Version 2.00 | 08/27/2025

User Manual

BE3600 Wi-Fi 7 Smart Mesh Router

M36

Preface

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

Manual Revisions

Revision	Date	Description
1.00	July 07, 2022	Initial release
2.00	August 27, 2025	Release for firmware update

Trademarks

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

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

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

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

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

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

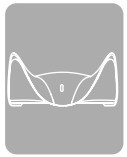
Power Usage

ErP Power Usage

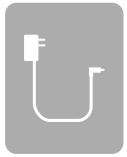
This device is an Energy Related Product (ErP) with High Network Availability (HiNA) that automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. If it is not needed during certain periods of time, it can be unplugged to save energy.

Table of Contents

Package Contents

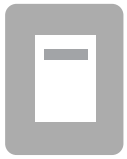


M36 BE3600 Wi-Fi 7 Smart Mesh Router



Power adapter (12V / 1.5A)

Ethernet Cable



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 from the one included with the device may cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based cable, DSL or fiber modem • IEEE 802.11be/ax/ac/n/g/b/a wireless clients • 10/100/1000/2500 Mbps Ethernet
Web Management Requirements	**Computer with the following:** • Windows, Macintosh, or Linux-based operating system • An installed Ethernet adapter or Wi-Fi interface **Browser requirements:** • Microsoft Edge • Mozilla Firefox 28 or higher • Apple Safari 6 or higher • Google Chrome 28 or higher
AQUILA PRO AI App Requirements	• iOS® or Android™ device (Please refer to the app's store page to check whether your device is compatible.)

Introduction

Engineered for seamless integration into a mesh system coupled with Wi-Fi 7 technology, the M36 ensures robust whole-home wireless coverage with exceptional performance and connectivity. Thanks to its innovative 360-degree spherical antenna design, strong and uninterrupted Wi-Fi facilitates video streaming, gaming, and more online collaboration for work and fun no matter where you are at your home.

Features

Speedier, More reliable, and Lower-latency Wi-Fi

The M36 model is an excellent choice for home creatives and streamers, offering a perfect balance of affordability, speed, and reliability with the benefits of Wi-Fi 7. This breakthrough in bandwidth utilization and latency reduction ensures seamless, high-performance wireless connectivity for demanding real-time applications, delivering a superb viewing experience.

IoT and MLO Zones to Separate Devices to Wireless Zones

Designed for large households and environments with numerous smart and mobile devices, the M36 provides fast, stable, and intelligent connectivity in every corner of your home. The router improves the connection stability of IoT devices by restricting them to wireless zones that are separate from major Wi-Fi zones and guest access. Similarly, the MLO zone allows devices supporting Multi-Link Operation (MLO) technology to use multiple bands for a single data stream simultaneously, significantly improving throughput and reliability.

Intelligent Traffic Optimizer

Quality of Service (QoS) lets you prioritize delay-sensitive traffic, ensuring it receives optimal bandwidth for smooth performance. The built-in AI engine also delivers weekly usage reports, giving you clear insights into your network's bandwidth consumption.

Intelligent AI Wi-Fi Optimizer

The innovative AI Wi-Fi Optimizer ensures that your wireless connectivity is optimized for smooth user experience. It also rates the overall wireless network condition and shows the number of times the engine has automatically optimized the network

according to the network's conditions and usage data.

Dynamic Power-saving Features for Carbon Reduction

The AI ECO Mode can be scheduled to activate dynamically according to data transmission and compute activity. When data transmission is low, power consumption can be reduced at the cost of wireless speed and coverage.

Always Up-to-Date with the Latest Features

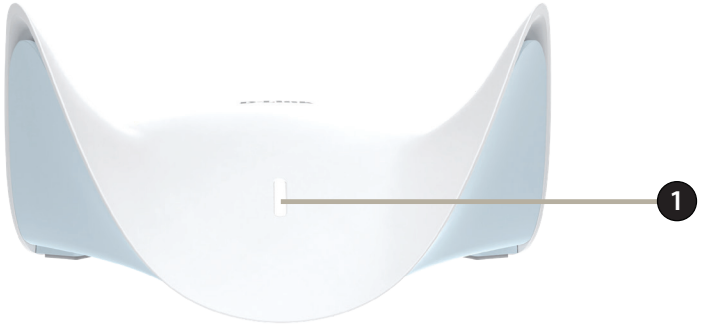
M36 will automatically check for daily updates to make sure that the device is always with the latest features and the most secure firmware. For extra peace of mind, the router will store a backup system image in its memory before proceeding with any update in the event that a failure occurs during a firmware update.

Fast Setup and Intuitive Management

Managing your Internet network could never be easier; just download D-Link's AQUILA PRO AI app for your mobile device and add your devices and assign them to specific rooms in your home. You could also use a web browser to access the setup wizard for basic setup options and more granular control. Supporting industry-standard Wi-Fi Protected Setup (WPS), M36 allows you to establish secure, encrypted connections to new devices with the press of a button.

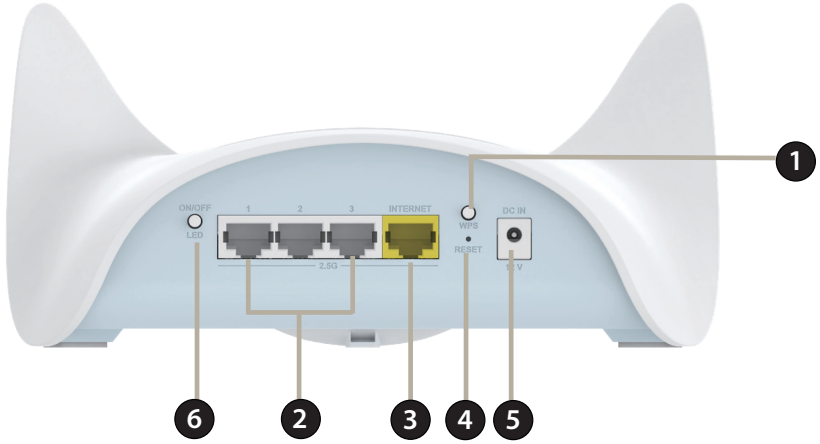
Hardware Overview

M36 LED Indicator



	Indicator	Color	Status	Router Mode	Extender Mode	Bridge Mode
1	Power/Status	White	Solid	Connected to the Internet with strong signal	Connected to the network with strong signal	Connected to the Internet with strong signal
			Breathing	Establishing a WPS connection	Uplink to main router is weak, or M36 is establishing a WPS connection	Establishing a WPS connection
		Orange	Breathing	Ready for connection or Internet connection is lost	Not connected to an uplink router	Not connected to an existing router
		White/ Orange	Interleaving	Firmware updating	Firmware updating	Firmware updating
		Red	Breathing	Resetting to factory default	Resetting to factory default	Resetting to factory default
			Solid	Powering on	Powering on	Powering on

M36 Rear Panel



1	**WPS Button**	Press this button to establish an instant connection to a wireless client using Wi-Fi Protected Setup (WPS).
2	**2.5 Gigabit LAN Ports (1- 3)**	Supports 10/100/1000/2500 Mbps network speeds. Connect Ethernet devices such as computers, switches, storage (NAS) devices, and game consoles.
3	**2.5 Gigabit WAN Port**	Supports 10/100/1000/2500 Mbps network speeds. Connect your broadband modem to this port using an Ethernet cable.
4	**Reset Button**	The reset button restores the router to its default settings. Insert a paperclip into the hole, wait for the LED to turn red, and then release.
5	**Power Connector**	Connect the included power adapter here to power on the device.
6	**LED ON/OFF Button**	Press and hold the LED ON/OFF Button for about 2 seconds to turn on or off the LED light on the front of the device. The LED can also be controlled via the Web Management (go to **Management > System Admin > Admin**).

Installation

This section will guide you through the installation of your M36.

