Version 1.01 | 11/17/2026



User Manual

5G NR BE7200 Wi-Fi 7 Router

G572

Preface

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

Manual Revisions

Hardware	Revision	Date	Description
A1	v1.00	11/19/2025	Initial release
A1	v1.01	11/17/2026	Modify regulatory information

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

Google, Android, Google Home, Google Play, and Google Chrome are trademarks of Google LLC.

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

Firefox is a trademark of Mozilla.org in the U.S. and other countries.

Copyright © 2026 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.

Table of Contents

Product Overview 1
Package Contents 1
System Requirements 2
Introduction 3
Features 3
Hardware Overview 4
Front View: LED Indicator 4
Rear View: Back Panel and LED Indicators 5
Bottom View: Reset Button 6

Installation 7
Before you Begin 7
Wireless Installation Considerations 8
Setup 9
D-Link FALCON Setup 10
Setup Wizard 11

Configuration 20
Home 21
Internet 22
Cellular 23
G572 25
Connected Clients 26
Extenders 28
Mesh Network 29
Settings 31
Wizard 31
Cellular 32
Failover 33
Internet - IPv4 34
IPv4 - Dynamic IP (DHCP) 35
IPv4 - Static IP 36
IPv4 - PPPoE 37
Internet - IPv6 39
IPv6 - Auto Detection 40
IPv6 - Static IPv6 42
IPv6 - Auto Configuration (SLAAC/DHCPv6) 44
IPv6 - PPPoE 46
IPv6 - 6rd 49
IPv6 - Local Connectivity Only 51
Internet - VLAN 52
Internet - VLAN 53
Wireless 54
Guest Zone 60
IoT Zone 62
MLO Zone 64
Network 66
D-Link Cloud 68
Operation Mode 69
Features 70
Parental Control 70
Data Cap 73
SMS 74
PIN 76
USSD 77

Firewall 78
Firewall Settings - IPv4/IPv6 Rules 80
Port Forwarding 82
Port Forwarding - Virtual Server 84
Static Routes - IPv4 86
Static Routes - IPv6 87
Dynamic DNS 88
Quick VPN 90
Management 91
Time & Schedule - Time 91
Time & Schedule - Schedule 92
System Log 93
System Admin - Admin 95
System Admin - System 96
User 97
Upgrade 98
Statistics 99
D-Link FALCON 100

Quick VPN 105
Important Information 106
iOS Devices 107
VPN Setup Instructions 107
Connect or Disconnect 109
Mac OS X 110
VPN Setup Instructions 110
Connect or Disconnect 112
Windows 113
VPN Setup Instructions 113
Connect or Disconnect 115
Android 116
VPN Setup Instructions 116
Connect or Disconnect 118

Connect a Wireless Client to Your Router 119
WPS Button 119
Windows® 11/10 120

Troubleshooting 122

Wireless Basics 124

Networking Basics 128

Wireless Security 130

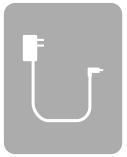
Technical Specifications 131

Regulatory Statements 132

Product Overview
Package Contents



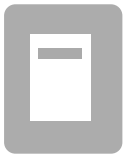
G572 5G NR BE7200 Wi-Fi 7 Router



Power Adapter (12V, 4A)



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 • A compatible Nano SIM/UICC card with mobile data service[1] • IEEE 802.11be/ax/ac/n/g/b/a & k/v wireless clients • 10/100/1000/2500 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Mac, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Microsoft Edge® • 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.)

1 Subject to services and service terms available from your carrier.

Introduction

With a powerful network processor, G572 packs in strong processing power to help you manage your home or office network. This powerful home router is designed with Wi-Fi utilization, mesh optimization, and parental control features.

Features

Multi-gigabit Ethernet and Cellular

The G572's 2.5-Gigabit Ethernet WAN port delivers smooth, buffer-free gaming and video calls, while giving you the flexibility of high-speed 5G and Wi-Fi networks without depending on fixed lines. Both Ethernet and cellular WAN connections can automatically fall back to each other to keep you online without interruption.

High-Speed Wireless Backed by Smart Zone Design

The G572 leverages Wi-Fi 7 with Multi-Link Operation (MLO) to achieve up to 7.2 Gbps throughput, offering enhanced capacity, lower latency, and reduced network congestion.

Always Up-to-Date with the Latest Features

The G572 will automatically check for daily updates and silently finish the installation 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

Setting up an Internet connection and managing your Internet utilization have 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), G572 lets you create encrypted connections to new devices by easily pressing on the WPS button.

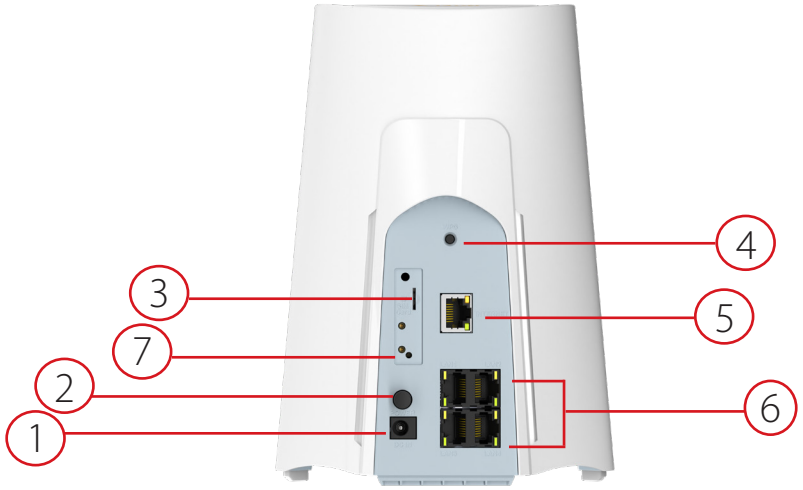
Hardware Overview

Front View: LED Indicator



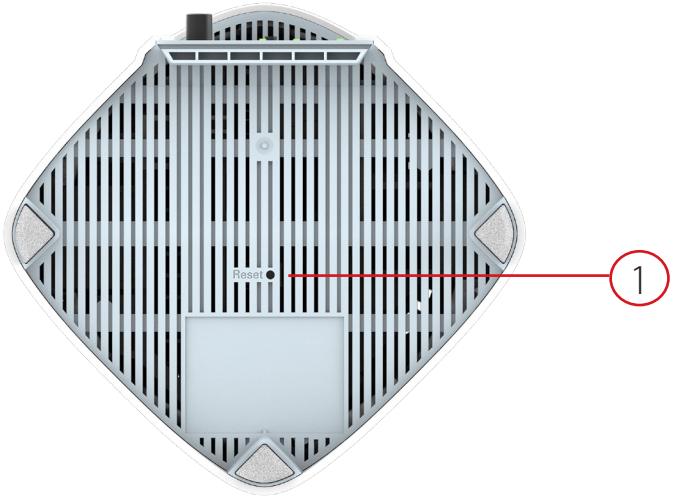
1	**Power/ Status**	Solid White	The device is on and ready for 5G/4G/3G or Wi-Fi connection.
		Blinking White	The device is in WPS process.
		Blinking Orange	The device is not inserted with a SIM card, inserted with a locked SIM card, or there is no cellular signal.
		Solid Red	The device has system errors.
		Blinking Red	The device is powering on, restoring to default factory defaults, 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	**SIM Card Slot**	Insert Nano SIM card (4FF) to establish a cellular network. Make sure the SIM is aligned with the notched corner in the correct orientation (shown on the panel) , then slide it in firmly until it fits securely into place.
4	**WPS Button**	Press WPS button to establish a secure Wi-Fi connection.
5	**Internet Port/Indicator**	Solid Orange: Ready for 2.5Gbps data transmission with an Ethernet cable connected. Blinking Orange: Data transmission in process at 2.5Gbps transfer rate. Solid Green: Ready for 10/100/1000 Mbps data transmission with an Ethernet cable connected. Blinking Green: Data transmission in process at 10/100/1000Mbps transfer rate.
6	**LAN Port/Indicator**	Solid Orange: Ready for 1Gbp data transmission with an Ethernet cable connected Blinking Orange: Data transmission in process at 1Gbp 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
7	**TS-9 Connector**	Connectors for optional TS-9 antennas for cellular signal reception.

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 G572.

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 **20**

D-Link FALCON Setup

The D-Link FALCON app allows you to install and configure your G572 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 **FALCON app** available on the App Store or on Google Play.

NOTE: Please activate your newly registered account within 7 days, and if the verification email landed in your Spam folder, first move the email to your Inbox folder so that you can click on the activation button for account activation.

Download on the App Store

GET IT ON Google Play

FALCON

Step 2

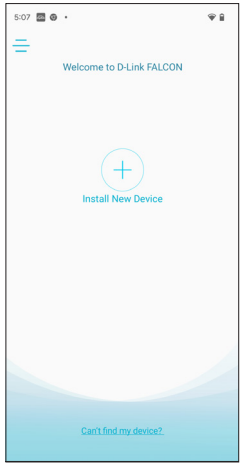
Launch the D-Link FALCON app from the home screen of your device.

Step 3

Sign in on the app using an email account. If you already have a D-Link account, you can tap **Sign In** at the bottom of the screen to be redirected to the login page. It allows you to use cloud services to control and manage your device.

Step 4

Tap **Install New Device** or **+** icon in the middle. Scan the Setup code on the device label located on the bottom of the router. Follow the on-screen instructions to complete the setup.





Setup Wizard

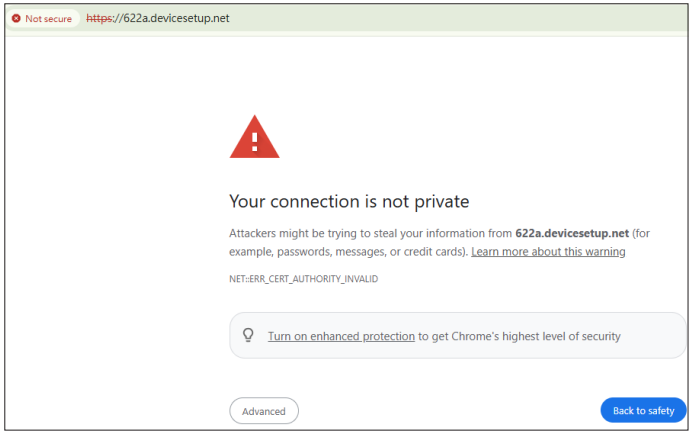
The setup wizard is designed to guide you through a step-by-step process of configuring your new G572 for Internet connection.

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.



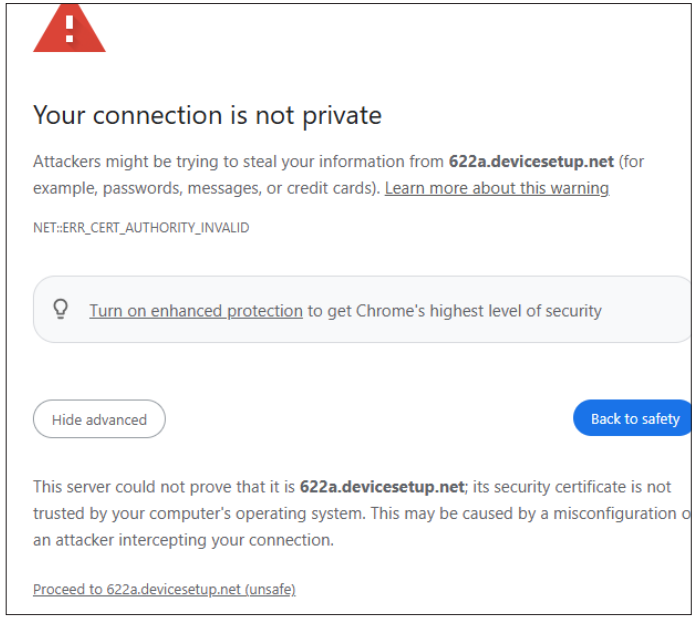
When your browser displays a security warning stating, "Your connection isn't private." You will also see Not Secure in the address bar, along with HTTPS crossed out with red lines. This is because the device's default management URL is not an actual Internet website with valid certificates. You can proceed with the setup by following these steps:

1. Click the "Advanced" button.

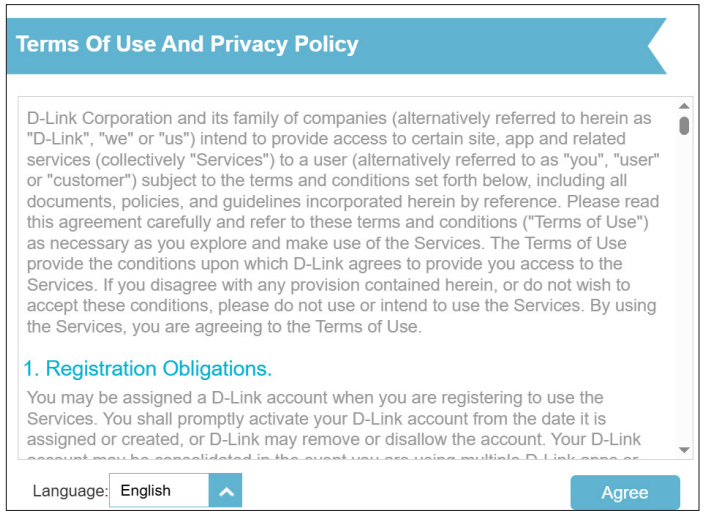


2. Click "Proceed to the default *management URL*".

Now you will be able to log in to your device.



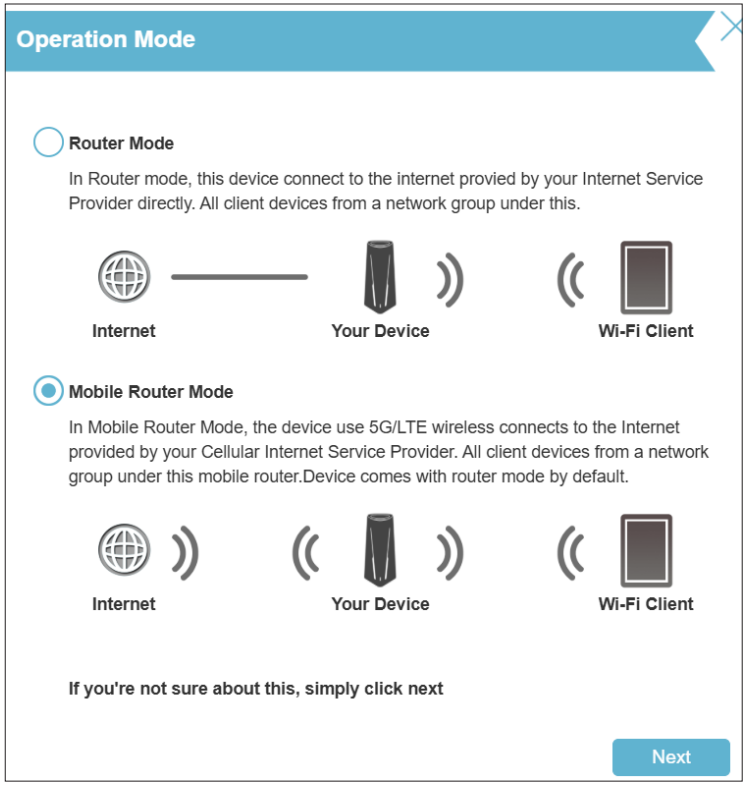
Agree to the **Terms of Use and Privacy Policy** before proceeding.



You will be prompted with the **Operation Mode** page to set up your router's mode. Select **Router Mode** to configure G572 as a default router. Select **Mobile Router Mode** to configure G572 as a mobile router.

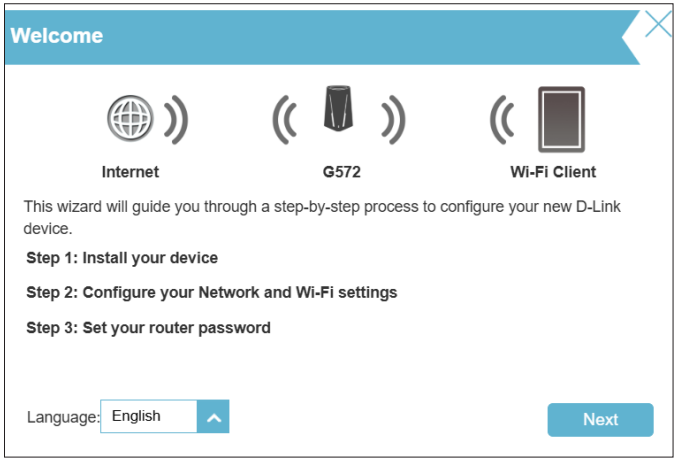
If configured with the Mobile Router Mode, you need to insert SIM card and unlock it with a correct PIN. Refer to **Rear View: Back Panel and LED Indicators** on page **5** and **PIN** on page **76**.

Click **Next** to continue



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

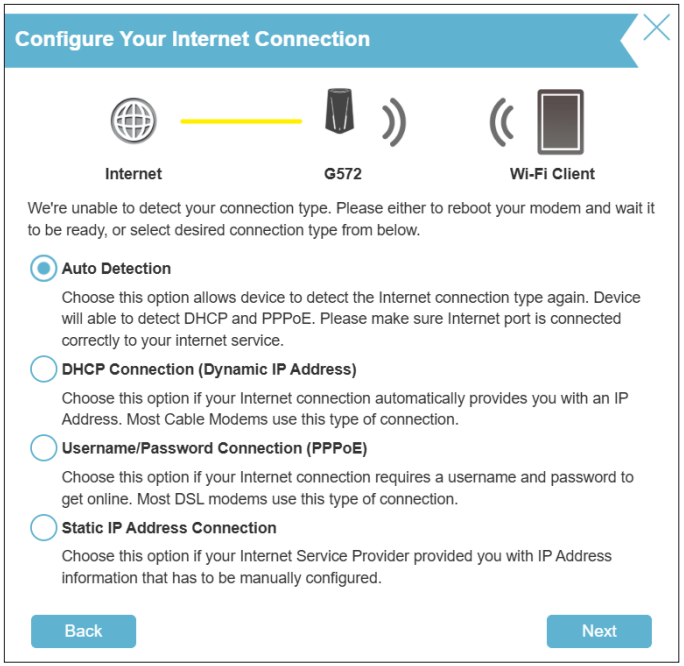
Click **Next** to continue.



If configured with the Router Mode, you need to 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.

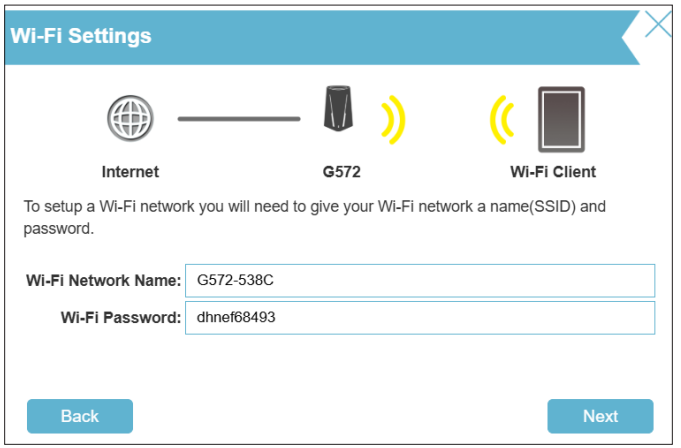


Type in a **Wi-Fi Network Name** and **Wi-Fi Password** to set up your Wi-Fi network. Your wireless clients will need this network password to be able to connect to your wireless network.

Note: The password must contain 10 to 63 characters, including both letters and numbers, and must not have identical consecutive characters.

Click **Next** to continue.

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



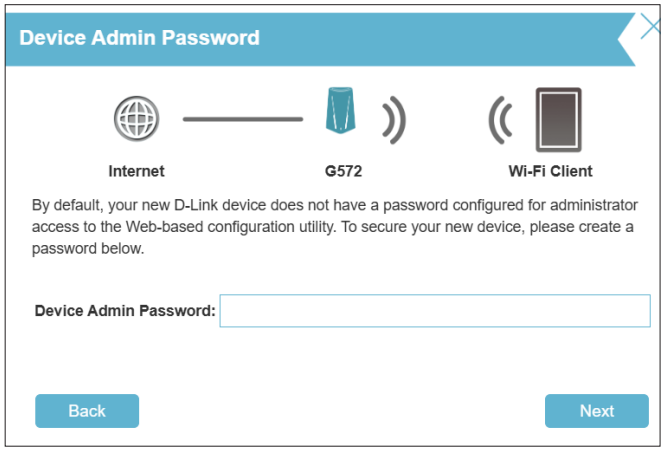
In order to secure the router's configuration page, please enter a password. You will be prompted for this password every time you log in to the router's web configuration utility.

Note: The password must contain 10 to 15 characters and include at least three of the following four character types:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0–9)
- Special characters or symbols, e.g., * and %.

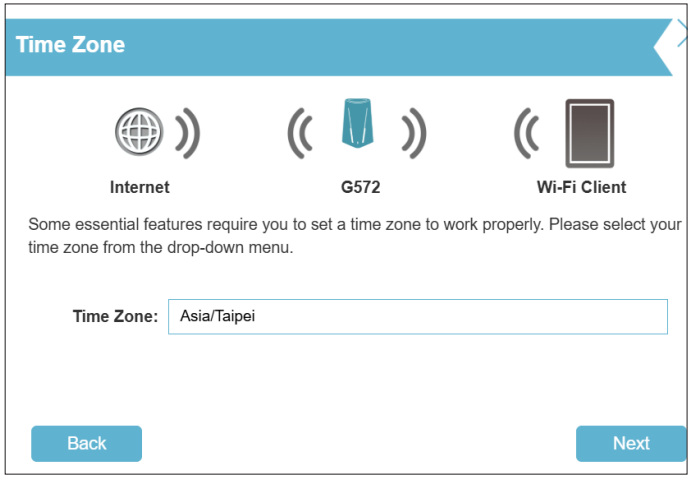
Note: It is strongly recommended that you change the default device password.

Click **Next** to continue.



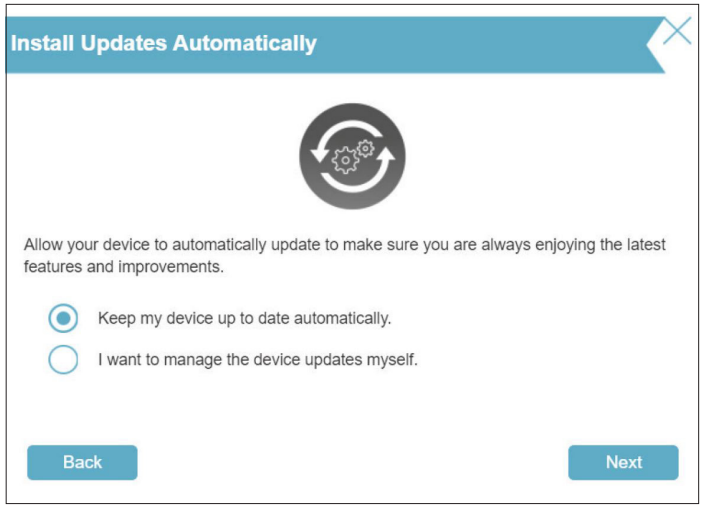
Select your time zone from the drop-down menu.

Click **Next** to continue.



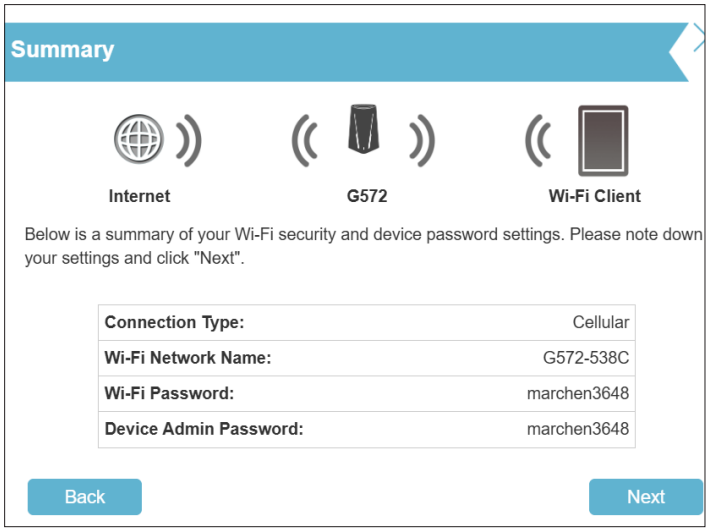
Keeping your router's firmware up-to-date provides you with the latest protection and new features over the air. Choose whether to keep your device up-to-date automatically or to manage the device updates by yourself.

Click **Next** to continue.



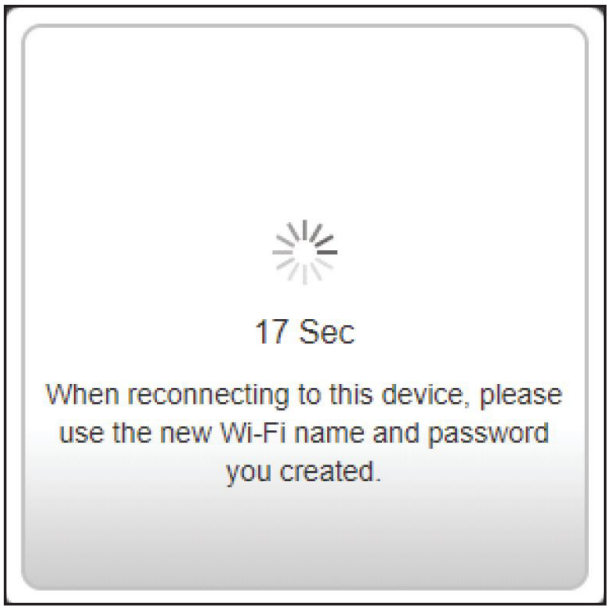
You will be presented with a summary of your settings.

