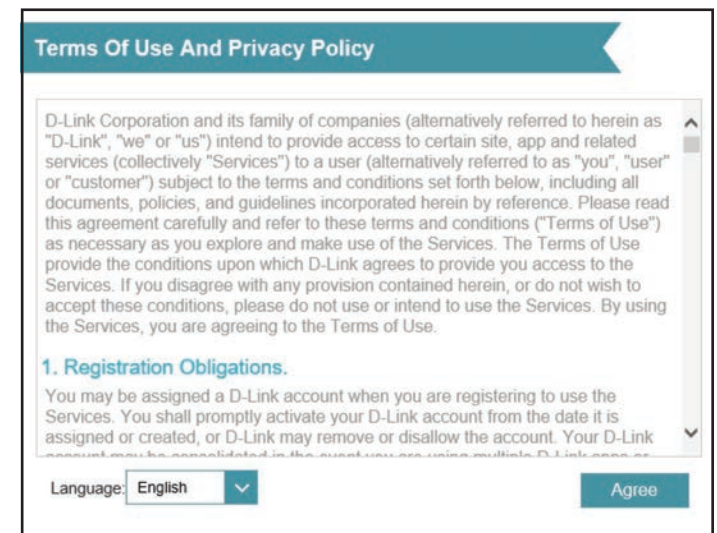
Setup Wizard

The setup wizard is designed to guide you through a step-by-step process of configuring your new G530 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.



You will be prompted with the **Operation Mode** page to set up your router's mode. Select **Router Mode** to configure G530 as a default router. Select **Mobile Router Mode** to configure G530 as a mobile router.

Click **Next** to continue

Operation Mode

☐ **Router Mode**
In Router mode, this device connect to the internet provied by your Internet Service Provider directly. All client devices from a network group under this.Device comes with router mode by default.



Internet Your Device Wi-Fi Client

☒ **Mobile Router Mode**
In Mobile Router Mode, the device use 4G/LTE wireless connects to the Internet provided by your Cellular Internet Service Provider. All client devices from a network group under this mobile router.



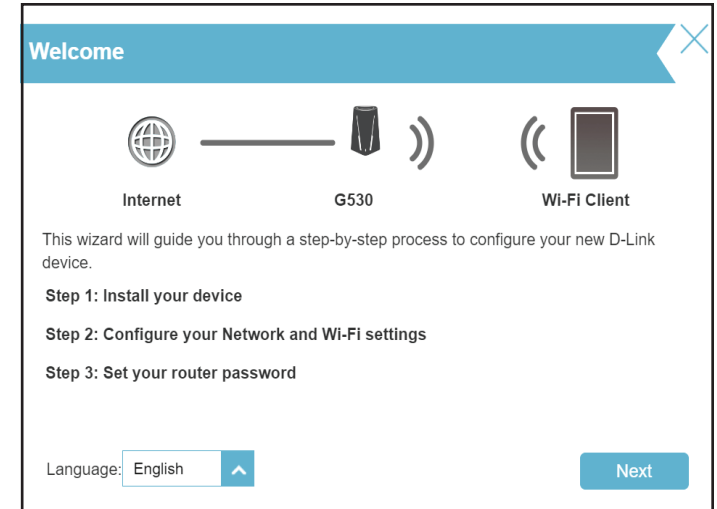
Internet Your Device Wi-Fi Client

If you're not sure about this, simply click next

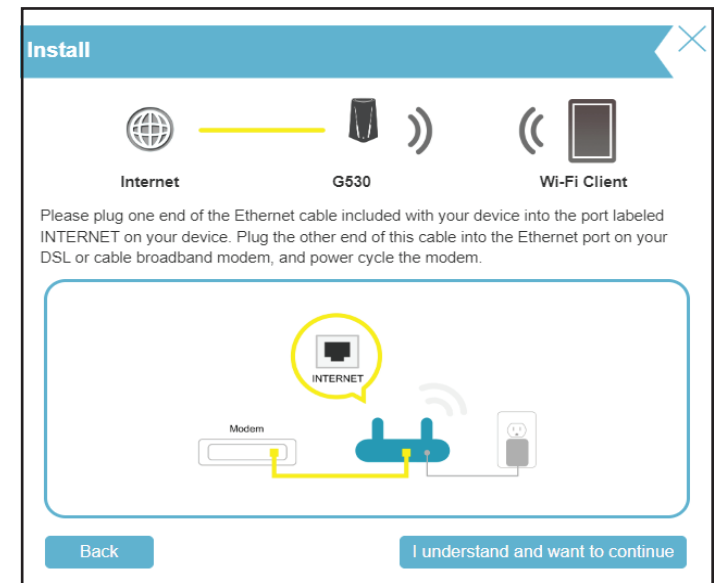
Next

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.

Configure Your Internet Connection


Internet


G530


Wi-Fi Client

We're unable to detect your connection type. Please either to reboot your modem and wait it to be ready, or select desired connection type from below.

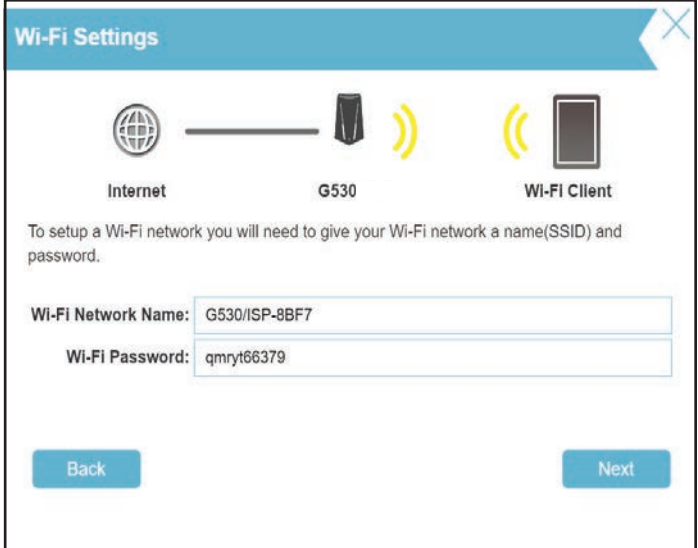
- ☒ **Auto Detection**
Choose this option allows device to detect the Internet connection type again. Device will able to detect DHCP and PPPoE. Please make sure Internet port is connected correctly to your internet service.
- ☐ **DHCP Connection (Dynamic IP Address)**
Choose this option if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- ☐ **Username/Password Connection (PPPoE)**
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- ☐ **Static IP Address Connection**
Choose this option if your Internet Service Provider provided you with IP Address information that has to be manually configured.

BackNext

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 49.*

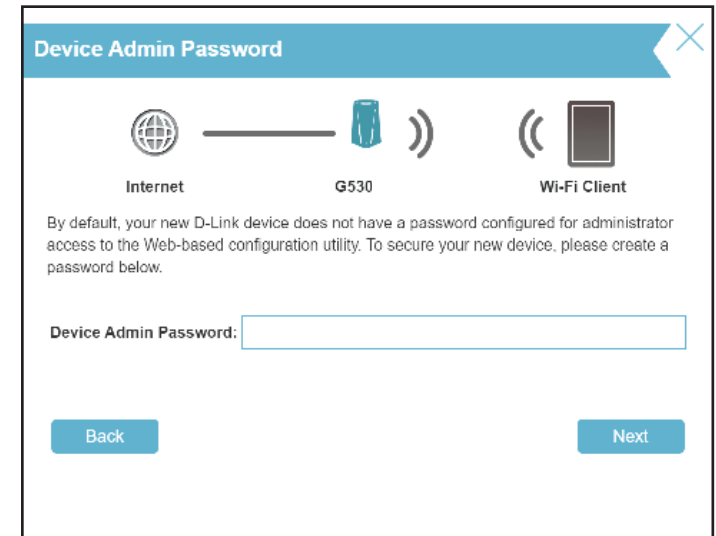


The image shows a 'Wi-Fi Settings' screen from a router's web interface. At the top, there's a blue header with the title 'Wi-Fi Settings' and a close button. Below the header, there's a diagram showing the connection flow: 'Internet' (represented by a globe icon) connected to 'G530' (represented by a router icon), which is then connected to 'Wi-Fi Client' (represented by a smartphone icon). Below the diagram, there's a text instruction: 'To setup a Wi-Fi network you will need to give your Wi-Fi network a name(SSID) and password.' Underneath this, there are two input fields: 'Wi-Fi Network Name:' with the value 'G530/ISP-8BF7' and 'Wi-Fi Password:' with the value 'qmryt66379'. At the bottom of the screen, there are two buttons: 'Back' on the left and 'Next' on the right.

In order to secure 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.

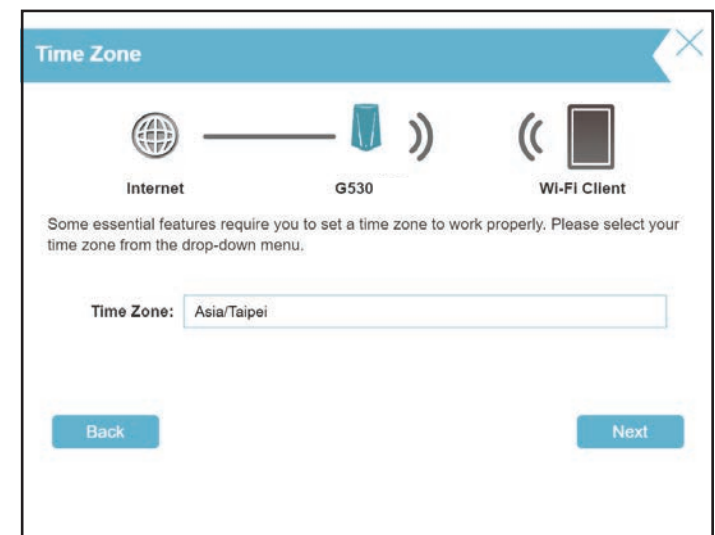
Click **Next** to continue.



The screenshot shows the 'Device Admin Password' configuration screen. At the top, there is a blue header bar with the title 'Device Admin Password' and a close button (X). Below the header, there is a network diagram showing 'Internet' connected to 'G530' (the router), which is then connected to a 'Wi-Fi Client'. The text below the diagram states: 'By default, your new D-Link device does not have a password configured for administrator access to the Web-based configuration utility. To secure your new device, please create a password below.' There is a text input field labeled 'Device Admin Password:'. At the bottom, there are two buttons: 'Back' and 'Next'.

Select your time zone from the drop-down menu.

Click **Next** to continue.



The screenshot shows the 'Time Zone' configuration screen. At the top, there is a blue header bar with the title 'Time Zone' and a close button (X). Below the header, there is a network diagram showing 'Internet' connected to 'G530' (the router), which is then connected to a 'Wi-Fi Client'. The text below the diagram states: 'Some essential features require you to set a time zone to work properly. Please select your time zone from the drop-down menu.' There is a text input field labeled 'Time Zone:' with 'Asia/Taipei' selected. At the bottom, there are two buttons: 'Back' and 'Next'.

Keeping your router's firmware up-to-date provides you with the latest protection 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.

Install Updates Automatically



Allow your device to automatically update to make sure you are always enjoying the latest features and improvements.

☒

Keep my device up to date automatically.

☐

I want to manage the device updates myself.

Back

Next

You will be presented with a summary of your settings.

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

Summary



Internet



G530





Wi-Fi Client

Below is a summary of your Wi-Fi security and device password settings. Please note down your settings and click "Next".

Connection Type:	Dynamic IP (DHCP)
Wi-Fi Network Name:	G530/ISP-8BF7
Wi-Fi Password:	qmryt66379
Device Admin Password:	Dlinkwriter24

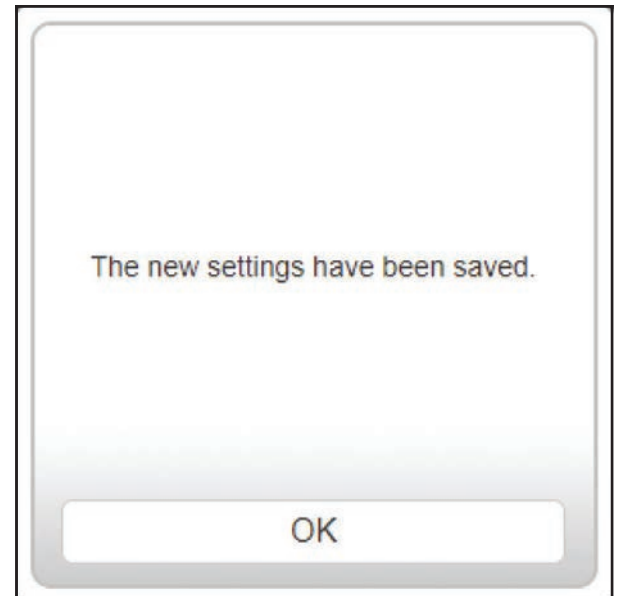
Back

Next

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 characters of the MAC address).



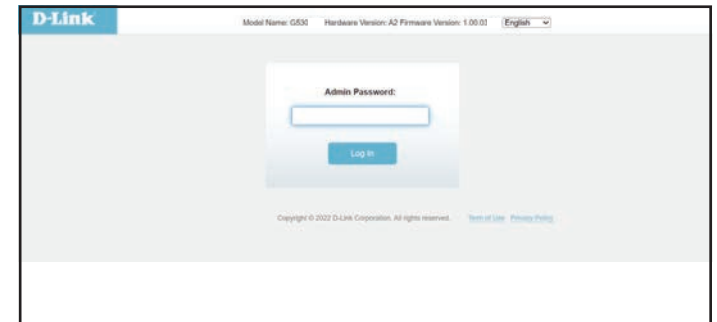
The Wi-Fi Name(SSID), Wi-Fi Password, and device password are printed on the device label and the Quick Installation Card.

Note: *If you cannot remember your password for login, use a paperclip to press the recessed **Reset** button on the bottom 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.

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

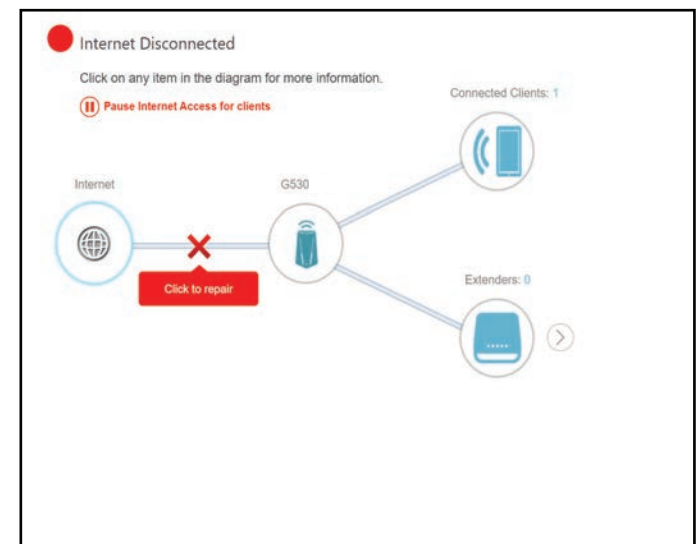
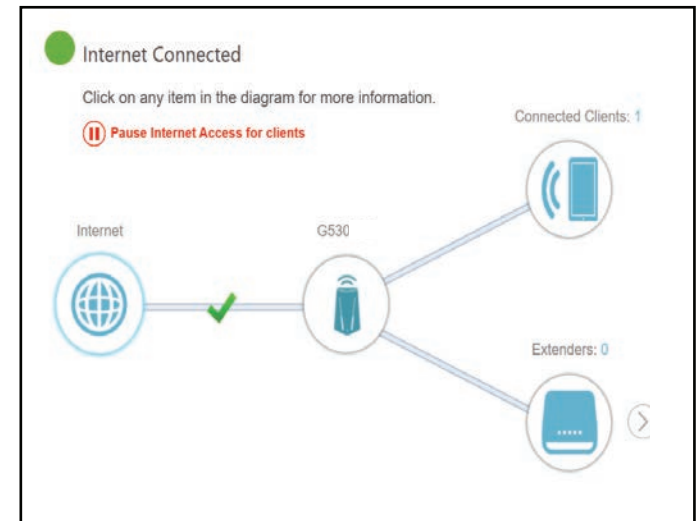


Home

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 11 for more information.



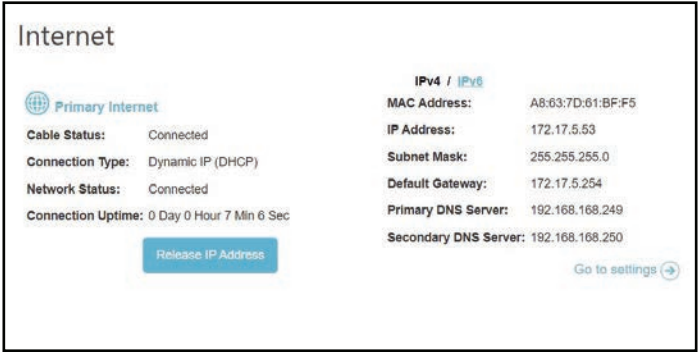
Internet

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 **28**.



G530

Click on the **G530** 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 **57** 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 **49** for more information.

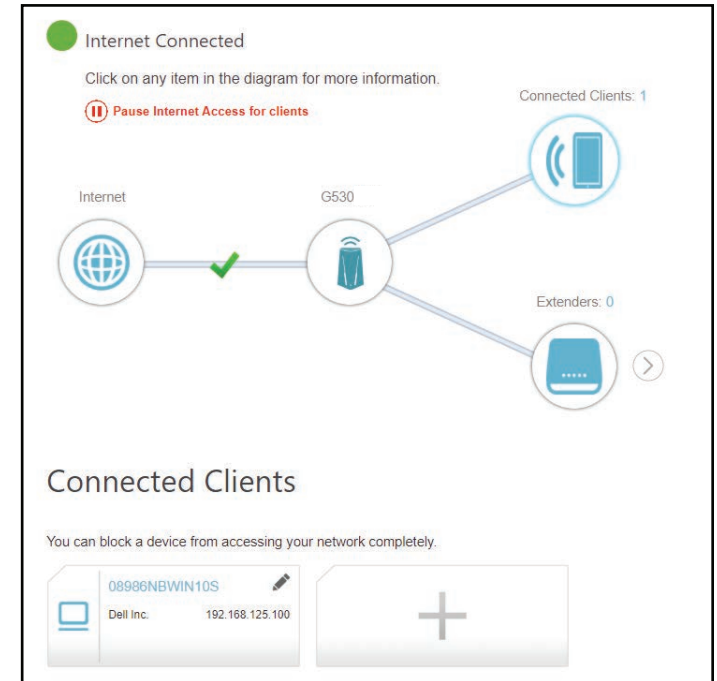


Connected Clients

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 time periods that the client can access the network. You can also block access to unwanted websites. Refer to Features > Parental Control on page 61 for more information.