Before You Begin

- Placement of a 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 a computer that was last connected directly to your Internet connection. Verify that it is connected to the Internet before connecting additional devices.
- If your Internet Service Provider (ISP) provided you with a modem/router combo, you will need to set it to "bridge" mode so that the router can work properly. Please contact your ISP or refer to the user manual of your modem/router device.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change your connection types (USB to Ethernet).
- If connecting to a DSL modem, be sure to have your DSL service information provided by your ISP 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 your time to label each cable first 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/gateway 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 radio frequency (RF) noise in your home or business. The key to maximizing wireless range is to follow the following guidelines:

General 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 router'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.
6. Place your device in an elevated position with at least 75 cm above the floor

Mesh Network Guidelines

The M36 supports mesh networking with other AQUILA PRO AI models. For a list of compatible models, please visit the M36 product page on the D-Link website. When planning your mesh network, consider factors such as home size, building materials, and wireless congestion in your environment.

1. Perform a site survey to check signal strength before positioning mesh points. The easiest way will be checking the number of bars displayed for the designated wireless network (To display the list of available wireless networks, select the Network icon  on the taskbar. Or you can go to **Network & Internet > Status > Network and Sharing Center**. Your connected networks are displayed. You can then select your Wi-Fi network name to have a better view of signal bars displayed for Signal Quality  .
2. Avoid placing mesh points behind thick walls or near microwaves, metal objects, or other potential sources of interference.
3. Use non-overlapping channels if multiple Wi-Fi networks are in use.
4. For multi-story homes, install at least one mesh point on each floor.
5. If your network environment includes many digital devices – such as wireless HDMI systems, IP cameras, or smart home gadgets – wireless performance may be affected. In such cases, consider placing mesh points closer together to maintain strong, stable connections.

Setup

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

- **AQUILA PRO AI app** - Use your compatible iOS or Android device to install and configure your router. Refer to **AQUILA PRO AI App Setup** on **page 11.**
- **Hardware Setup** - This section explains how to set up your M36. Refer to **Hardware Setup** on **page 14.**
- **Setup Wizard** - The wizard will launch when you log in to the router using your PC for the first time. Refer to **Setup Wizard** on **page 16**.
- **Manual Setup** - Log in to the router for manual configuration of your router Refer to **Configuration** on **page 24.**

AQUILA PRO AI App Setup

The AQUILA PRO AI app allows you to install and configure your device from your compatible Android or iOS devices.

Note: *The screenshots may be different depending on your mobile device's OS version or platform.*

Step 1

Search and install the free **AQUILA PRO AI 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

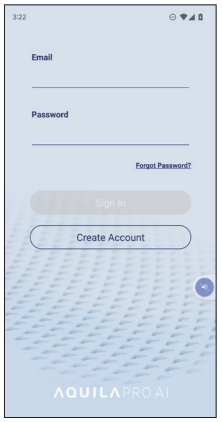
AQUILA PRO AI

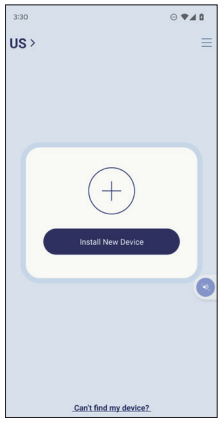
Step 2

Launch the AQUILA PRO AI 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** to be redirected to the login page. It allows you to use cloud services to control and manage your device including third-party voice control apps.



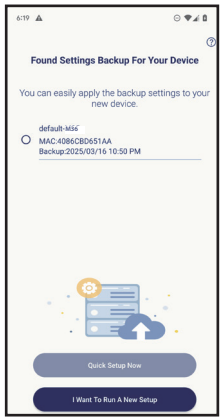


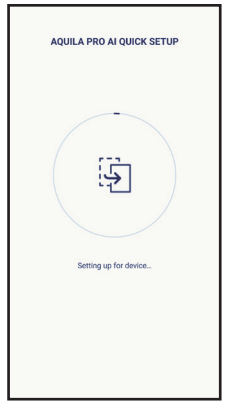
Step 4

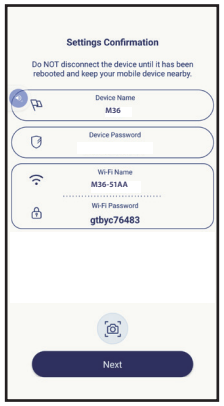
Tap **Install New Device** or **+** icon in the middle. Scan the Setup code on the device label located on the bottom of the router. Follow the on-screen instructions to complete the setup.

Step 5

During the setup process, you will be required to set the basic configurations such as Wi-Fi name and password as well as the device name. The App's Quick Setup allows you to apply previous settings to expedite the setup process. Tap Quick Setup Now to eliminate steps for basic device configuration. You can later manage the backups by going to the Device Backups menu of your Account (Refer to **Device Information and Settings** on **page 109**).

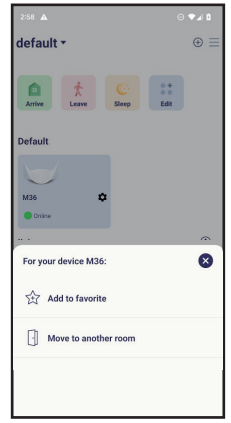




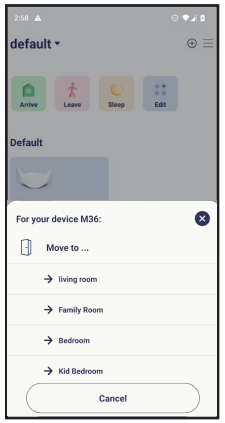


Step 6

You will see the registered device in the Home screen of the App. You can add the device to your **Favorites** for quick access with a long-press on the device icon. When you tap the **Favorites** tab at the bottom of the Home screen, you can see all your favorites.

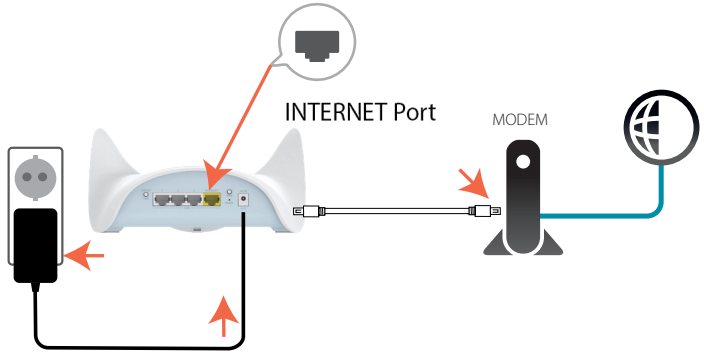


If you have placed the device in the designated room of your home during device setup, you will see it listed under the room. You can relocate the device or add it to a new room by simply long-pressing the device icon and choose **Move to another room**.

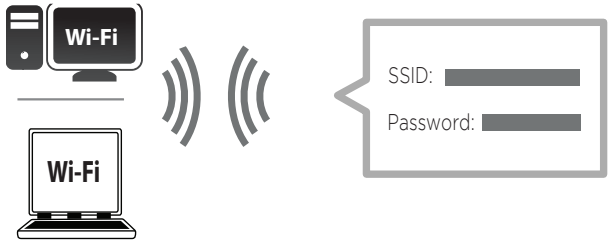


Hardware Setup

Step 1
Position the M36 close to your Internet-connected modem. Turn off and unplug the power to your cable or DSL/fiber broadband modem. This is required. In some cases, you may need to turn it off for up to five minutes. Connect an Ethernet cable to the modem and to the Internet port of M36. Next, connect the power adapter and plug M36 into a power outlet.

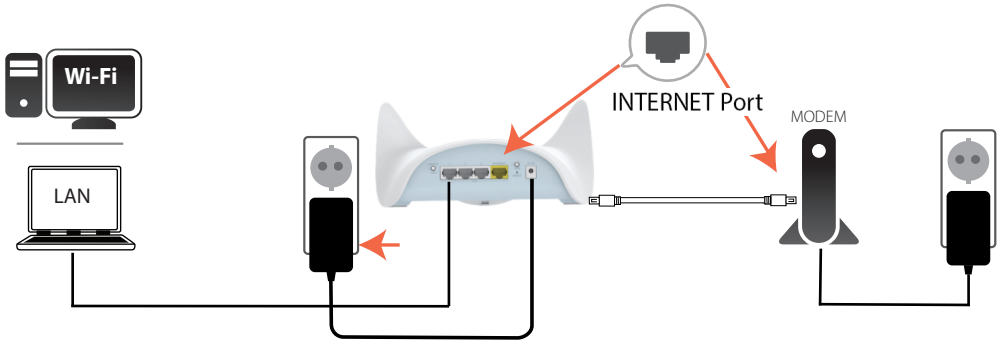


Step 2
Wait for the M36 to boot up. When the router's LED light starts breathing orange, wirelessly connect your computer to the Wi-Fi name (SSID) printed on the device label.