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



Please wait while the device settings are saved.

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

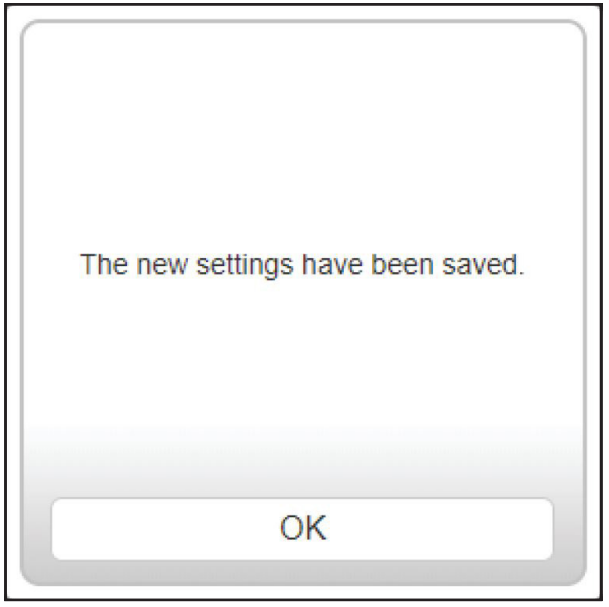


Your new settings have been saved and your router is now configured.

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

Congratulations, your device has been successfully configured!

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



Configuration

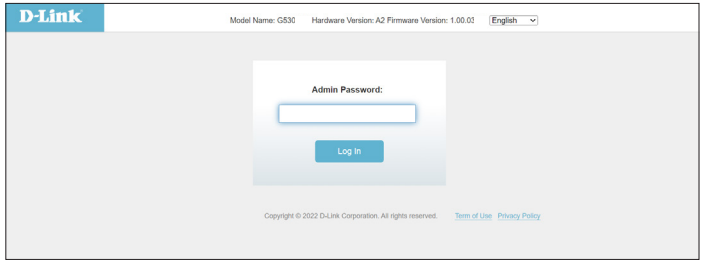
If this is your first time installing the router, open your web browser and enter the default management address at **http://XXXX.devicesetup.net/**. (where XXXX represents the last 4 characters of the MAC address).



The Wi-Fi Name(SSID), Wi-Fi Password, and device password are printed on the device label on the bottom of the device.

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.



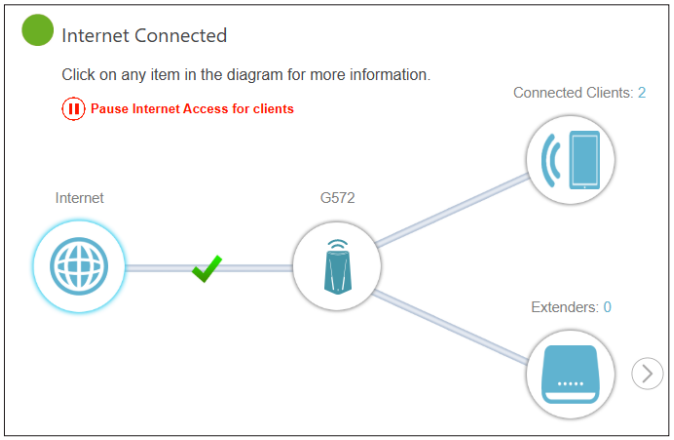
The left pane has quick access to **Settings**, **Features,** and **Management** functions.

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.

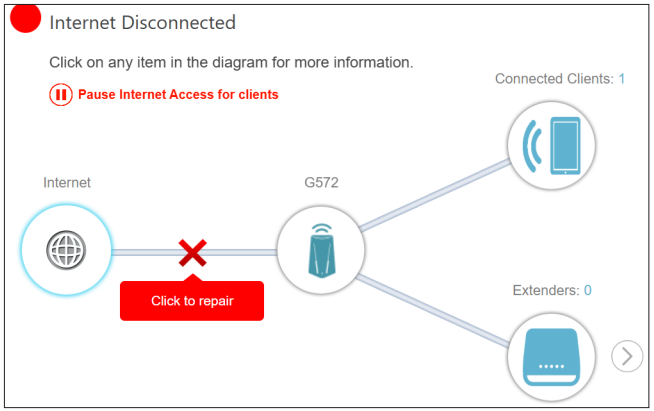
The Home page displays whether the router is currently connected to the Internet.



Click **Pause Internet Access for clients** to temporarily disconnect the Internet connection; alternatively, click **Resume Internet Access** to resume the Internet access if previously paused.

To reconfigure the Internet settings, click **Go to settings** at the bottom right.

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.



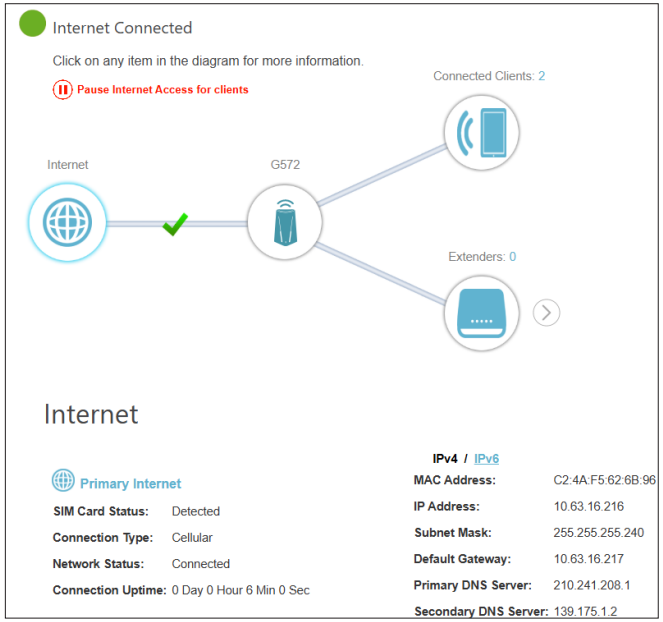
Internet

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.

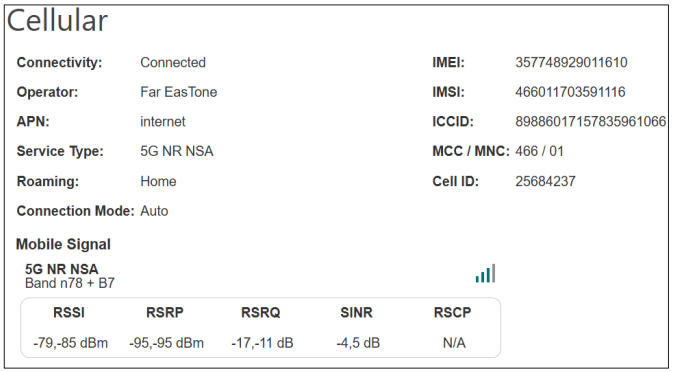
Click **Release IP Address** to disconnect from the Internet. To reconnect, click **Renew IP Address**.

To reconfigure the Internet settings, refer to **Internet - IPv4** on page **34**.



Cellular

On the **Cellular** section, you can view the mobile connection parameter information such as IMEI and IMSI.
To reconfigure the Internet settings, refer to **Cellular** on page **32**.



Connectivity Displays whether the device is connected to a cellular network.

Operator Displays the cellular operator.

APN Access Point Name (APN) is used to set up a network connection to enable Internet access through cellular communication.

Service Type Displays the cellular technology: Auto, 5G NSA, 5G SA, or LTE.

Roaming Displays whether roaming is enabled or disabled. If enabled, additional service charge may apply depending on your plan.

Connection Mode Auto or via Manual dial-up.

IMEI The International Mobile Equipment Identity is a unique number assigned to every mobile device.

IMSI The SIM card has a unique number called an International Mobile Subscriber Identity (IMSI). This is used to identify and authenticate users on cellular devices.

ICCID The Integrated Circuit Card Identity is a unique number assigned to each SIM card.

MCC/MNC The Mobile Country Code/The Mobile Network Code.

Cell ID Indicates the cell tower or site.

Mobile Signal Auto or the band number is displayed.

RSSI Received Signal Strength Indication, which measures the power of a received radio signal.

RSRP Reference Signal Received Power, which measures the power level in the LTE cell network.

RSRQ Reference Signal Received Quality (RSRQ), which measures the quality of the received reference signal and is helpful in determining the amount of interference.

SINR Signal-to-interference-plus-noise ratio, which measures the quality of wireless signal by taking account of noise and other interfering factors.

RSCP Received Signal Code Power, which measures the signal strength of a received radio signal.

G572

Click on the **G572** 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 **66** for more information.

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

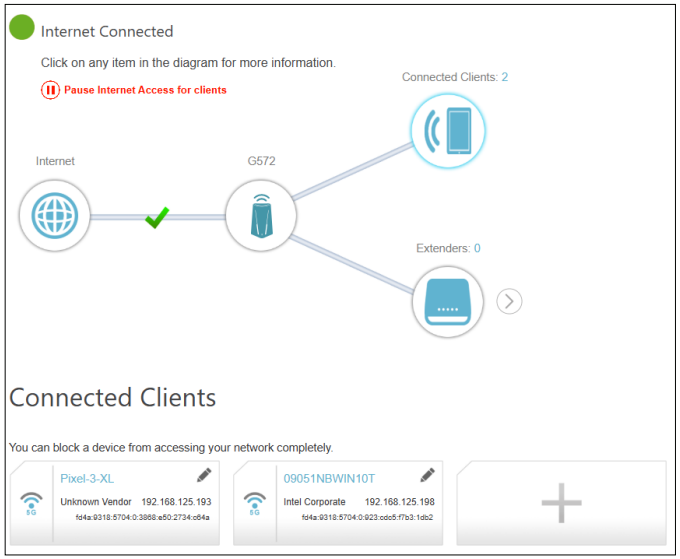


Connected Clients

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

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

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



Edit Rule

Name Enter a custom name for this client.

Vendor Displays the vendor of the client.

MAC Address Displays the MAC address of the client.

IP Address Displays the current IP address of the client.

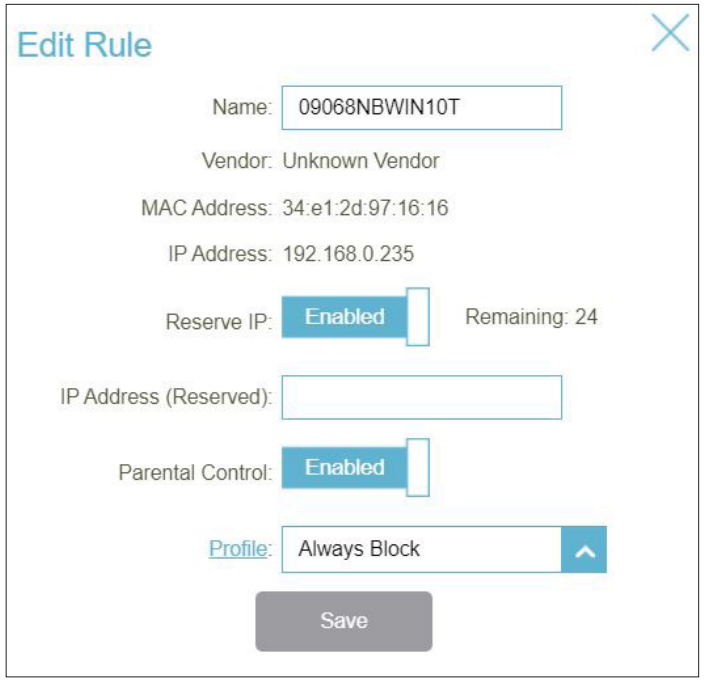
Reserve IP Click **Enable** to reserve an IP address for the client.

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

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

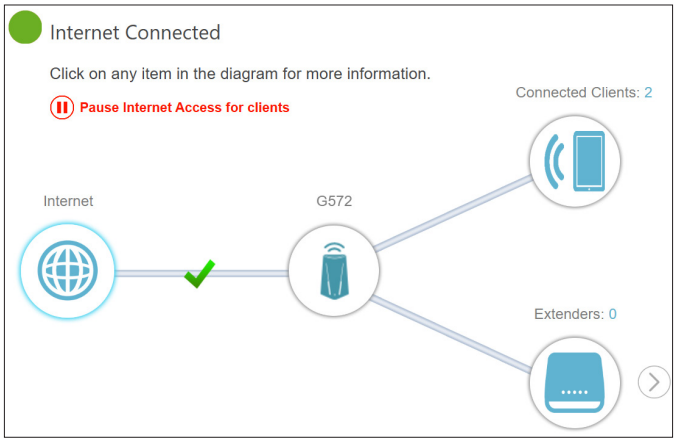
Profile Use the drop-down menu to select a profile to be used for Parental Control. The profile can be set to **Always Block** to have this client blocked from accessing the Internet, or you can create your own profiles to specify the time periods that the client can access the network. You can also block access to unwanted websites. Refer to **Features > Parental Control** on page **70** for more information.

Click **Save** when you are done.



Extenders

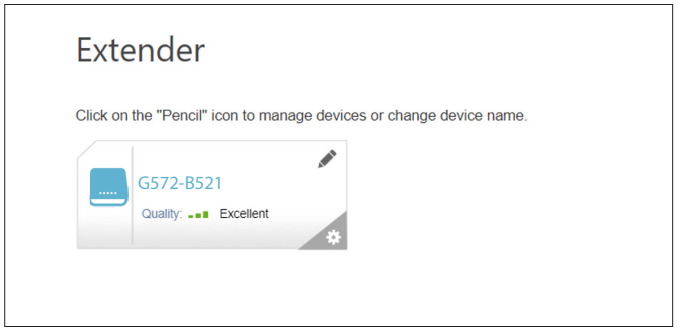
Click on the **Extenders** icon to view details about all additional devices in your Mesh Wi-Fi network.



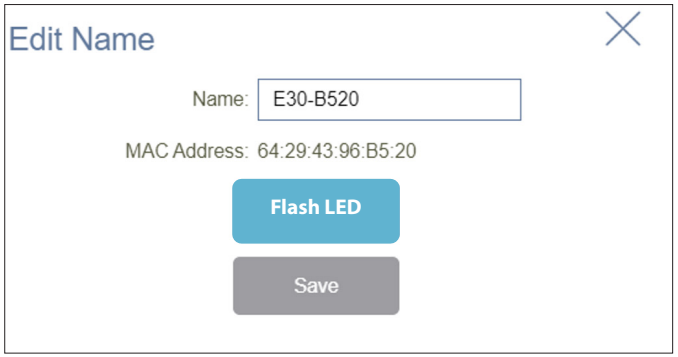
To edit the Extender name, click on the pencil icon in the top-right of the box of the Extender that you want to rename.

To reboot an Extender, click the settings icon in the bottom-right of the Extenders's box and click **Reboot**.

To remove an Extender from your Mesh Wi-Fi network, click the settings icon in the bottom-right of the Extender's box and click **Remove**.

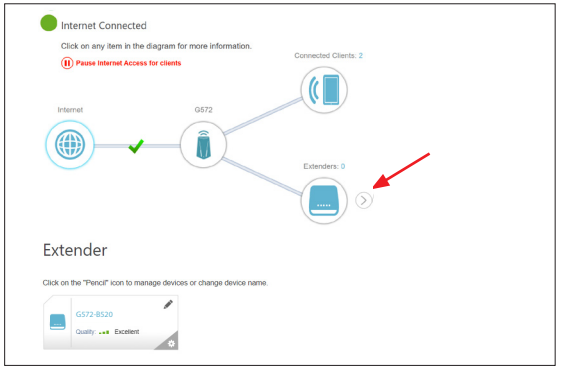


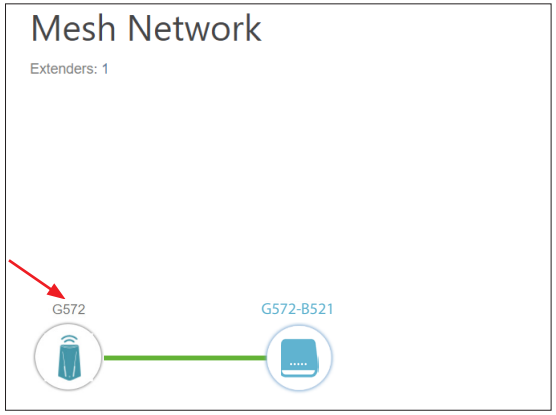
Edit Name	
Name	Enter a name for the Mesh Point.
MAC Address	Displays the MAC address of the Mesh Point.
	Click **Flash LED** to visually identify the Extender.
	Click **Save** when you are done.

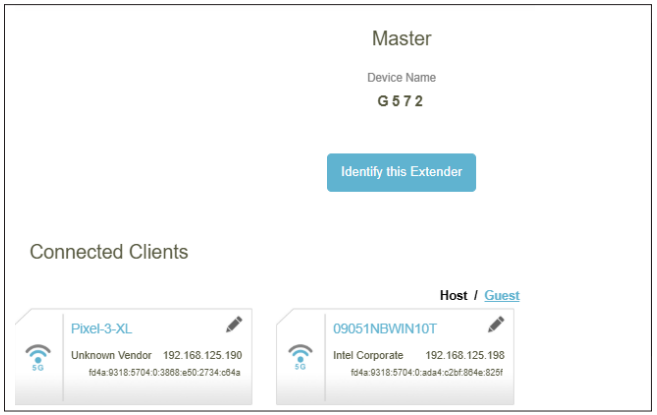


Mesh Network

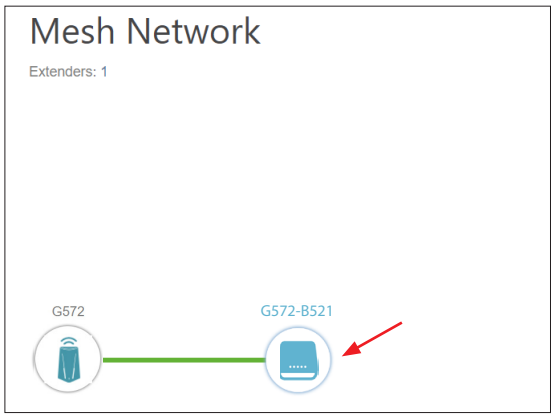
To access the **Mesh Network** page, click the arrow next to the extender icon. Under the **Mesh Network** page, you can view details of the master device and every extender within the network. Click **G572** to view the status of the main router. Click the pencil icon on the connected client(s) to edit configuration. Configuration details are explained on the next page. Click **Identify this Extender** to visually confirm the location of your router. The router's LED should breathe white several times.

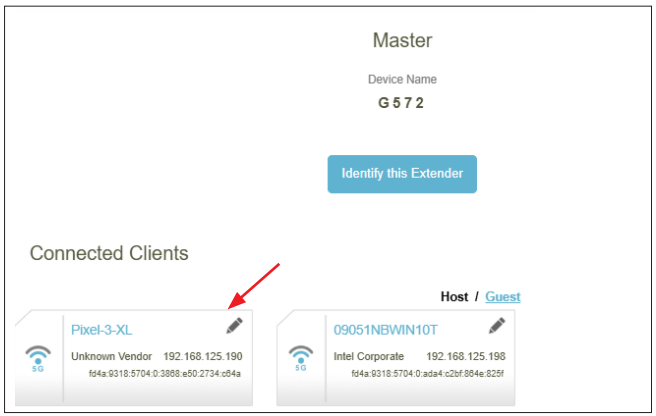




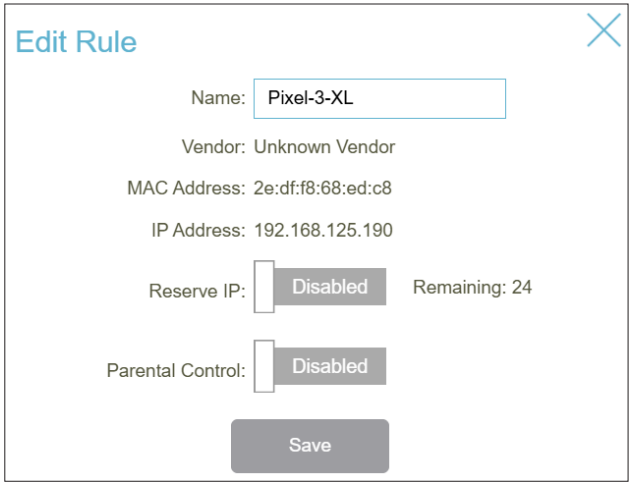


Click the **Extender** icon to view details of the extender and list of connected clients. Click the pencil icon on the connected client(s) to edit configuration. Configuration details are explained on the next page. Click **Identify this Extender** to visually confirm the location of your extender. The router's LED should breathe white several times.





Edit Rule



Name Displays the name of this client. You can edit the client's name here.

Vendor Displays the vendor of the device.

MAC Address Displays the MAC address of the device.

IP Address Displays the current IP address of this client.

Reserve IP Enable to reserve an IP address for this client.

IP Address (Reserved) Specify an IP address for the DHCP server to assign to this client.

Parental Control Enable or disable parental control to allow or block this user's access to the network.

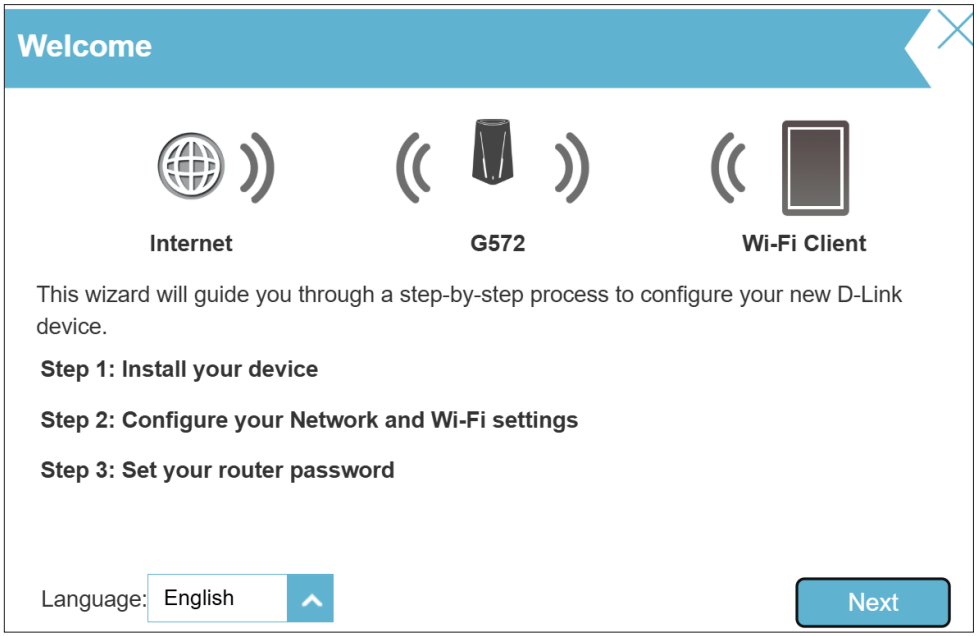
Profile If **Parental Control** is enabled, use the drop-down menu to select a time schedule that the rule will be enabled on. The schedule may be set to **Always Block**, or you can create your own schedules in the **Schedule** section. Refer to **Parental Control** on page **70** for more information.

Click **Save** when you are done.

Settings
Wizard

Go to **Settings > Wizard** to open the setup wizard. This is the same wizard that appears when you start the router for the first time. Refer to **Setup Wizard** on page **11** for details.

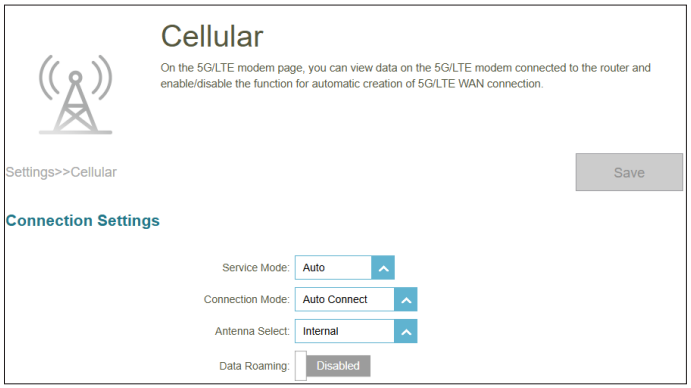
Note: *When the Wizard is opened, the router will disconnect from the Internet.*



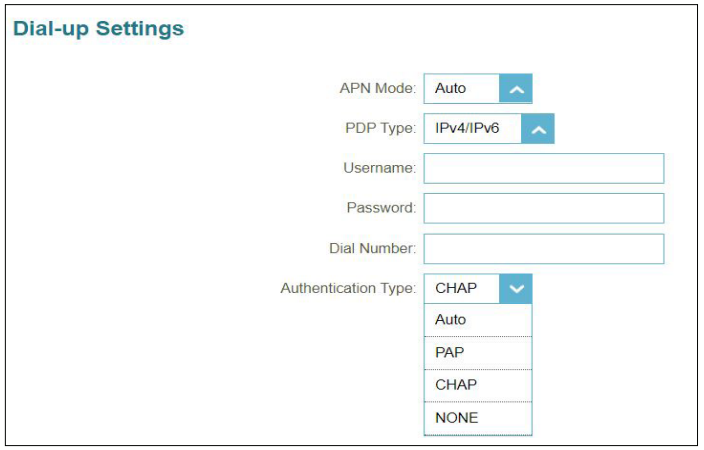
Cellular

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 a 3G/LTE WAN connection.

Connection Settings	
Service Mode	Select **5G NR NSA, 5G NR SA, LTE** or **Auto** to let the system determine the mode automatically.
Connection Mode	Select Auto Connect or Manual Connect.
Antenna Select	Select either Internal or External for the antenna type.
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 the IP addressing mechanism.
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.