Click **Save** when you are done.

Edit Rule

Name:09068NBWIN10T

Vendor:Unknown Vendor

MAC Address:34:e1:2d:97:16:16

IP Address:192.168.0.235

Reserve IP:Enabled

Remaining:24

IP Address (Reserved):

Parental Control:Enabled

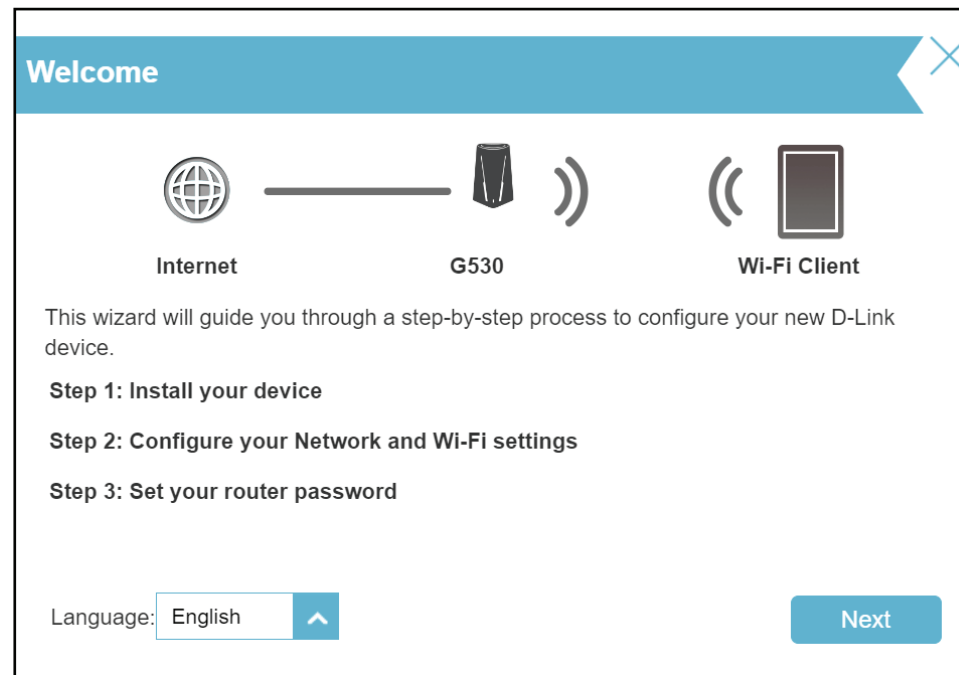
Profile:Always Block

Save

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 **11** for details.

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



Cellular

Go to **Settings > Cellular** to configure your cellular connection. You can view data on the LTE modem connected to the router and enable/disable the function for automatic creation of 3G/LTE WAN connection.

Connection Settings

Service Mode: Select **5G NR NSA**, **5G NR SA**, **LTE**, **3G** or **Auto** to let the system determine.

Connection Mode: Select Auto Connect or Manual Connect.

Data Roaming: Enable or disable **Data Roaming**.

Dial-up Settings

APN Mode: Select Manual or Auto for APN mode.

APN Name: When APN Mode is set to manual, enter the name of your APN.

PDP Type: Select IPv4, IPv6, or IPv4/IPv6 for PDP type.

Username: Enter your username.

Password: Enter your password

Dial Number: Enter the dial number

Authentication Type: Select PAP, CHAP, NONE, or Auto for your authentication type.

Failover

Go to **Settings->Failover** to configure the WAN backup function. The G530's failover feature allows you to set your router to automatically switch to a backup Internet connection if your primary Internet connection is lost. When the main connection is recovered, the device will switch back on its own.

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

Failover

On the WAN Failover page, you can enable the WAN backup function, which provides you with uninterrupted access to the Internet. When your main connection breaks down, your device activates the backup connection; and when the main channel is recovered, the device switches to it and disconnects the reserve one.

Save

When Failover is enabled, the following options will appear.

Checking Method: Select between **DNS Query + ICMP Ping, ICMP Ping, DNS Query, or Auto.**

Target Host 1: Enter an IP address for Host 1.

Target Host 2: Enter an IP address for Host 2.

Timeout Limit (ms): Enter the timeout limit in milliseconds.

Retry Times: Enter the retry time.

Interval: Enter the interval in seconds.

Failover Settings

Enable: ☒ Enabled

Checking Method: DNS Query + ICMP... ▼

Target Host 1: Auto

Target Host 2: DNS Query + ICMP Ping

Timeout Limit (ms): ICMP Ping

Retry Times: DNS Query

Interval: 5

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 33. 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 **Dynamic IP (DHCP)**, **Static IP**, and **PPPoE** for your connection type.

Secure DNS: Enable the secure DNS 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.



For **IPv4 - Dynamic IP (DHCP)** refer to page 29

For **IPv4 - Static IP** refer to page 30

For **IPv4 - PPPoE** refer to page 31

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.

Host Name:

Primary DNS Server:

Secondary DNS Server:

MTU:

1500

MAC Address Clone:

<< MAC Address

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.

Secure DNS: Enable the secure DNS 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.

The screenshot shows the 'Internet' settings page. At the top, there's a globe icon and the title 'Internet'. Below it, a note says: 'Use this section to configure your Internet Connection type. There are several connection types to choose. If you are unsure of your connection method, please contact your Internet Service Provider. Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.' Below this, there's a breadcrumb 'Settings >> Internet >> IPv4' and a 'Save' button. The 'My Internet Connection is:' dropdown is set to 'Static IP'. Below this, there are input fields for 'IP Address', 'Subnet Mask', 'Default Gateway', and 'Primary DNS Server'. An 'Advanced Settings...' link is at the bottom right. Further down, there's a 'Secure DNS' toggle set to 'Enabled', a 'Status' indicator showing 'Connected', a 'DNS over HTTP Provider' dropdown set to 'Google', and an 'Allow fall-back' toggle set to 'Enabled'.

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.

The screenshot shows the 'Advanced Settings' section. It includes input fields for 'Secondary DNS Server' and 'MTU' (set to 1500). There's also a 'MAC Address Clone' section with an input field and a dropdown menu set to '<< MAC Address'.

IPv4 - PPPoE

Select **Point-to-Point Protocol over Ethernet (PPPoE)** 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. The default is 5 minutes. To disable this feature, select **Always on** or **Manual** as the reconnect mode.

Secure DNS: Enable the secure DNS 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.

The screenshot shows the 'Internet' configuration page. At the top, there's a globe icon and the title 'Internet'. Below it, a note says: 'Use this section to configure your Internet Connection type. There are several connection types to choose. If you are unsure of your connection method, please contact your Internet Service Provider. Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.' The breadcrumb trail is 'Settings >> Internet >> IPv4'. There are 'IPv4' and 'Save' buttons. The 'My Internet Connection is:' dropdown is set to 'PPPoE'. Below this are fields for 'Username', 'Password', 'Reconnect Mode' (set to 'On demand'), and 'Maximum Idle Time' (set to '5 minutes'). There is an 'Advanced Settings' link. The 'Secure DNS' toggle is set to 'Enabled'. The 'Status' is 'Connected'. The 'DNS over HTTP Provider' is set to 'Google', with a 'Privacy Policy' link next to it. The 'Allow fall-back' toggle is set to 'Enabled'.

Advanced Settings... - Dynamic IP

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**.

IP Address: When **Static IP** is selected as the address mode, the column for IP address will appear. 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 (1280~1500)- 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.

The screenshot shows a web-based configuration interface for 'Dynamic IP'. It includes the following fields and controls:

- Address Mode:** A dropdown menu currently set to 'Dynamic IP'.
- Service Name:** A text input field containing 'Dynamic IP'.
- Primary DNS Server:** A text input field containing 'Static IP'.
- Secondary DNS Server:** An empty text input field.
- MTU:** A text input field containing '1492'.
- MAC Address Clone:** A text input field that is empty, with a button labeled '<< MAC Address' to its right.

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 28

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 34

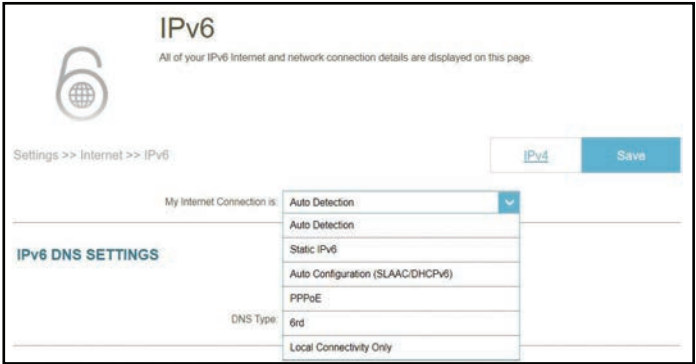
For **IPv6 - Static IPv6** refer to page 36

For **IPv6 - Auto Configuration (SLAAC/DHCPv6)** refer to page 38

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

For **IPv6 - 6rd** refer to page 44

For **IPv6 - Local Connectivity Only** refer to page 46



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.

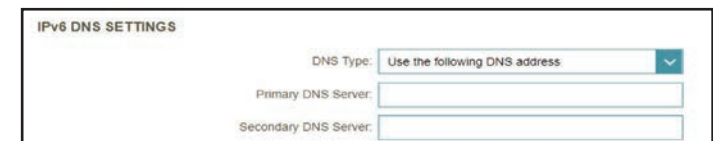


IPv6 DNS Settings

DNS Type: Select either **Obtain a 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

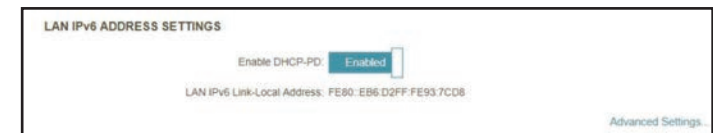
Enable DHCP-PD: Enable or disable DHCP prefix delegation.

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 .
<i>If you select SLAAC+RDNSS or SLAAC+Stateless DHCP as the Autoconfiguration Type:</i>	
Router Advertisement Lifetime:	Enter the router advertisement lifetime (in minutes). The default is 30 minutes.
<i>If you select Stateful DHCPv6 as the Autoconfiguration Type:</i>	
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.

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Enable Automatic DHCP-PD in LAN: ☒ Enabled

Autoconfiguration Type: SLAAC+Stateless DHCP

Router Advertisement Lifetime: 30 minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Enable Automatic DHCP-PD in LAN: ☒ Enabled

Autoconfiguration Type: SLAAC+RDNSS

Router Advertisement Lifetime: 30 minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Enable Automatic DHCP-PD in LAN: ☒ Enabled

Autoconfiguration Type: Stateful DHCPv6

IPv6 Address Range (Start): :::::00

IPv6 Address Range (End): :::::00

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.

The screenshot shows the 'IPv6' configuration page. At the top, there's a header 'IPv6' with a subtext 'All of your IPv6 Internet and network connection details are displayed on this page.' Below this is a breadcrumb trail 'Settings>>Internet>>IPv6' and three tabs: 'VLAN', 'IPv4', and 'Save'. The 'Static IPv6' option is selected under 'My Internet Connection is:'. The 'Use Link-Local Address' is set to 'Disabled'. There are input fields for 'IPv6 Address', 'Subnet Prefix Length', 'Default Gateway', 'Primary DNS Server', and 'Secondary DNS Server'.

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.

The screenshot shows the 'LAN IPv6 ADDRESS SETTINGS' page. It features an input field for 'LAN IPv6 Address' followed by a '/64' suffix. Below this, it displays the 'LAN IPv6 Link-Local Address' as 'FE80::AA63:7DFF:FE81:C262/64'. There is a link for 'Advanced Settings...' at the bottom right.

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.

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment:

Enabled

Autoconfiguration Type:

SLAAC+Stateless DHCP

Router Advertisement Lifetime:

30

minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment:

Enabled

Autoconfiguration Type:

SLAAC+RDNSS

Router Advertisement Lifetime:

30

minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment:

Enabled

Autoconfiguration Type:

Stateful DHCPv6

IPv6 Address Range (Start):

fff:00:00:00:00:00:00:01

IPv6 Address Range (End):

fff:00:00:00:00:00:00:00

IPv6 Address Lifetime:

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 a 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.

Settings>>Internet>>IPv6

VLAN IPv4 Save

My Internet Connection is: Auto Configuration (SLAAC/DHCPv6)

IPv6 DNS SETTINGS

DNS Type: Use the following DNS address

Primary DNS Server:

Secondary DNS Server:

LAN IPv6 ADDRESS SETTINGS

Enable DHCP-PD: Enabled

LAN IPv6 Link-Local Address: /64

Advanced Settings...

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: Enabled

Enable Automatic DHCP-PD in LAN: Disabled

Autoconfiguration Type: SLAAC+Stateless DHCP

Router Advertisement Lifetime: 30 minutes

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:** If **DHCP-PD** is enabled in the previous LAN IPv6 Address Settings, enable or disable automatic 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:** If **DHCP-PD** is disabled in the previous LAN IPv6 Address Settings, enter the IP address retention period in minutes. The default is 10080 minutes.

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Enable Automatic DHCP-PD in LAN: ☒ Enabled

Autoconfiguration Type:

Router Advertisement Lifetime: minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Enable Automatic DHCP-PD in LAN: ☒ Enabled

Autoconfiguration Type:

Router Advertisement Lifetime: minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Enable Automatic DHCP-PD in LAN: ☒ Enabled

Autoconfiguration Type:

IPv6 Address Range (Start):

IPv6 Address Range (End):

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.

The screenshot shows the 'IPv6' configuration page. At the top, there's a header 'IPv6' with a sub-header 'All of your IPv6 Internet and network connection details are displayed on this page.' Below this is a breadcrumb trail 'Settings>>Internet>>IPv6'. There are three tabs: 'VLAN', 'IPv4', and 'Save'. The 'Save' tab is active. The main form contains the following fields: 'My Internet Connection is:' with a dropdown menu showing 'PPPoE'; 'PPPoE Session:' with a dropdown menu showing 'Create a new session'; 'Username:' with a text input field; 'Password:' with a text input field; 'Address Mode:' with a dropdown menu showing 'Dynamic IP'; 'Service Name:' with a text input field; 'Reconnect Mode:' with a dropdown menu showing 'Always on'; and 'MTU:' with a text input field showing '1492 bytes'.

IPv6 DNS Settings

- DNS Type:

Select either **Obtain a 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.

IPv6 DNS SETTINGS

DNS Type: Obtain a DNS server address automatically

IPv6 DNS SETTINGS

DNS Type: Use the following DNS address

Primary DNS Server:

Secondary DNS Server:

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.

LAN IPv6 ADDRESS SETTINGS

Enable DHCP-PD: Enabled

LAN IPv6 Link-Local Address: FE80::AA63:7DFF:FE61:C262/64

LAN IPv6 ADDRESS SETTINGS

Enable DHCP-PD: Disabled

LAN IPv6 Address: /64

LAN IPv6 Link-Local Address: FE80::AA63:7DFF:FE61:C262/64

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.

The screenshot shows the 'ADDRESS AUTOCONFIGURATION SETTINGS' page. It includes four settings: 'Enable Automatic IPv6 Address Assignment' (set to 'Enabled'), 'Enable Automatic DHCP-PD in LAN' (set to 'Enabled'), 'Autoconfiguration Type' (a dropdown menu currently showing 'SLAAC+RDNSS'), and 'Router Advertisement Lifetime' (a text input field). The dropdown menu for 'Autoconfiguration Type' is open, showing four options: 'SLAAC+RDNSS', 'SLAAC+Stateless DHCP', 'SLAAC+Stateless DHCP', and 'Stateful DHCPv6'.

This screenshot shows the same settings page, but with 'SLAAC+Stateless DHCP' selected in the 'Autoconfiguration Type' dropdown menu. The 'Router Advertisement Lifetime' field now contains the value '30' and is followed by the unit 'minutes'.

This screenshot shows the settings page with 'Stateful DHCPv6' selected in the 'Autoconfiguration Type' dropdown menu. Below this, two new fields appear: 'IPv6 Address Range (Start):' with a value of '1' and 'IPv6 Address Range (End):' with a value of '00'. Both fields are followed by a small square icon.

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.

Advanced Settings...

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Autoconfiguration Type: SLAAC+Stateless DHCP

Router Advertisement Lifetime: 30 minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Autoconfiguration Type: SLAAC+Stateless DHCP

Router Advertisement Lifetime: 30 minutes

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: ☒ Enabled

Autoconfiguration Type: Stateful DHCPv6

IPv6 Address Range (Start): 1

IPv6 Address Range (End):

IPv6 Address Lifetime: 10080 minutes

IPv6 - 6rd

IPv6 **rapid deployment (6rd)** 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.

Settings>>Internet>>IPv6

VLANIPv4Save

My Internet Connection is: 6rd

Assign IPv6 Prefix: Not Available

Primary DNS Server:

Secondary DNS Server:

6RD MANUAL CONFIGURATION

Enable Hub and Spoke Mode: Enabled

6rd Configuration: 6rd DHCPv4 Option

LAN IPv6 ADDRESS SETTINGS

LAN IPv6 Address:

LAN IPv6 Link-Local Address: /64

Advanced Settings...

ADDRESS AUTOCONFIGURATION SETTINGS

Enable Automatic IPv6 Address Assignment: Enabled

Autoconfiguration Type: SLAAC+Stateless DHCP

Router Advertisement Lifetime: 30 minutes

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.

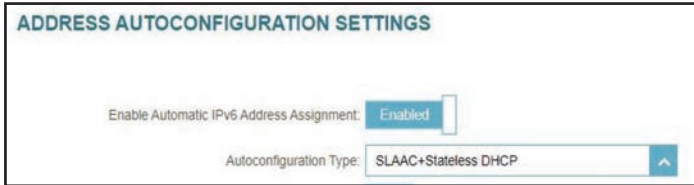
LAN IPv6 Address Settings

- LAN IPv6 Address:** Displays the router’s LAN IPv6 address.
- LAN IPv6 Link-Local Address:** Displays the router’s LAN link-local address.