Step 3
Type **https://xxxx.devicesetup.net/** into a web browser and follow the on-screen instructions to complete the setup.
(xxxx represents the last 4 characters of the MAC address)

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

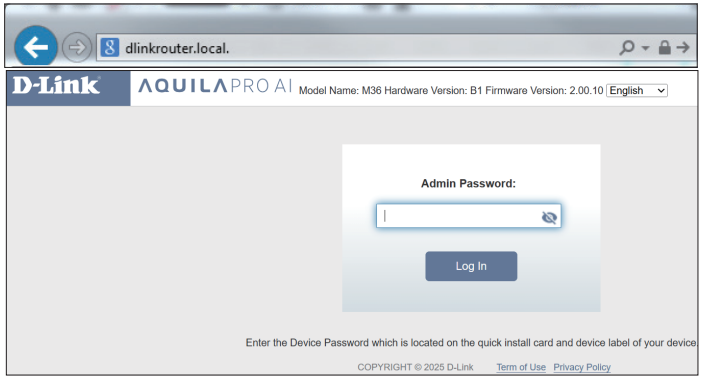


If you are connecting to a broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and connecting to a website. If the website does not load, proceed to **Setup Wizard** on **page 16**.

Setup Wizard

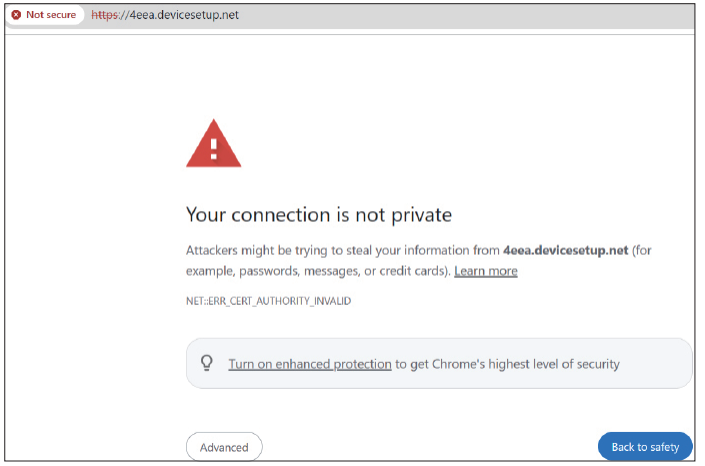
The setup wizard is designed to guide you through a step-by-step process to configure your new M36 for Internet connection.

If this is your first time configuring the router, open your web browser and enter **https://xxxx.devicesetup.net/** into the browser (xxxx represents the last 4 characters of the MAC address). Enter the **Admin Password** and click **Log In** to start the configuration process. (Click the eye icon to show or hide the entered password) The web address and default admin password are printed on the device label on the bottom of the device.
The default HTTPS version of the Web management page may display a security warning message alerting you of possible data breach. Refer to the below steps for additional instructions when you see such warning.



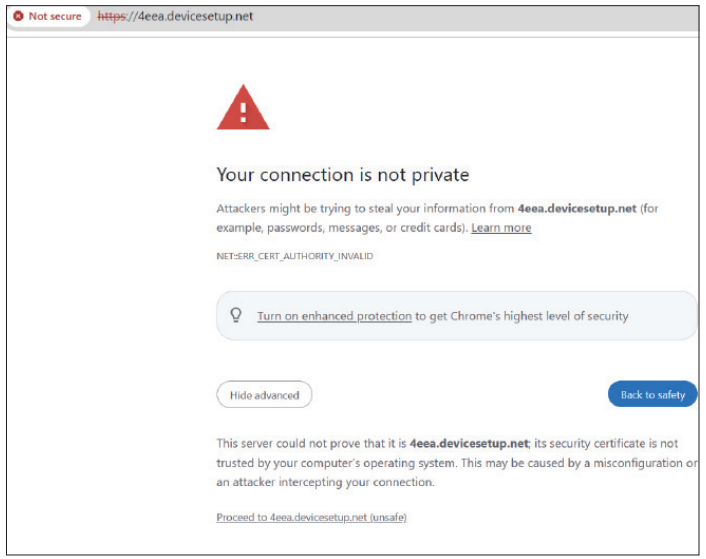
When your browser displays a security warning stating, "Your connection isn't private." You will also see Not Secure in the address bar, along with HTTPS crossed out with red lines. This is because the device's default management URL is not an actual Internet website with valid certificates. You can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

1. Click the "Advanced" button.

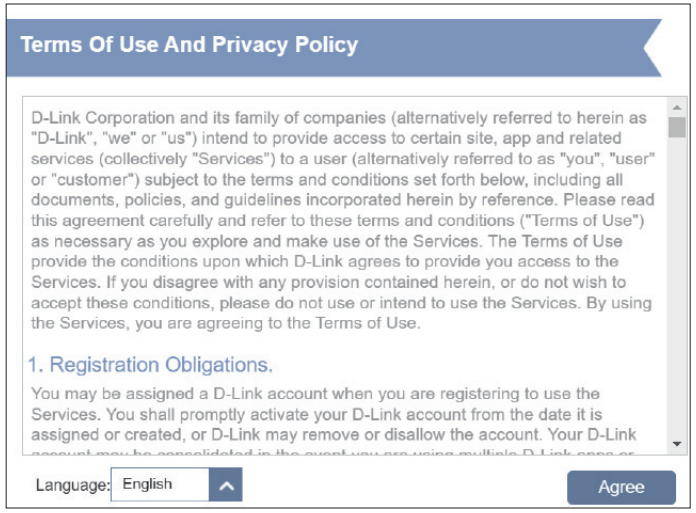


2. Click "Proceed to the default *management URL*".

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

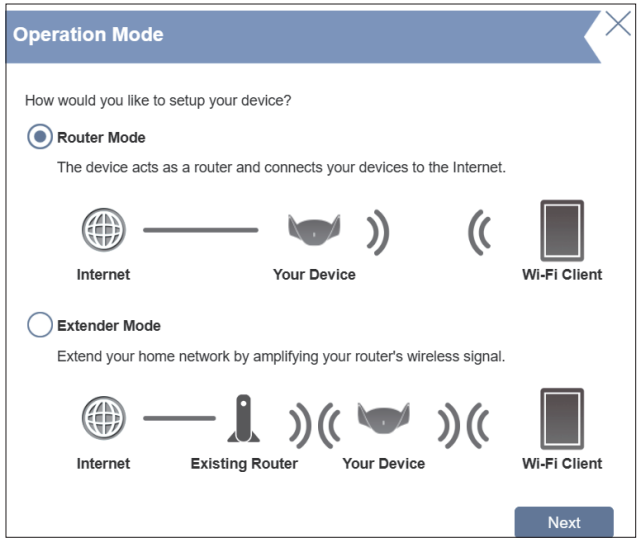


Agree to the **Terms of Use and Privacy Policy** before proceeding.



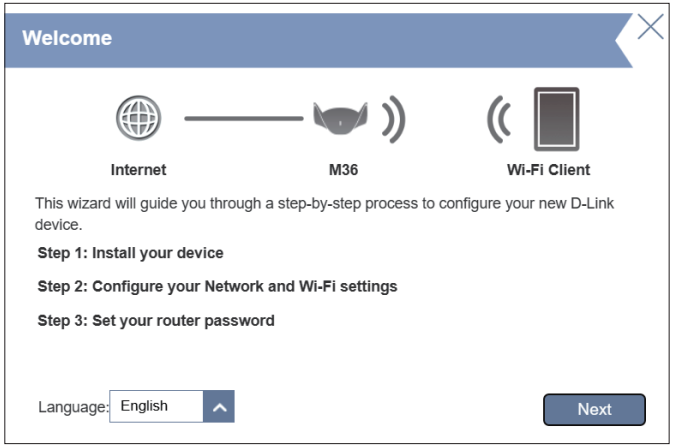
You will be prompted with the **Operation Mode** page to set up your router's mode. Select **Router Mode** to configure M36 as a standalone router. Select **Extender Mode** to configure M36 as an extender.