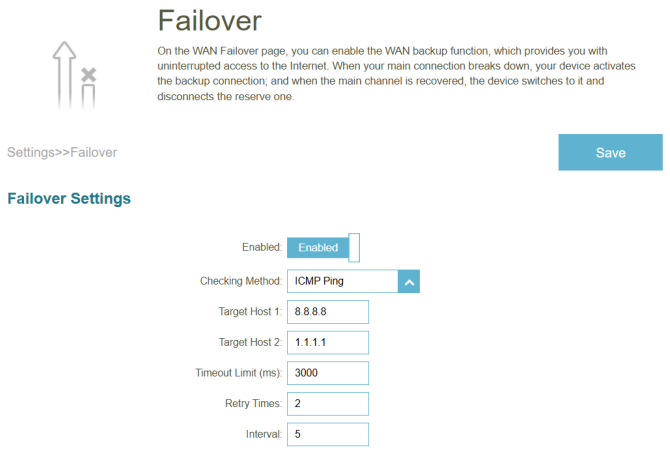


Failover

Go to **Settings > Failover** to configure the WAN backup function. The G572's failover feature allows you to set your router to switch to a backup Internet connection automatically if your primary Internet connection is lost. And when the primary connection is recovered, the device will switch back on its own. The Failover function is *disabled* by default.

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

Failover Settings	
Enabled	Enable or disable the Failover function.
Checking Method	Select the method for checking Internet connectivity: Auto, DNS Query+ICMP Ping, ICMP Ping, or DNS Query.
Target Host 1	Enter the destination's IP address to send the DNS query and/or ICMP request.
Target Host 2	Enter the destination's IP address to send the DNS query and/or ICMP request.
Timeout Limit (ms)	Enter the timeout value to wait for the destination to respond to each request (1-10,000).
Retry Times	The number of trying times that a request should be sent if no response is received within the timeout limit (1-10).
Interval	Enter the wait time before sending another request (1-600) in seconds.



Internet - IPv4

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

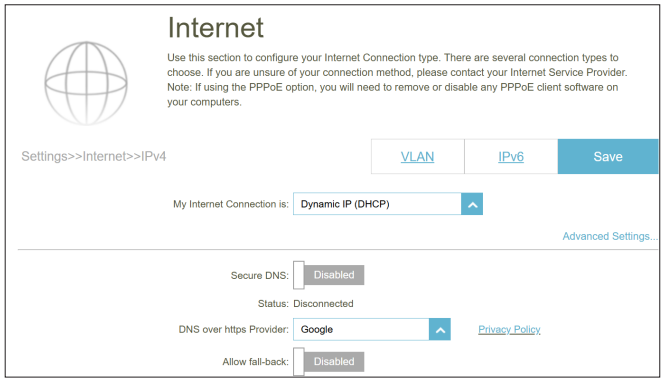
To configure IPv6 Internet and network connection details, click the **IPv6** tab. Refer to **Internet - IPv6** on page **39**.
Click **Save** at any time to save the changes you have made on this page.

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 HTTPS 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.



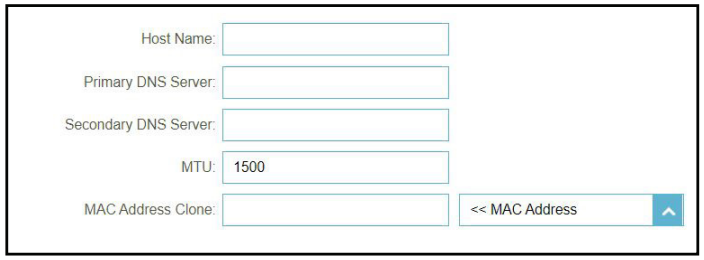
For **IPv4 - Dynamic IP (DHCP)** refer to page **35**

For **IPv4 - Static IP** refer to page **36**

For **IPv4 - PPPoE** refer to page **37**

IPv4 - Dynamic IP (DHCP)

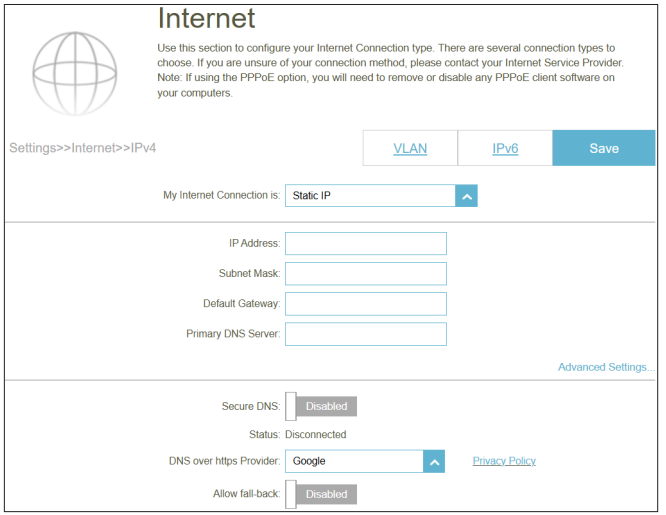
Select **Dynamic IP (DHCP)** to obtain IP address information automatically from your Internet Service Provider (ISP). Select this option if your ISP does not specify an IP address to use. Click **Save** at any time to save the changes you have made on this page.



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.

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.

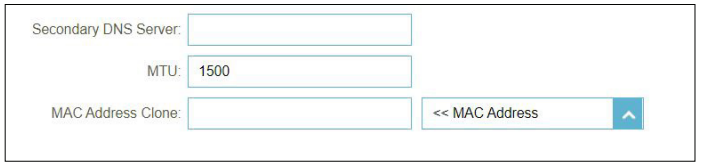
Primary DNS Server Enter the primary DNS server IP address provided by your ISP.

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

DNS over HTTPS 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.

Advanced Settings...



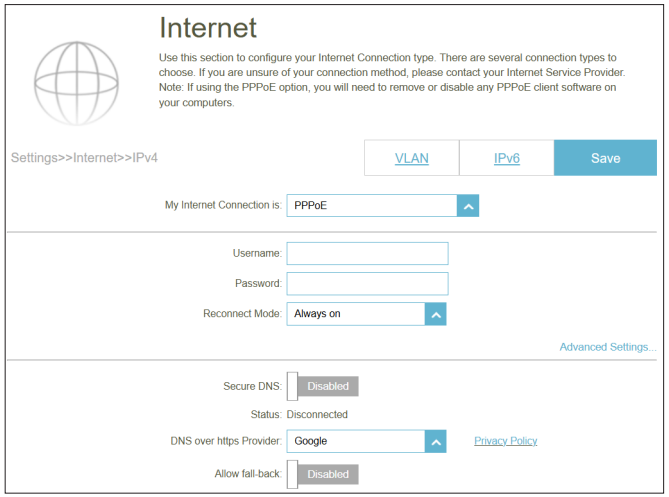
Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP.

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.

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**.

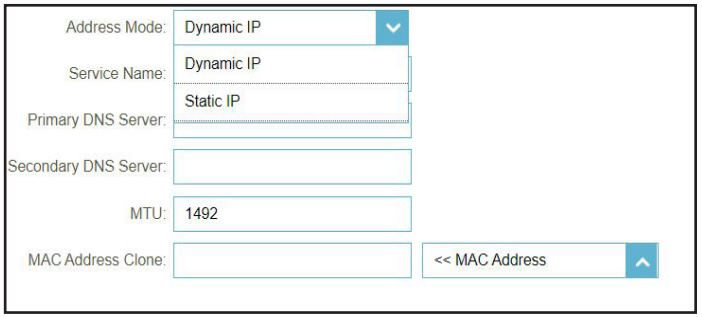
Maximum Idle Time Configurable when **On Demand** is selected. Enter a maximum idle time during which the Internet connection is maintained during inactivity. The default is 5 minutes. To disable this feature, select **Always on** or **Manual** as the reconnect mode.

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

DNS over HTTPS 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.

Advanced Settings



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

IP Address When **Static IP** is selected as the address mode, the field 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 1492.

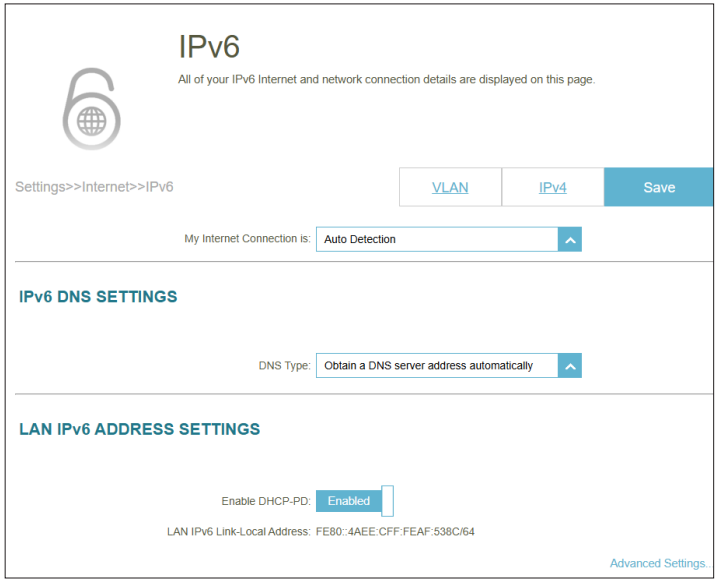
MAC Address Clone The default MAC address is set to the Internet port's physical interface MAC address on the router. You can replace the Internet port's MAC address with the MAC address of a connected client.

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 **34**

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 **40**

For **IPv6 - Static IPv6** refer to page **42**

For **IPv6 - Auto Configuration (SLAAC/DHCPv6)** refer to page **44**

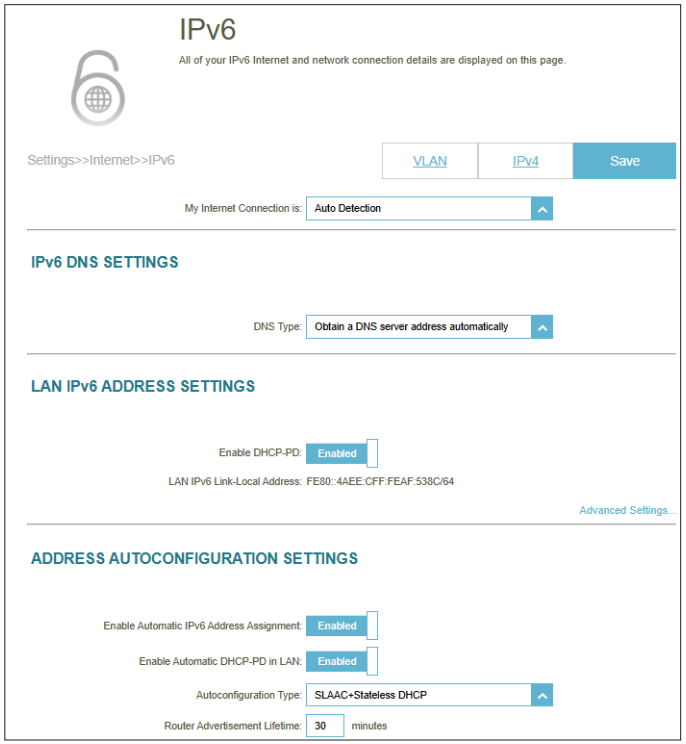
For **IPv6 - PPPoE** refer to page **46**

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

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

IPv6 - Auto Detection

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



IPv6 DNS Settings

DNS Type — Select either **Obtain 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.

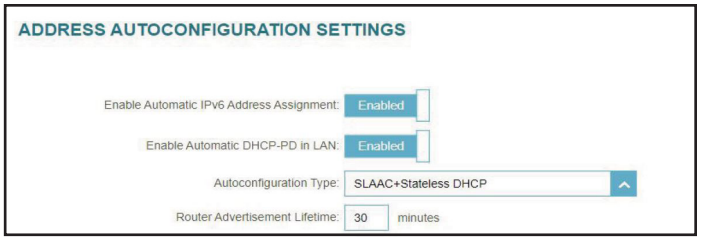
LAN IPv6 Link-Local Address — Displays the router's LAN link-local address, which is used only within the local network.

*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

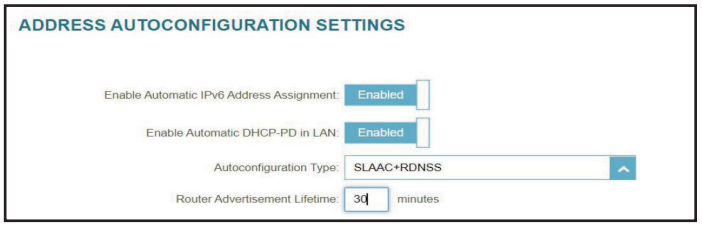


Enable Automatic IPv6 Address Assignment — Enable or disable the Automatic IPv6 Address Assignment feature.

Enable Automatic DHCP-PD in LAN — Enable or disable DHCP-PD for other IPv6 devices connected to the LAN interface. This option is available only when DHCP-PD is enabled in LAN IPv6 Address Settings.

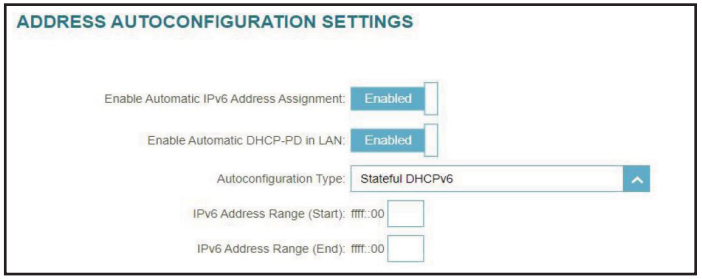
Autoconfiguration Type — Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*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 10 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. This option is available only if the DHCP-PD is disabled in the above LAN IPv6 Address Settings.

IPv6 - Static IPv6

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



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

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

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

Default Gateway Enter the default gateway for your IPv6 connection.

Primary DNS Server Enter the primary DNS server address.

Secondary DNS Server Enter the secondary DNS server address.

LAN IPv6 Address Settings



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

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

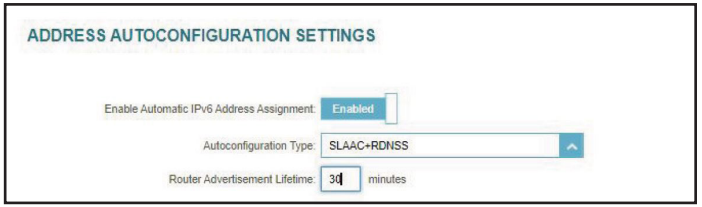
Advanced Settings... - Address Autoconfiguration Settings



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

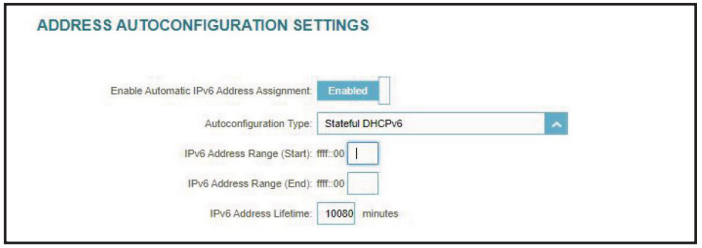
Autoconfiguration Type — Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

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



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

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



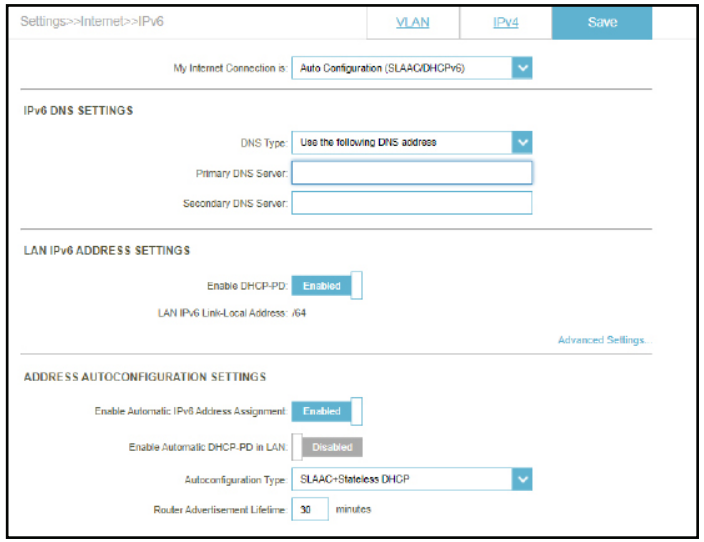
IPv6 Address Range (Start) — Enter the start IPv6 address for the DHCP server's IPv6 assignment.

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

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

IPv6 - Auto Configuration (SLAAC/DHCPv6)

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



IPv6 DNS Settings

DNS Type: Select either **Obtain 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.

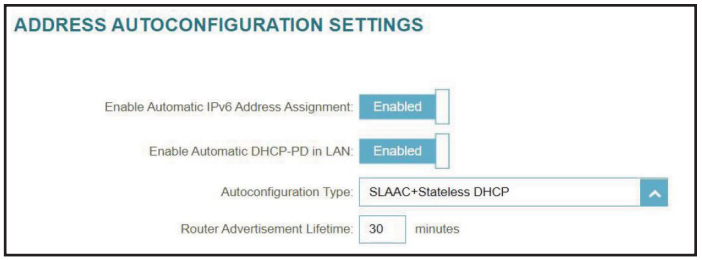
LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

*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.

Advanced Settings... - Address Autoconfiguration Settings

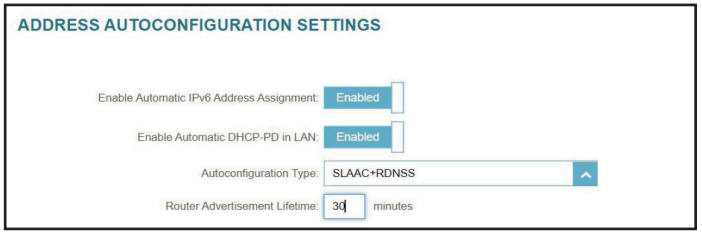


Enable Automatic IPv6 Address Assignment: Enable or disable the Automatic IPv6 Address Assignment feature.

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 devices connected to the LAN interface.

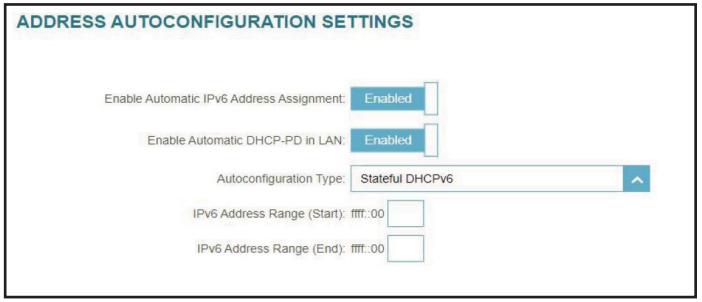
Autoconfiguration Type: Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*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 10 minutes.

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



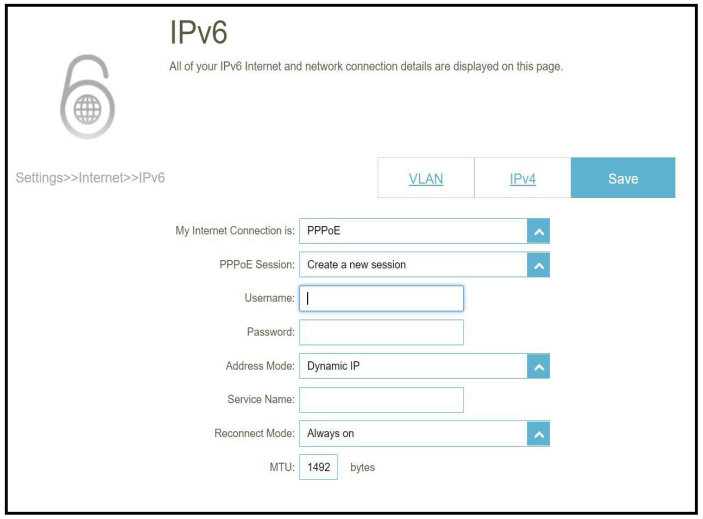
IPv6 Address Range (Start): Enter the start IPv6 address for the DHCP server's IPv6 assignment.

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.

IPv6 - PPPoE

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



PPPoE Session: Create a new PPPoE session.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

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

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

Service Name: Enter the ISP service name (optional).

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

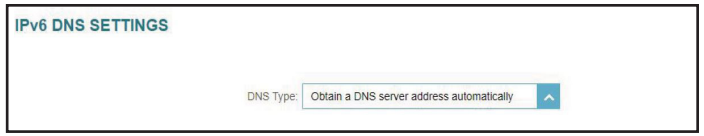
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP. The default is 1492 bytes.

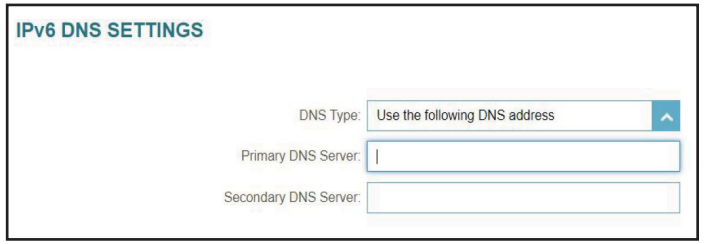
IPv6 DNS Settings

DNS Type: Select either **Obtain 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.





LAN IPv6 Address Settings

Enable DHCP-PD: Enable or disable prefix delegation.

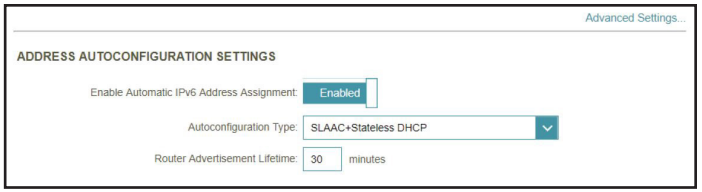
LAN IPv6 Address: Configurable if the above DHCP-PD is disabled. Enter the IP address provided by your ISP.

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





Advanced Settings... - Address Autoconfiguration Settings

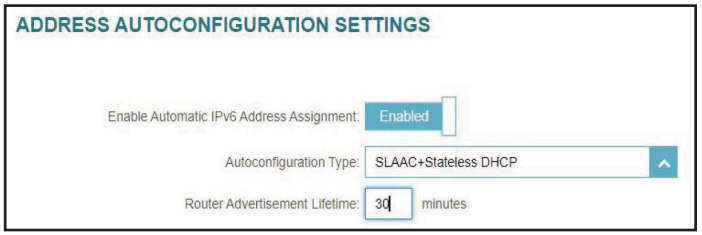


Enable Automatic IPv6 Address Assignment: Enable or disable the Automatic IPv6 Address Assignment feature.

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

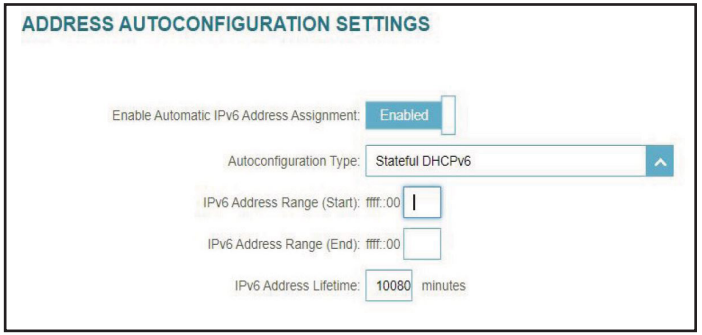
Autoconfiguration Type: Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*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:*



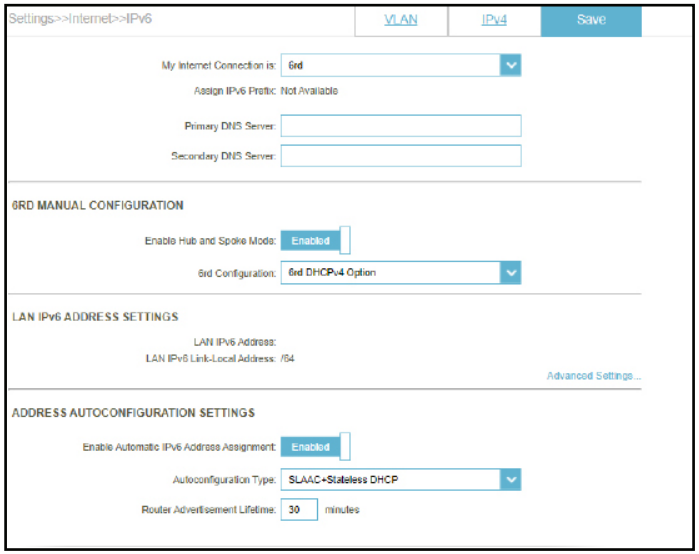
IPv6 Address Range (Start): Enter the start IPv6 address for the DHCP server's IPv6 assignment.

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

IPv6 Address Lifetime: 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.

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.

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.