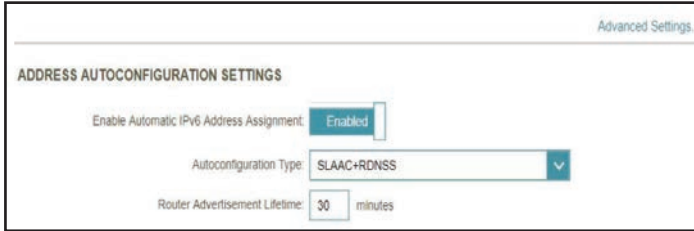
Advanced Settings... - Address Autoconfiguration Settings

- 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**.



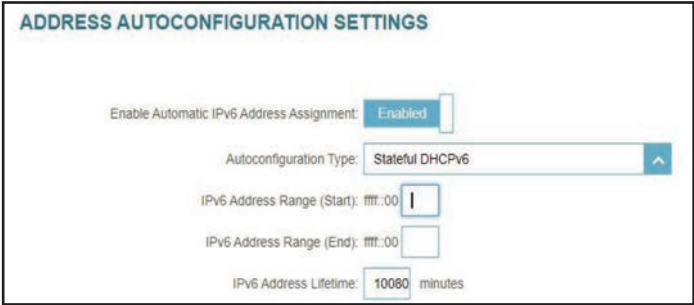
If you select **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** as the Autoconfiguration Type:

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



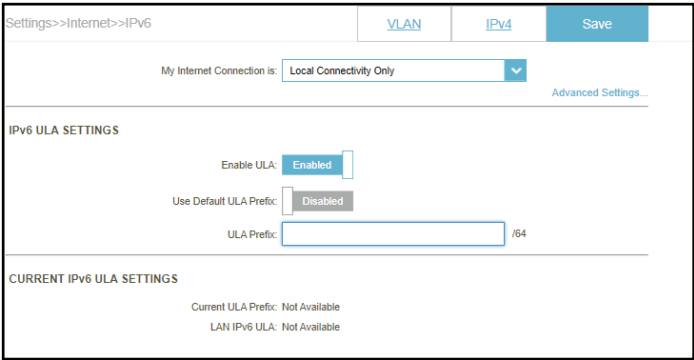
If you select **Stateful DHCPv6** as the Autoconfiguration Type:

- 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

In the Settings menu on the bar at the top-left of the page, click **Internet** to see the Internet configuration options for the IPv4 connection details, then click the **VLAN** link to access the configuration options for the VLAN connection details.

VLAN allows for services such as Triple-Play to be used, and divides a network into segments that can only be accessed by other devices in the same VLAN.

To configure the IPv4 Internet and view network connection details, click the **IPv4** link. Refer to **IPv4 on page 28**

To configure the IPv6 Internet and view network connection details, click the **IPv6** link. Refer to **IPv6 on page 33**

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

Status: Displays the current ULA prefix. lick to enable or disable the Triple-Play VLAN feature. More configuration options will be available if the Status is enabled.



Internet - VLAN

If Triple-Play Status 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 menu to assign to the corresponding VLAN (0-7). Traffic with a higher priority ID takes precedence over traffic with a low priority ID tag.

Internet

A Triple-Play (VLAN) is a switched network that is logically segmented by function, project team, or application, without regard to the physical location of the users. You can configure which hardware port will be assigned to a VLAN, and all packets from a network device in a VLAN will only be forwarded to other devices in the same VLAN.

Settings>>Internet>>VLAN

IPv6 IPv4 Save

Triple-Play

Status: Enabled

Internet VLAN

VLAN TAG: Disabled

Internet VLAN ID:

Priority ID: 0

IPTV VLAN

VLAN TAG: Disabled

IPTV VLAN ID:

Priority ID: 0

VOIP VLAN

VLAN TAG: Disabled

VoIP VLAN ID:

Priority ID: 0

Interface Traffic Type Setting

LAN Port : From the drop-down menu, you can select the type of connection (Internet, IPTV, or Voice over IP) coming from the WAN connection to each interface on the router.

Interface Traffic Type Setting

LAN Port: Internet

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 fastest 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 password to use for wireless security. Wireless clients will need to enter this password to successfully connect to the network.

Wireless

Use this section to configure the wireless settings for your D-Link Router. Please make sure that any changes made in this section will need to be updated on your wireless device.

Settings >> Wireless Guest Zone Save

Wi-Fi Mesh

Status: Enabled

Smart Connect

Status: Enabled

Wireless

Status: Enabled

Wi-Fi Name (SSID):

Password:

[Advanced Settings](#)

Wireless - Advanced Settings...

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

Transmission Power: Select a 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.

Wireless

Status:

Enabled

Wi-Fi Name (SSID):

R1-G416-BD3A

Password:

kkqur47847

Advanced Settings...

Security Mode:

WPA3-Personal

Transmission Power:

High

Schedule:

Always Enable

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 password to use for wireless security. Wireless clients will need to enter this password to connect to the network.

Smart Connect

Status:

Disabled

2.4GHz

Status:

Enabled

Wi-Fi Name (SSID):

G416-8D3A

Password:

kkqr47847

Advanced Settings...

Security Mode:

WPA3-Personal

802.11 Mode:

Mixed 802.11b/g/n

Wi-Fi Channel:

Auto

Transmission Power:

High

Channel Width:

Auto 20/40 MHz

HT20/40 Coexistence:

Enabled

Visibility Status:

Visible

Schedule:

Always Enable

 +

5GHz

Status:

Enabled

Wi-Fi Name (SSID):

G416-8D3A

Password:

kkqr47847

Advanced Settings...

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 security protection among these modes. Note that WPS will be disabled if WPA3 is in use.

802.11 Mode (2.4GHz): Select a desired wireless networking standard to use. The available options for the 2.4 GHz wireless network are **Mixed 802.11b/g/n/ax**, **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 a desired channel from 1-13. The default is **Auto** (recommended).

Transmission Power: Select a 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/a) devices, or select **20 MHz** if you are using a mix of 802.11b/g/a devices.

HT20/40 Coexistence (2.4GHz): Enable or disable HT20/40 Coexistence.

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.

2.4GHz

Status: ☒ Enabled

Wi-Fi Name (SSID):

Password:

[Advanced Settings...](#)

Security Mode:

802.11 Mode:

Wi-Fi Channel:

Transmission Power:

Channel Width:

HT20/40 Coexistence: ☒ Enabled

Visibility Status:

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 security protection among these modes. Note that WPS will be disabled if WPA3 is in use.

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

DFS Channel: If Auto Channel is selected, select this option to help find one with the least interference.

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

Channel Width (5GHz): Select **Auto 20/40/80/160 MHz** or **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 a 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

Status: ☐ Enabled

Wi-Fi Name (SSID):

Password:

[Advanced Settings...](#)

Security Mode:

802.11 Mode:

Wi-Fi Channel:

Transmission Power:

Channel Width:

Visibility Status:

Schedule:

Wi-Fi Protected Setup

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

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



Guest Zone

Go to **Settings > Wireless**, then click on 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 separated 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

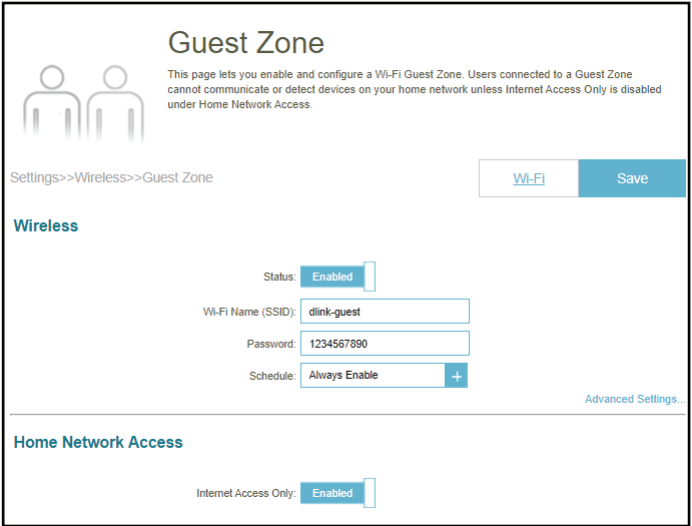
Status: Enable or disable the Guest Zone feature. The status is disabled by default.

Wireless Name (SSID): Create a name for your wireless network using up to 32 characters.

Password: Create a password to use for wireless security. 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-Persoanl**, or **WPA3-Personal**. WPA3 provides the highest level of security protection among these modes. Note that WPS will be disabled if WPA3 is in use.

Security Mode: WPA2/WPA3-Personal

Home Network Access

Internet Access Only: Enabled

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 **192.168.125.1**. 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://G530/ISP-xxxx.local/** (where xxx represents the last 4 characters of your router's MAC address). You can replace **G530/ISP-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 your computers. If enabled, your computers will use the router's settings for DNS service.

Network

Use this section to configure the network settings for your device. You can enter a name for your device in the management link field, and use the link to access web UI in a web browser. We recommend you change the management link if there are more than one D-Link devices within the network.

Settings > Network

Save

Network Settings

LAN IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Management Link: http://G416-BD3A.local/

Local Domain Name:

Enable DNS Relay: Enabled

[Advanced Settings](#)

DHCP Server

Status:

Enable or disable the DHCP server.

DHCP IP Address Range:

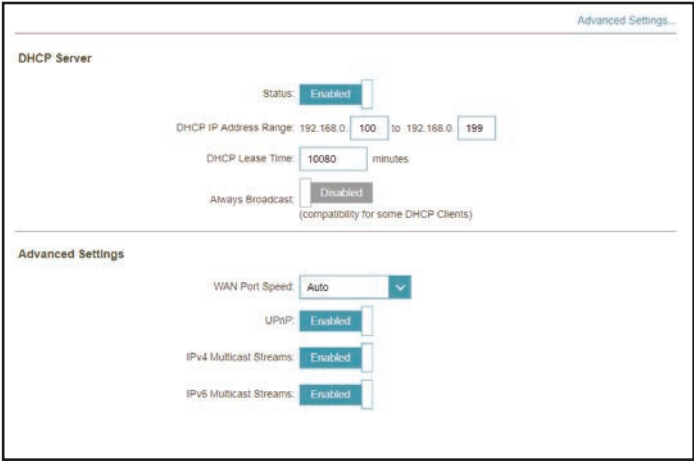
Enter the start and end IP addresses for the DHCP server's IP assignment. **Note:** *If you statically assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.*

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:

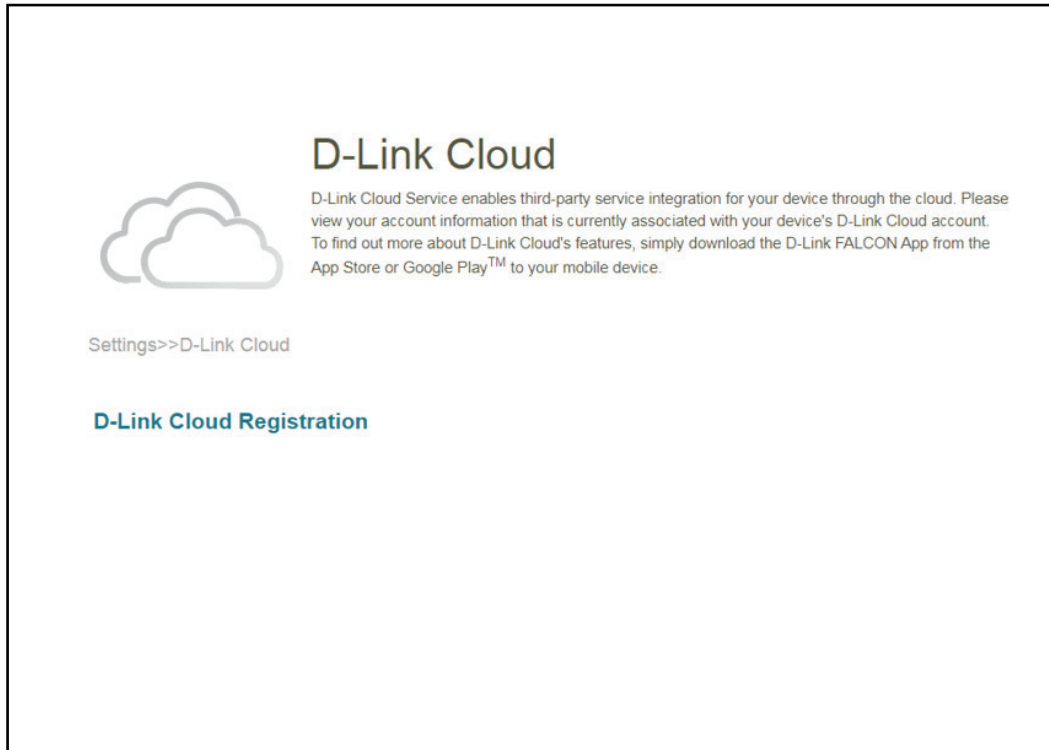
Allow or disallow IPv4 multicast traffic to pass through the router from the Internet. This is enabled by default.

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 shows whether you are registered with D-Link Cloud Service and your email address associated with the account. It enables you to manage your device anytime, anywhere and check the status of your router. Use the D-Link FALCON app to find out more about D-Link Cloud's features.

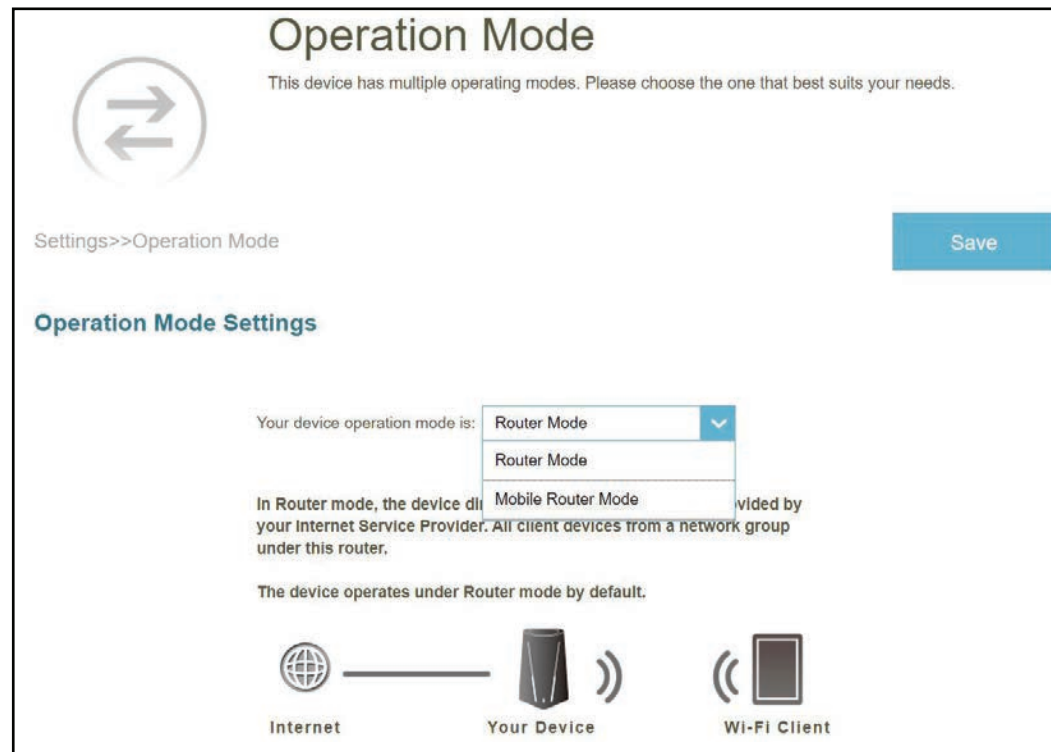


Operation Mode

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 or Mobile Router.

Router Mode: In this mode, G530 directly connects to the Internet provided by your ISP. All client devices from a network group are connected and managed under this router. This is the default mode.

Mobile Router: In this mode, G530 connects to the Internet via 5G/LTE network provided by your Cellular Internet Service Provider. All client devices from the network group are connected and managed under this mobile router.



The screenshot shows the 'Operation Mode' configuration page. At the top, there is a circular icon with two arrows forming a loop. Below it, the title 'Operation Mode' is displayed, followed by the text 'This device has multiple operating modes. Please choose the one that best suits your needs.' A breadcrumb trail 'Settings>>Operation Mode' is on the left, and a blue 'Save' button is on the right. The section 'Operation Mode Settings' contains a dropdown menu labeled 'Your device operation mode is:' with 'Router Mode' selected. Below the dropdown, text explains that in Router mode, the device connects directly to the Internet Service Provider (ISP) and manages all client devices. A note states that the device operates under Router mode by default. At the bottom, a network diagram shows 'Internet' connected to 'Your Device', which is then connected to 'Wi-Fi Client'.

Operation Mode

This device has multiple operating modes. Please choose the one that best suits your needs.

Settings>>Operation Mode

Save

Operation Mode Settings

Your device operation mode is: Router Mode

In Router mode, the device directly connects to the Internet Service Provider. All client devices from a network group are managed under this router.

The device operates under Router mode by default.

Internet — Your Device — Wi-Fi Client

Features

Parental Control

Go to **Features > Parental Control** to configure parental control policies. You can configure schedules that restrict online hours 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:

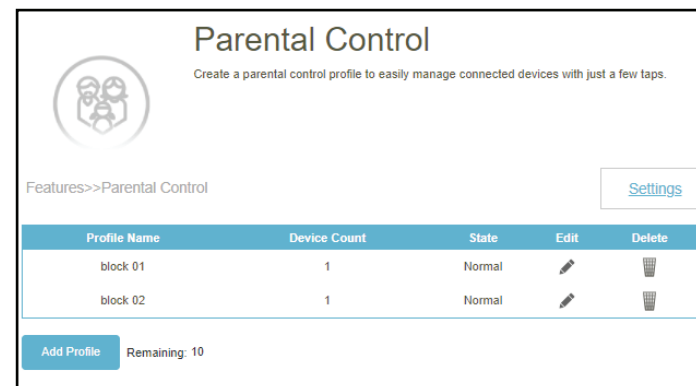
- Profile Name:** The name describes this profile.
- Device Count:** The number of devices that this policy will be applied to.
- State:** Displays the current status of Internet accessibility, i.e. Normal, Schedule Paused, or Paused on Demand.
- Edit:** Edit this access profile.
- Delete:** Remove this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

A maximum of 12 profiles can be defined. Once a profile has been set, you will start receiving weekly reports on Internet access activity of the clients through AI Assistant.