Click **Next** to continue



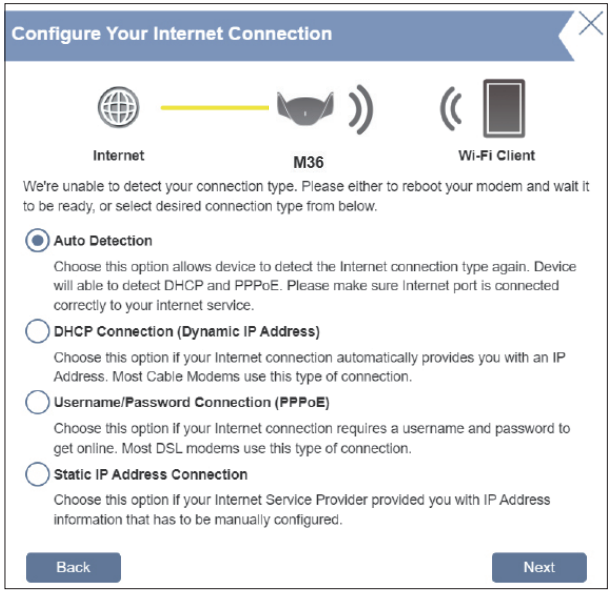
Connect the router and the modem with an Ethernet cable.

Click **I understand and want to continue**



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

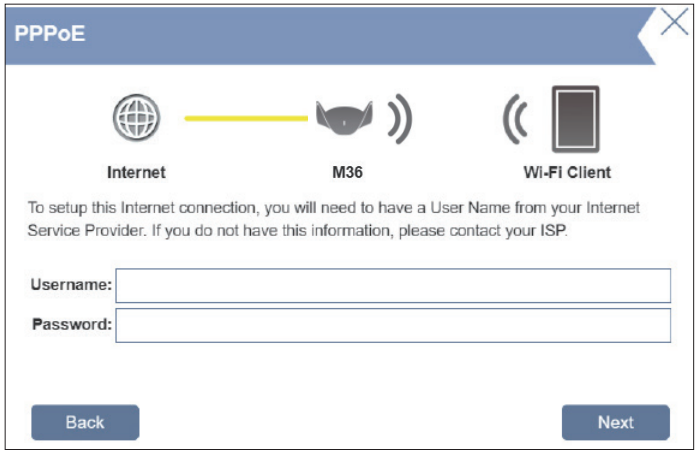
Click **Next** to continue.



If the router detected a connection or you manually selected **PPPoE**, enter your PPPoE username and password. If you do not have this information, please contact your ISP.

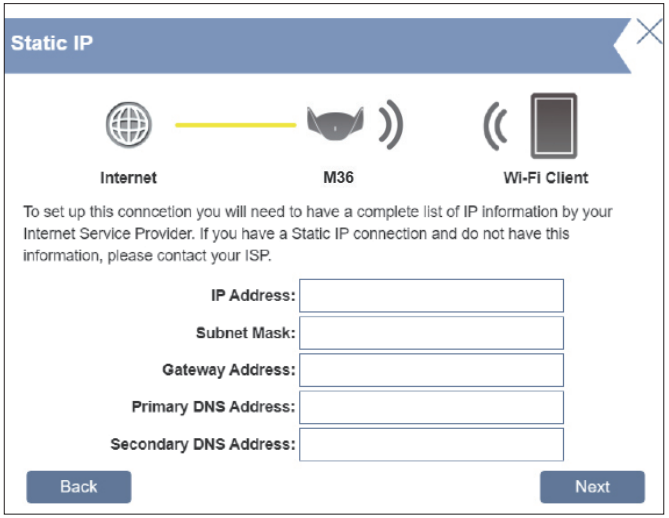
Click **Next** to continue.

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



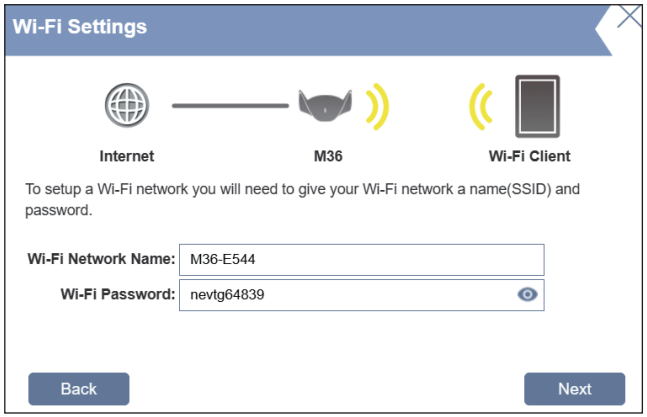
If the router detected a connection or you manually selected **Static IP**, enter the IP and DNS settings supplied by your ISP. If you do not have this information, please contact your ISP.

Click **Next** to continue.



If the router detected a connection or you manually selected **DHCP connection**, enter a **Wi-Fi Network Name** and **Wi-Fi Password** to set up your Wi-Fi network. The **Wi-Fi Password** must be 10 to 63 characters containing both letters and numbers and having no identical characters next to each other. Your wireless clients will need to have this passphrase to be able to connect to your wireless network.

Click **Next** to continue.



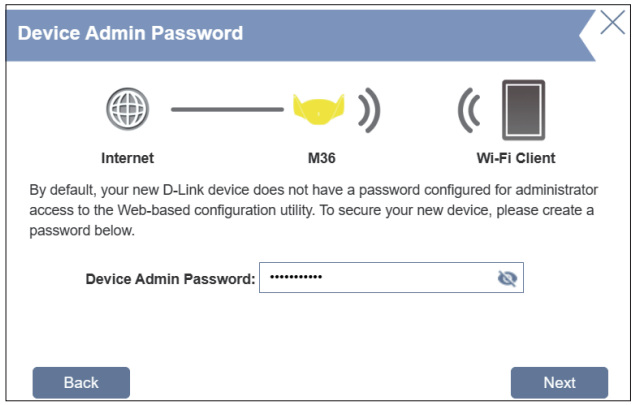
Notes:

1. *The router's Smart Connect feature presents a single wireless network. When connecting clients to an extension 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 60.**

To better protect the router's configuration access, please enter a password. You will be prompted for this password every time you want to use the router's web management interface.

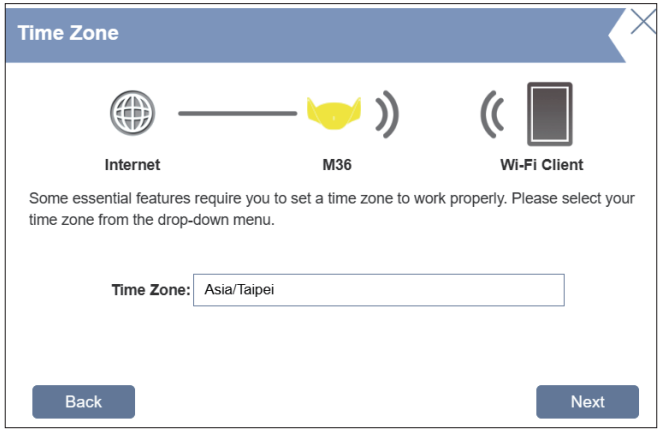
Note: It is strongly recommended that you change the default device password. The password must contain 10 to 15 characters and include both numbers and letters that are not identical next to each other.

Click **Next** to continue.



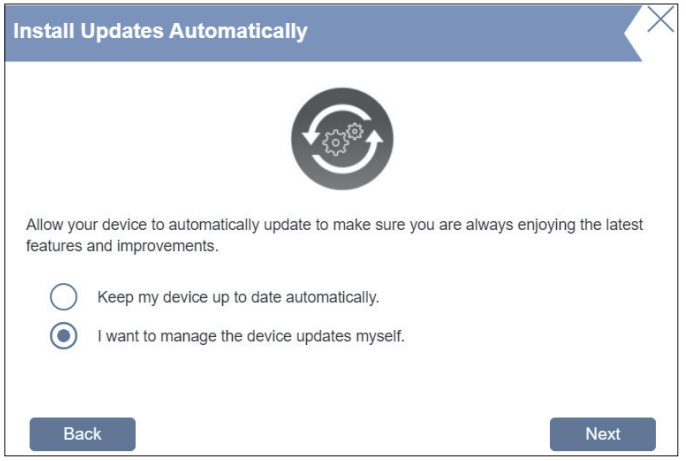
Select your time zone from the drop-down menu.