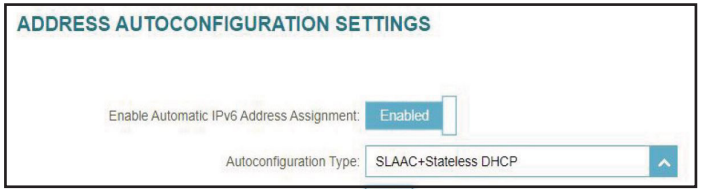
LAN IPv6 Address Settings



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

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

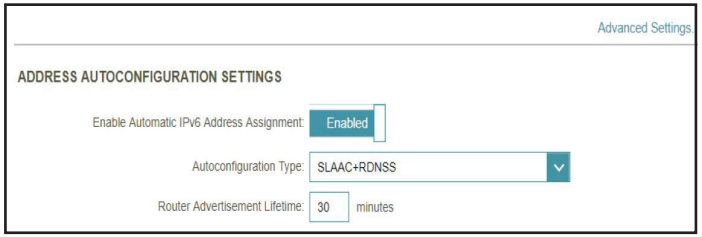
Advanced Settings... - Address Autoconfiguration Settings



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

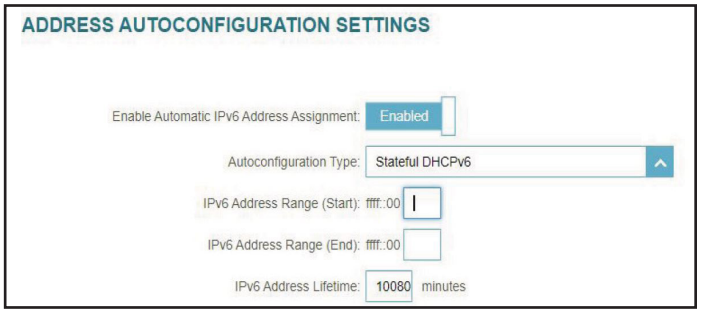
Autoconfiguration Type: Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.

*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:*



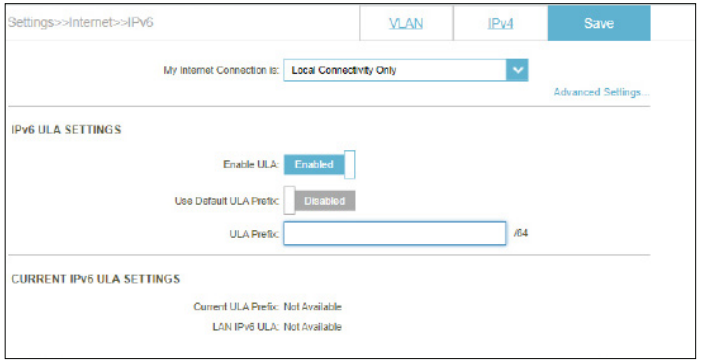
IPv6 Address Range (Start): Enter the start IPv6 address for the DHCP server's IPv6 assignment.

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

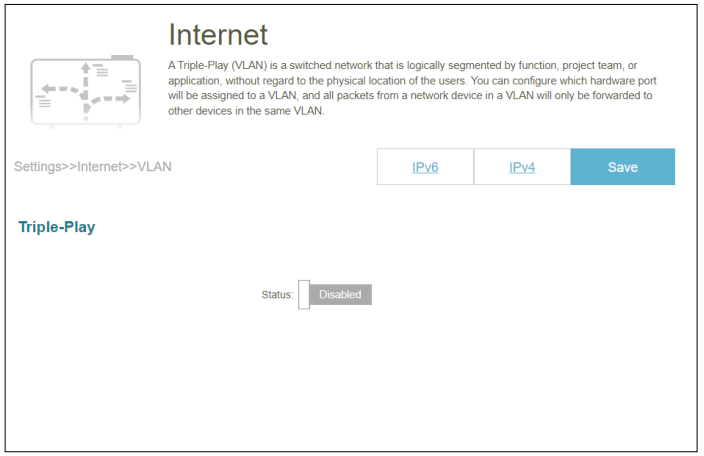
In the Settings menu on the bar at the top-left of the page, click **Internet** to see the Internet configuration options for the IPv4 connection details, then click the **VLAN** link to access the configuration options for the VLAN connection details.

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 **Internet - IPv4** on page **34**
To configure the IPv6 Internet and view network connection details, click the **IPv6** link. Refer to **Internet - IPv6** on page **39**

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

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



Internet - VLAN

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

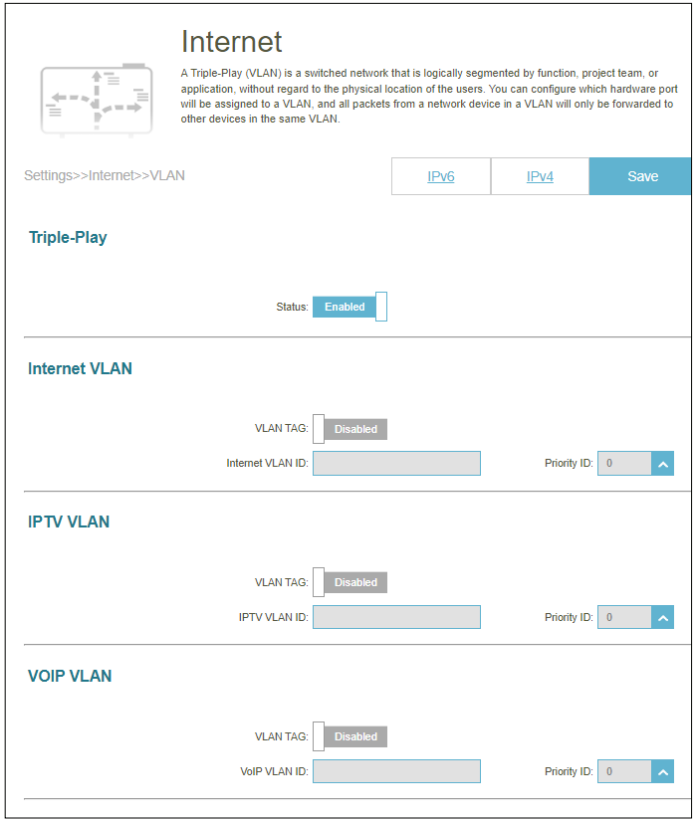
VLAN TAG Enable VLAN TAG to enter VLAN ID, as provided by your ISP

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.

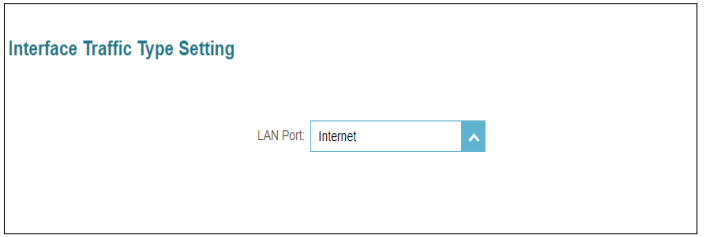
VoIP VLAN ID Enter the VLAN ID for your VoIP network, as provided by your ISP.

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.



Interface Traffic Type Setting

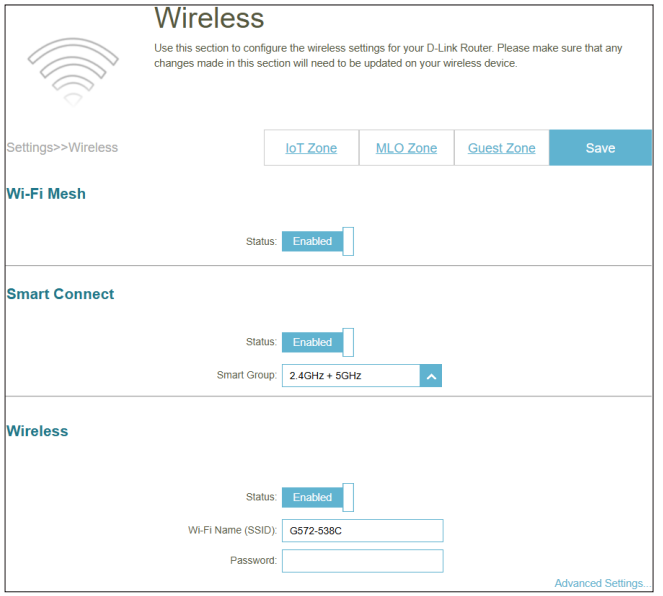
LAN Port From the drop-down menu, you can select the type of connection (Internet, IPTV, or Voice over IP) coming from the WAN connection to each interface on the router.



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.

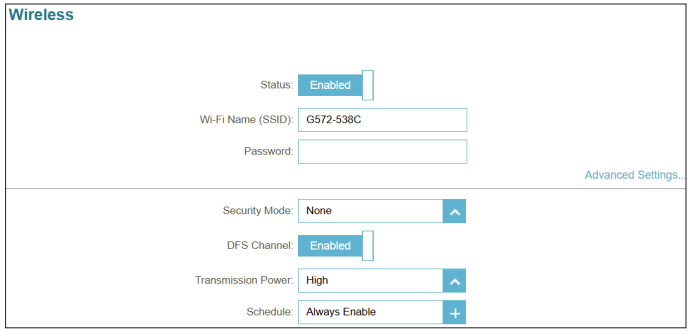
If Smart Connect is **Enabled***:*

Wireless

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

Password: Create a password 10–63 characters long containing both letters and numbers. Do not use identical characters in a row. Wireless clients will need to enter this password to successfully connect to the network.

Wireless - Advanced Settings...



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

DFS Channel: Enable Dynamic Frequency Selection (DFS) channels to use additional channels if the router is not in an area close by an airport or a radar station. If enabled, the router will listen for radar signals, and if radar signals are detected, it will automatically switch to a new channel. The default is disabled.

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.

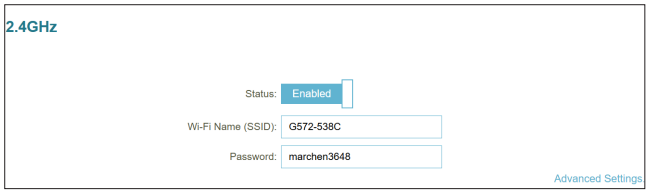
Smart Connect



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

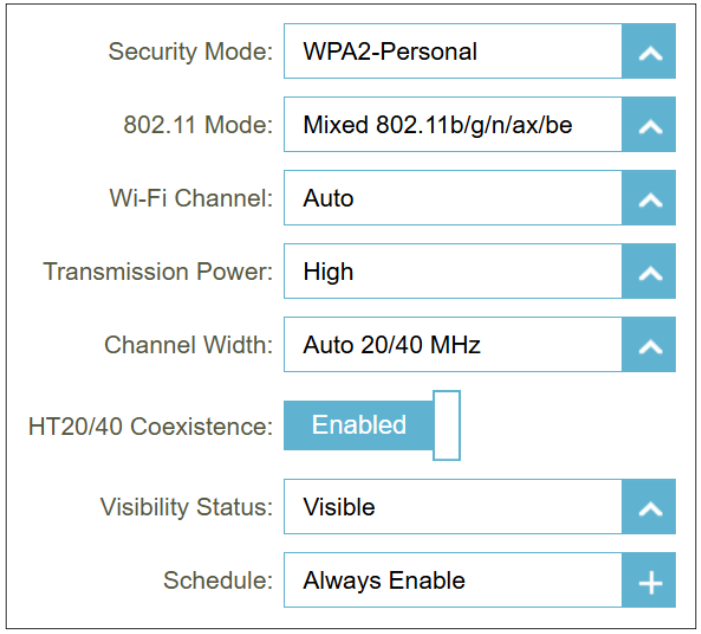


Status: Enable or disable the 2.4GHz / 5GHz wireless network.

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

Password: Create a password 10–63 characters long containing both letters and numbers. Do not use identical characters in a row.

2.4GHz - Advanced Settings...



Security Mode: Choose **None, Enhanced Open (AES), WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of security among these. The Enhanced Open provides access without requiring authentication but will encrypt data transmitted between the client and the router. Note that WPS will be disabled unless WPA2 encryption is enabled.

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/be, Mixed 802.11b/g/n/ax, Mixed 802.11b/g/n, Mixed 802.11b/g, Mixed 802.11g/n,** or **802.11b, 802.11g,** 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 802.11n and above devices, or select **20 MHz** if you are using only 802.11b/g devices.

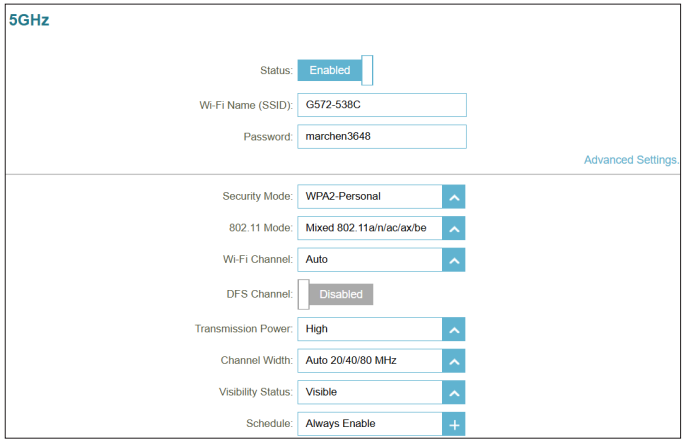
HT20/40 Coexistence (2.4GHz): Enable or disable HT20/40 Coexistence if Auto 20/40 MHz is selected above. It allows the router to switch between 20 and 40 MHz automatically

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

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

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

5GHz - Advanced Settings...



Security Mode: Choose **None, Enhanced Open (AES), WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of security among these. The Enhanced Open provides access without requiring authentication but will encrypt data transmitted between the client and the router. Note that WPS will be disabled unless WPA2 encryption is enabled.

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/be, Mixed 802.11a/n/ac/ax, Mixed 802.11a/n/ac, 802.11a/n,** or **802.11ac only, 802.11a only,** and **802.11n** only.

Wi-Fi Channel: Select a desired channel. The default is **Auto** (recommended).

DFS Channel: Enable Dynamic Frequency Selection (DFS) channels to use additional channels if the router is not in an area close by an airport or a radar station. If enabled, the router will listen for radar signals, and if radar signals are detected, it will automatically switch to a new channel. The default is disabled.

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

Channel Width (5GHz): Select **Auto 20/40/80 or 20/40/80/160MHz** (with DFS enabled) if you are using a mix of a/n and above such as 802.11ac as well as 802.11ax and 802.11be devices, and select **20/40 MHz** if you are using 802.11n/a devices, or select **20 MHz** if you are using only 802.11a devices only.

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.

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 Push Button Configuration (PBC) functionality. Enabling this feature will allow wireless clients to connect to the Wi-Fi through an encrypted connection established through pressing the WPS button.

Guest Zone

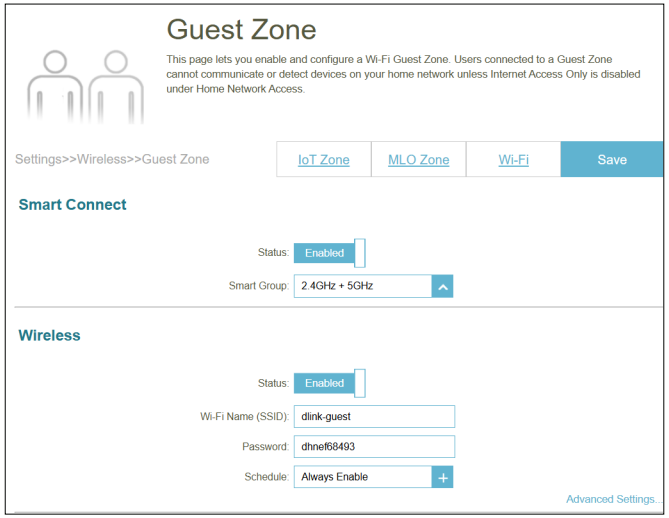
Go to **Settings > Wireless**, then click on the **Guest Zone** tab to configure your guest Wi-Fi.

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.

Smart Connect *If Smart Connect is **Enabled** , 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 10–63 characters long containing both letters and numbers. Do not use identical characters in a row.
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.

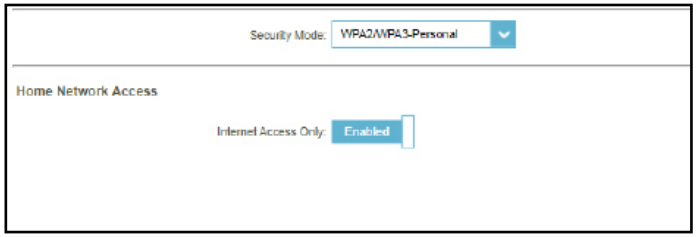


Advanced Settings

Security Mode Choose **None, Enhanced Open (AES), WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of security among these. The Enhanced Open provides access without requiring authentication but will encrypt data transmitted between the client and the router. Note that WPS will be disabled unless WPA2 encryption is 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.

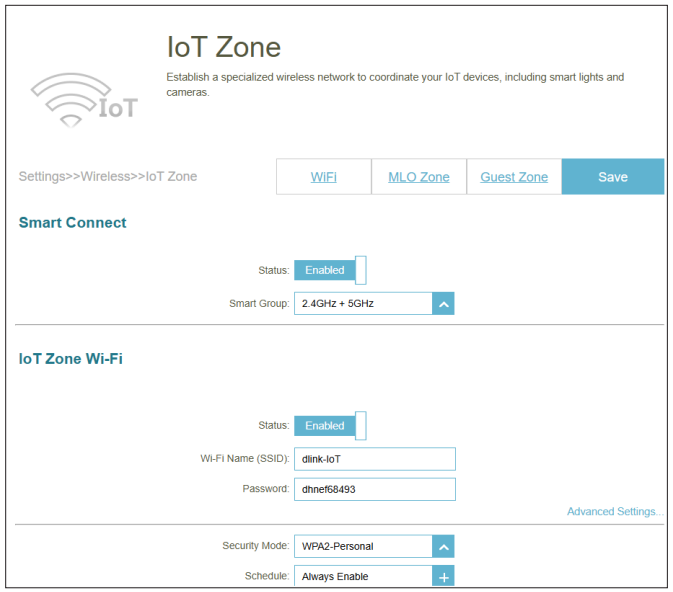


IoT Zone

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

IoT Zone feature enables you to create a wireless network for connecting and managing IoT devices. This zone will be separate from your main Wi-Fi network.

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



Smart Connect	*If Smart Connect is **Enabled** , 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 10–63 characters long containing both letters and numbers. Do not use identical characters in a row.
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, Enhanced Open (AES), WPA/WPA2-Personal, WPA2-Personal, WPA2/WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of security among these. The Enhanced Open provides access without requiring authentication but will encrypt data transmitted between the client and the router. Note that WPS will be disabled unless WPA2 encryption is enabled.

MLO Zone

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

The **MLO Zone** feature enables you to create a wireless network for Multi-link Operation (MLO). This zone allows for bandwidth aggregation from different bands to reduce congestion and disconnection. It will be separate from your main Wi-Fi network.

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

Wireless	
Status	Enable or disable the MLO Wi-Fi network. The default is disabled.
Wi-Fi Name (SSID)	Enter a name for your MLO wireless network.
Password	Create a password for your guest Wi-Fi network. Wireless clients will need to enter this password to successfully connect to the 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.



Advanced Settings

Security Mode Select the Wi-Fi security: **Enhanced Open (AES)** or **WPA3-Personal.** Choose **WPA3-Personal** for better security protection. Choose **Enhanced Open** for connection with data encryption but without requiring authentication.

To use MLO, make sure that your network adapter and operating system support Wi-Fi 7. For Windows, Wi-Fi 7 MLO requires Windows 11 version 24H2 or later.

To obtain the version of Windows, go to **Start** > **Settings** , select **System**, and navigate to **About**, you will then see information about edition and version.

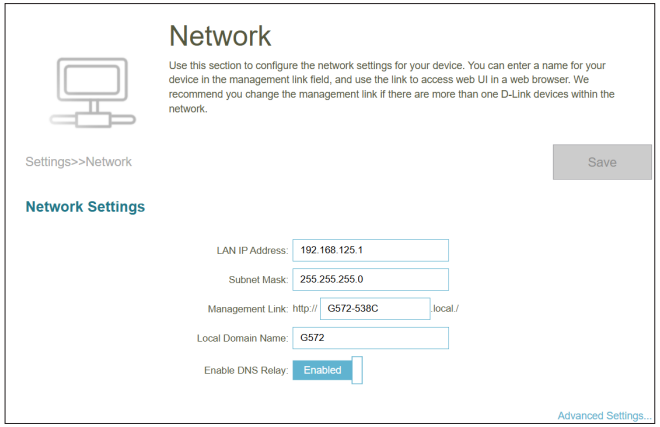
To check if the MLO is active, go to **Settings > Network & Internet** and select **Wi-Fi**. Select your Wi-Fi connection to display its properties, then check the information listed under Network band. And if there are two bands listed, MLO is working.

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://G572-xxxx.local/** (where xxxx represents the last 4 characters of your router's MAC address). You can replace this address shown in the text field.
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.



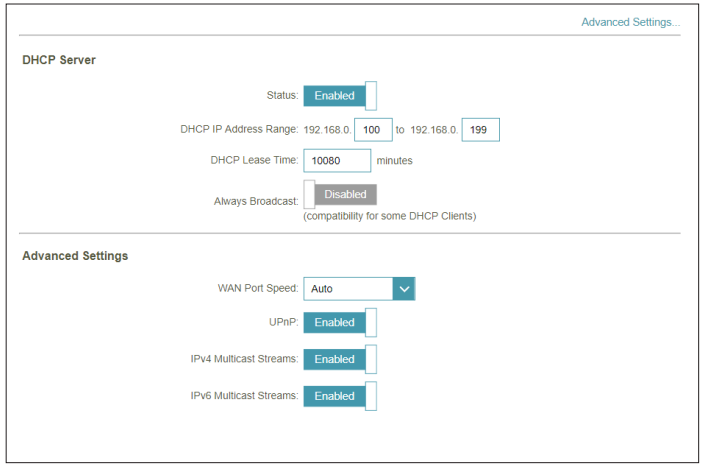
DHCP Server

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**, **2500 Mbps**, or **Auto** (recommended).

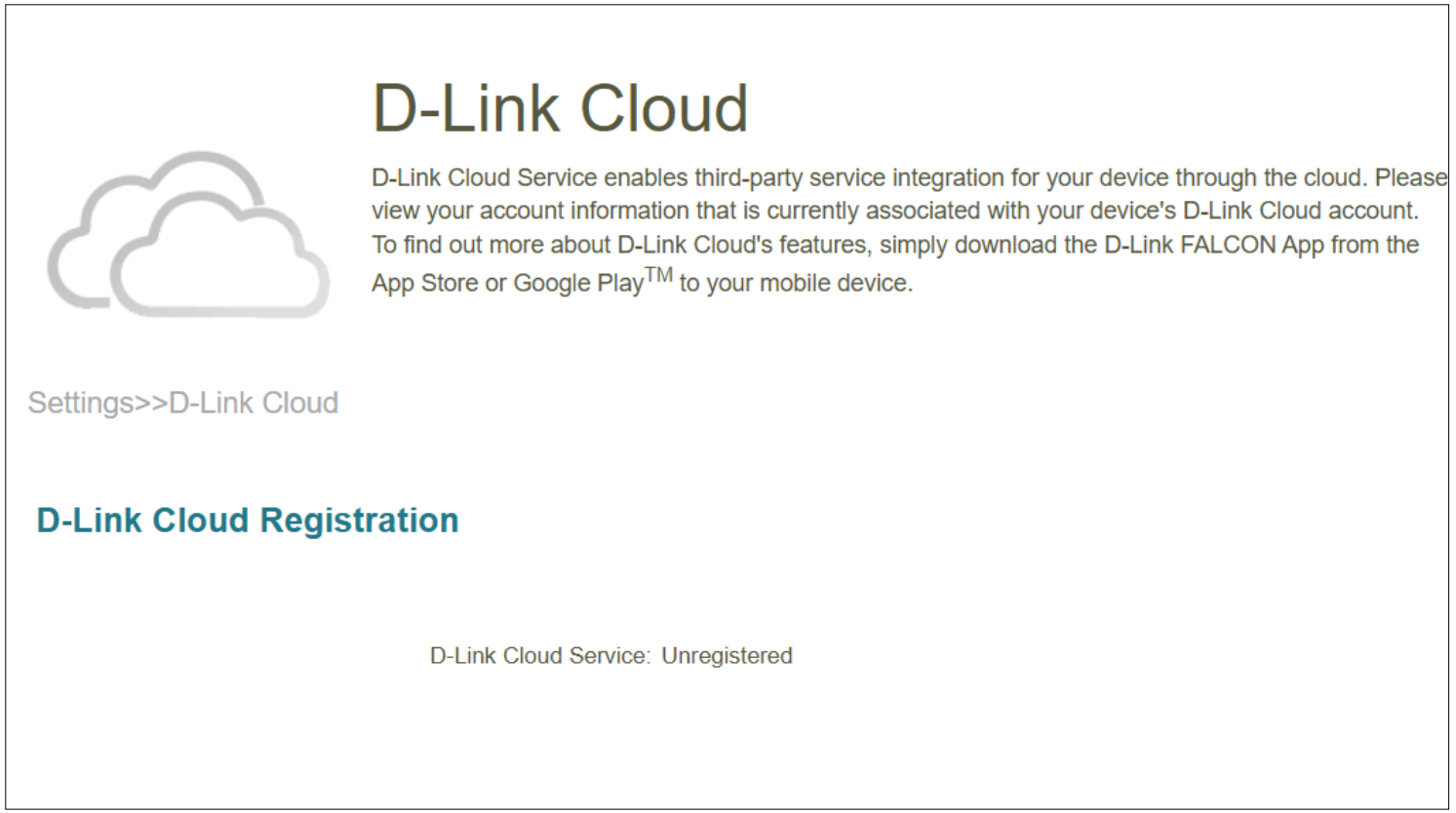
UPnP — Enable or disable Universal Plug and Play (UPnP). UPnP provides compatibility with networking equipment, software, and peripherals. This is enabled by default.

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.