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 a 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

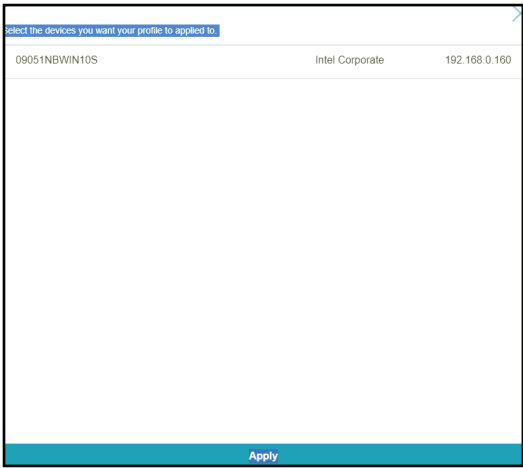
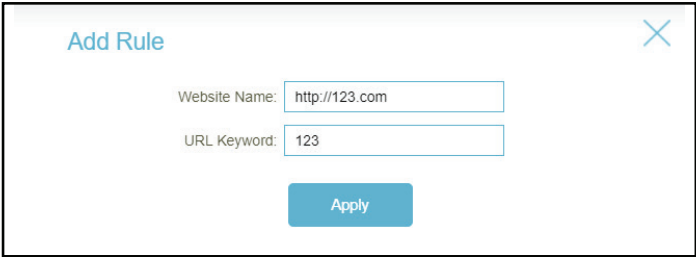
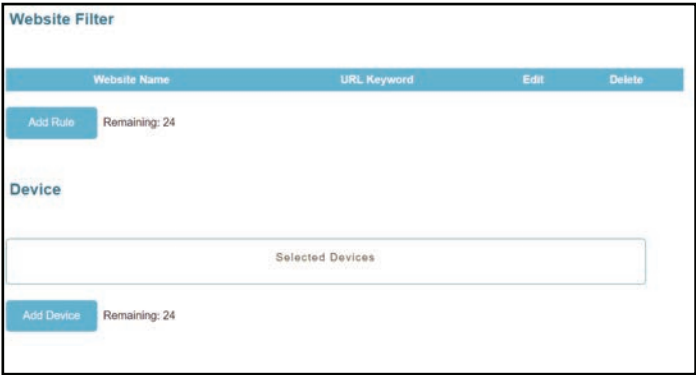
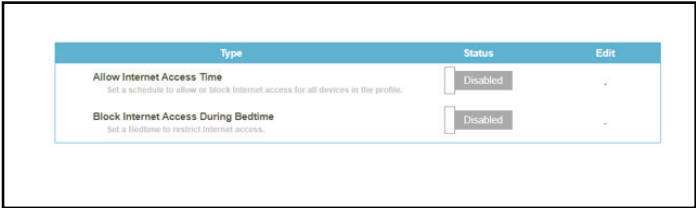
Click **Add Rule** to add a new website to be blocked:

- Website Name:** Enter a 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 into 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 **Pause for Internet Access** of specified devices of the profile immediately.



Click **Settings** to view the messages that will be displayed to the Internet access restricted users.

Blocked Webpage Message

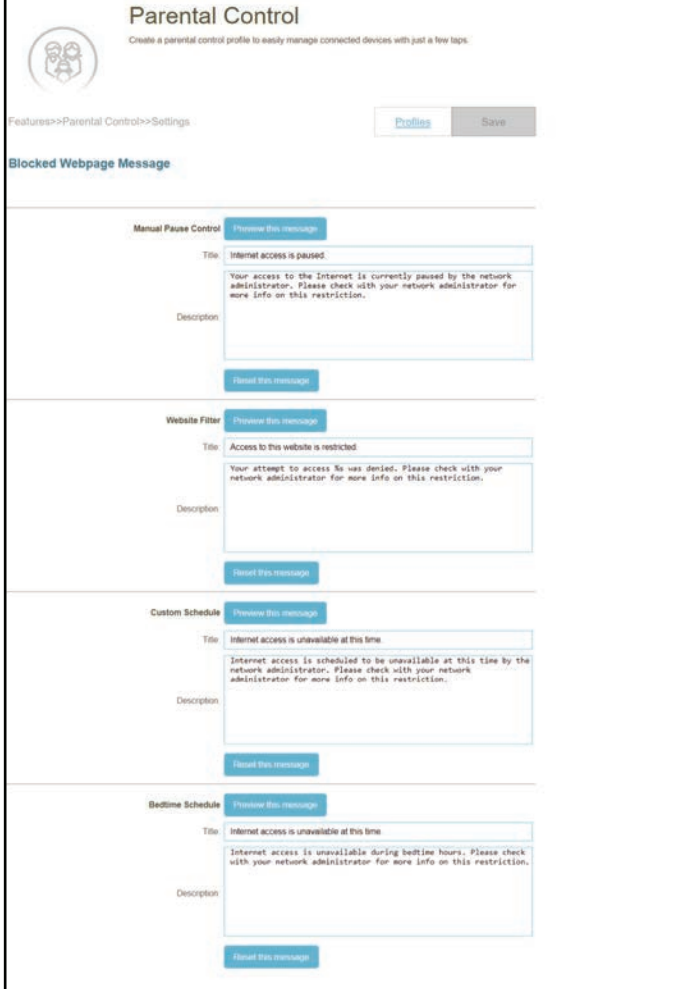
You can view and customize displayed messages and titles in **Settings** when **Manual Pause Control**, **Website Filter**, **Custom Schedule**, and **Bedtime Schedule** is enabled.

Title: Enter a title for the message in the text box.

Description: State a message to inform users about the restricted Internet access.

Reset this message: Click this button to reset the modified message to its factory default.

Preview this message: Displays the presentation of the message on a new webpage.



Parental Control
Create a parental control profile to easily manage connected devices with just a few taps.

Features > Parental Control > Settings

[Profiles](#) [Save](#)

Blocked Webpage Message

Manual Pause Control [Preview this message](#)

Title: Internet access is paused

Description: Your access to the Internet is currently paused by the network administrator. Please check with your network administrator for more info on this restriction.

[Reset this message](#)

Website Filter [Preview this message](#)

Title: Access to this website is restricted

Description: Your attempt to access this website has been denied. Please check with your network administrator for more info on this restriction.

[Reset this message](#)

Custom Schedule [Preview this message](#)

Title: Internet access is unavailable at this time

Description: Internet access is scheduled to be unavailable at this time by the network administrator. Please check with your network administrator for more info on this restriction.

[Reset this message](#)

Bedtime Schedule [Preview this message](#)

Title: Internet access is unavailable at this time

Description: Internet access is unavailable during bedtime hours. Please check with your network administrator for more info on this restriction.

[Reset this message](#)

Data Cap

Go to **Features -> Data** to configure the Data Cap settings for your device. You can monitor the data usage in real-time and receive alert messages when you reached your data usage allowance.

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

Blocked Webpage Message

Data Cap: Enable or disable data cap.

Amount: Set the maximum data usage allowance in GB.

Warning Ratio (%): Set the Warning Ratio to which an alert message will be triggered.

Reset Date Monthly: Enter a day of the month in which the data cap will be reset.

Send SMS: Enable or disable **Send SMS** when the data cap is reached

Phone Number: When **Send SMS** is enabled, enter the phone number for an alert message to be sent.

Note: Sending SMS messages may incur additional fees. Please contact your ISP for more information.

The screenshot shows the 'Cellular Data Cap Settings' page. At the top, it says 'Advanced>>Cellular Data Cap'. Below that, the title 'Cellular Data Cap Settings' is displayed. The settings include:

- Data Cap:** A toggle switch set to 'Enabled'.
- Amount:** A text input field containing '1' followed by 'GB'.
- Warning Ratio (%):** A dropdown menu set to '100%' with an upward arrow icon.
- Reset Date monthly:** A text input field containing '1'.
- Current data consumption:** A label showing '0.000 GB'.
- Reset data:** A blue button.
- Send SMS:** A toggle switch set to 'Disabled'.

SMS

Go to **Features** -> **SMS** to send or receive SMS messages. This page shows all messages that are stored on the SIM card. Click **Save** at any time to save the changes you have made on this page.

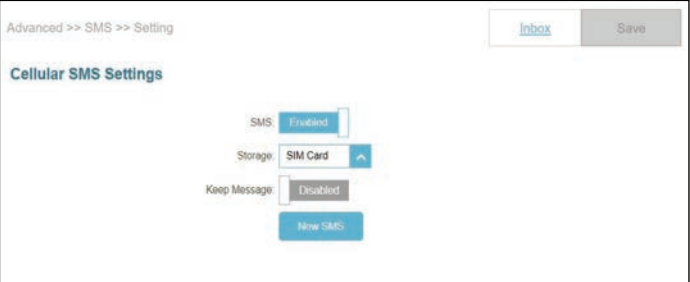
Cellular SMS Settings

SMS: Enable or disable the SMS receiving function.

Storage: Select **SIM Card** or **Modem** to store the SMS messages.

Keep Message: Enable or disable Keep Message.

Keep Number: Set the amount of SMS messages to be saved. Up to 20 messages can be saved.

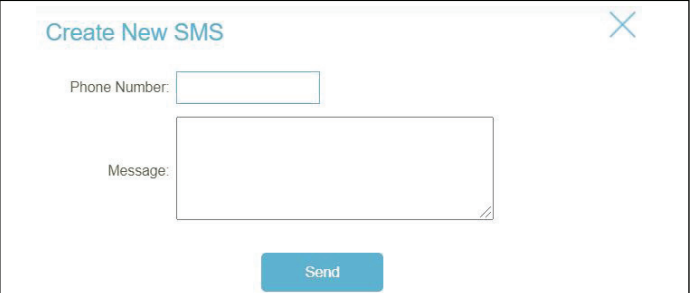


Click **New SMS** to create new SMS messages.

Cellular SMS Settings

Phone Number: Enter the phone number of a recipient.

Message Enter your message here.



From the SMS page, click on **Inbox** to manage the SMS messages you have received. Select a message to display its contents in the SMS window. After you read it, you can delete it or reply to the sender.

Inbox

Status: Displays the status of the message.

ID: Displays the sender's ID.

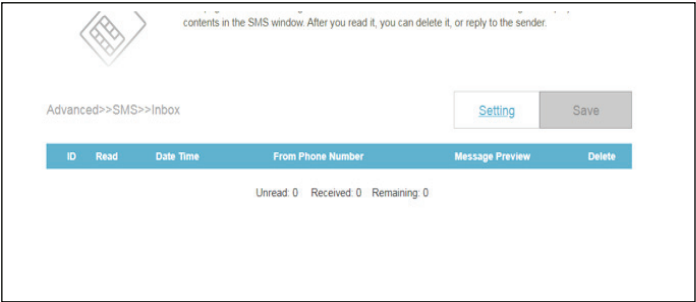
UnRead: Displays whether the message has been read or not.

Date Time: Displays the time and date at which the message is received.

From Phone Number: Displays the phone number of the sender.

Message Preview: Displays a preview of the selected message.

Delete: Deletes the selected SMS message.



PIN

Go to **Features** -> **Pin** to configure your SIM card's PIN. Click **Save** at any time to save the changes you have made on this page.

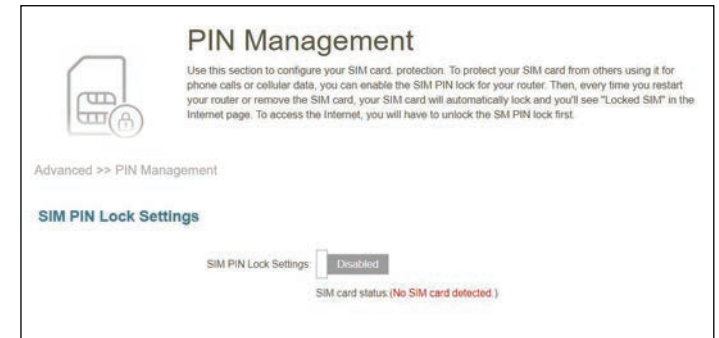
Inbox

SIM PIN Lock Settings: Enable or disable SIM PIN Lock

SIM card status: Displays the status of your SIM card.

To change your SIM's PIN, enter a new PIN in the PIN text field. After enabling your PIN protection, you'll have to input your PIN whenever your SIM card is switched.

Click **Apply** when you are done.



Firewall

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

To configure your IPv4 firewall rules, click the **IPv4 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on page 70
To configure your IPv6 firewall rules, click the **IPv6 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on page 70

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. It is not recommended to enable DMZ unless the clients 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 and ensure 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. Through such a simple firewall configuration, you can directly deny access to computers behind the router.

IPv6 Ingress Filtering: Enable or disable IPv6 ingress filtering for preventing incoming packets from suspicious senders.

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

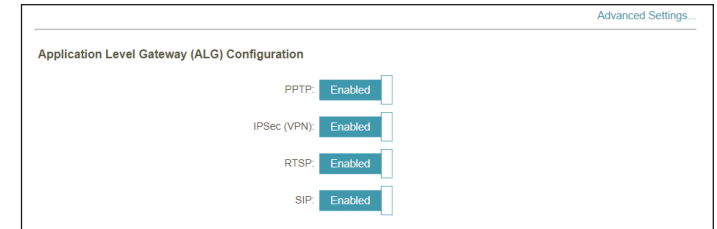
Different ALGs provide special handling for specific protocols or applications. A number of ALGs for common applications are enabled by default as stated below.

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 to your corporate network, try to turn off this ALG. Please check with the system administrator of your corporate network for whether your VPN client supports NAT traversal.

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

SIP Allows devices and applications using Voice over IP (VoIP) 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 to turn off this ALG.



Firewall Settings - IPv4/IPv6 Rules

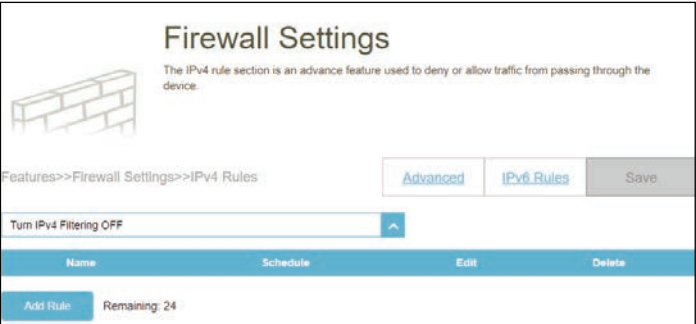
Go to **Features > Firewall**, then click the **IPv4 Rules** tab or the **IPv6 Rules** tab to configure rules for filtering the inbound/outbound traffic based on parameters like IP address with ports.

To configure the Firewall Advanced settings, click the **Advanced** link. Refer to **Firewall** on page **68**

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 you want to **ALLOW** or **DENY** the rules you create. You can also choose to turn **OFF** filtering.

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, and using the drop-down menu to 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, and using the drop-down menu to 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 a traffic protocol 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 a time schedule that the rule will be enabled on. 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 **82** for more information.
- Click **Apply** when you are done.

A maximum of 24 rules can be defined.

Create New Rule

Name:

Source IP Address Range:

WAN

Destination IP Address Range:

LAN

Protocol & Port Range:

TCP

Schedule:

Always Enable

Apply

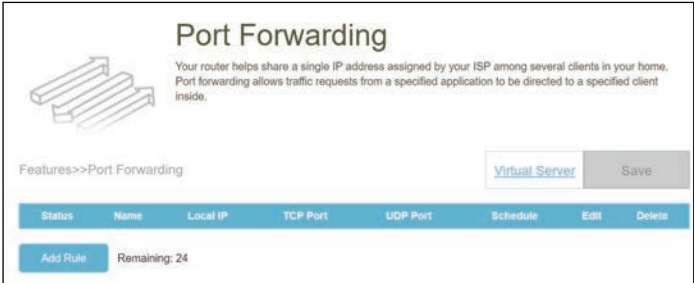
Port Forwarding

Go to **Features > Port Forwarding** to specify a port or a range of ports to be 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 74.

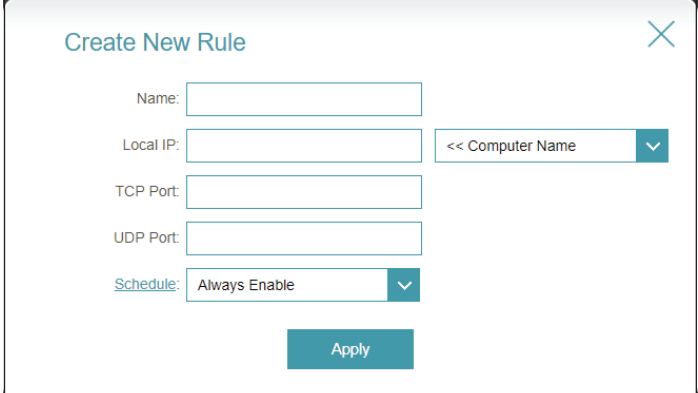
Click **Save** at any time to save the changes you have made on this page.

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 device 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 forward. You can enter a single port or a range of ports and separate ports with a comma (for example: 24,1009,3000-4000).
- UDP Port:** Enter the UDP ports that you want to forward. You can enter a single port or a range of ports and separate ports with a comma (for example: 24,1009,3000-4000).
- Schedule:** Use the drop-down menu to select a time schedule that the rule will be enabled on. 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 **82** for more information.



The screenshot shows a 'Create New Rule' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field.
- Local IP:** A text input field followed by a dropdown menu showing '<< Computer Name'.
- TCP Port:** A text input field.
- UDP Port:** A text input field.
- Schedule:** A dropdown menu currently set to 'Always Enable'.
- Apply:** A blue button at the bottom right.

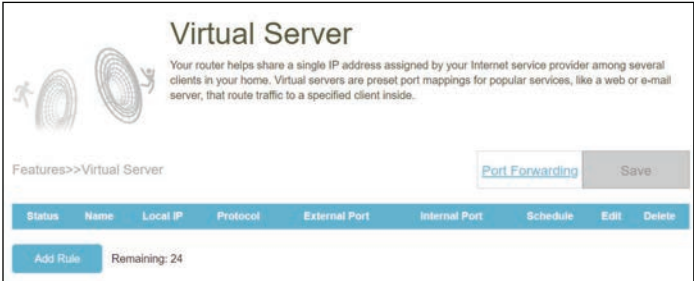
Port Forwarding - Virtual Server

Go to **Features > Port Forwarding** to click on the **Virtual Server** tab for configuring its settings and specifying a single 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 72

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 a requested service, the router redirects the external service request to an appropriate internal host.