Click **Next** to continue.



Keeping your router's firmware up-to-date can ensure you're always getting the latest security update 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. You can click the eye icon to show or hide the configured password.

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

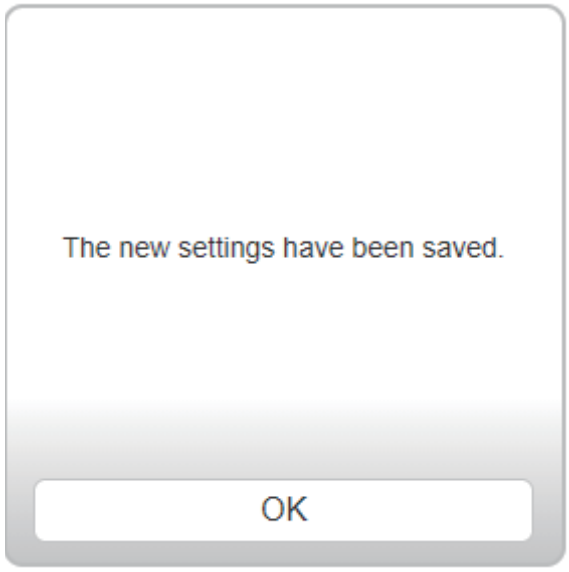
Please wait while the device settings are being saved.

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.

You can log in to the web management by entering your saved Admin Password.

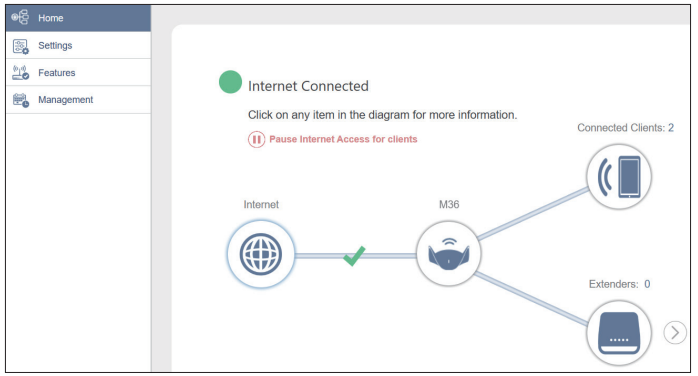


Configuration
Accessing the Web Management Interface

1. Type **https://xxxx.devicesetup.net/** in the address bar. (xxxx represents the last 4 characters of the MAC address)
2. Enter the admin password.
   - If this is your first time logging in, please enter the password printed on the device label located on the bottom of the device.
   - If you have previously completed the Setup Wizard, enter the password you created during initial setup.
   - If you can't remember your password for login, press the Reset button to restore the router to its default settings.

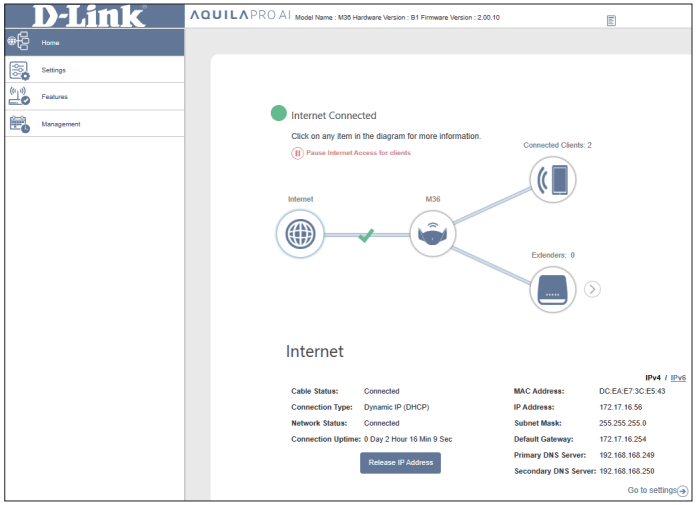
The router's home page will display its current connection status.
The left panel has quick access to **Settings**, **Features** and **Management**.

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



Home

The **Home** page displays the current status of your network in the form of an interactive diagram. You can click on each icon to display information about each node of the network in the middle of the screen. The menu bar at the top-left corner of the page will allow you to quickly navigate to other pages. Refer to the following pages for a description of each section.

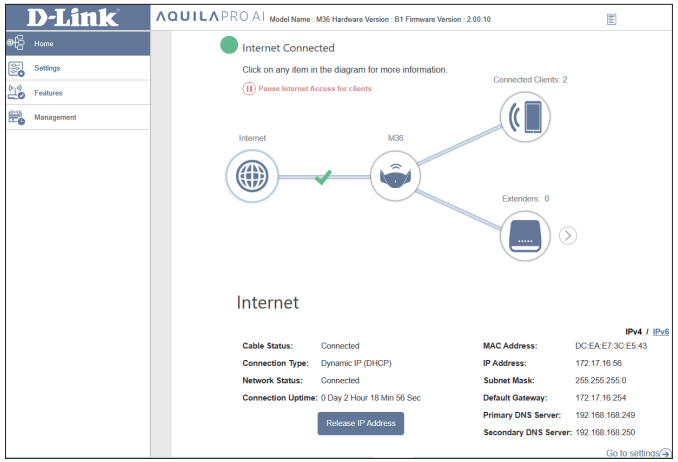


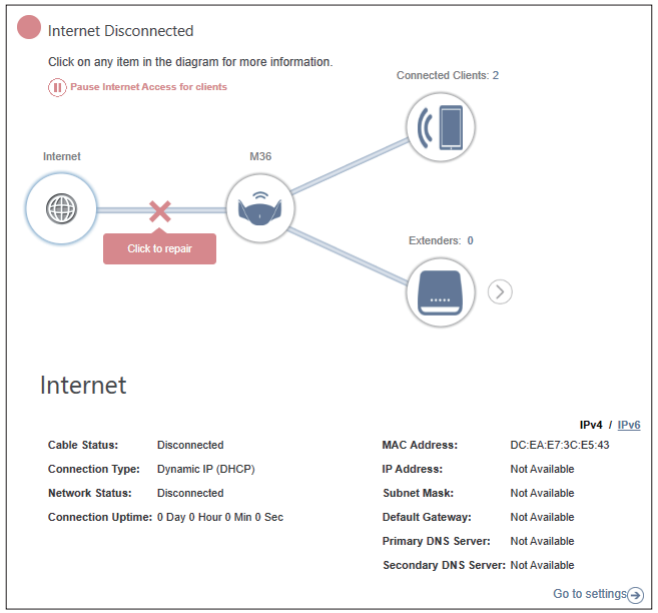
Internet

Click on the **Internet** icon to bring up more details about your Internet connection. Click **IPv4** or **IPv6** to see details of the IPv4 and IPv6 connection respectively.

The **Home** page displays whether or not the router is currently connected to the Internet. If it is disconnected, click **Click to repair** to bring up the setup wizard, refer to **Setup Wizard** on **page 16** for more information.

Click **Release IP Address** to release the current IP address and disconnect from the Internet. If you wish to reconnect to the Internet, click **Renew IP Address**.

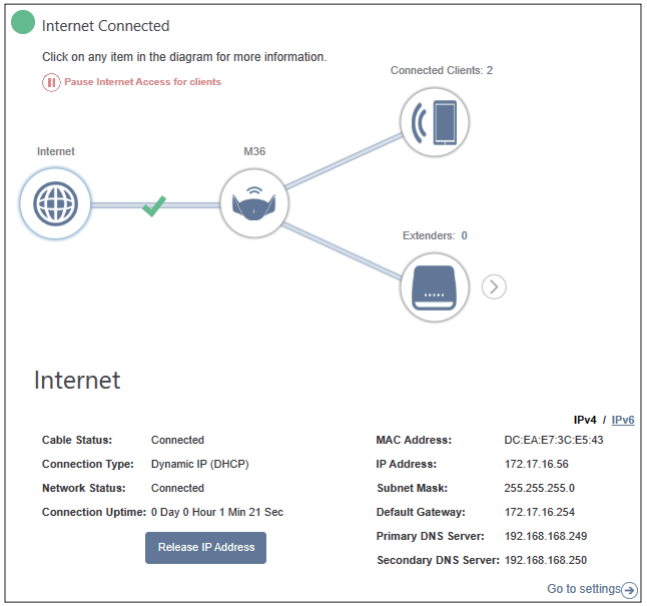




Internet

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.