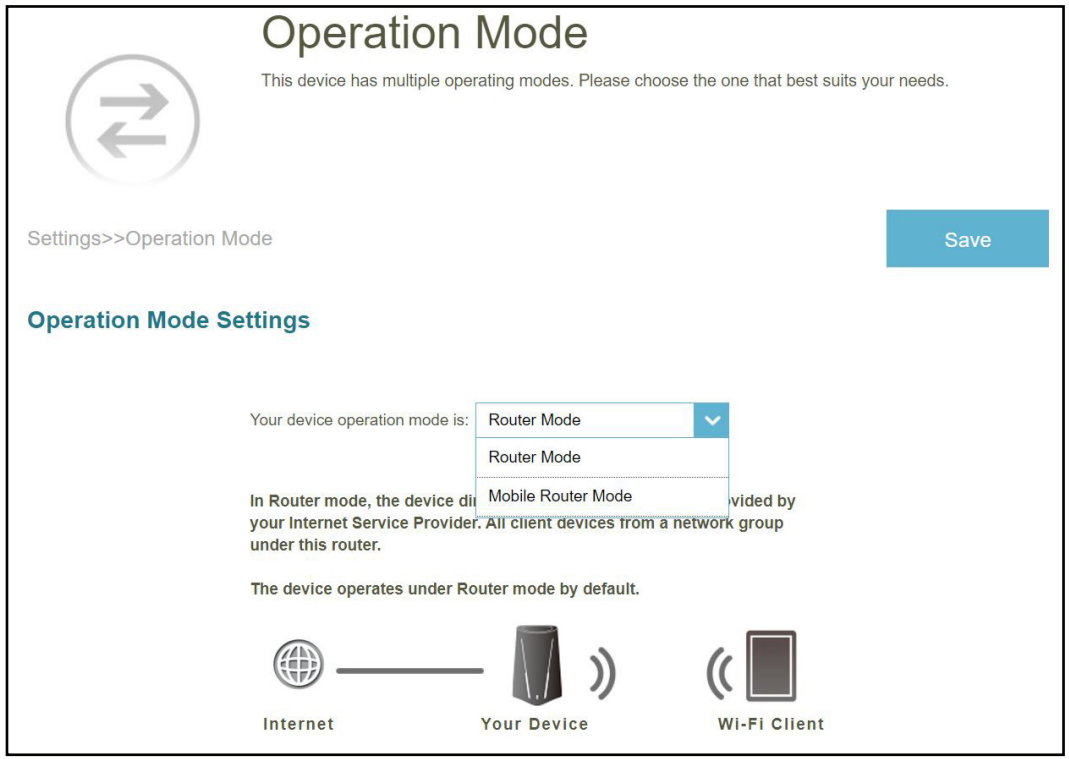


Operation Mode

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, G572 connects to the Internet directly through a wired connection, such as DSL. All client devices from a network group are connected and managed under this router. This is the default mode.

Mobile Router: In this mode, G572 connects to the Internet via 5G/LTE network provided by mobile Internet service Provider. All client devices from a network group are connected and managed under this router.



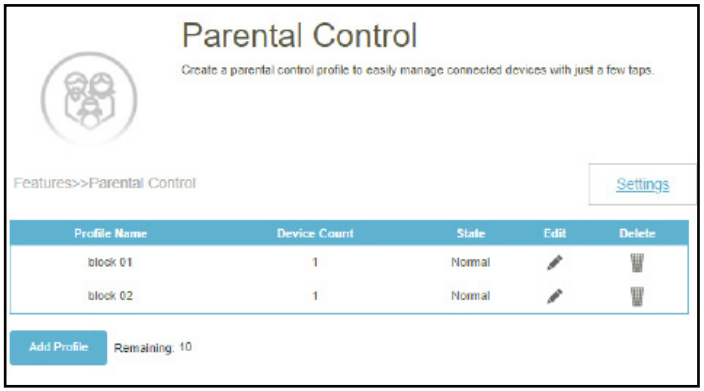
Features

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:

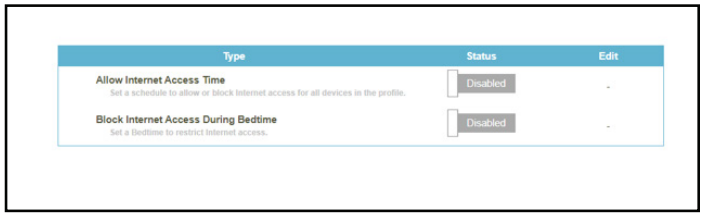
Schedule

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.

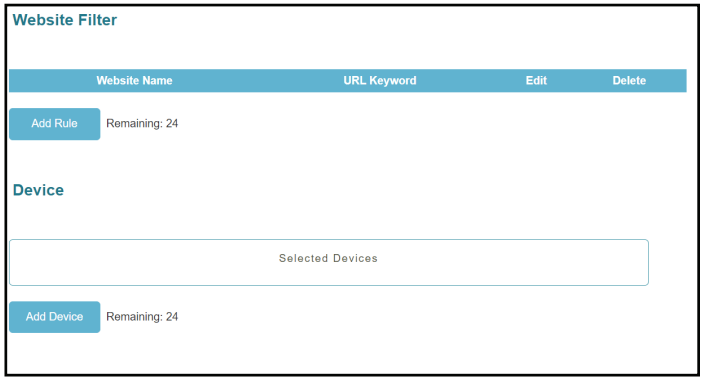
To add a schedule:
Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule. **If no time periods are selected, 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.



Note: The Bedtime schedule takes precedence over Allow Internet schedule.

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

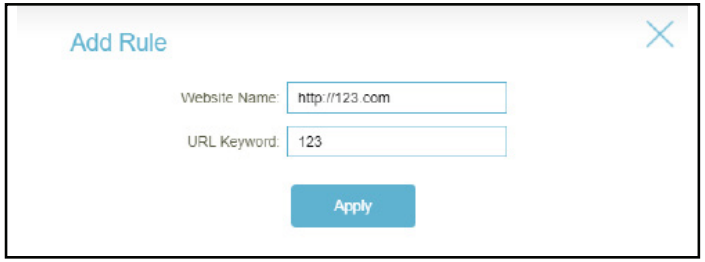


Website Filter

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."

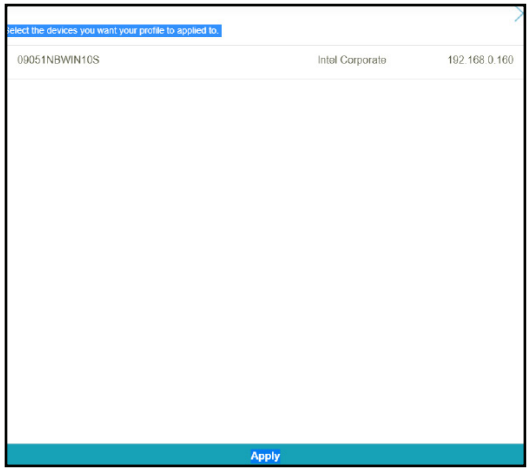
URL Keyword: This blocks access to websites based on the keywords with matching URLs. For example, use "ABC" to block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC. Enter the same website name as the above in this field to block only a specific URL.



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

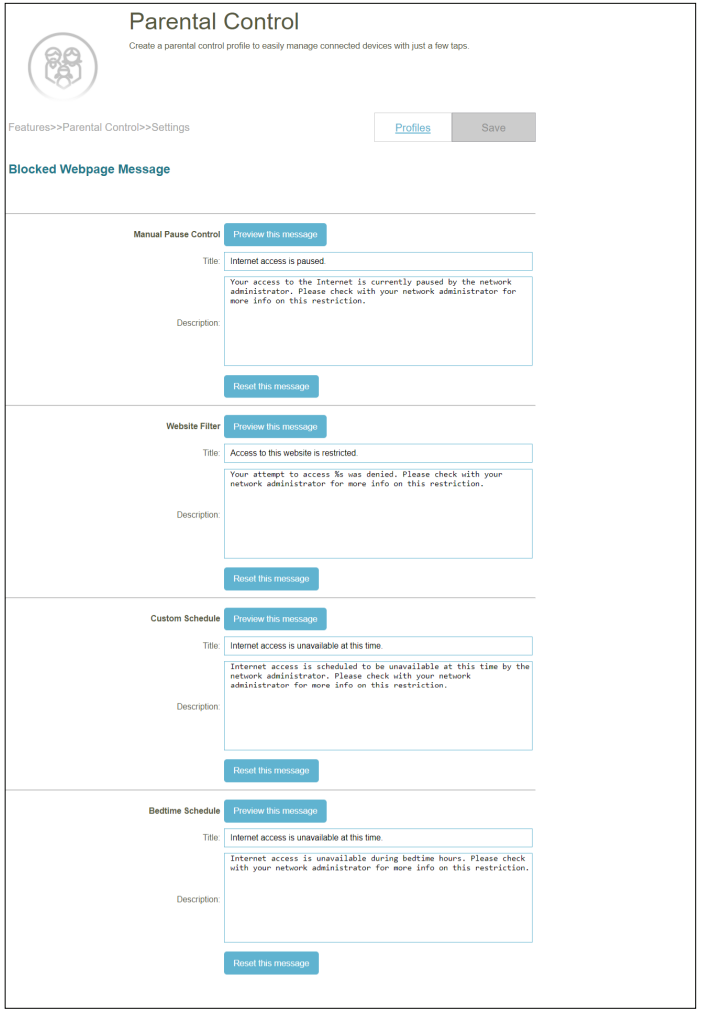
You can view and customize displayed messages and titles in **Settings** when **Manual Pause Control, Website Filter, Custom Schedule,** and **Bedtime Schedule** is enabled.

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.

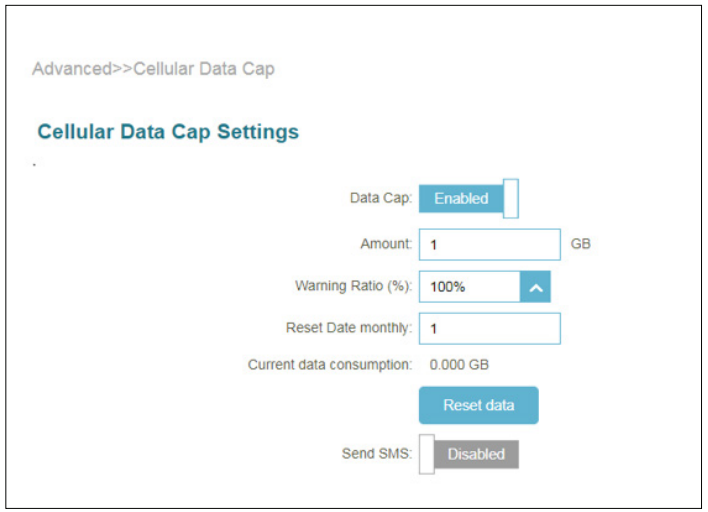


Data Cap

Go to **Features > Data Cap** 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.

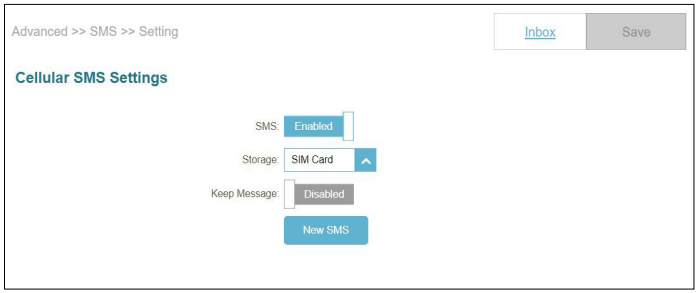


Note: Sending SMS messages may incur additional fees. Please contact your ISP for more information.

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.

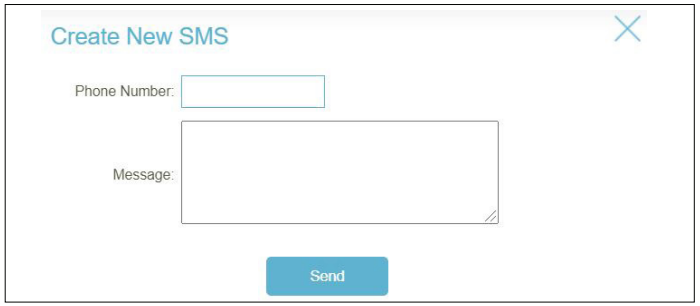
Cellular SMS Settings	
SMS	Enable or disable the SMS receiving function.
Storage	Select **SIM Card** or **Module** to store the SMS messages.
Keep Message	Enable or disable Keep Message.
Keep Number	Set the amount of SMS messages to be saved. Up to 20 messages can be saved.



Click **New SMS** to create a new SMS message.

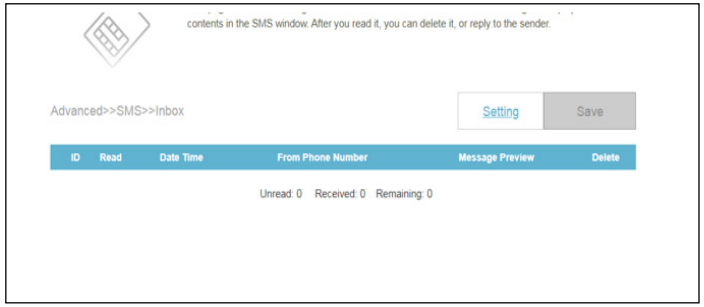
Cellular SMS Settings	
Phone Number	Enter the phone number of a recipient. For international numbers, enter "+" followed by the country code for international numbers.
Message	Enter your message here.

Then click **Send**.



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

Inbox	
ID	Displays the sender's ID.
Read/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.



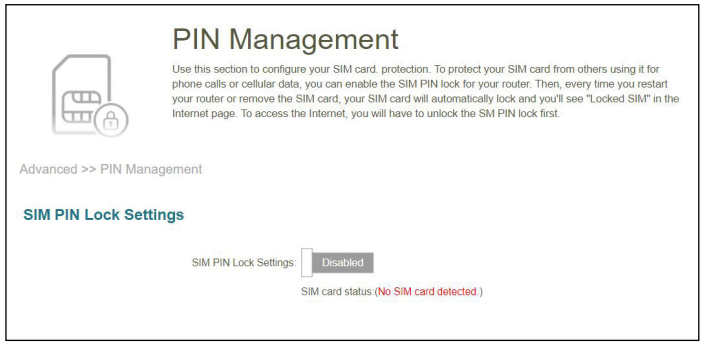
PIN

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

PIN Management	
SIM PIN Lock Settings	Enable or disable PIN lock on the SIM card.
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 reinstalled.

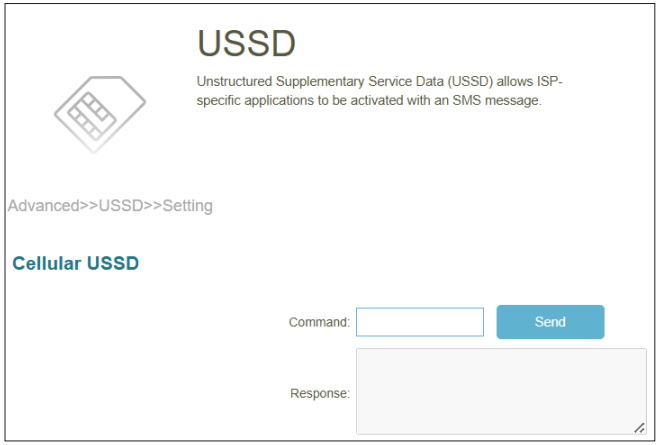
Click **Apply** when you are done.



USSD

Go to **Features > USSD** to USSD command. Unstructured Supplementary Service Data (USSD) allows ISP-specific applications to be activated with an SMS message. It allows you to check account information such as data usage or balance.

Cellular USSD	
Command	Enter a predefined code or symbols and click **Send**.
Response	Displays the result.

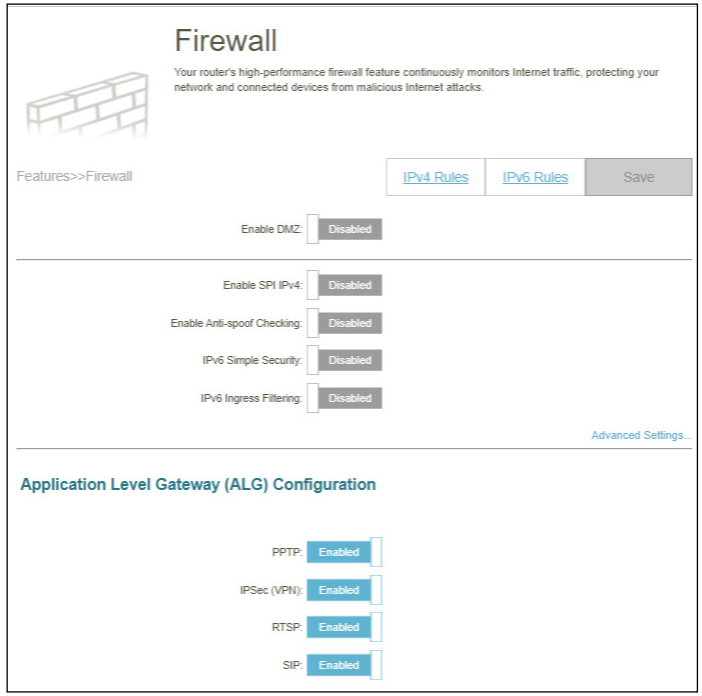


Firewall

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 **80**
To configure your IPv6 firewall rules, click the **IPv6 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on page **80**

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.

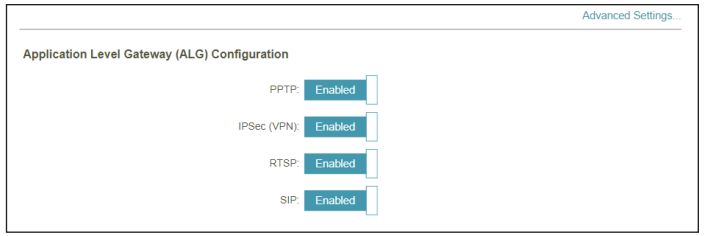
Enable SPI IPv4: Enabling Stateful Packet Inspection (SPI) or dynamic packet filtering helps prevent cyber attacks by tracking more states per session to validate and ensure that the traffic passing through the session conforms to the protocol.

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

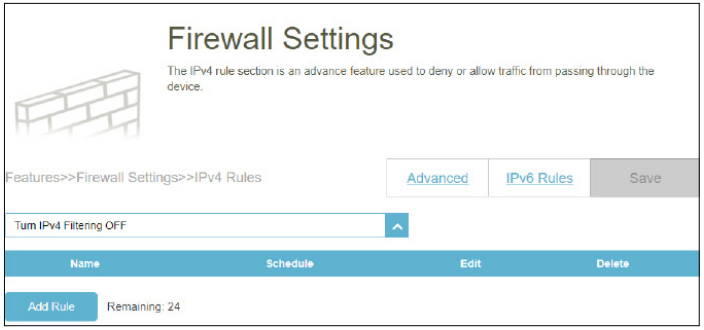
Go to **Features > Firewall**, then click the **IPv4 Rules** tab or the **IPv6 Rules** tab to configure rules for filtering the inbound/outbound traffic based on parameters like IP address with ports.

To configure the Firewall Advanced settings, click the **Advanced** link. Refer to **Firewall** on page **78**

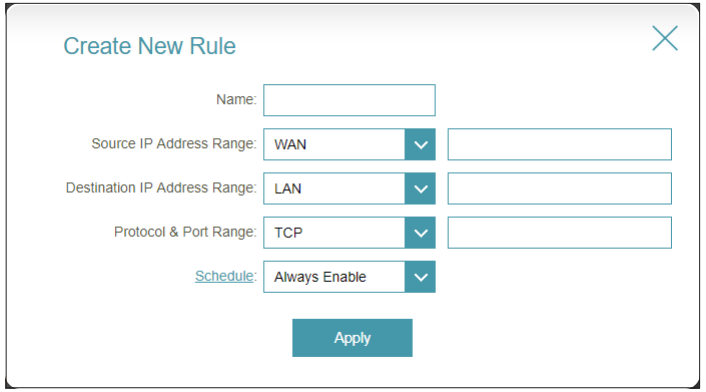
Click **Save** at any time to save the changes you have made on this page.

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 **92** for more information.

Click **Apply** when you are done.

A maximum of 24 rules can be defined.

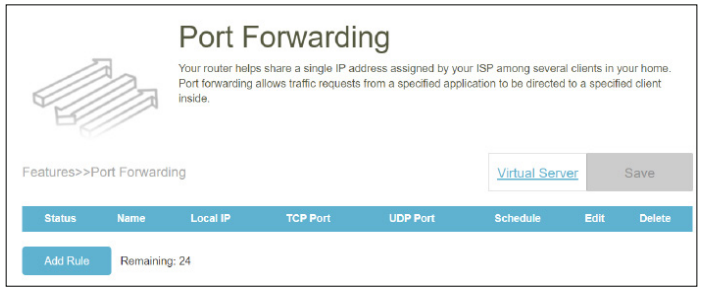
Port Forwarding

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.

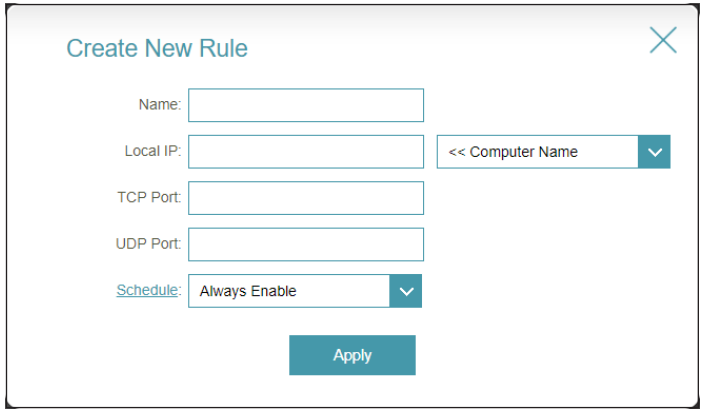
To configure the Virtual Server settings, click the **Virtual Server** link. Refer to **Port Forwarding - Virtual Server** on page **84**.

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 **92** for more information.

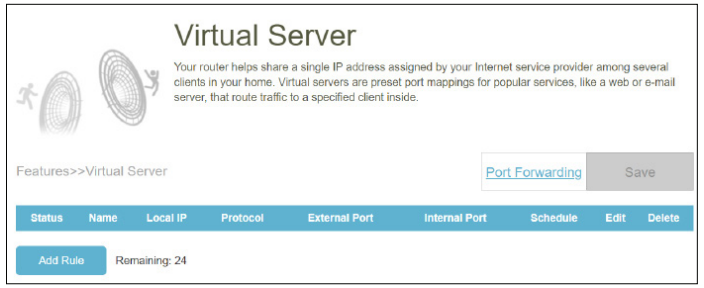
Port Forwarding - Virtual Server

Go to **Features > Port Forwarding** to click on the **Virtual Server** tab for configuring its settings and specifying a single public port or known service 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.

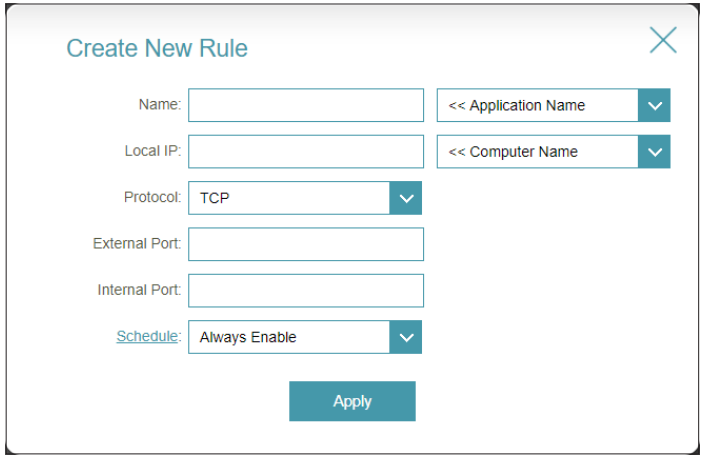
To configure the Port Forwarding settings, click the **Port Forwarding** link. Refer to **Port Forwarding** on page **82**

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 **92** for more information.

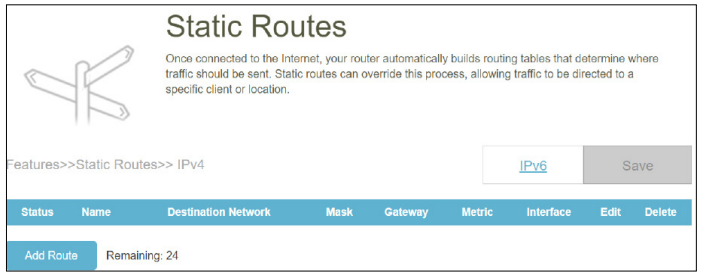
Static Routes - IPv4

Go to **Features > Static Routes** to define custom routes that control the pathway of data traffic to reach its destination.

To configure the Static Route IPv6 settings, click the **IPv6** tab. Refer to **Static Routes - IPv6** on page **87**

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 network IP address of this route.

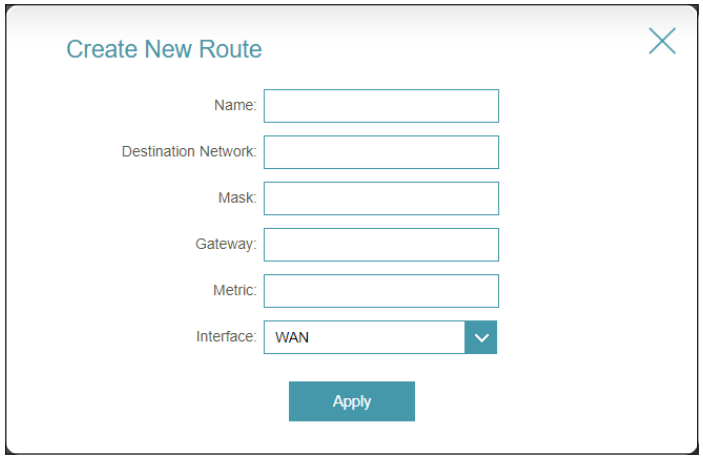
Mask: Enter the subnet mask of the route.