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

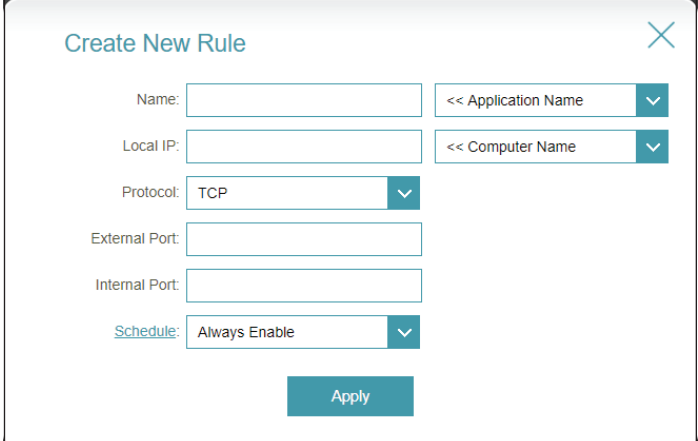
Protocol: Select a traffic protocol to allow or deny (**TCP**, **UDP**, **Both**, or **Other**).

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

External Port: If you select **TCP**, **UDP**, or **Both** as the protocol, enter the public port you want to forward.

Internal Port: If you select **TCP**, **UDP**, or **Both** as the protocol, enter the private port you want to open.

Schedule: Use the drop-down menu to select a time schedule that the rule will be enabled on. 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 **82** for more information.



The screenshot shows a 'Create New Rule' dialog box with a close button (X) in the top right corner. The form contains the following fields and options:

- Name:** A text input field followed by a dropdown menu showing '<< Application Name'.
- Local IP:** A text input field followed by a dropdown menu showing '<< Computer Name'.
- Protocol:** A dropdown menu currently set to 'TCP'.
- External Port:** A text input field.
- Internal Port:** A text input field.
- Schedule:** A dropdown menu currently set to 'Always Enable'.
- Apply:** A blue button at the bottom right.

Static Routes - IPv4

Go to **Features > Static Routes** to define custom routes and control that external data traffic from a specified IP address to be forwarded to a specified client in the LAN behind the router.

To configure the Static Route IPv6 settings, click the **IPv6** tab. Refer to **Static Routes - IPv6** on page 77

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 this route.

Mask: Enter the subnet mask of the route.

Gateway: Enter your next hop gateway to be taken if this route is in use.

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

Interface: Select an interface that the IP packet must use to transit out of the router when this route is in use.

Click **Apply** when you are done.

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 **76**.

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 IP address of this route.
- PrefixLen:** Enter the number of prefix bits of the IP address that will take this route.
- Gateway:** Enter your next hop gateway to be taken if this route is in use.
- Metric:** Enter a route metric value between 1 and 128. This value indicates the cost of using this route and with 1 as the lowest cost.
- Interface:** Select an interface that the IP packet must use to transit out of the router when this route is in use.

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. Enabling this feature will reveal further configuration options.

Status: Displays the current dynamic DNS connection status.

Server Address: Select a Dynamic DNS server 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 username.

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.

The screenshot shows the 'Dynamic DNS' configuration page. At the top, there's a title 'Dynamic DNS' and a brief description: 'Dynamic Domain Name Service allows your router to associate an easy-to-remember domain name such as [YourDomainName].com with the regularly changing IP address assigned by your Internet Service provider. This feature is helpful when running a virtual server.' Below this, there's a 'Save' button. The main configuration area includes:

- 'Enable Dynamic DNS:' with a toggle switch set to 'Enabled'.
- 'Status:' showing 'Disconnected'.
- 'Server Address:' with a dropdown menu currently showing 'no-ip.com'.
- 'Host Name:', 'User Name:', and 'Password:' (masked with asterisks) text input fields.
- 'Time Out:' with a value of '24' and a unit of 'hours'.

 At the bottom, there's a table with columns: 'Status', 'Host Name', 'IPv4 Address', 'Edit', and 'Delete'. Below the table is an 'Add Record' button and a status 'Remaining: 10'.

A maximum of 10 records can be defined.

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 for DDNS configuration. Alternatively, select the network interface for DDNS configuration.

Click **Apply** when you are done.

A maximum of 10 records can be defined.

Status	Host Name	IPv6 Address	Edit	Delete
Add Record	Remaining: 10			

Create New Record ✕

Host Name:

IPv6 Address: << Computer Name ▼

Apply

Quick VPN

Go to **Features > Quick VPN**. This page will help you configure the Quick VPN feature of your router. For more information about Quick VPN, refer to **Quick VPN** on page **92**. 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 with an IP address from your ISP using DHCP, it may frequently change, requiring clients credentials to be set up again. A DDNS address can avoid this hassle.

To configure the User settings and grant users with Virtual Private Network (VPN) permission, go to **Management > User**. Refer to **User** on page **87**.

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.

Username: Enter a username.

Password: Enter a password containing both numbers and letters with 8 to 32 characters in length and with a combination of numbers and letters.

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 an authentication protocol type: **MSCHAPv2**, **PAP**, or **CHAP**. **MSCHAPv2** is set as default.

MPPE: Select the encryption cipher strength for Microsoft Point-to-Point (MPPE) Encryption: **None**, **RC4-40**, or **RC4-128**. **None** is set as default.

Quick VPN

Quickly and easily create a profile for secure remote access to a Local Area Network (LAN). This profile can be used to configure other devices to connect to your LAN via a secure VPN tunnel.

Features >> Quick VPN User Save

General

L2TP over IPSec: Enabled

Username:

Password:

PSK:

VPN Profile for iOS Device and Mac OS X: Export

[Advanced Settings...](#)

Advanced

Authentication Protocol: MSCHAPv2

MPPE: None

Management

Time & Schedule - Time

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

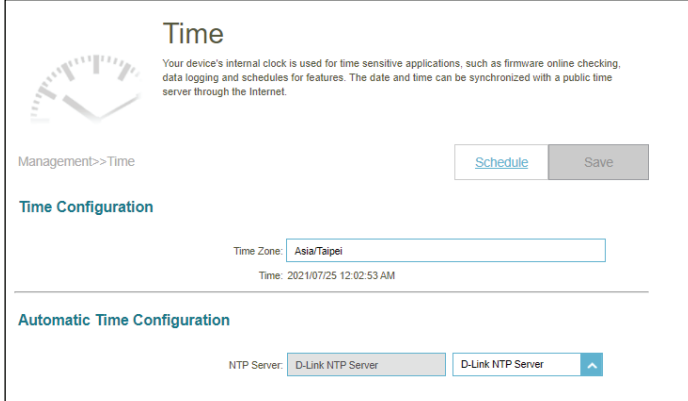
To configure the Schedule settings, click the **Schedule** tab. Refer to **Time & Schedule - Schedule** on page 82

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.

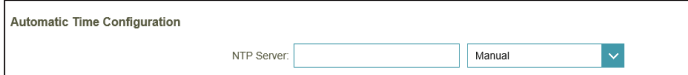
Time: Displays the current date and time of the router.



The screenshot shows the 'Time' configuration page. At the top, there is a clock icon and the title 'Time'. Below the title, a note states: 'Your device's internal clock is used for time sensitive applications, such as firmware online checking, data logging and schedules for features. The date and time can be synchronized with a public time server through the Internet.' Below this, there are two tabs: 'Schedule' (highlighted in blue) and 'Save' (grey). Under the 'Schedule' tab, the breadcrumb 'Management >> Time' is shown. The 'Time Configuration' section contains a 'Time Zone' dropdown menu set to 'Asia/Taipei' and a 'Time' display showing '2021/07/25 12:02:53 AM'. The 'Automatic Time Configuration' section features an 'NTP Server' dropdown menu with 'D-Link NTP Server' selected.

Automatic Time Configuration

NTP Server: Select one of the following servers from the drop-down menu 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 domain name.



The screenshot shows the 'Automatic Time Configuration' section. It includes a label 'Automatic Time Configuration' and an 'NTP Server' dropdown menu. The dropdown menu is currently set to 'Manual'.

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 81

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

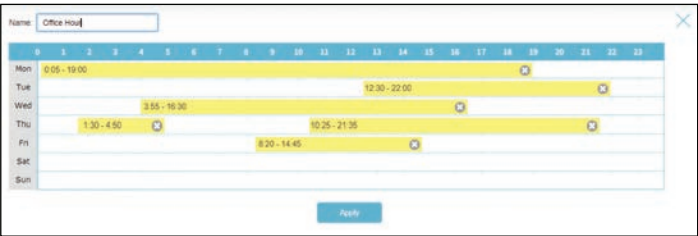
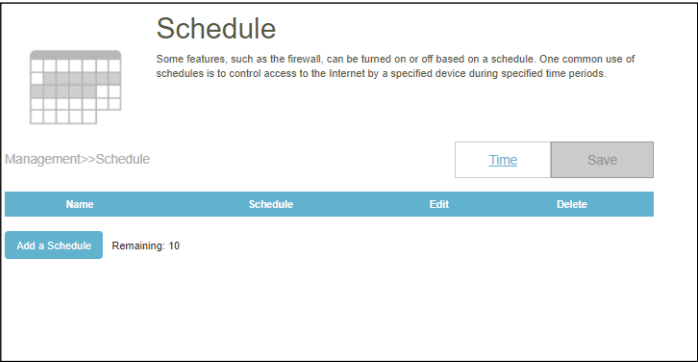
If you wish to remove a schedule, click  in the Delete column. If you wish to edit a schedule, click  in the Edit column. If you wish to create a new schedule, click the **Add a Schedule**.

On the Schedule creation page, enter a name for 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 copy of the system log to your hard drive. 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.

System Log

On-board diagnostics run continually in the background to monitor the health of your router. The results are recorded in the system log if it is enabled. This info can be used to diagnose common problems or help Customer Support resolve issues more quickly.

Management>>System Log

Save

Log Settings

System Log:

Check System Log

SysLog Settings

Enable Logging to Syslog Server:

Disabled

E-mail Settings

Enable E-mail Notification:

Disabled

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 options:

From E-mail Address: Enter an email address your SysLog messages will be sent from.

To E-mail Address: Enter an email address your SysLog messages will be sent to

SMTP Server Address: Enter your SMTP server address.

SMTP Server Port: Enter your SMTP server port. The default is 25.

Enable Authentication: Enable this option if your SMTP server requires authentication.

Account Name: Enter your SMTP account name.

Password: Enter your SMTP account password.

E-mail Log When Full or On Schedule

Send When Log Full: If enabled, the router is set to automatically send the log when it is full.

Send on Schedule: If enabled, the router is set to send the log according to a set schedule periodically, so an administrator can always be up to date on the router's operation.

Schedule: If you want to 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 82 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 86

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.

Advanced Settings... - Administration

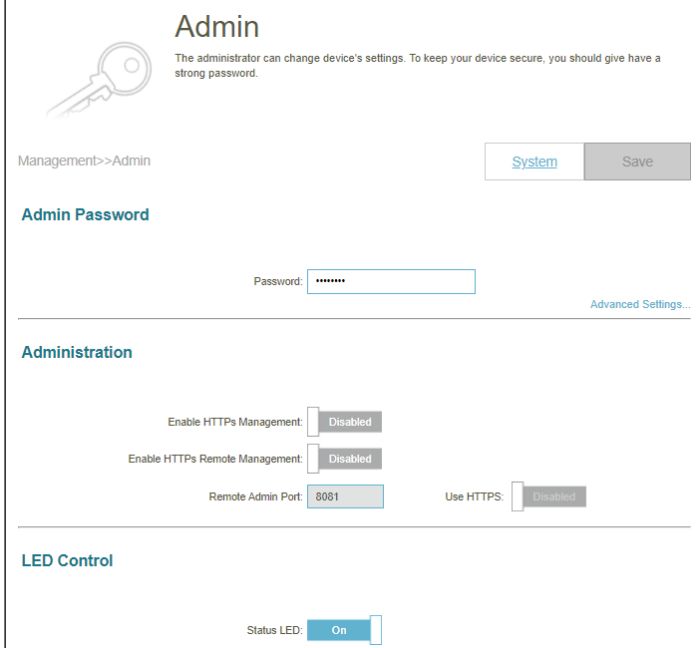
Enable HTTPS Management: Enable HTTPS to connect the router securely.

Enable HTTPS Remote Management: Enable Remote Management over the Internet using 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.



Admin
The administrator can change device's settings. To keep your device secure, you should give have a strong password.

Management>>Admin

Admin Password

Password:

[Advanced Settings...](#)

Administration

Enable HTTPS Management: ☐ Disabled

Enable HTTPS Remote Management: ☐ Disabled

Remote Admin Port:

Use HTTPS: ☐ Disabled

LED Control

Status LED: ☒ On

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 85

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

System

Save Settings to Local Hard Drive:

Click **Save** to download a backup file (bin type) of your current configuration settings to your local hard drive. This backup can later be used to restore your settings.

Load Settings from Local Hard Drive:

Click **Select File** to 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 **Reboot** 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 an 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:

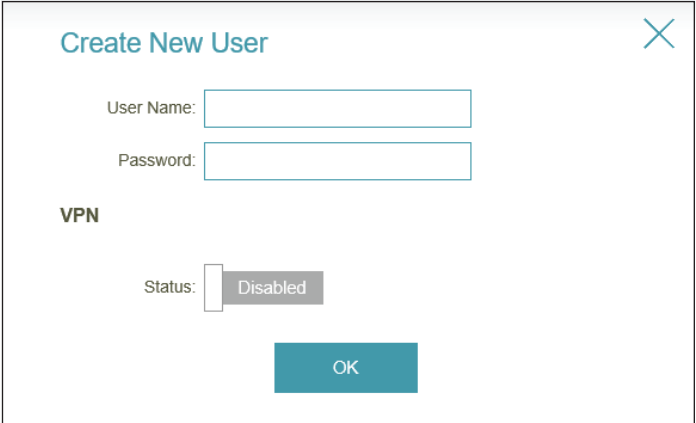
User Name: Enter a username for the new user account.
Maximum length: 20 characters.

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

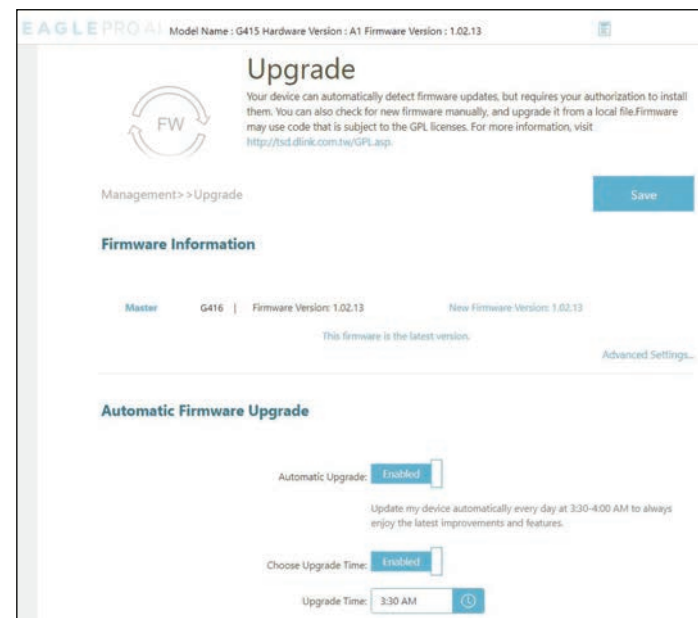
- Current Firmware Version:** Displays the current firmware version for both the main router as well as the extenders.
- Check for New Firmware:** Click this button to prompt the router to automatically check for a new firmware version. If a newer version is found, it will prompt you to install it.

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.



Data Usage

Go to **Management > Data Usage**. On the Data Usage page you can view the amount of Uplink and Downlink traffic statistics 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.

Data Usage

You can view the **Internet, LAN, Wi-Fi 2.4 GHz, or Wi-Fi 5 GHz**. The real-time network traffic in GB/s will be shown.

The table below shown the total number of data usage that are sent and received through the interface.

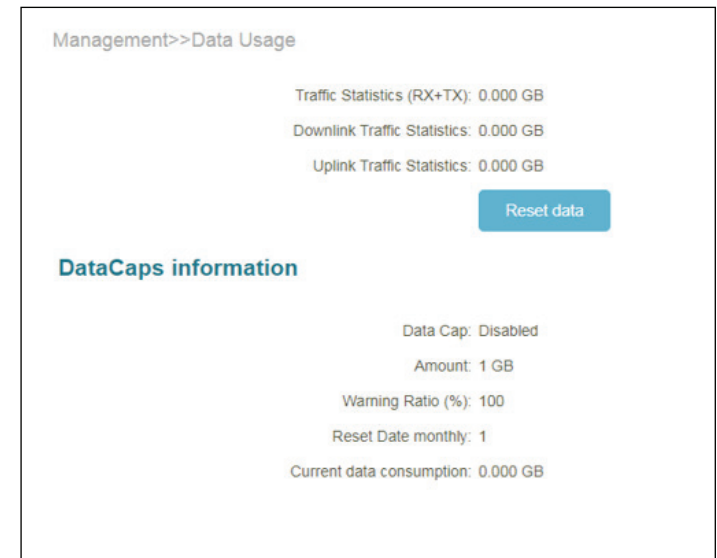
The traffic counter will reset data if the device is rebooted.

Data Usage

Traffic Statistics (Rx+Tx):	Displays the current traffic statistics of the router.
Downlink Traffic Statistics:	Displays the current downlink traffic statistics of the router.
Uplink Traffic Statistics:	Displays the current uplink traffic statistics of the router.

Datacaps information

Datacap:	Display Data Cap Enable or Disabled.
Amount:	Display amount of data usage.
Warning ratio(%):	Display the warning ratio of data usage in percentage.
Reset Date monthly:	Display number of reset date montly.
Current Data Consumption:	Display the whole current data consumption.



D-Link FALCON

With the D-Link FALCON app on your smart devices, you can get the G530 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 D-Link FALCON app is especially designed to ease your management work with the following features:

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 for individual devices during designated time periods.

AI Parental Control:

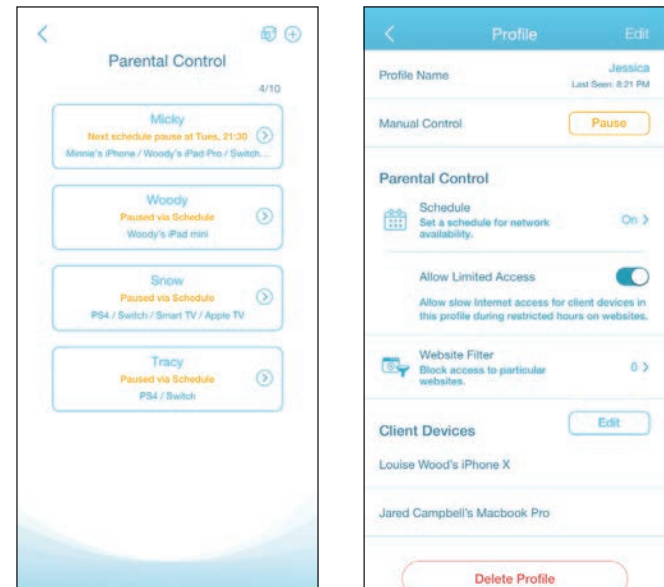
To enable this function, navigate to the **Home** screen, and tap **Parental Control**.