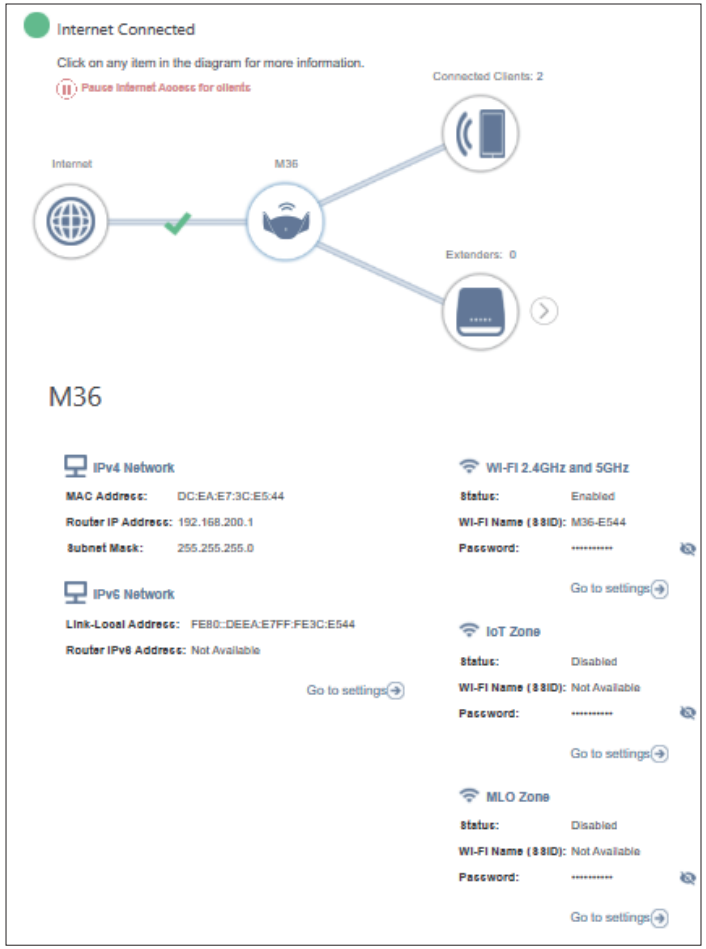


M36

Click on the **M36** icon to view details about the wireless and local network settings. This includes IPv4 and IPv6 local networks, and Wi-Fi information.

To reconfigure network settings, either click **Go to settings** at the bottom of the page, or click **Settings** on the left panel and select **Network**. Refer to **Network** on **page 71** for more information.

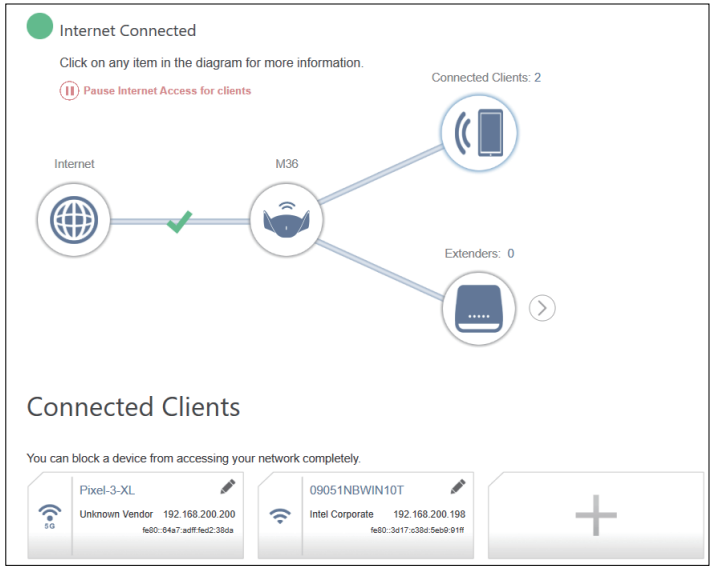
To reconfigure wireless settings, either click **Go to settings**, on the lower right, or click **Settings** on the left pane and select **Wireless**. Refer to **Wireless** on **page 60** for more information.



Connected Clients

Click on the **Connected Clients** icon to view details about the clients currently connected to the router.

To edit each client's settings, click the pencil icon on the client you want to edit.



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.

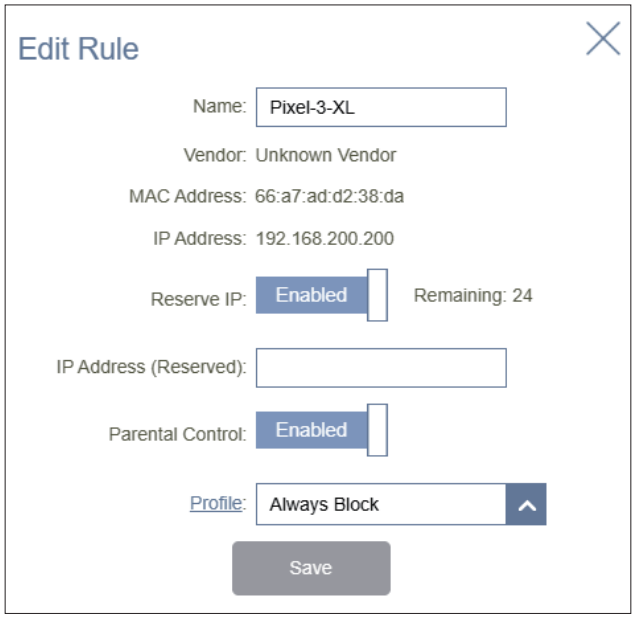
Reserve IP Enable to reserve an IP address for this client.

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.

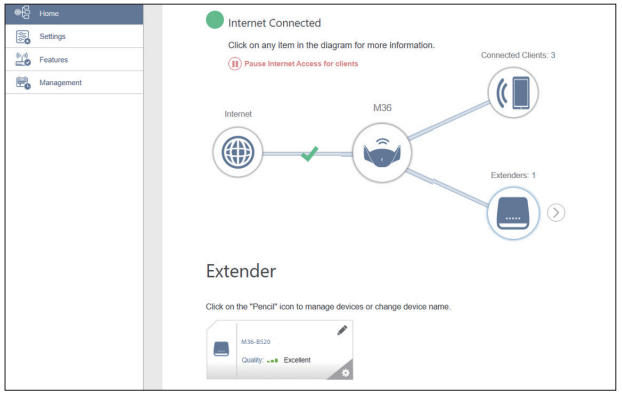
Profile If **Parental Control** is enabled, use the drop-down menu to select a predefined profile. Refer **Parental Control on page 75** for more information.

Click **Save** when you are done.



Extenders

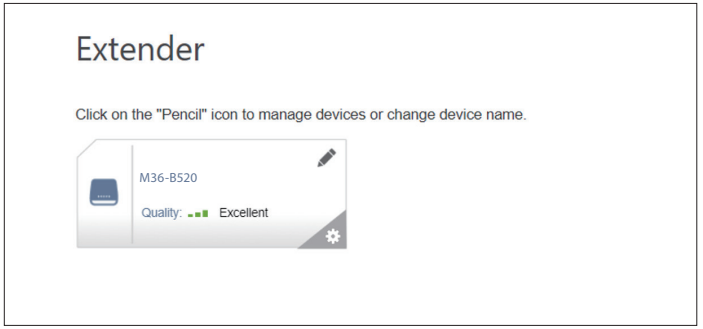
Click on the **Extenders** icon to view details about all additional devices in your mesh Wi-Fi network.