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.



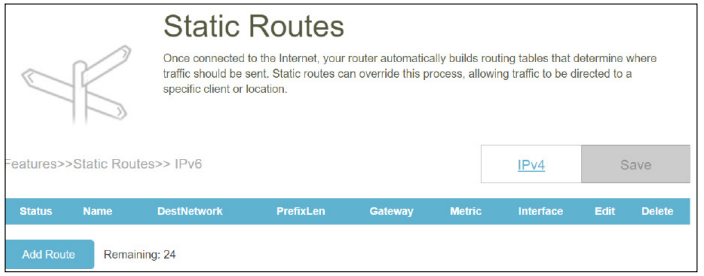
Static Routes - IPv6

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 **86**.

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.

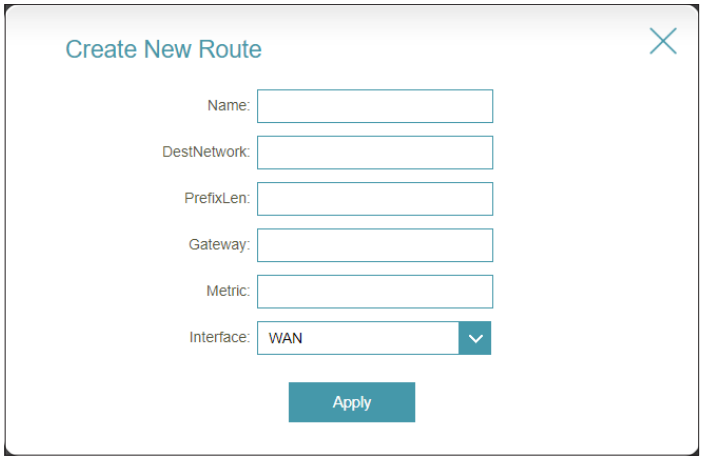
DestNetwork: Enter the destination network IP address of this route.

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.

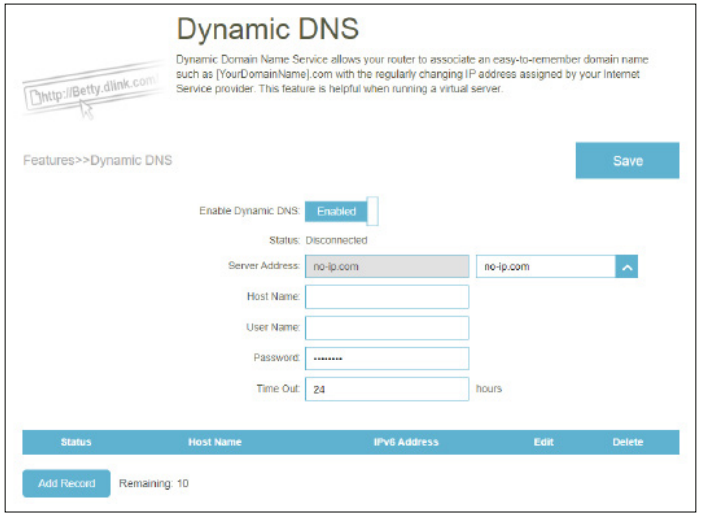
Server Address: Select a Dynamic DNS server from the drop-down menu.

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.

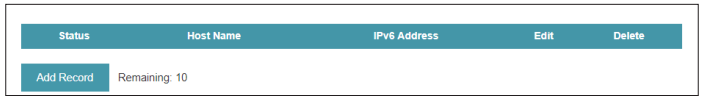
Time Out: Enter a time-out value (in hours) to indicate how often the router should update its Dynamic DNS settings.



A maximum of 10 records can be defined.

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

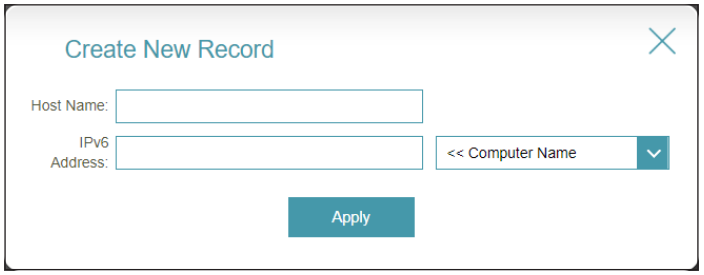
If you wish to remove a record, click in the Delete column. If you wish to edit a record, click in the Edit column. If you wish to create a new record, click the **Add Record** button.



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.

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 **105**. 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 client 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 **97.**

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 Create a password 10–32 characters long that combines letters and numbers, without repeating characters consecutively.

PSK: Enter a Pre-shared Key between 8 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. The profile can be imported conveniently to these devices later for quick connection configuration.

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.

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.

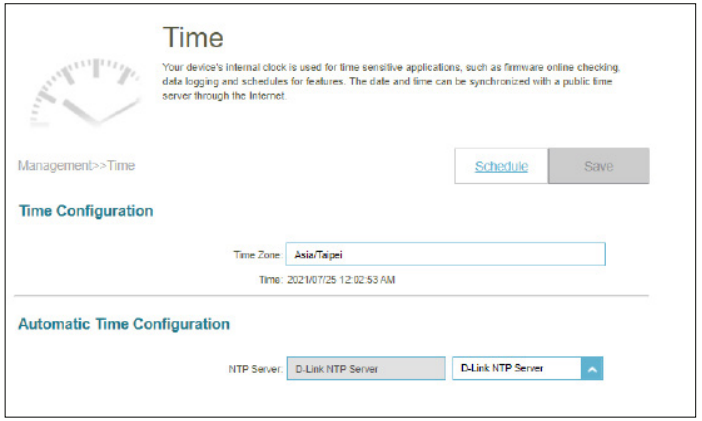
To configure the Schedule settings, click the **Schedule** tab. Refer to **Time & Schedule - Schedule** on page **92**

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

Time Configuration

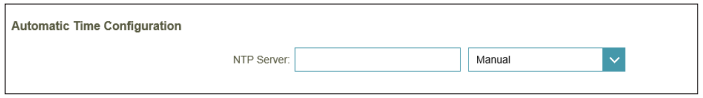
Time Zone Select your time zone from the drop-down menu.

Time Displays the current date and time of the router.



Automatic Time Configuration

NTP Server Select 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.

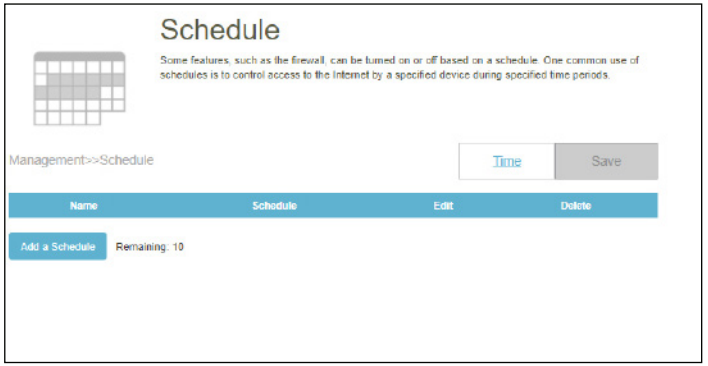


Time & Schedule - Schedule

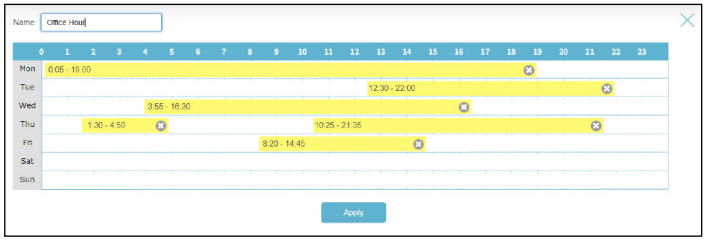
Go to **Management > Time & Schedule**, then click the **Schedule** tab. The **Schedule** page allows you to control some of the functions based on a pre-configured schedule; for example, Port Forwarding in **Features > Port Forwarding** and Firewall Settings in **Features > Firewall** as well as sending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

To configure the Time settings, click the **Time** tab. Refer to **Time & Schedule - Time** on page **91**

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.

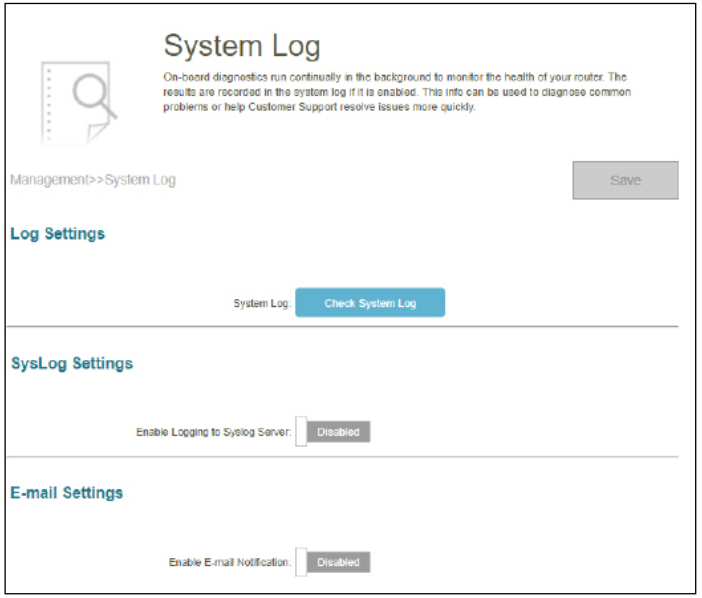
Log Settings

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.

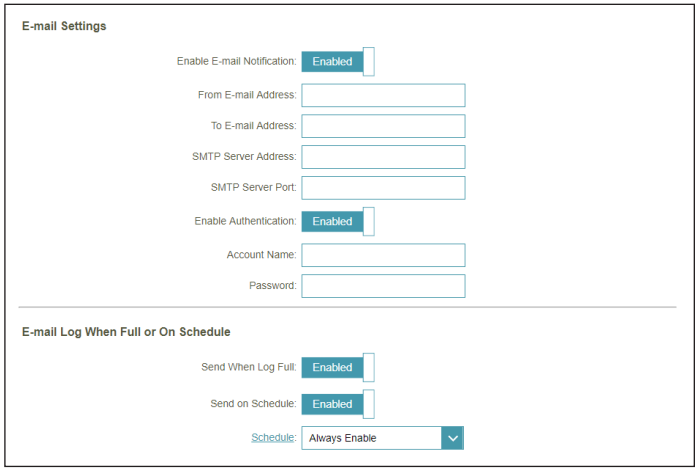
SysLog Settings

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.



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.

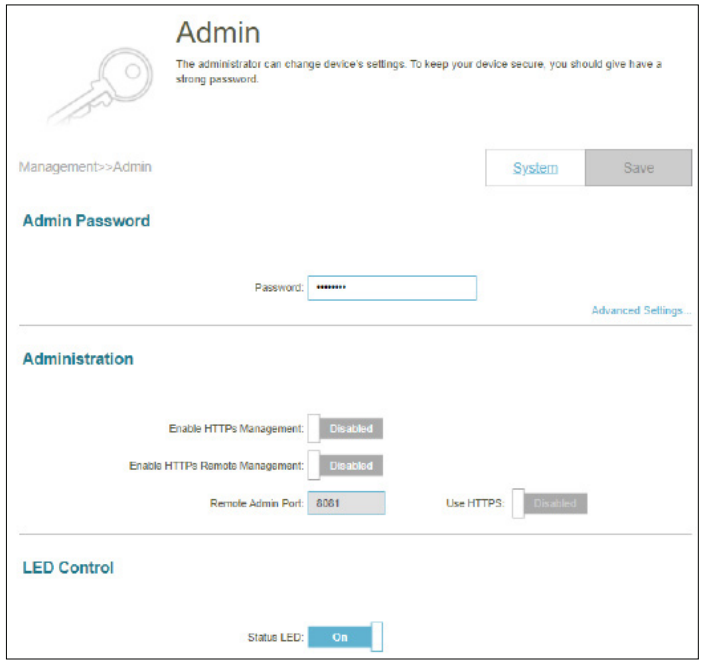
Schedule If you want to enable **Send On Schedule**, use the drop-down menu to select a schedule to apply. The schedule may be set to **Always Enable**, or you can create your own schedules in the Schedules section. Refer to **Time & Schedule - Schedule** on page **92** for more information.

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 **96**

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.

The password must contain 10 to 15 characters and include at least three of the following four character types:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0–9)
- Special characters or symbols, e.g., * and %.

Advanced Settings... - Administration

Enable HTTPS Management — Enable HTTPS to connect the router with security protection. The default is enabled.

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. The default is 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 **95**

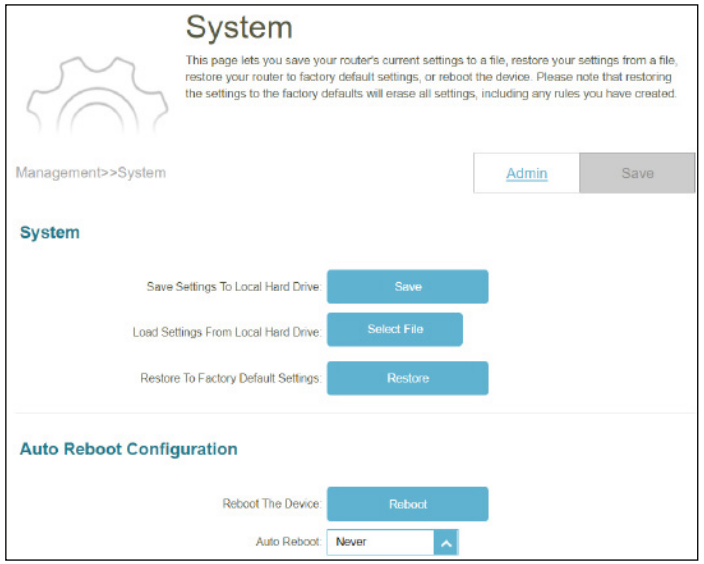
Click **Save** at any time to save the changes you have made on this page.

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.

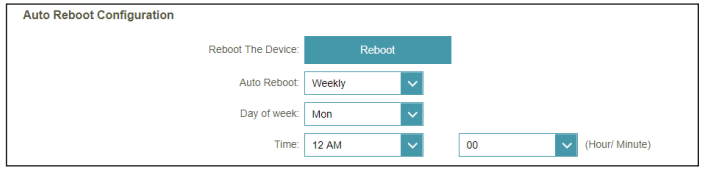
Restore to Factory Default Settings: This option will restore the router back to the default configurations stored in the firmware. Any settings that have not been saved will be lost, including any rules that you have created. If you want to back up the current router configuration settings before restoring 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.

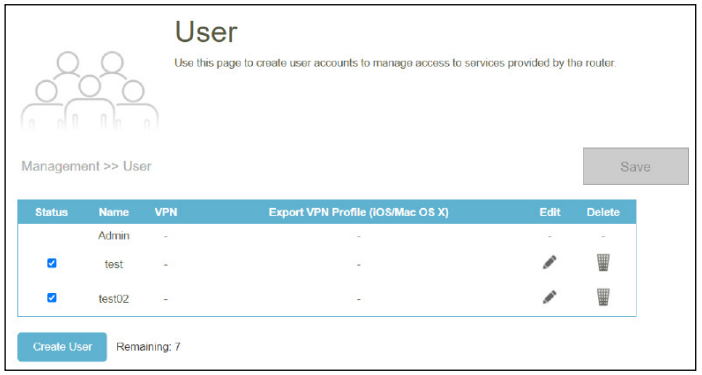
Auto Reboot: You may set the router to automatically reboot at a set time. The options are **Never, Daily,** or **Weekly**. You may set the day, and hour and minute of the day for an automatic reboot.



User

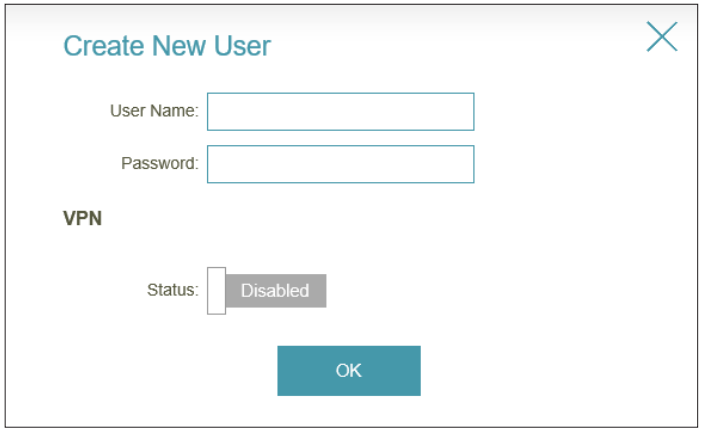
Go to **Management > User**. The User page is used to create, manage, and delete user accounts with VPN connection permission.

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. Create a password 10–15 characters long that combines letters and numbers, without repeating characters consecutively.

VPN

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

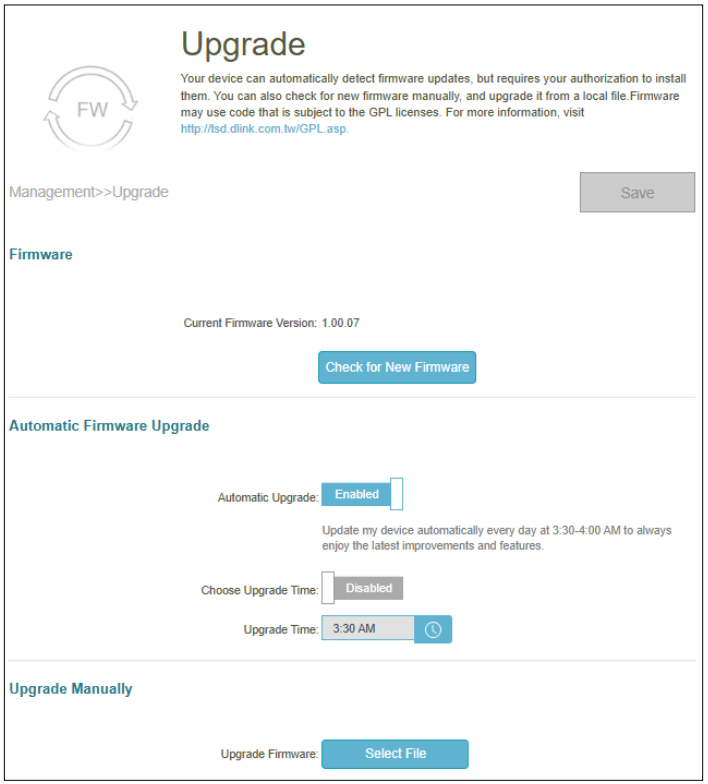
A maximum of 9 users (not including the Admin) can be created. Click **OK** to close the screen.

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	
Select File	If you wish to upgrade manually, first download the firmware file. Then, click the **Select File** button and locate the file to install the new firmware.
Automatic Firmware Upgrade	
Automatic Upgrade	If enabled, the router will automatically upgrade to the newest firmware. The system will automatically upgrade to the latest firmware every day at 3:30-4:00 AM.
Choose Upgrade Time	Enable this function to set the router to automatically upgrade its firmware at a set time every day.
Upgrade Time	Configurable if **Choose Upgrade Time** is enabled. Set the hour and minute to automatically upgrade the router.

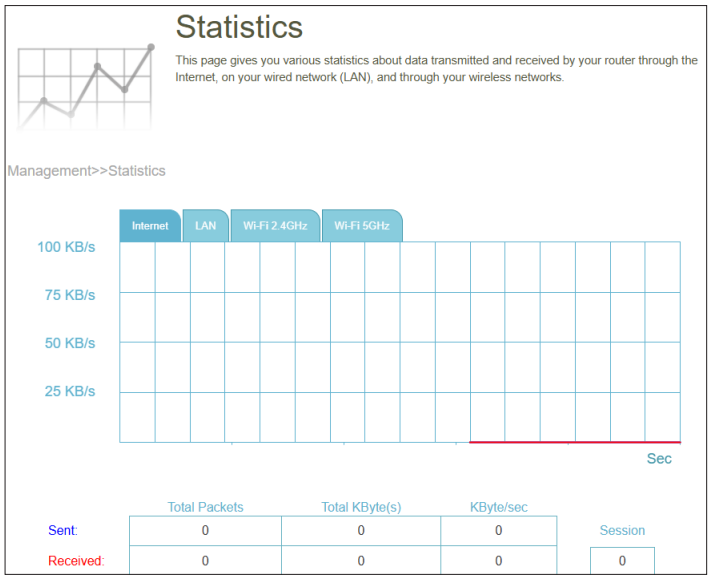


Statistics

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

You can view the **Internet**, **LAN**, **Wi-Fi 2.4 GHz**, and **Wi-Fi 5 GHz** by clicking on the respective tabs at the top of the graph. The graph will update in real time. To clear the information of the graph, click **Clear**.

The table below for each interface and radio frequency shows the total number of packets and data that are sent and received through the interface.
The traffic counter will reset if the device is rebooted.



D-Link FALCON

The G572 can be set up fast using the D-Link FALCON app on your smart devices. Plug in your router, go to the app, and follow the simple steps to set up your home network. The new D-Link FALCON app is specifically designed to simplify your management tasks with these features:

AI Wi-Fi Optimizer: The Wi-Fi optimizer automatically connects to the best available channel for seamless, reliable coverage across your home.

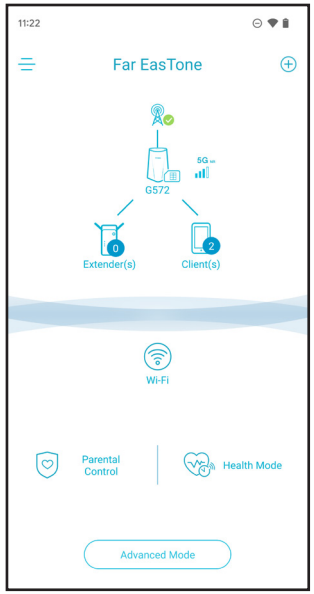
Mobile Data Usage Monitoring: The mobile data usage displays the cumulative mobile data usage up to the current day of the billing cycle.

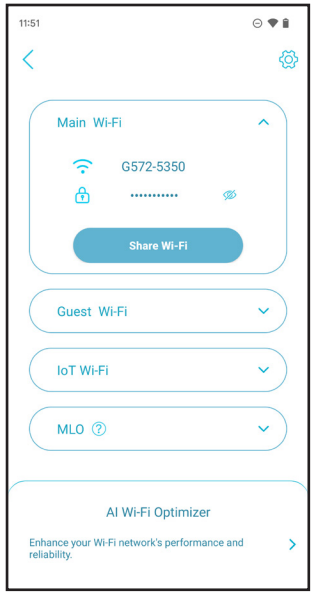
AI Parental Control: The Parental Control provides the highest flexibility of Internet accessibility control and website filtering. It allows administrators to restrict devices to reduced speeds or no Internet access during designated time periods.

Health Mode: The Health Mode helps improve your sleep by turning off the Internet connection at night automatically.

AI Wi-Fi Optimizer

From the home screen, tap **Wi-Fi**. Then, tap **AI Wi-Fi Optimizer** at the bottom of the screen. Your wireless connection will automatically choose the optimal channel for Internet access through the established Wi-Fi system.





Mobile Data Usage Monitoring

The Mobile Data Usage page displays a report of mobile data consumption. Tap a date on the graph to display the exact cumulative usage as of that date. You can also configure a usage threshold. When the threshold is reached, an SMS notification is sent, allowing you to adjust your usage and avoid potential surcharges.

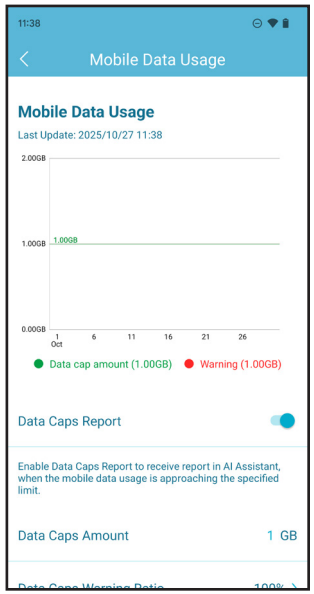
From the home screen, tap the main router, then scroll down **Internet Settings** and tap **Mobile Data Usage**. You can configure the following settings related to mobile data usage:

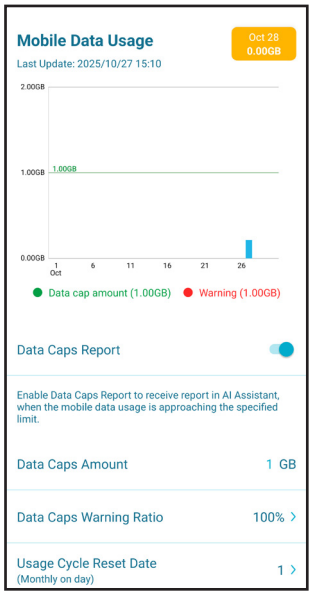
Data Cap Amount: Specify the maximum allowed monthly data usage.

Data Cap Warning Ratio: Set the percentage of the data cap at which an SMS notification will be sent.

Usage Cycle Reset Date: Define the day of the month when the usage counter resets.

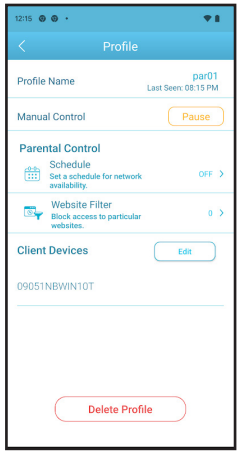
Send SMS to Me: Enable this option to receive SMS notifications automatically when usage approaches the set threshold.