Then use the following procedure to add a new profile:

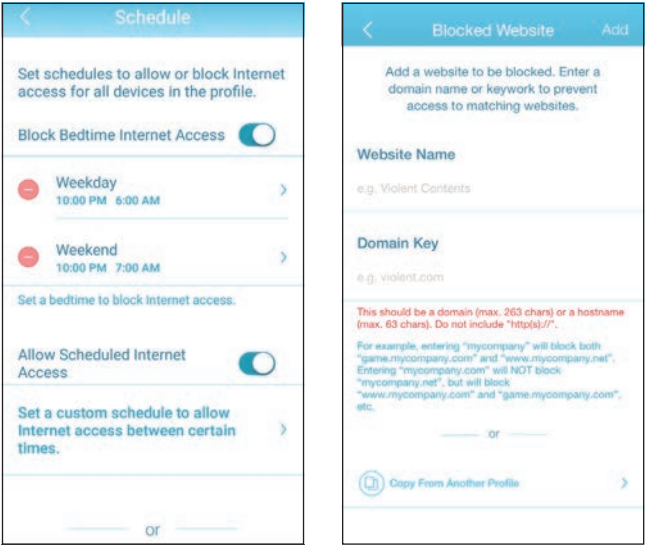
1. Tap **Start**.
2. Name this profile. Then tap **Next** to continue.
3. Select client devices to which the profile will be applied.
4. Tap **Done** to proceed.
5. The profile summary will be displayed. On this page you can tap **Pause** to immediately pause Internet to the devices specified in the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

You can set schedules to restrict Internet access.

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



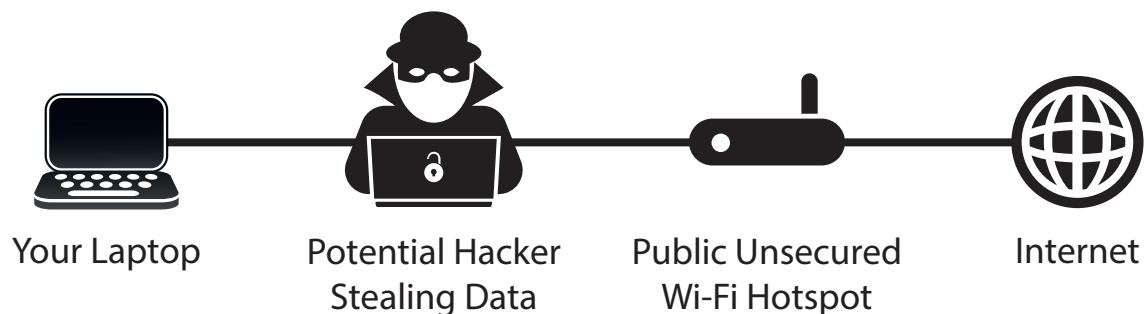
You can also block specific websites on this page to prevent the specified devices from accessing certain websites. To do this, tap **Website Filter**, tap **Add Website**, then enter the website name and the domain keyword, for example, enter *violent.com* to block all access to this site and *violent*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



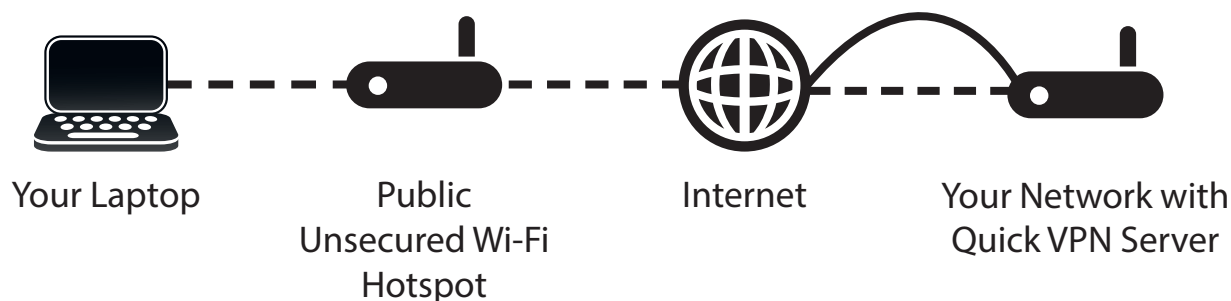
Quick VPN

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 securely 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



————— Unencrypted Data - - - - - Encrypted Data

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.

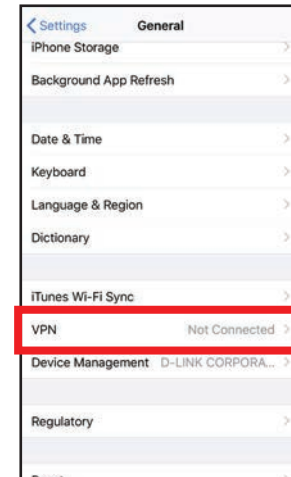
- Quick VPN only provides an added layer of security against specific types of snooping attacks and does not guarantee complete data integrity or protection. Only traffic in the tunnel between your router and device will be encrypted, WAN traffic will leave your D-Link Quick VPN enabled router unencrypted.
- 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.
- Your 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

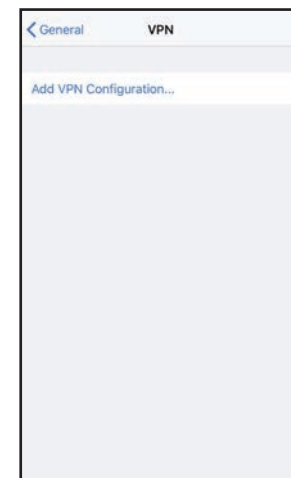
VPN Setup Instructions

This section provides Quick VPN setup instructions for iOS devices. Refer to **Quick VPN** on page **80** 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).

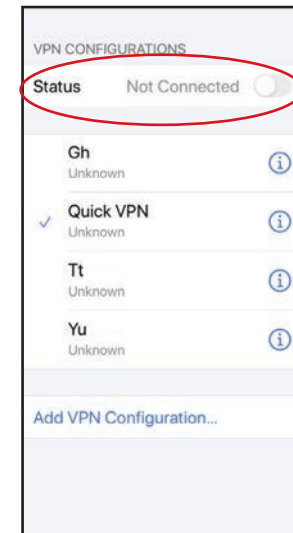
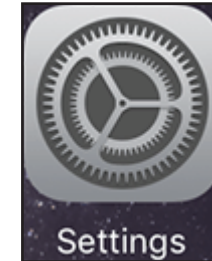
Tap **Done** to close the configuration window.

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

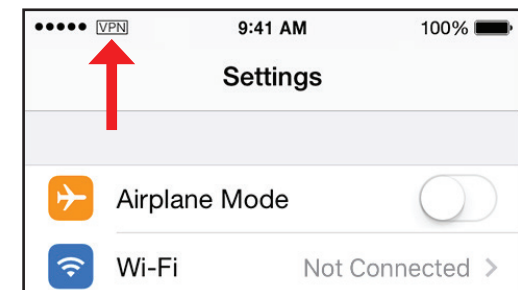
The screenshot shows the 'Quick VPN' configuration window on an iOS device. At the top, there are three buttons: 'Cancel' (blue), 'Quick VPN' (black), and 'Done' (blue). Below the buttons is a light blue header bar. The main content area is white and contains the following fields: 'Type' (set to 'IPsec'), 'Description' (set to 'Quick VPN'), 'Server' (set to 'IP/DDNS_address_of_QuickVPN'), 'Account' (set to 'vpn'), 'Password' (masked with three dots), 'Use Certificate' (a toggle switch that is currently off), 'Group Name' (empty), and 'Secret' (masked with seven dots). At the bottom, there is a light blue section labeled 'PROXY' with three buttons: 'Off' (blue), 'Manual' (white), and 'Auto' (white).

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

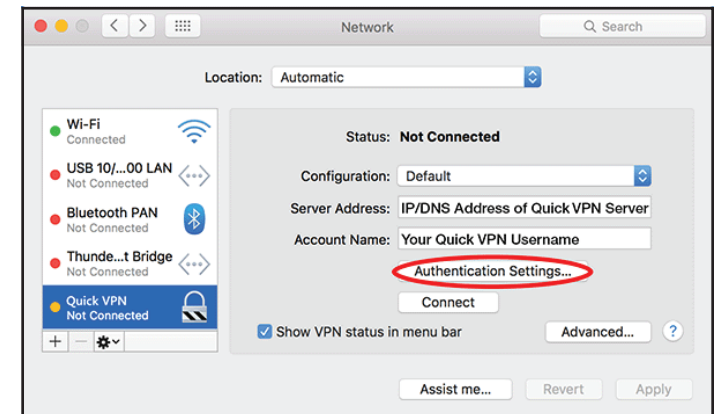
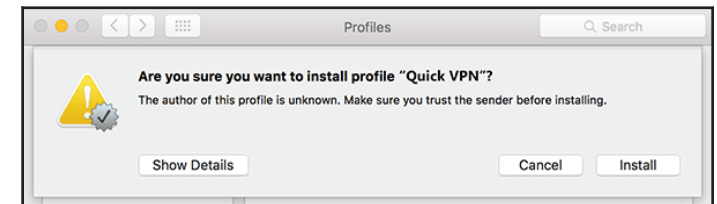
VPN Setup Instructions

This section provides Quick VPN setup instructions for OS X using the **Export** Profile function. Refer to **Quick VPN** on page **80** for your router setup instructions.

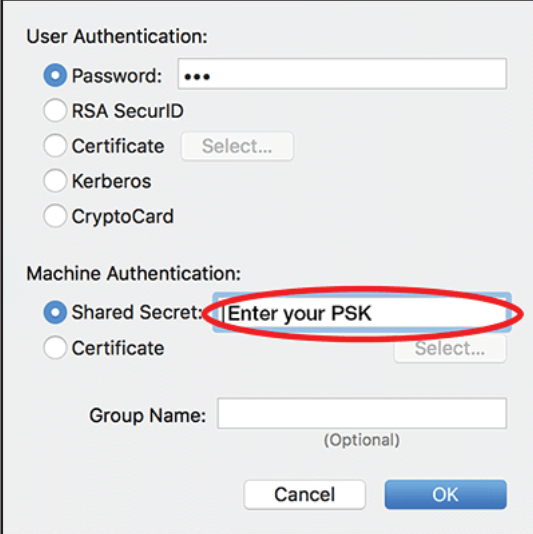
Open the exported profile. The Install Profile dialogue will appear; click **Continue** and **Install**.

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

Go to **Apple > 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**.



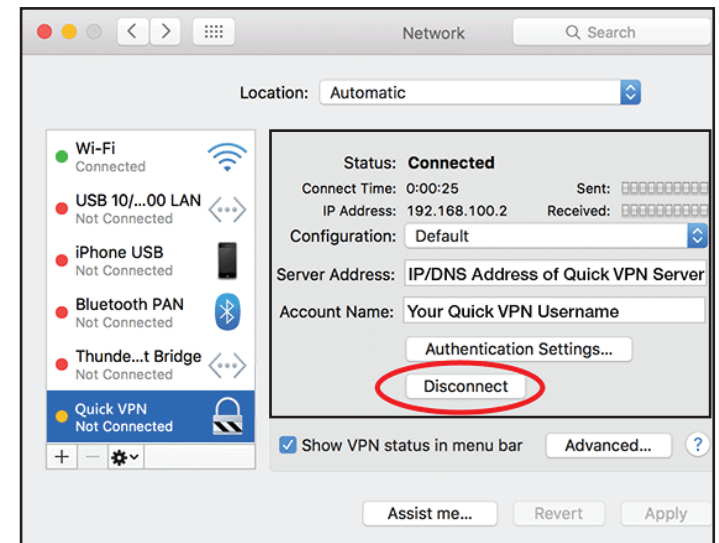
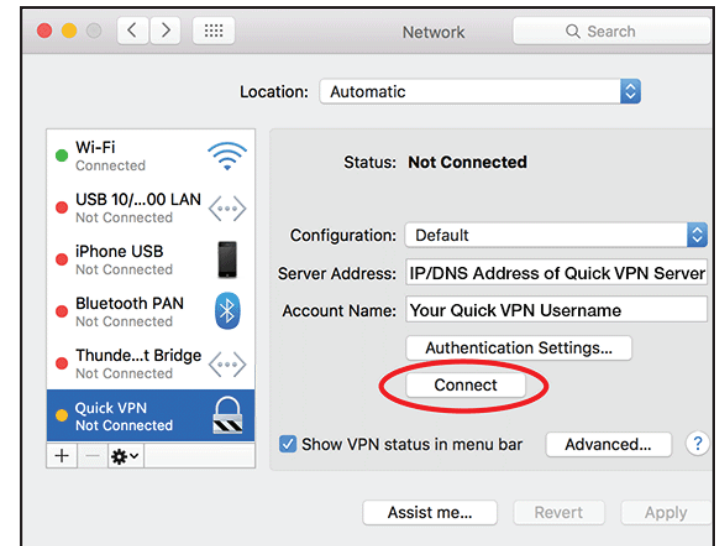
The screenshot shows a VPN configuration window with two main sections: 'User Authentication' and 'Machine Authentication'. In the 'User Authentication' section, 'Password' is selected with a radio button, and there is a text field with three dots. Other options like 'RSA SecurID', 'Certificate', 'Kerberos', and 'CryptoCard' are unselected. In the 'Machine Authentication' section, 'Shared Secret' is selected with a radio button, and its text field contains the text 'Enter your PSK', which is circled in red. There is also a 'Certificate' option with a 'Select...' button. Below these sections is a 'Group Name' field with '(Optional)' text underneath it. At the bottom right are 'Cancel' and 'OK' buttons.

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 **Apple > System Preferences... > Network**.

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



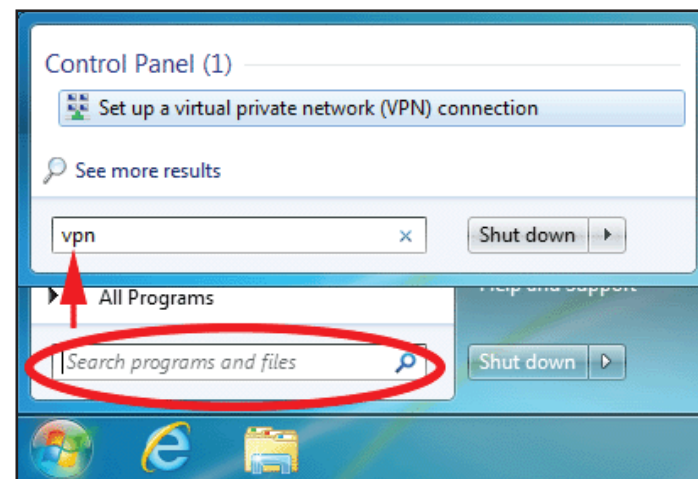
Windows 7

VPN Setup Instructions

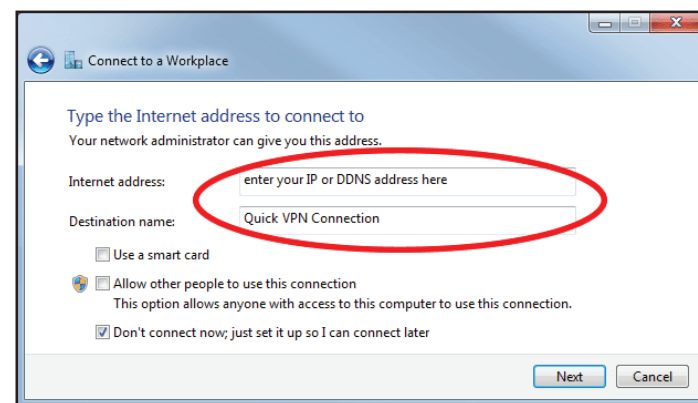
This section provides Quick VPN setup instructions for Windows 7. Refer to **Quick VPN** on page **80** for your router setup instructions.

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

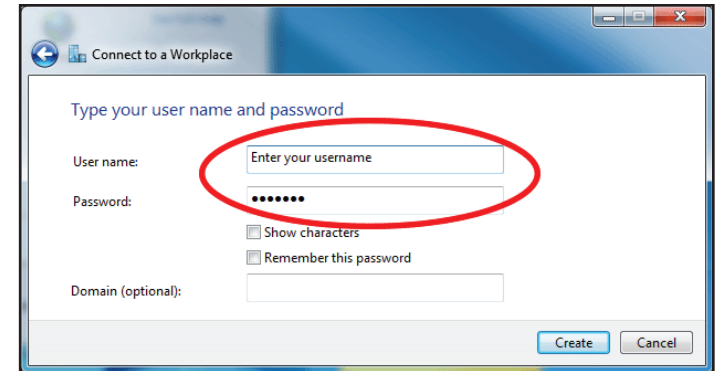
Select **Set up a virtual private network (VPN) connection**.



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**.

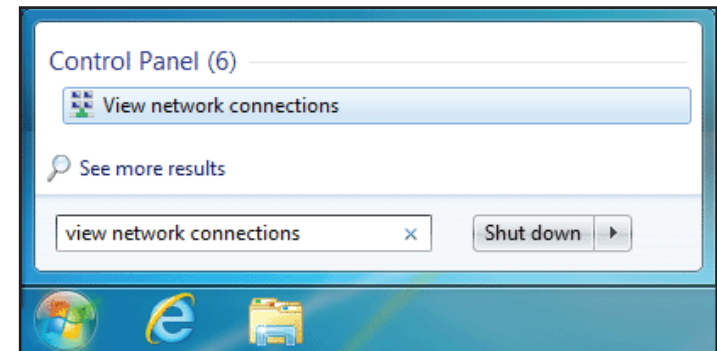


Enter your **Username**. If you would like windows to save your password, enter your **Password** and check **Remember this password**. Click **Create** to continue.