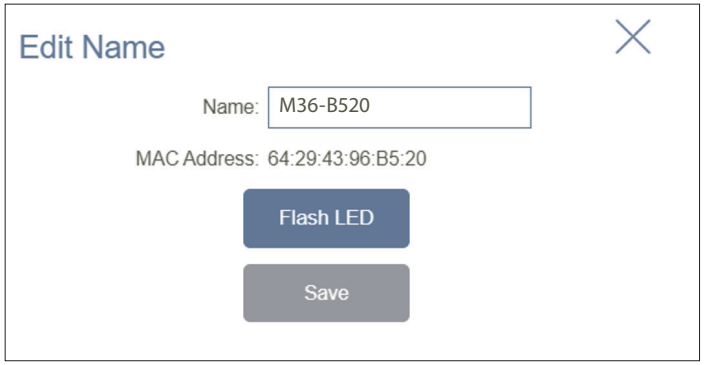
To edit the extender name, click on the pencil icon in the top-right of the box of the Extender that you want to rename.

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**.

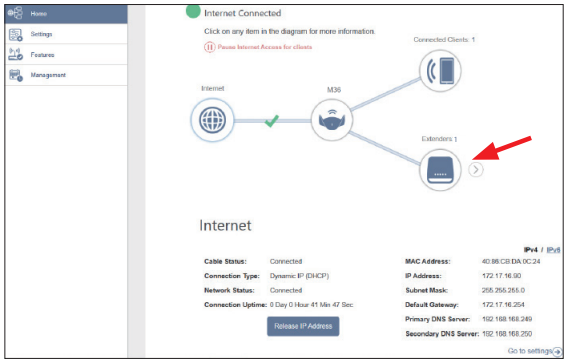


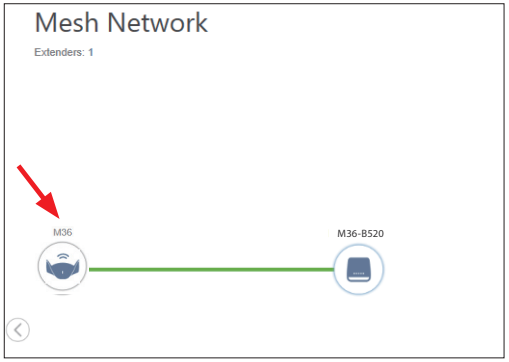
Edit Name	
Name	Enter a name for the mesh point.
MAC Address	Displays the MAC address of the mesh point.
	Click **Flash LED** to visually identify the extender.
	Click **Save** when you are done.



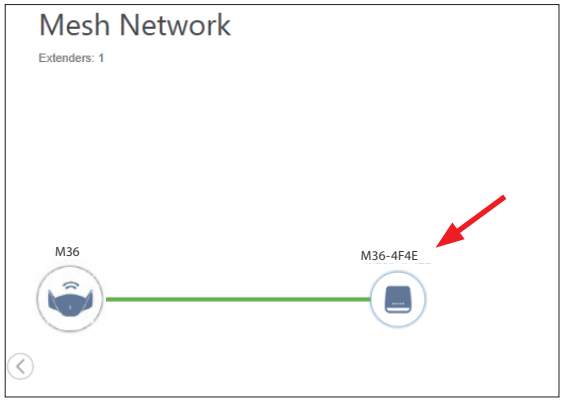
Mesh Network

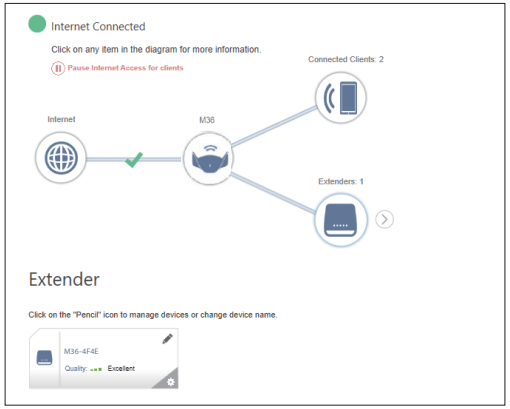
To access the **Mesh Network** page, click the arrow next to the extender icon. Under the **Mesh Network** page, you can view details of the main router and every extender within the network. Click **M36** to view the status of the main router. Click the pencil icon on the connected client(s) to edit 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.

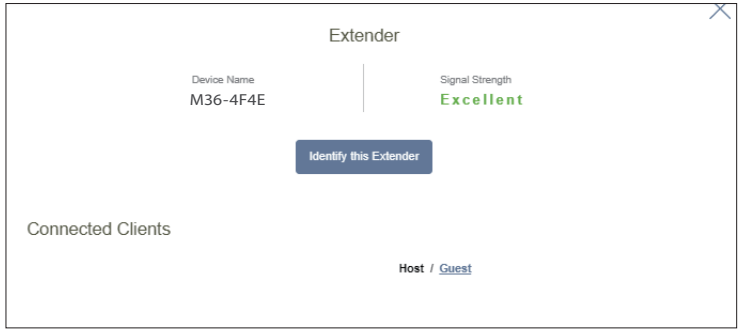




Click the **Extender** icon to view details of the extender and list of connected clients. Click the pencil icon on the connected client(s) to edit configuration. Configuration details are explained on the next page. Click **Identify this Extender** to visually confirm the location of your extender. 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.

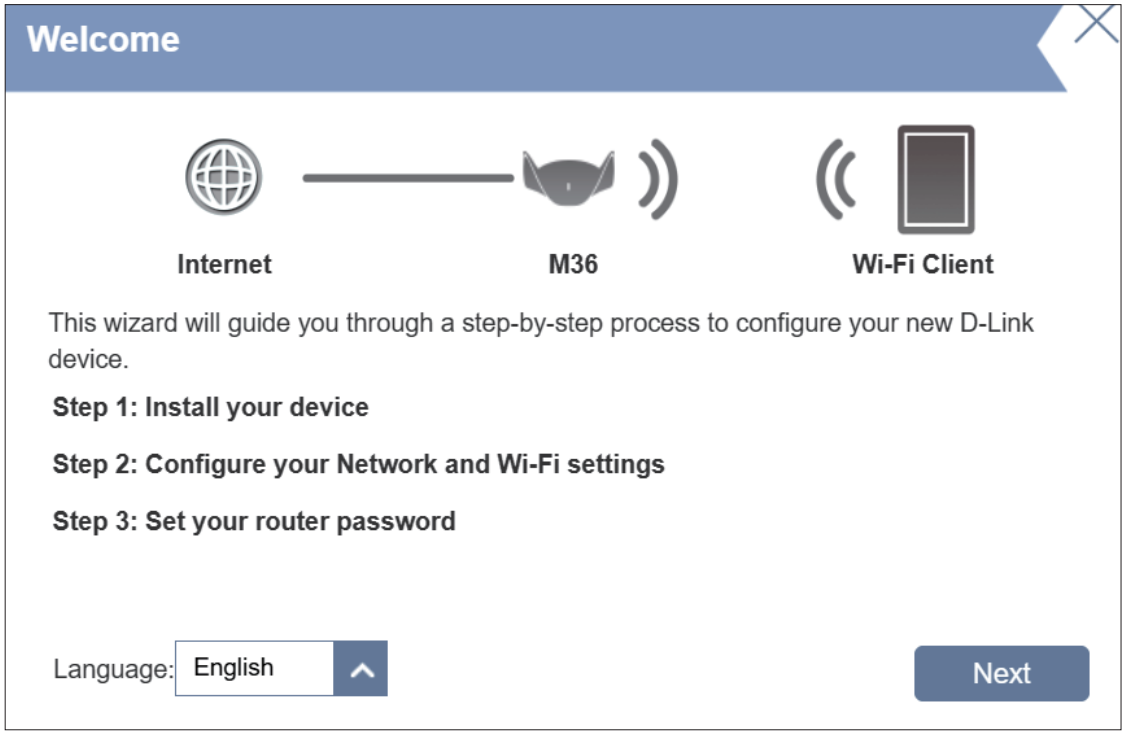
Profile If **Parental Control** is enabled, use the drop-down menu to select a predefined profile. Refer **Parental Control on page 75** for more information.

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 configuring the router for the first time. Refer to **Setup Wizard** on **page 16** for details.