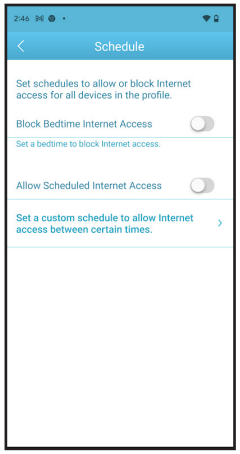




AI Parental Control:

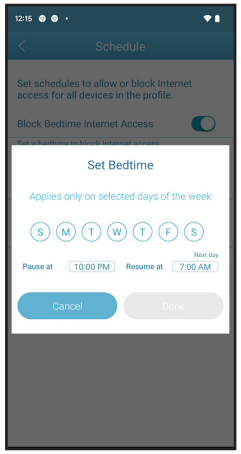
From the home screen, tap **Parental Control**. Then follow the steps below to add a new control profile:
1. Tap + icon.
2. Name this profile.
3. Select client devices to which the profile will be applied.
4. Tap **Done** to complete.
5. The profile summary will be displayed. On this page, you can tap **Pause** to pause the Internet immediately to the devices specified in the profile.

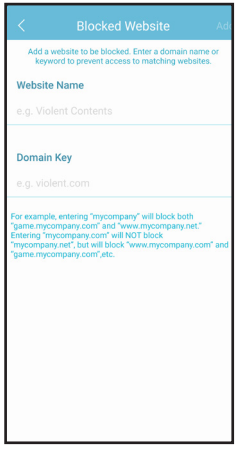




You can set custom and bedtime schedules to restrict Internet access during the defined days and time periods. Once the custom scheduled access is enabled, devices will be blocked from Internet access except the defined allowed time periods. For bedtime scheduling, select days of the week with restricted time periods. Up to 2 bedtime schedules can be defined.

Note: If there is time overlap between your bedtime schedules and custom schedules, you will be required to reconfigure the overlapped schedules.

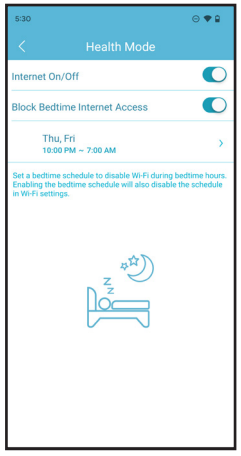


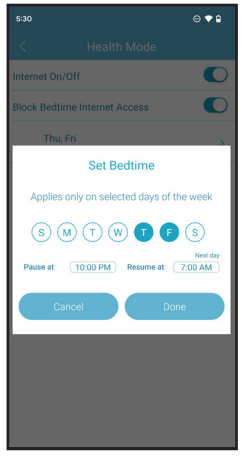


You can also block specific websites. To do this, tap **Website Filter**, tap **Add Website**, then enter the website name and the domain key. For example, enter "violent.com" to block both "violent.com" and "www.violent.com". And enter the domain key "violent" to block any URLs containing violent.

Health Mode:

The app enables you to proactively improve sleep quality by restricting Internet access during nighttime. Tap **Health Mode** to set the bedtime during which Internet access will be blocked. To schedule a bedtime, select the weekdays and the start and end time for the bedtime schedule.





Wi-Fi Settings:

From the home screen, tap **Wi-Fi,** and tap the gear icon. Here you can configure Wi-Fi settings for Main and Guest wireless network as well as other Wi-Fi zones. These zones are separate from your main wireless network and you can control Internet access and allowed wireless band in these zones. The following explain the differences of these zones:

Main Wi-Fi: The primary Wi-Fi used by trusted devices such as computers, NAS, mobile devices for works and leisure.

Guest Wi-Fi: A separate network designated for devices that need Internet connections only but not access to the internal resources.

IoT Wi-Fi: A dedicated network for Internet of Things (IoT) devices such as smart cameras, smart sensors, and other smart home gadgets.

MLO Wi-Fi: Multi-Link Operation aggregates multiple bands to enable dynamic traffic transmission across multiple links, improving speed and reliability for compatible devices.

Share Wi-Fi: Click this button to send a copy of the Wi-Fi setting with the configured password using one of the instant messaging utilities installed on your phone with other devices.

Wi-Fi Mesh: Mesh network ensures reliable wireless connectivity across the main router and mesh points. The default is enabled.

Smart Connection: Enable this feature to allow client devices to connect automatically to either the 2.4 GHz band or 5 GHz band, depending on the supported frequency. Disable this feature to configure each band separately. The default is enabled.

Wi-Fi Name: The name of the wireless network that appears on the Wi-Fi scan list.

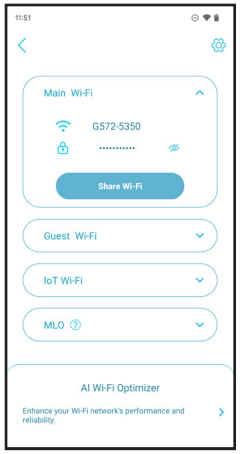
Password: Enter the password or network key for connecting with the Wi-Fi network.

Security: Select the security standard: WPA3, WPA2/WPA3, WPA2, or WPA/WPA2. It is recommended that you use the strongest security protocol - WPA3. Note for MLO zone, only WPA3 is available.

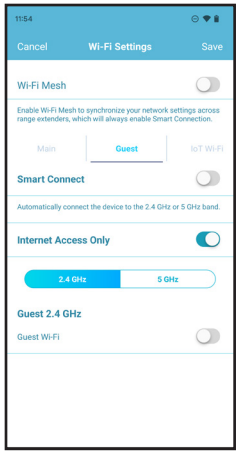
Wi-Fi Schedule: Select the time during which the wireless network will be available.

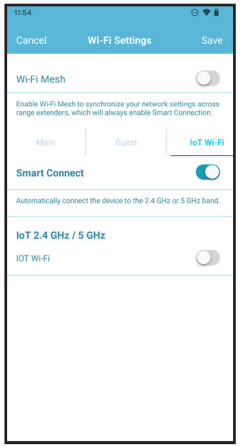
Internet Access Only: Enable or disable the Internet access for the Guest zone. This option is only available for the Guest zone.

After changing the configurations on this page, click **Save** at the top right.











Other Features

Advanced Mode

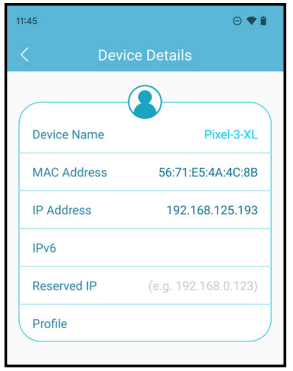
The advanced mode provides links to the web management interfaces of the device. Note that this feature is only available with local access. To access, tap the the **Advanced Mode** button from **Home**.

Device Information and Settings

From **Home**, tap the device (**main router)** in the mesh network topology to view its information and settings: name, IP and MAC address, hardware and firmware version, time zone, and model number. You can also configure the Internet connection method and change the device password on this page. It also provides basic device maintenance functions: Status LED, Identfy Device, Restart the Device, and Reset to Factory Default.

Failover Settings: Failover ensures continuous Internet connectivity (the default is disabled). When the primary connection becomes unavailable, the secondary Internet connection automatically takes over. To configure this feature, tap the **2nd Internet (Failover WAN**) under **Settings,** then enable **Dual WAN** to display configuration options. Tap Dual WAN Type to configure how the primary connection should be checked for conection status. Then tap **Internet Connection** to configure the backup connection method.



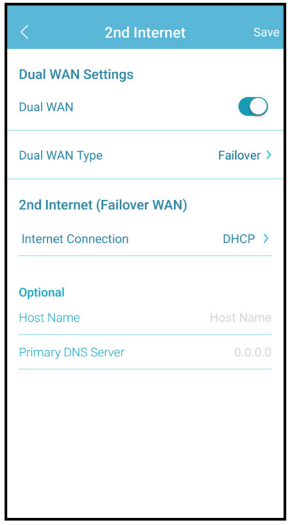


Client Information and Statistics

From **Home**, tap the device **(Clients)** in the mesh network topology to view clients currently online or blocked. Tap a device to obtain its information: name, IP and MAC address, and parental control profile.

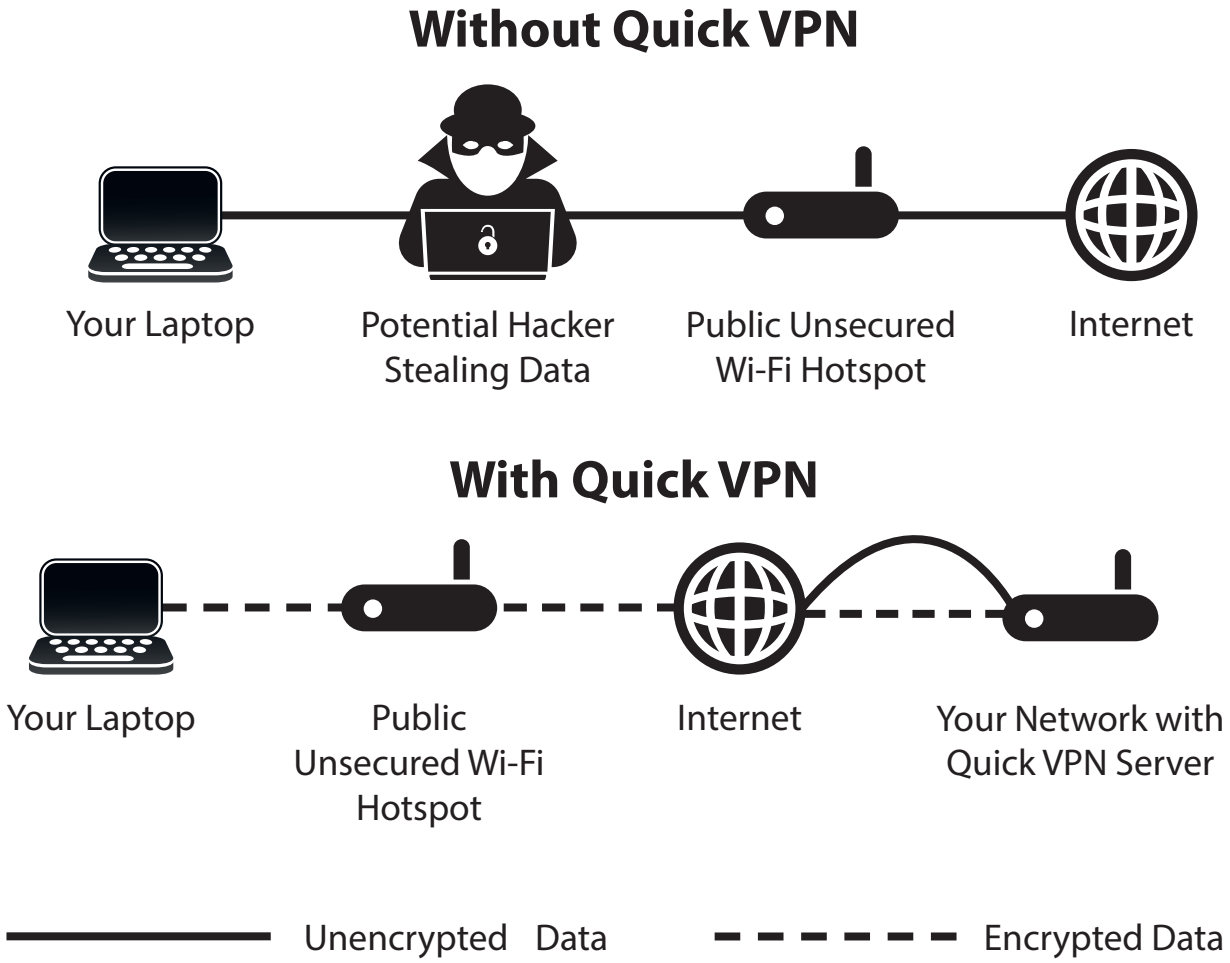
Extender Information

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



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.



Important Information

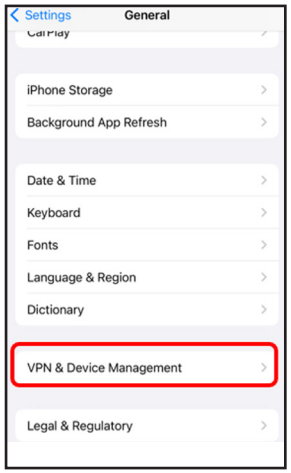
The following instructions explain and help you to configure your D-Link Quick VPN enabled router and devices to create a Virtual Private Network (VPN). This feature is provided for advanced users who wish to connect remotely and use their router's Internet connection to add a layer of security while 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.

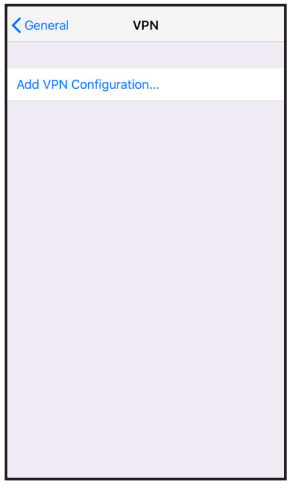
iOS Devices
VPN Setup Instructions

This section provides Quick VPN setup instructions for iOS devices. Refer to **Quick VPN** on page **90** for your router's setup instructions.

Go into **Settings** on your compatible iOS device.
Scroll to and tap **General**.
Scroll to and tap **VPN & Device Management**.



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.

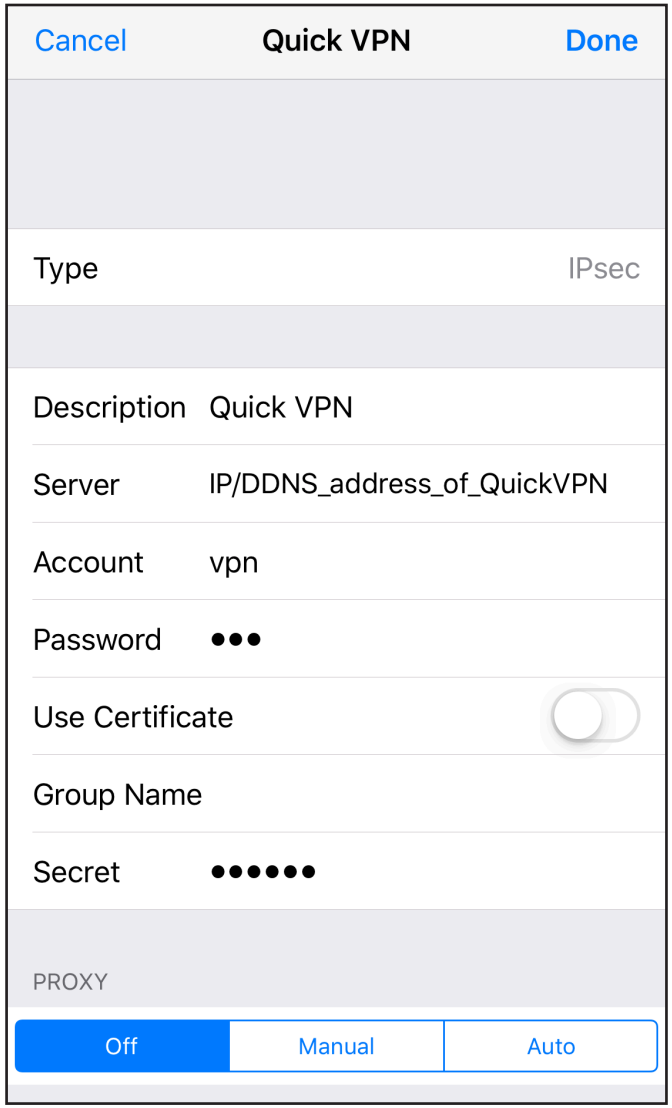
Account: Enter the Username used to authenticate login to the VPN server.

Password: Enter Password used to authenticate login to the VPN server.

Secret: Enter your Passkey (PSK).

Tap **Done** at the top right corner of the page to finish adding the configuration.

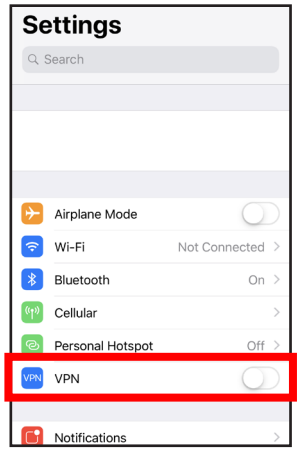
Your iOS device is now configured to connect to your Quick VPN server.



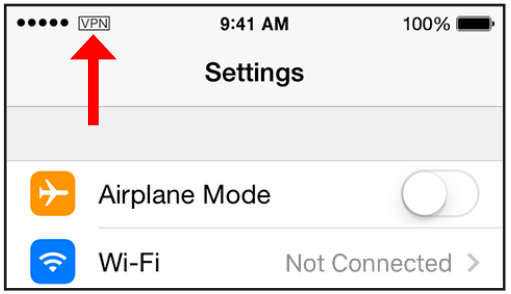
Connect or Disconnect

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





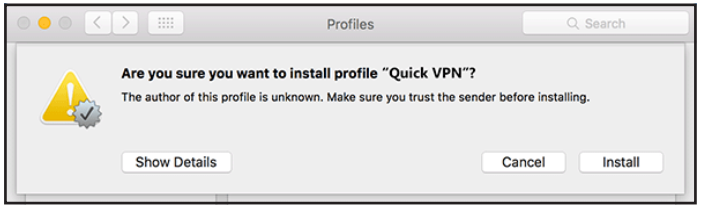
The VPN icon will appear in the notification area at the top of your screen indicating that your device is currently connected to the Quick VPN server.



Mac OS X
VPN Setup Instructions

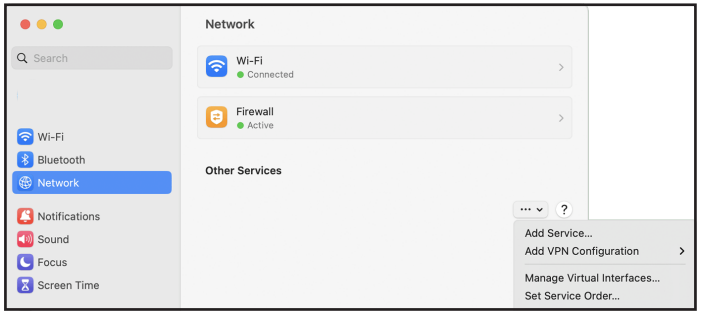
This section provides Quick VPN setup instructions for OS X using the **Export** Profile function.Refer to **Quick VPN** on page **90** for your router's setup instructions.

Open the exported profile. You can double-click it to set up your VPN connection.



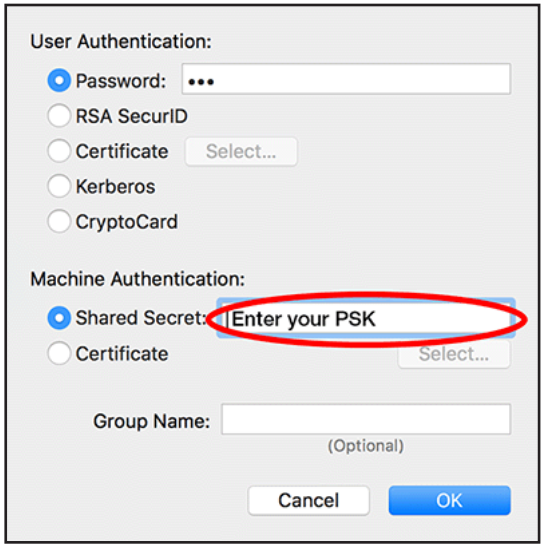
Enter your user account password when prompted. Close the **Profiles** dialogue.

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



If you would like to enter VPN settings manually, click the Action pop-up menu, choose Add VPN Configuration, then click the Configuration pop-up menu to set up the L2TP over IPSec VPN.

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



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

Connect or Disconnect

You can connect to or disconnect from your Quick VPN server using the VPN status menu in the menu bar (at the top of the screen).

1. Click the VPN status menu in the menu bar.
2. Choose the Quick VPN to connect to or disconnect from.

To display VPN status menu in the menu bar, select Apple menu > **System Settings**, and click Control Center in the sidebar.
Then select Menu Bar Only, click the pop-up menu next to VPN, and choose **Show the VPN status menu.**

Windows
VPN Setup Instructions

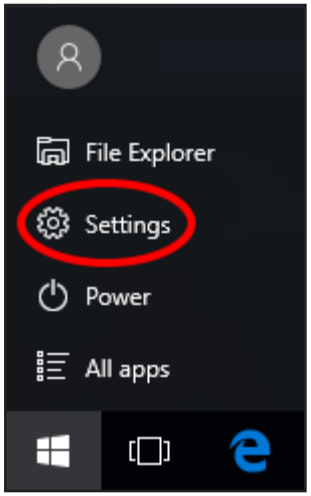
This section provides Quick VPN setup instructions for Windows 11/10. Refer to **Quick VPN** on page **90** for your router's setup instructions.

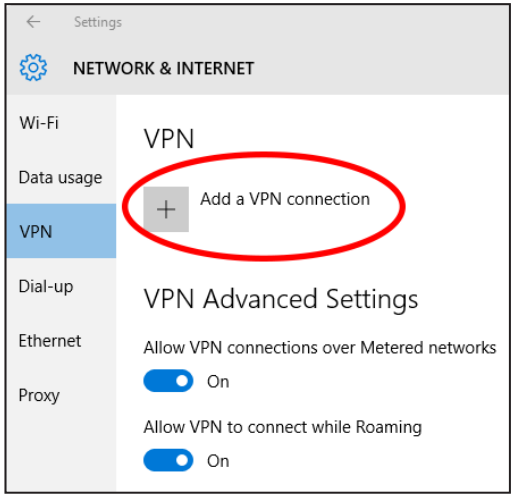
This section provides Quick VPN setup instructions for Windows 11/10.

Click **Start** > **Settings** > **Network & Internet** > **VPN > Add a VPN Connection** on **Windows 10.**

Or

Click **Start** > **Settings** > **Network & Internet** > **VPN > Add VPN** on **Windows 11**.

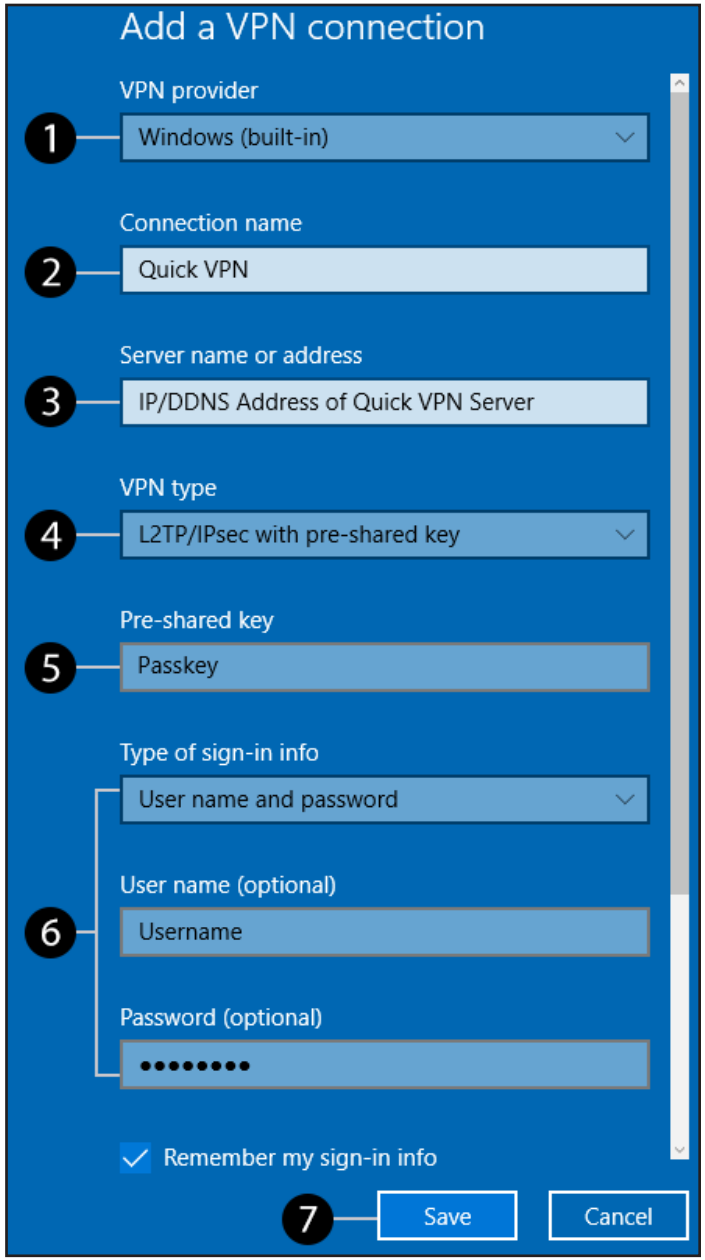




1. Select **Windows (built-in)** from the **VPN Provider** drop down menu.
2. Create a name for your VPN connection.
3. Enter your **IP/DDNS address** of your Quick VPN server.
4. Select **L2TP/IPSec with pre-shared key** from **VPN type**.
5. Enter the **Passkey.**
6. Select **User name and password**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

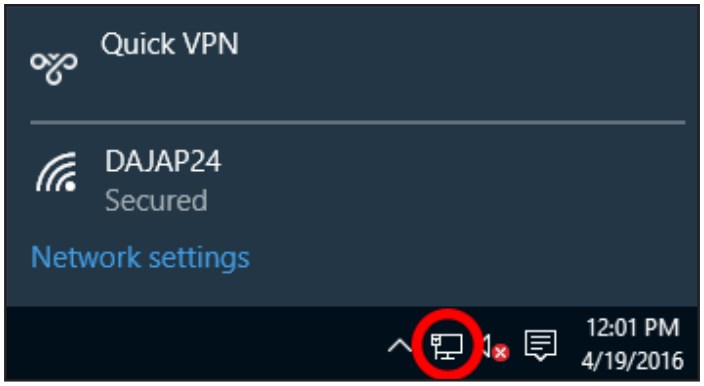
   If you would like windows to remember your sign-in information, enter your **User name, Password,** and select **Remember my sign-in info**
7. Choose **Save**.