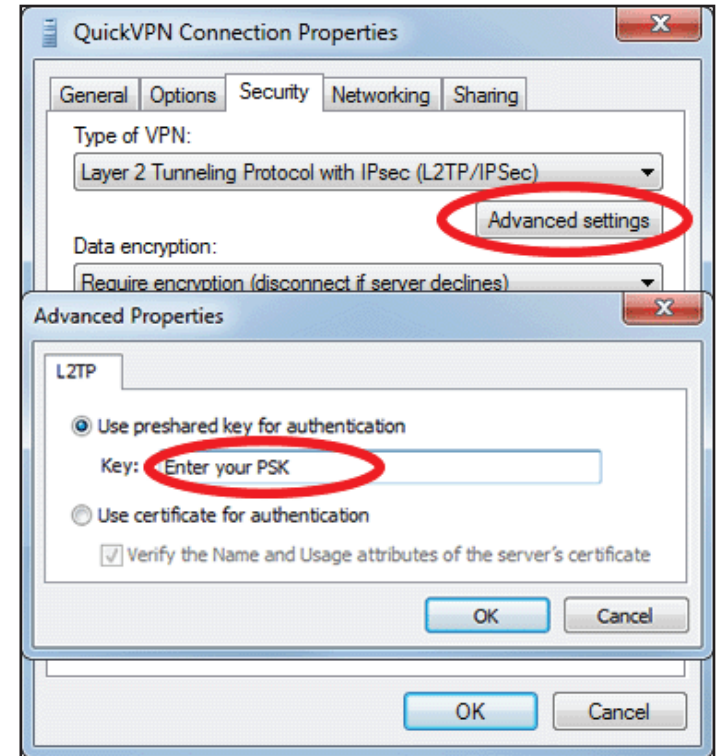
Do not click **Connect Now**.

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



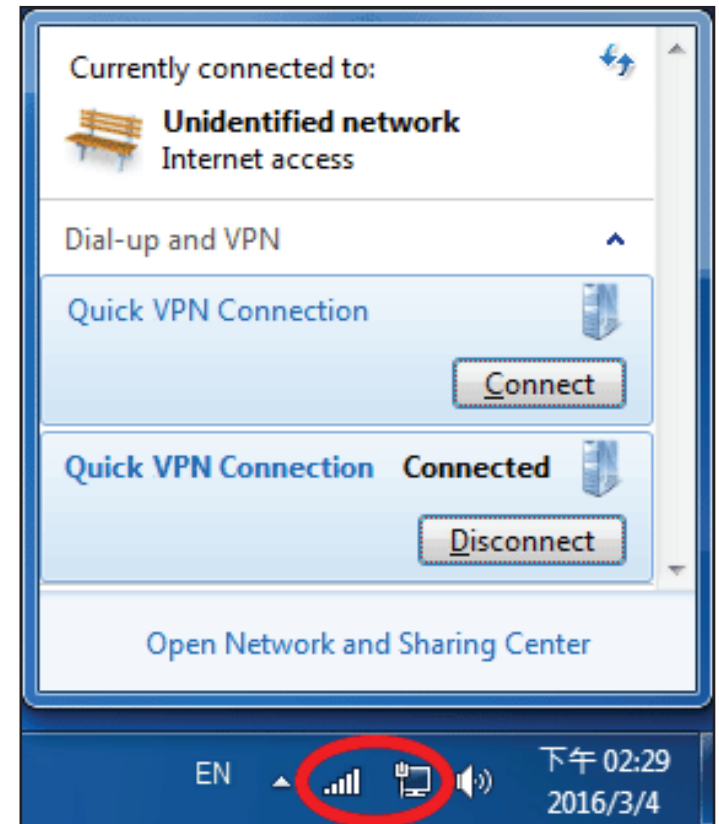
Click **Advanced settings**. Enter your **Passkey** in the **Key** text box under **Use preshared key for authentication**. Click **OK** to close **Advanced Properties** and click **OK** to close **Quick VPN Connection Properties**.

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

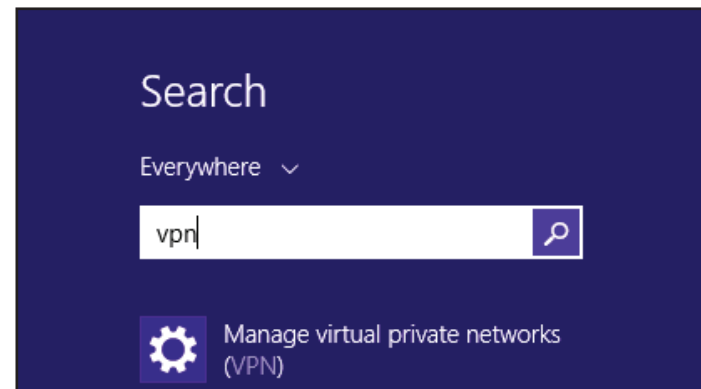
VPN Setup Instructions

This section provides Quick VPN setup instructions for Windows 8.1/8. Refer to **Quick VPN** on page **80** for your router setup instructions.

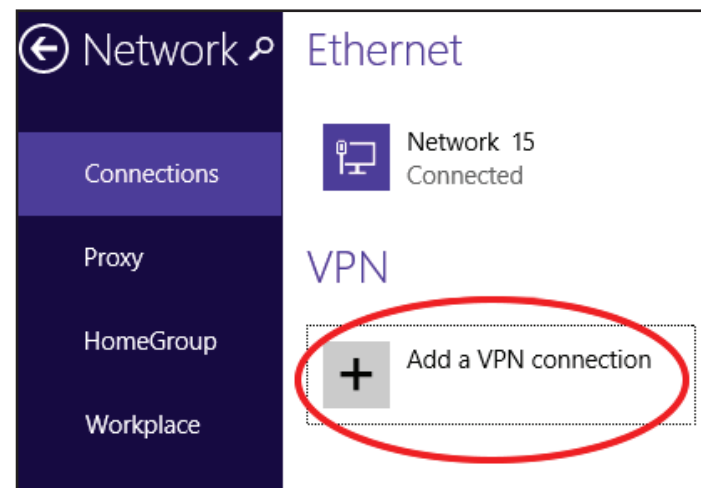
This section provides Quick VPN setup instructions for Windows 8.1/8.

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

Select **Manage virtual private networks**.



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

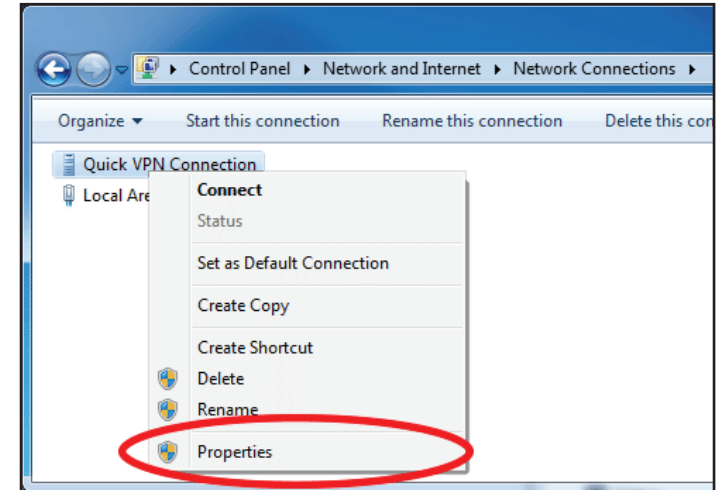


- 1 Select **Microsoft** from **VPN Provider**.
- 2 Create a name for your VPN connection.
- 3 Enter your **IP/DDNS address** of your Quick VPN server.
- 4 Select **User name and password** from **Type of sign-in info**.
- 5 If you would like windows to remember your sign-in information, enter your **User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

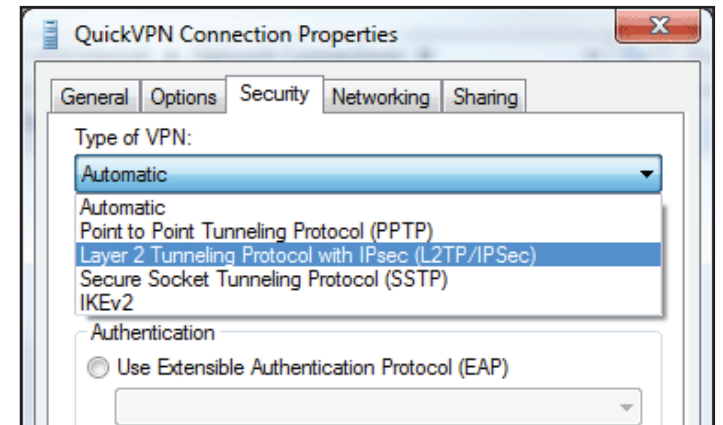
The screenshot shows the 'Add a VPN connection' window with the following fields and steps:

- Step 1:** VPN provider dropdown menu set to 'Microsoft'.
- Step 2:** Connection name text box containing 'Quick VPN'.
- Step 3:** Server name or address text box containing 'IP/DDNS Address of Quick VPN Server'.
- Step 4:** Type of sign-in info dropdown menu set to 'User name and password'.
- Step 5:** A group of fields including 'User name (optional)' with 'Username', 'Password (optional)' with masked characters, and a checked 'Remember my sign-in info' checkbox.
- Step 6:** The 'Save' button.

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

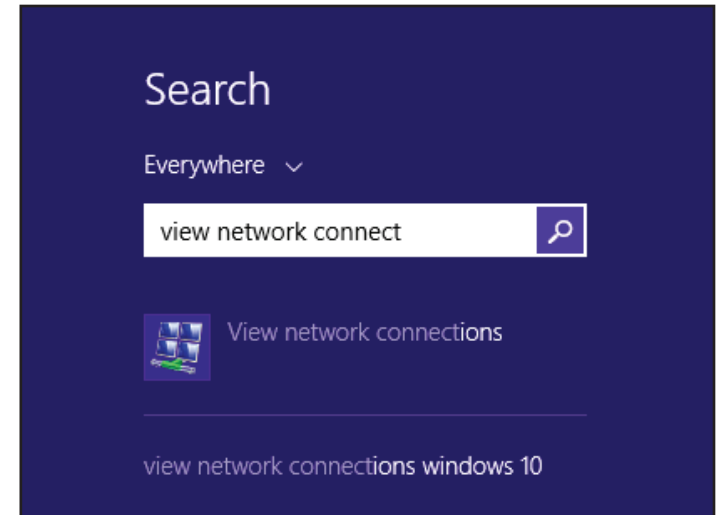


Select the **Security** tab. For the **Type of VPN**, select **Layer 2 Tunneling with IPsec (L2TP/IPSec)**.



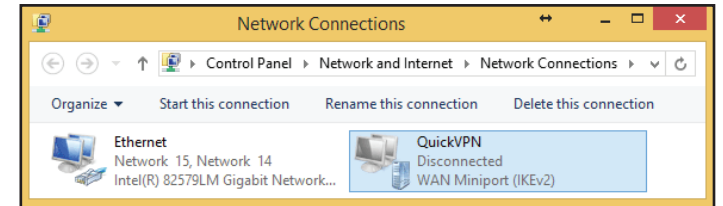
Click the **Start** button and type **view network connections**.

Select **View network connections**.



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

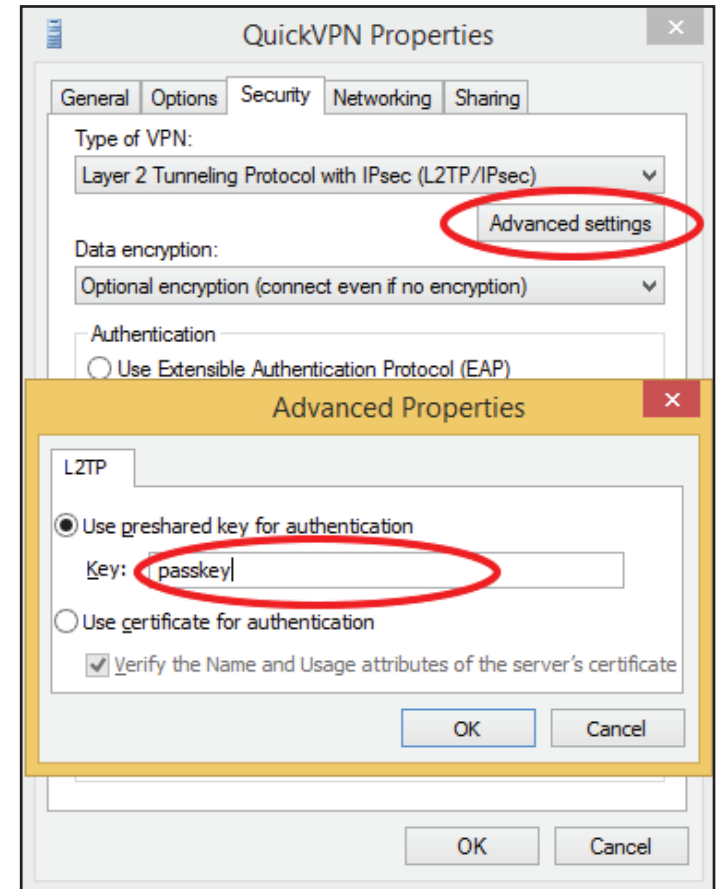
For the **Type of VPN**, select **Layer 2 Tunneling with IPsec (L2TP/IPSec)**.



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

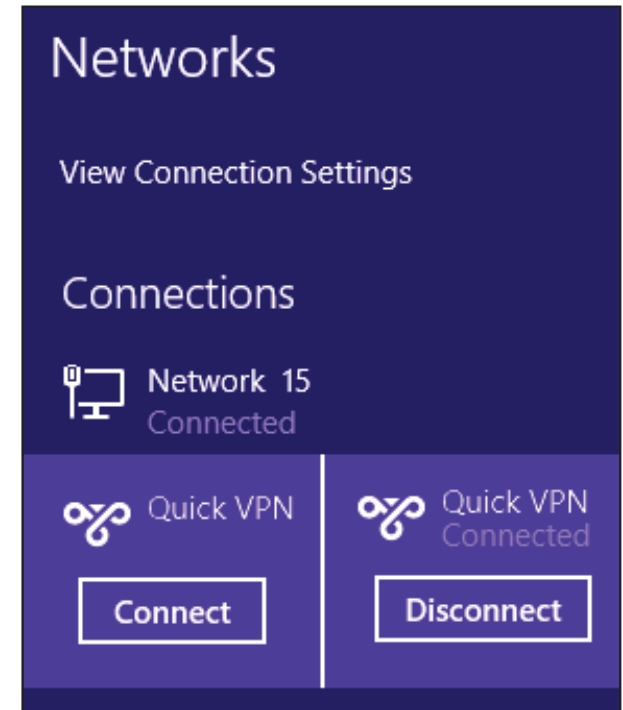
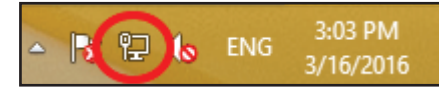
Click **OK** to close **Advanced Properties** and click **OK** to close **Quick VPN Properties**.

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.



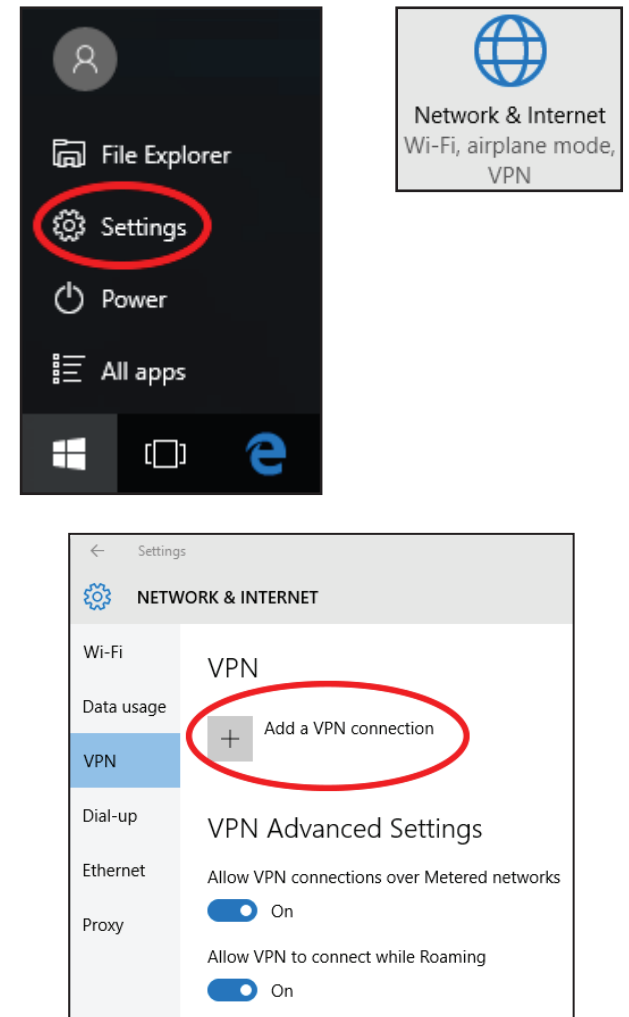
Windows 10

VPN Setup Instructions

This section provides Quick VPN setup instructions for Windows 10. Refer to **Quick VPN** on page **80** 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.