Your Windows 11/10 system is now configured to connect to your Quick VPN server.



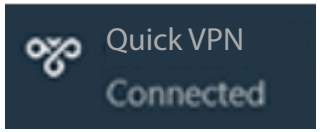
Connect or Disconnect

To connect to or disconnect from your Quick VPN server:



On **Windows 10**:

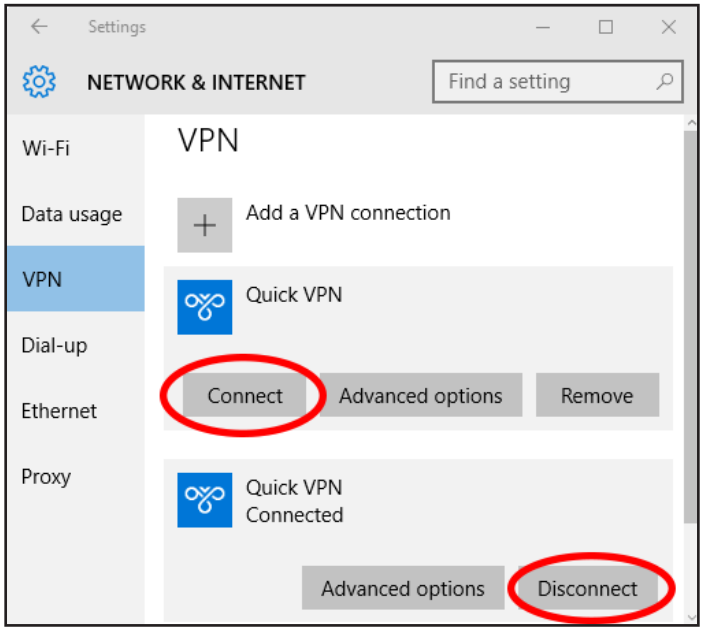
Click on the **Network (** or) icon in the notification area of the Windows taskbar and click on your Quick VPN connection. The **Network & Internet** Settings page will open. Click on the **Connect** or **Disconnect** button. Once the VPN is connected, its status (displayed underneath the connection name) will change to Connected.



On **Windows 11**:

Click on the **Network, Volume, Battery** icon. .
Select the Connect or disconnect of your Quick VPN connection.
A blue shield appears when you are connected to a VPN.

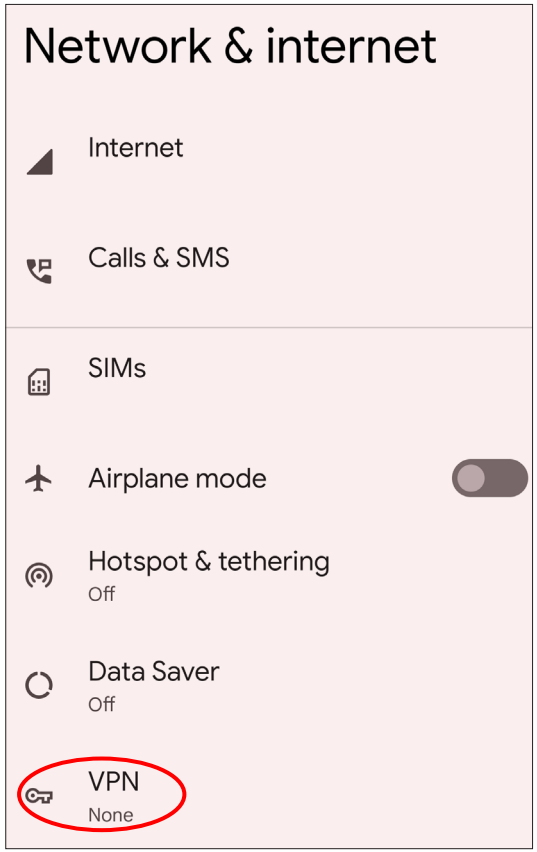


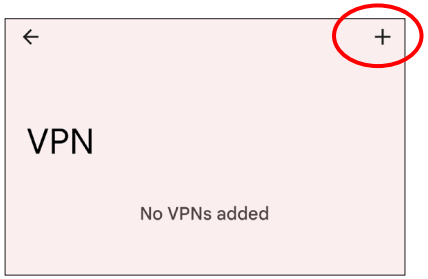


Android
VPN Setup Instructions

This section provides Quick VPN setup instructions for Android devices. Your device's screens may vary. Refer to **Quick VPN** on page **90** for your router's setup instructions.

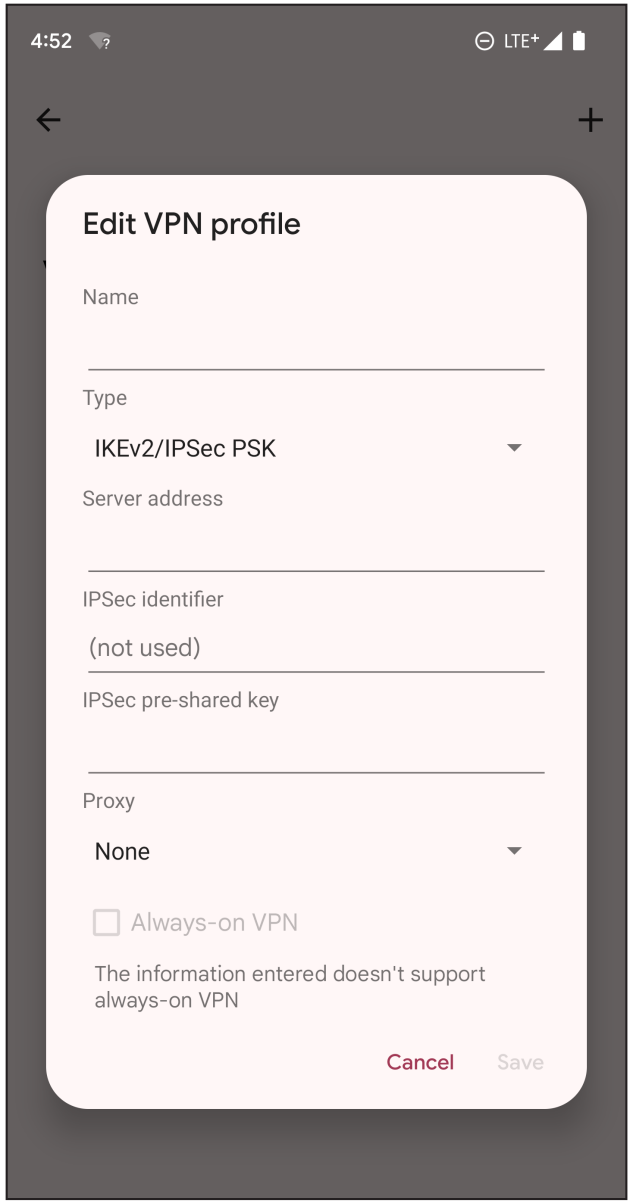
Go to **Network & Internet** > **VPN** > **+**





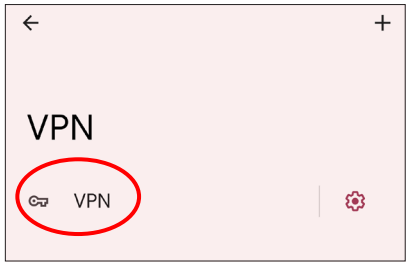
1. Enter a name for your VPN connection.
2. Select **L2TP/IPSec PSK** for **Type.**
3. Enter the **IP/DDNS address** of your Quick VPN server.
4. Enter your **Passkey** in **IPSec pre-shared key** field.
5. Choose **Save**.

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

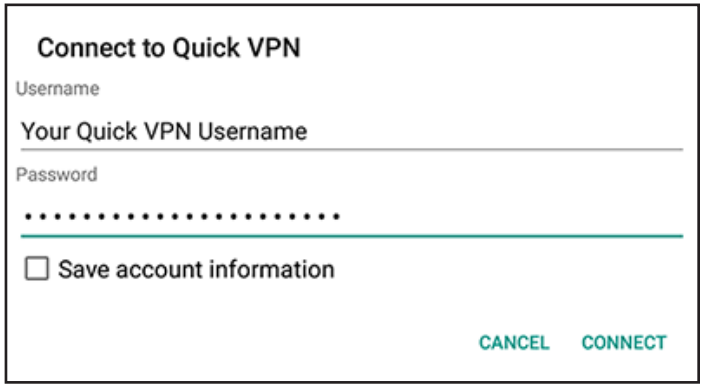


Connect or Disconnect

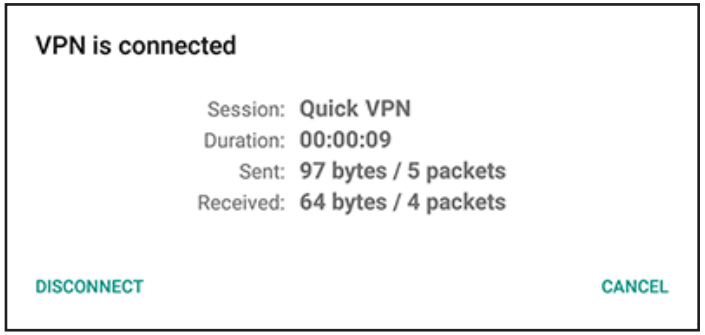
To connect to or disconnect from your Quick VPN server, go to **Network & Internet** > **VPN** and select the **Quick VPN** connection you created.



To connect, enter your **Username** and **Password** and select **CONNECT**.



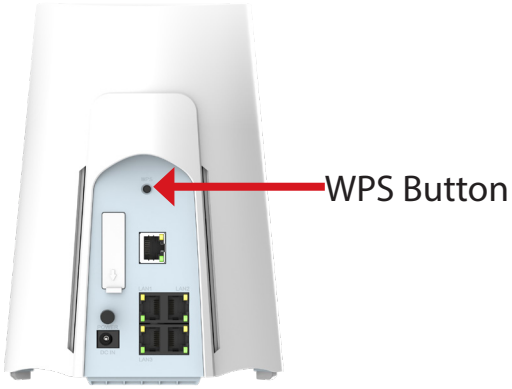
To disconnect, select **DISCONNECT**.



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 the user manual for the wireless device you want to connect to and follow the steps below:

Step 1 - Press the WPS button on the router for about 2 seconds. 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).

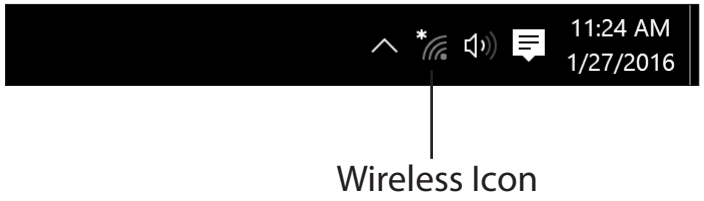
Step 3 - Allow up to 1 minute for your connection to be configured. Once the LEDs stop blinking, you will be connected securely.

Windows® 11/10

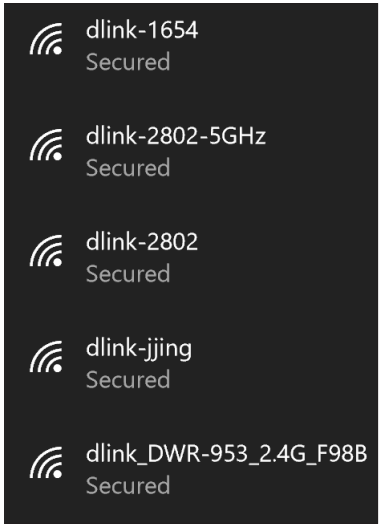
When connecting to the G572 wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise, refer to the product label on the bottom of the device for the default Wi-Fi network SSID and password or enter the Wi-Fi credentials set during the product configuration.

Note: To enjoy the benefits such as Multi-Link Operation (MLO) offered by Wi-Fi 7 and WPA3, please make sure that your operating system and wireless network adapter support Wi-Fi 7. For Windows, make sure your are running Windows 11 (version 24H2 or later).

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



Clicking on the Network icon , , or to enable Wi-Fi to display a list of wireless networks which are within the range of your computer. Select the desired network by clicking on the SSID.



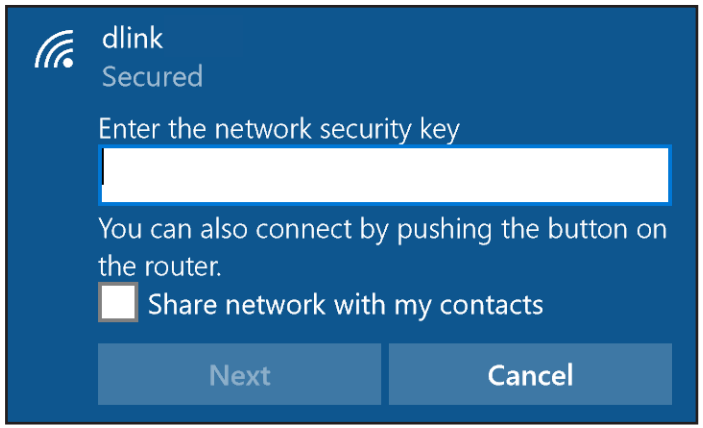
To connect to the SSID, click **Connect.**

To automatically connect with the router when your device next detects the SSID, click 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.

You can also use Wi-Fi Protected Setup (WPS) to connect to the router. Press the WPS button on your router and you will be automatically connected.



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 Edge®
  - 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 (refer to **Bottom View: Reset Button** on page **6)**. 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

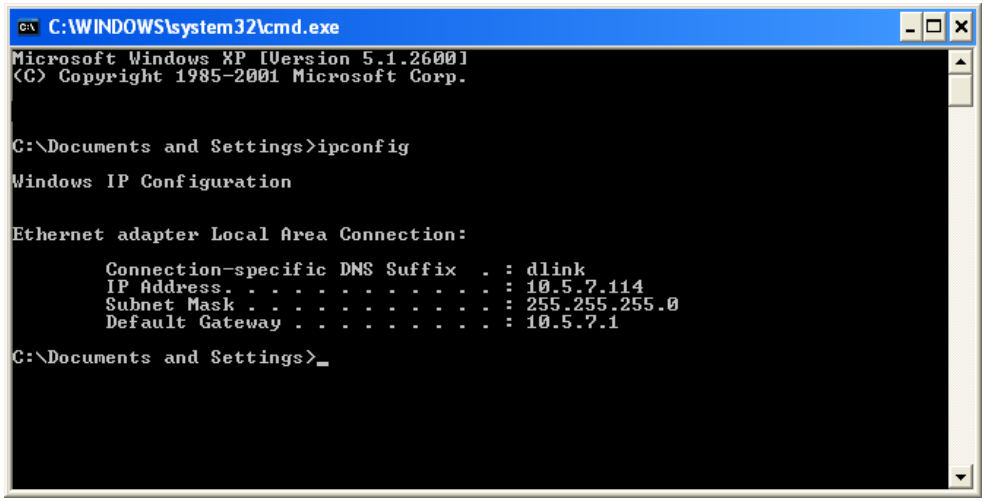
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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.



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® 11/10	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.**

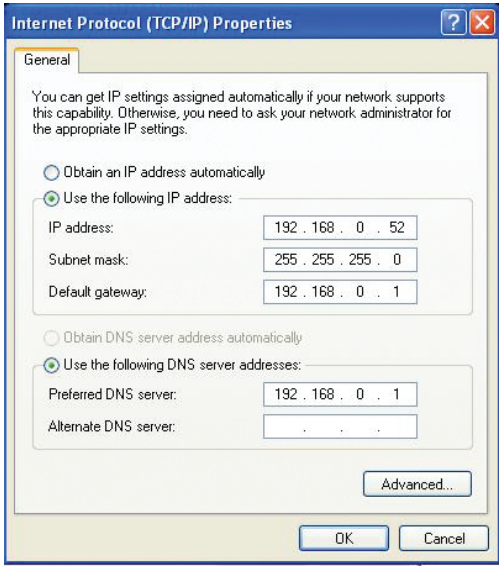
3. Under **IP assignment**, select **Edit**. For Windows 7/8/XP), select **Internet Protocol Version 4 (TCP/IPv4) Properties** or **Internet Protocol Version 6 Properties (TCP/IPv6)**. Then select **Use the Following IP Address**.

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

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 alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point. 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.

Technical Specifications

Device Interfaces
- 4 x Gigabit Ethernet LAN ports
- 1 x 2.5-Gigabit Ethernet WAN port
- 1 x WPS button
- 1 x Reset button
- 1 x Power button
- 1 x Nano SIM card slot (4FF)
- 1 x Power connector
- 2 x TS-9 connectors

Band Information[2]:
- 5G: n1/n3/n5/n7/n8/n20/n28/n38/n40/n41/n75/n76/n77/n78
- LTE Band: B1/B3/B5/B7/B8/B20/B28/B32/B38/B40/B41/B42/B43/B46
- WCDMA: B1/B5/B8

Standards[1,2,3]
- IEEE 802.11be
- IEEE 802.11ax
- IEEE 802.11ac
- IEEE 802.11n/g/b/a
- IEEE 802.3u/ab

Antenna Types
- 10 x Wi-Fi internal antennas
- 4 x LTE/5G NR internal antennas (2 of them can be substituted with external TS-9 antennas)

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

Data Signal Rates[1,2]
- 5G NR (SA mode) Downlink up to 7.01 Gbps/Uplink up to 2.5 Gbps
- 5G NR (NSA mode) Downlink up to 5.67 Gbps/Uplink up to 1.46 Gbps
- LTE Downlink up to 1.6 Gbps/Uplink up to 211 Mbps
- DC-HSPA Downlink up to 42.2 Mbps/Uplink up to 11.5 Mbps

Wi-Fi Data Rates[1,3]

7200 Mbps (5 GHz up to 5764 Mbps/ 2.4 GHz up to 1376 Mbps)

Power
- Input: 100-240V, 50/60 Hz
- Output: 12V, 4A

Temperature
- Operating: 0 to 40 °C (32 to 104 °F)
- Storage: -10 to 70 °C (14 to 158 °F)

Humidity
- Operating: 10% to 90% maximum, non-condensing
- Storage: 0% to 95% maximum, non-condensing

Certifications
- CE

Dimensions
- L x W x H: 137 x 146 x 205 mm (5.39 x 5.74 x 8.07 in)

Weight
- 660 g (23.28 oz)

1 Maximum wireless signal rate derived from IEEE Standards. Actual performances may vary due to settings, cabling, temperature, network configuration, interface, device compatibility, environmental and on-site conditions, and other similar factors. References to power capability, signal or processing speed, signal range or distance, data encryption, storage capacity, display properties, or other performance metrics are based on optimal conditions derived from industry standards and provided for informational purposes only. Specifications may be subject to change without prior notice.

2 Frequency Range varies depending on country's regulation.

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

Regulatory Statements

Federal Communication Commission Interference Statement

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

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

Non-modifications Statement:

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

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

Caution:

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

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

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

Note

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

IMPORTANT NOTICE:

FCC Radiation Exposure Statement

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

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

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

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

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

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

(1) this device may not cause interference, and

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

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

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

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

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.



	Frequency Band(s) **Frequenzband** **Bandes de fréquence** **Bandas de Frecuencia** **Frequenza/e** **Frequentie(s)**	**Max. Output Power (EIRP)** **Max. Output Power** **Puissance max en sortie (PIRE)** **Potencia máxima de Salida** **Potenza max. Output** **Max. Output Power**
Wi-Fi 2.4 GHz	2401 ~ 2483 MHz	100 mW
Wi-Fi 5 GHz	5150 ~ 5250 MHz	200 mW
	5250 ~ 5350 MHz	200 mW
	5470 ~ 5725 MHz	1W
WCDMA Band 1	1920 ~ 1980 MHz	25 dBm
WCDMA Band 5	824 ~ 849 MHz	25 dBm
WCDMA Band 8	880 ~ 915 MHz	25 dBm
LTE Band 1/ CA 1C	1920 ~ 1980 MHz	25 dBm
LTE Band 3/ CA 3C	1710 ~ 1785 MHz	25 dBm
LTE Band 5/ CA 5B	824 ~ 849 MHz	25 dBm
LTE Band 7/ CA 7C	2500 ~ 2570 MHz	25 dBm
LTE Band 8/ CA 8B	880 ~ 915 MHz	25 dBm
LTE Band 20	832 ~ 862 MHz	25 dBm
LTE Band 28	703 ~ 748 MHz	25 dBm
LTE Band 38 (PC2)	2570 ~ 2620 MHz	28 dBm
LTE Band 40/ CA 40C	2300 ~ 2400 MHz	25 dBm

LTE Band 41 (PC2)	2496 ~ 2690 MHz	28 dBm
LTE Band 42 (PC2)	3400 ~ 3600 MHz	28 dBm
LTE Band 43 (PC2)	3600 ~ 3800 MHz	28 dBm
LTE CA 38C	2570 ~ 2620 MHz	25 dBm
LTE CA 41C	2496 ~ 2690 MHz	25 dBm
LTE CA 42C	3400 ~ 3600 MHz	25 dBm
LTE CA 43C	3600 ~ 3800 MHz	25 dBm
5G NR Band n1	1920 ~ 1980 MHz	25 dBm
5G NR Band n3	1710 ~ 1785 MHz	25 dBm
5G NR Band n5	824 ~ 849 MHz	25 dBm
5G NR Band n7	2500 ~ 2570 MHz	25 dBm
5G NR Band n8	880 ~ 915 MHz	25 dBm
5G NR Band n20	832 ~ 862 MHz	25 dBm
5G NR Band n28	703 ~ 748 MHz	25 dBm
5G NR Band n38 (PC2)(MIMO)	2570 ~ 2620 MHz	28 dBm
5G NR Band n40	2300 ~ 2400 MHz	25 dBm
5G NR Band n40 (MIMO)	2300 ~ 2400 MHz	28 dBm
5G NR Band n41 (PC2)(MIMO)	2496 ~ 2690 MHz	28 dBm
5G NR Band n77 (PC2)(MIMO)	3300 ~ 4200 MHz	28 dBm
5G NR Band n78 (PC2)(MIMO)	3300 ~ 3800 MHz	28 dBm

European Community Declaration of Conformity:

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

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

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

Warning Statement:

The power outlet should be near the device and easily accessible.

Manufacturer :

Company Name : D-Link Corporation

Address: No.289 Sinhu 3rd Rd, Neihu District, Taipei City, 114

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

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

Usage Notes:

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

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

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

Gebrauchshinweise:

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

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

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

Notes d'utilisation:

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

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

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

Notas de uso:

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

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

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

Note per l'uso

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

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

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

Gebruiksaanwijzingen:

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

SAFETY INSTRUCTIONS

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

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

SICHERHEITSVORSCHRIFTEN

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

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

CONSIGNES DE SÉCURITÉ

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

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

INSTRUCCIONES DE SEGURIDAD

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

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

ISTRUZIONI PER LA SICUREZZA

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

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

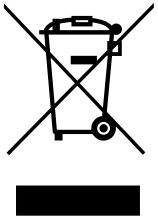
VEILIGHEIDSINFORMATIE

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

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

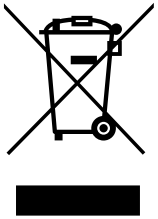
Disposing and Recycling Your Product

ENGLISH EN



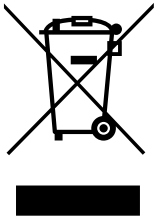
This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will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

DEUTSCH DE



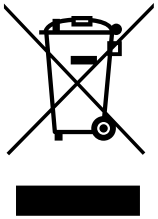
Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde 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.

FRANÇAIS FR



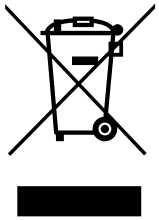
Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et règlementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront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

ESPAÑOL ES



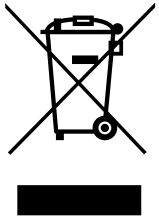
Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida 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.

ITALIANO IT



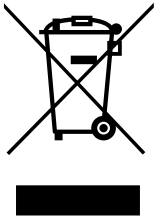
La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto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

NEDERLANDS NL



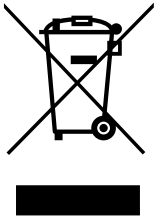
Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te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

POLSKI PL



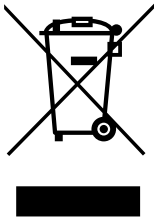
Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie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

ČESKY CZ



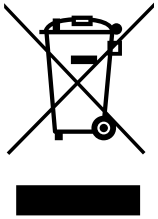
Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek dosslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací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

MAGYAR **HU**



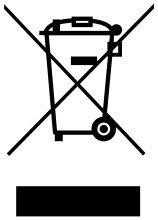
Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által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

NORSK **NO**



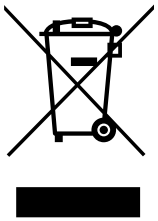
Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden.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

DANSK **DK**



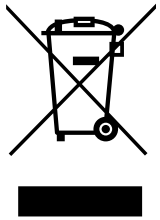
Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid.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

SUOMI **FI**



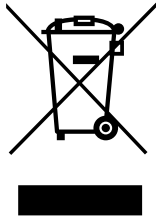
Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen.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

SVENSKA SE



Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

PORTUGUÊS PT



Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.