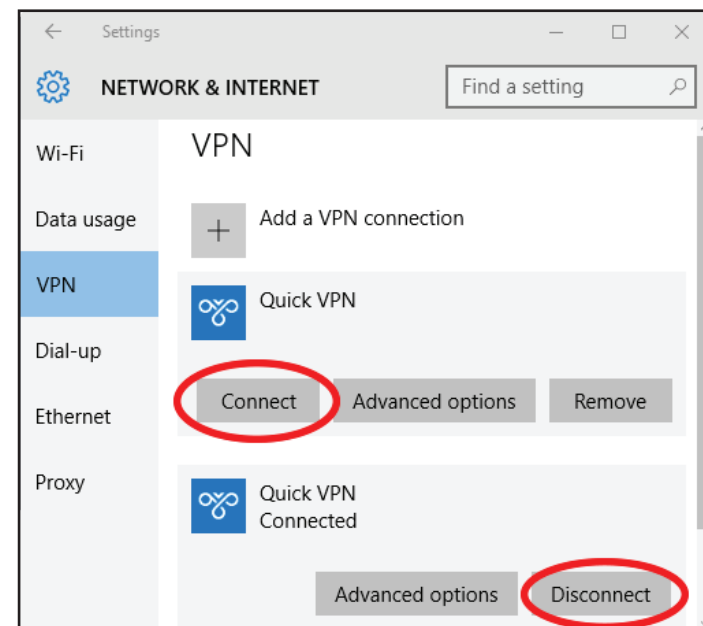
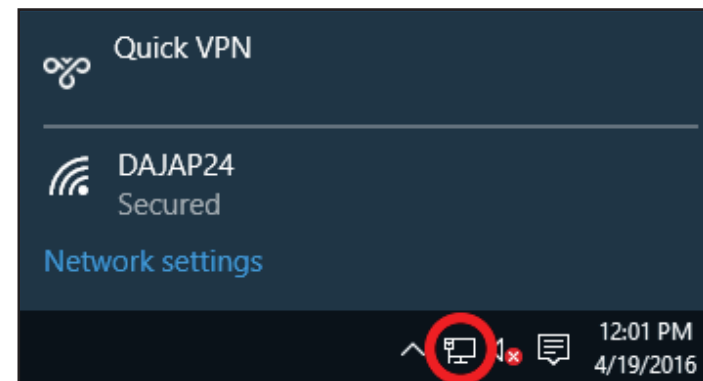
The screenshot shows the 'Add a VPN connection' window in Windows 10. It has a blue header with the title 'Add a VPN connection'. Below the title are several fields and options, each with a numbered callout (1-7) pointing to it. Callout 1 points to the 'VPN provider' dropdown menu, which is set to 'Windows (built-in)'. Callout 2 points to the 'Connection name' text box, which contains 'Quick VPN'. Callout 3 points to the 'Server name or address' text box, which contains 'IP/DDNS Address of Quick VPN Server'. Callout 4 points to the 'VPN type' dropdown menu, which is set to 'L2TP/IPsec with pre-shared key'. Callout 5 points to the 'Pre-shared key' text box, which contains 'Passkey'. Callout 6 points to the 'Type of sign-in info' dropdown menu, which is set to 'User name and password'. Below this, there are two more text boxes: 'User name (optional)' containing 'Username' and 'Password (optional)' containing a series of dots. At the bottom, there is a checkbox labeled 'Remember my sign-in info' which is checked. To the right of the checkbox are two buttons: 'Save' and 'Cancel'. Callout 7 points to the 'Save' button.

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.

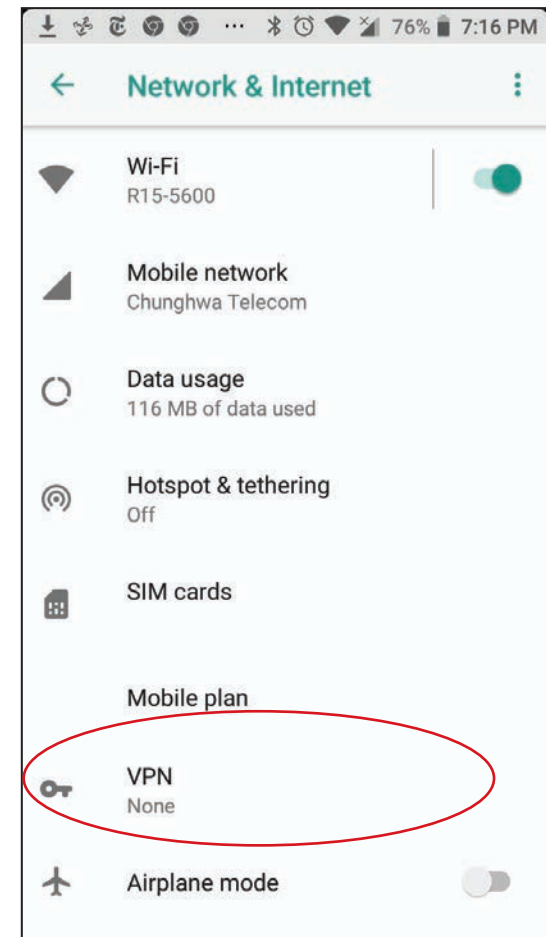


Android

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 **80** for your router setup instructions.

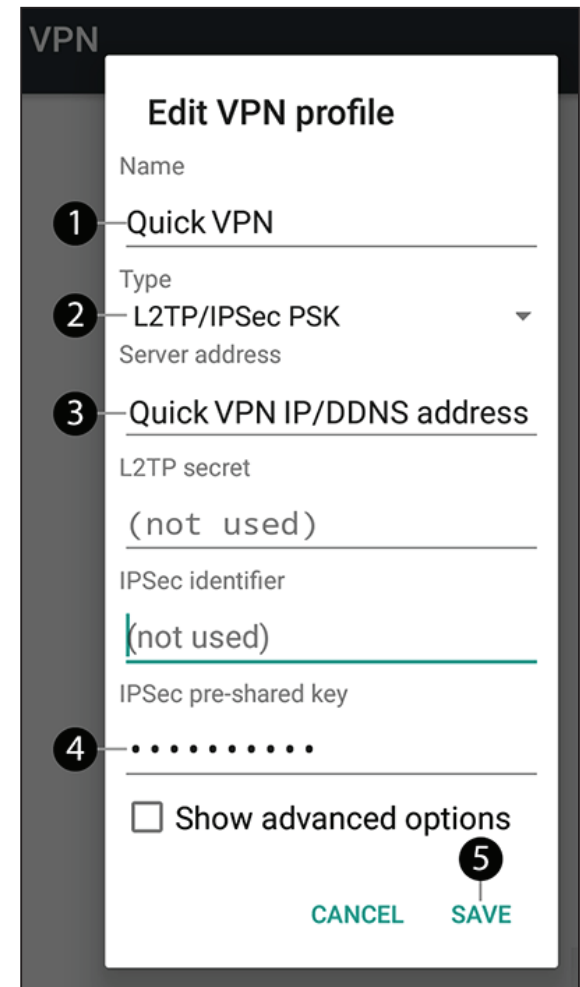
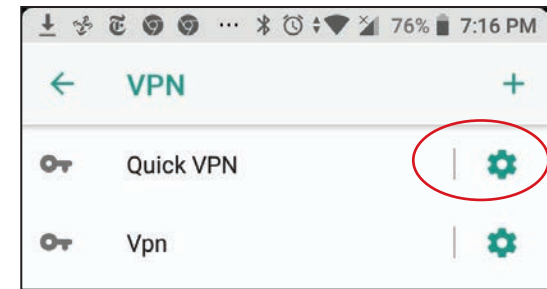
Go to **Settings** > **Network & Internet** > **VPN**



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

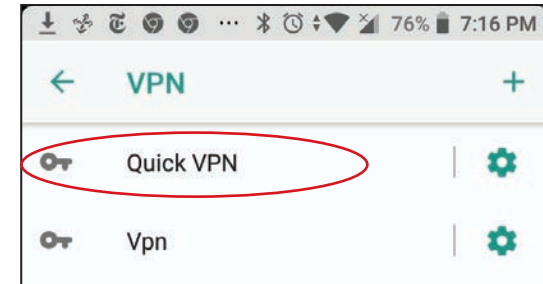
- 1 Enter a name for your VPN connection.
- 2 Select **L2TP/IPSec PSK** for **Type**.
- 3 Enter the **IP/DDNS address** of your Quick VPN server.
- 4 Enter your **Passkey** in **IPSec pre-shared key** field.
- 5 Choose **Save**.

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**.

Connect to Quick VPN

Username

Your Quick VPN Username

Password

.....

☐ Save account information

CANCEL CONNECT

To disconnect, tap **DISCONNECT**.

VPN is connected

Session: Quick VPN

Duration: 00:00:09

Sent: 97 bytes / 5 packets

Received: 64 bytes / 4 packets

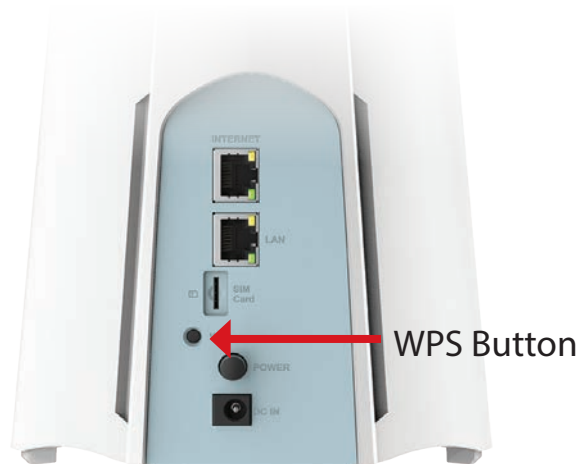
DISCONNECT CANCEL

Connect a Wireless Client to Your Router

WPS Button

The easiest and most secure 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 securely.

Windows® 10

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

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.

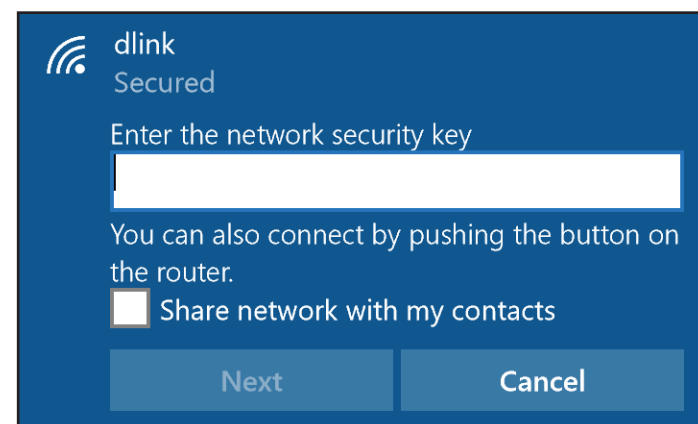
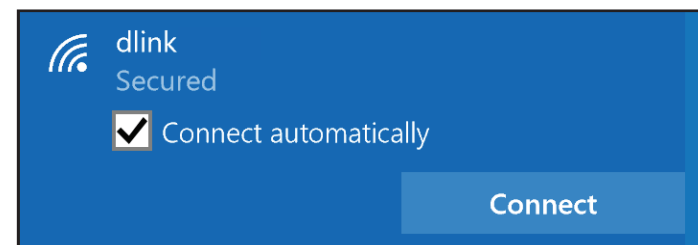
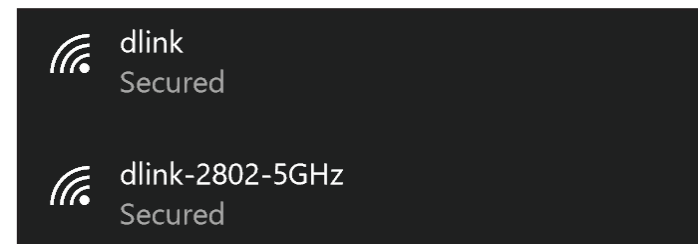
To connect to the SSID, click **Connect**.

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.



Wireless Icon



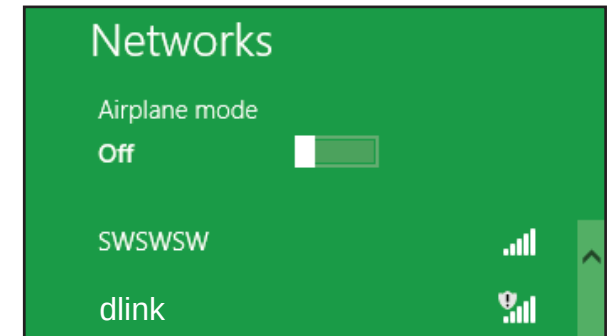
Windows® 8 - WPA/WPA2

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



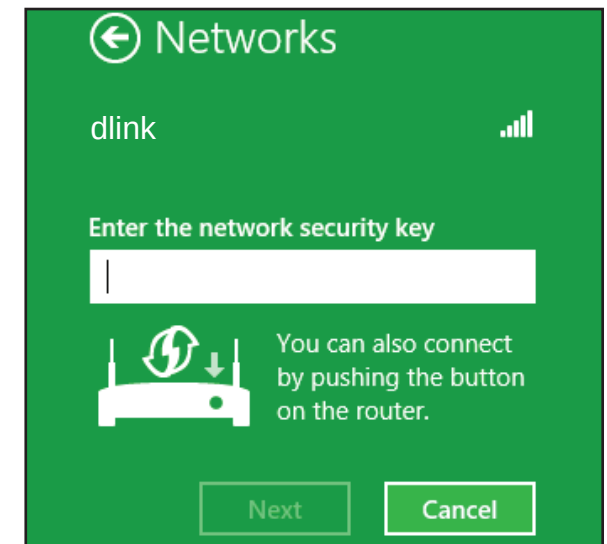
Wireless Icon

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.

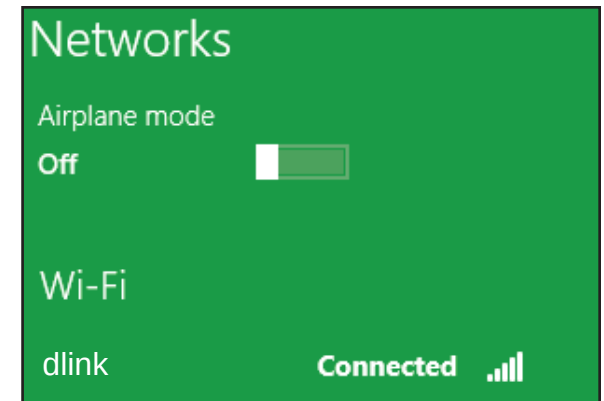


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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

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



Wireless Icon

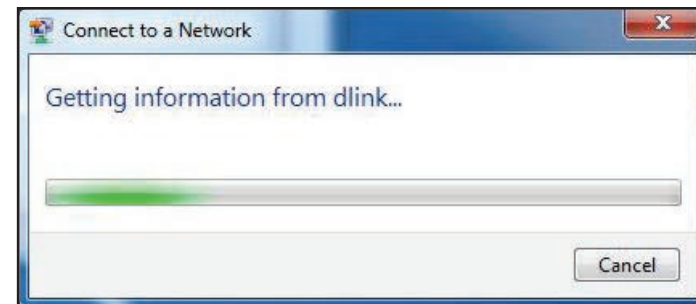
The utility will display any available wireless networks in your area.

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 **128** 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 (**192.168.125.1** 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® 10 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 management. 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 management.
- 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 default IP address is **192.168.125.1**. When logging in, enter the default device password printed on the device label.

Wireless Basics

Based on industry standards, D-Link wireless products provide easy-to-use and compatibly high-speed wireless connectivity within your home, business, or public accessible wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless products family will allow you to securely access the data you want, when, and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of through 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 do.

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 technology work?

Wireless works similarly to how cordless phones work: through radio signals, data is transmitted from point A to point B. But there are restrictions for wireless technology: how you can access the network. You must be within the range of a wireless network area to be able to connect your computer. There are, basically, 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 away. 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, both the speed and wireless operation range of WPAN are both less than those of WLAN, and WPAN in return doesn't consume as much power as WLAN does. 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?

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

Home Uses/Benefits

- Gives everyone at home broadband access
- Web surfing, email and instant message checking, etc.
- Gets rid of the cables around your 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 technology 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 as you may not know 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

When you install a wireless network, here are a few things to keep in mind:

Centralize your router or access point

Make sure you place a router/access point at 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 to boost the signal to extend the coverage range.

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 the same frequency.

Wireless Encryption

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

Networking Basics

Check your IP address

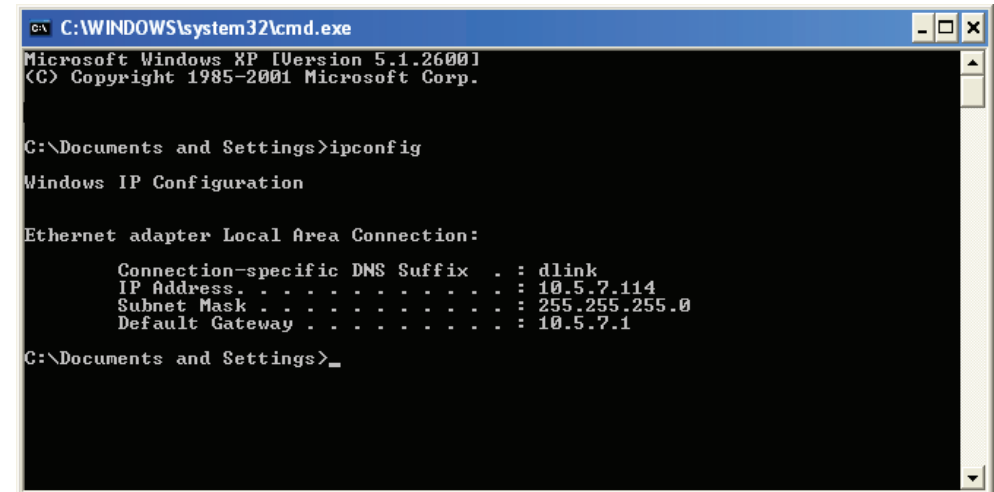
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>
```

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**. Choose the network you want to modify, right-click (Windows 7/8/XP) and then select **Properties**.

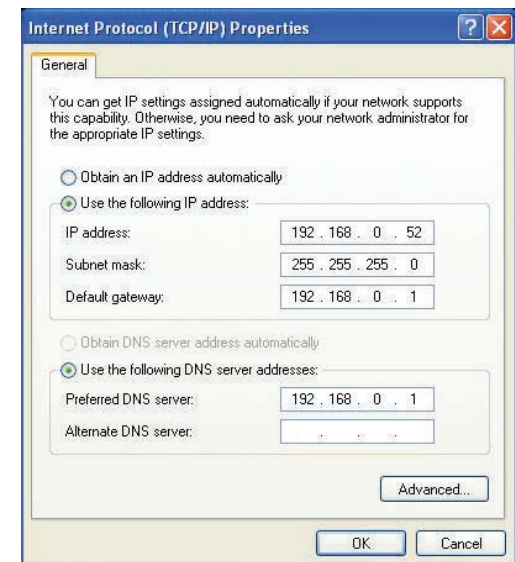
3. Under **IP assignment**, select **Edit**. For Windows 7/8/XP), select **Internet Protocol Version 4 (TCP/IPv4) Properties** or **Internet Protocol Version 6 Properties (TCP/IPv6)**. Then select **Use the Following IP Address**.

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 introduces the different encryption levels and types you can use to protect your data from intruders. The router offers the following types of security:

- 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?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles keys using a hashing algorithm and by adding an integrity-checking feature to ensure that the keys have not been tampered. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication through the extensible authentication protocol (EAP), which is generally missing in WEP. 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 alphanumeric 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. Furthermore, 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 security among these with an increased cryptographic capability and the requirements of the Protected Management Frames (PMFs) to facilitate protection from snooping attack.

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.

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.

Disposing and Recycling Your Product



EN

ENGLISH



This symbol on the product or packaging means that according to local laws and regulations this product should 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 réglementations 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.

D-Link Corporation

14420 Myford Road Suite 100, Irvine, California 92606, United States

Telephone : +1-714-885-6333