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

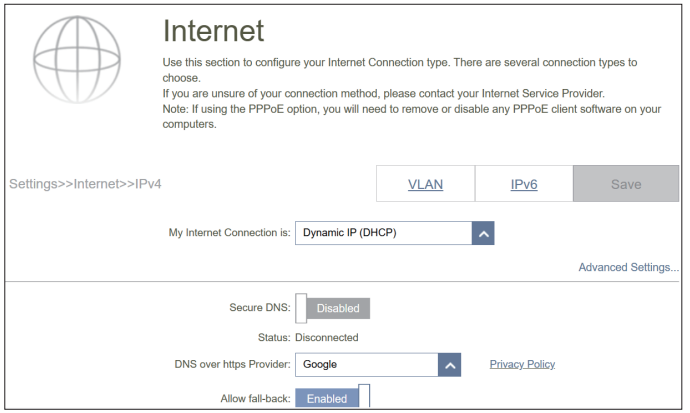


Internet
IPv4

In the **Settings** menu bar on the top-left side of the page, click **Internet** to see the Internet configuration options.

To configure IPv6 Internet and view the network's connection details, click on the **IPv6** tab. Refer to **IPv6** on **page 45**.
To configure VLAN connection details, click on the VLAN link. Refer to **Internet - VLAN on page 58**.

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. Click **Advanced Settings...** to expand the list and see all of the options.

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

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

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

For **Static IP**, refer to **IPv4 - Static IP** on **page 35**.

For **Dynamic IP (DHCP)**, refer to **IPv4 - Dynamic IP (DHCP)** on **page 36**.

For **PPPoE**, refer to **IPv4 - PPPoE** on **page 37**.

For **PPTP**, refer to **IPv4 - PPTP** on **page 39**.

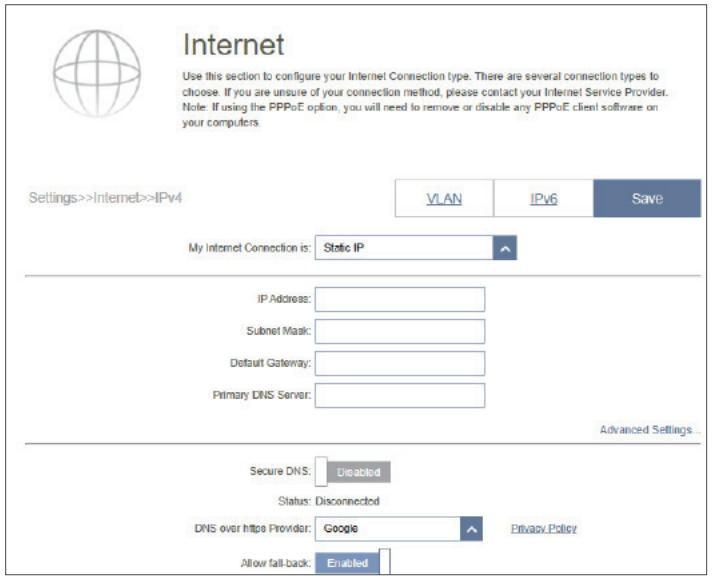
For **L2TP**, refer to **IPv4 - L2TP** on **page 41**.

For **IPv4 as a Service**, refer to **IPv4 as a Service** on **page 43**.

To configure an **IPv6** connection, click the **IPv6** link. Refer to **page 45.**

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 assigned by your ISP.

Advanced Settings...

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

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

MAC Address Clone Use the drop-down menu to replace the Internet port's MAC address with the MAC address of a connected client.

IPv4 - Dynamic IP (DHCP)

Select **Dynamic IP (DHCP)** to automatically obtain IP address information from your ISP. Select this option if your ISP does not specify an IP address for 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 automatically obtained from your ISP.

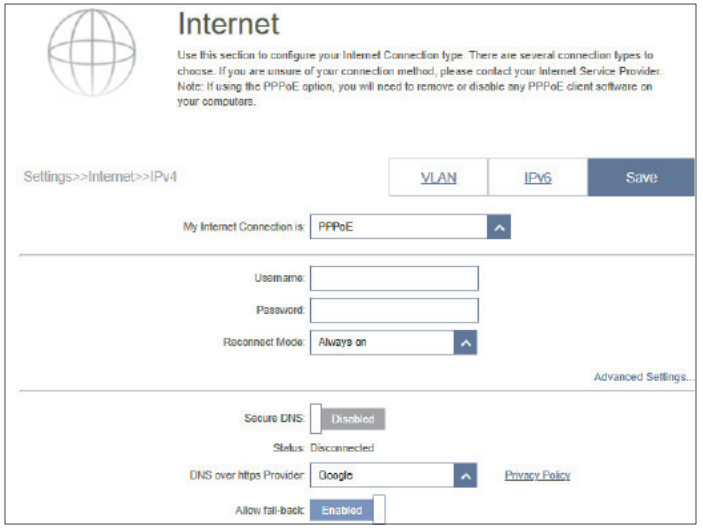
Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

MTU Maximum Transmission Unit - The default is 1500. You may need to change the MTU for optimal performance with your ISP.

MAC Address Clone Use the drop-down menu to replace the Internet port's MAC address with the MAC address of a connected client.

IPv4 - PPPoE

Select **PPPoE** if your ISP provides and 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.



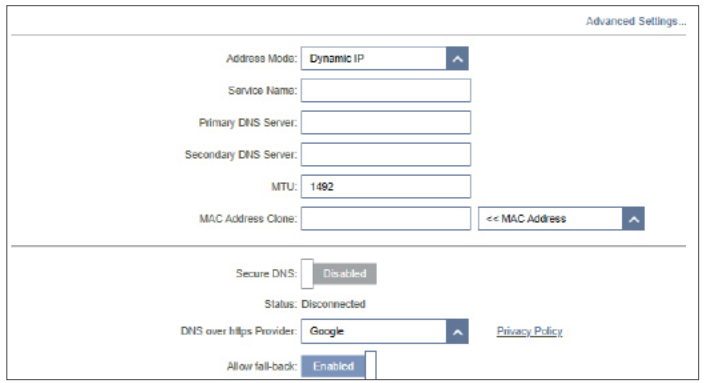
Username Enter the username provided by your ISP.

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 for the Internet connection to be maintained during inactivity. To disable this feature, select **Always on** or **Manual** as the reconnect mode. The default time is 5 minutes.

Advanced Settings...



Address Mode Select **Static IP** if your ISP assigned you the IP address and DNS server addresses. In most cases, select **Dynamic IP**.

If you select **Dynamic IP** as the Address Mode:

Service Name Enter the ISP service name (optional).

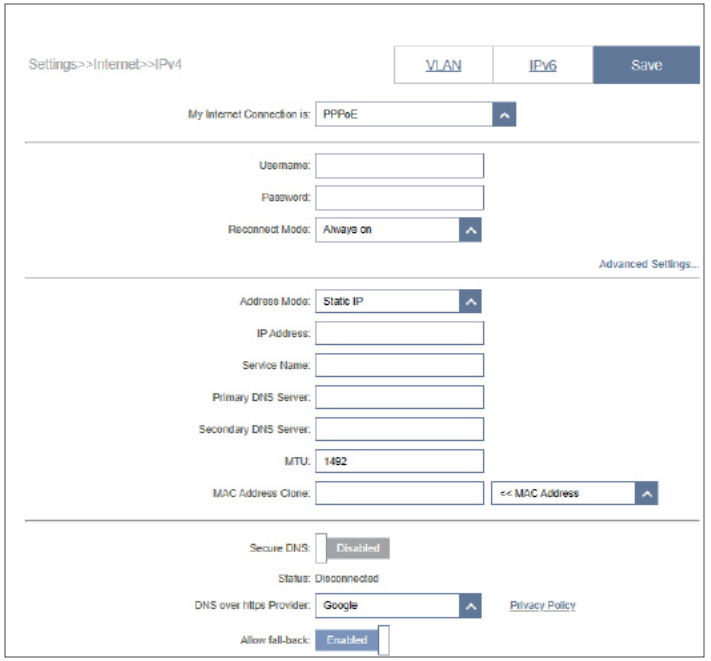
Primary DNS Server Enter the primary DNS server IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

Secondary DNS Server Enter the secondary DNS server IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

MTU Maximum Transmission Unit (1280~1500)- The default is 1492. You may need to change the MTU for optimal performance with your ISP.

IPv4 - PPPoE (continued)

MAC Address Clone: The default MAC address is set as 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.



If you select **Static IP** as the Address Mode:

IP Address Enter the IP address provided by your ISP.

Service Name Enter the ISP service name (optional).

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

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

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

MAC Address Clone Use the drop-down menu to replace the Internet port's MAC address with the MAC address of a connected client.

IPv4 - PPTP

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

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

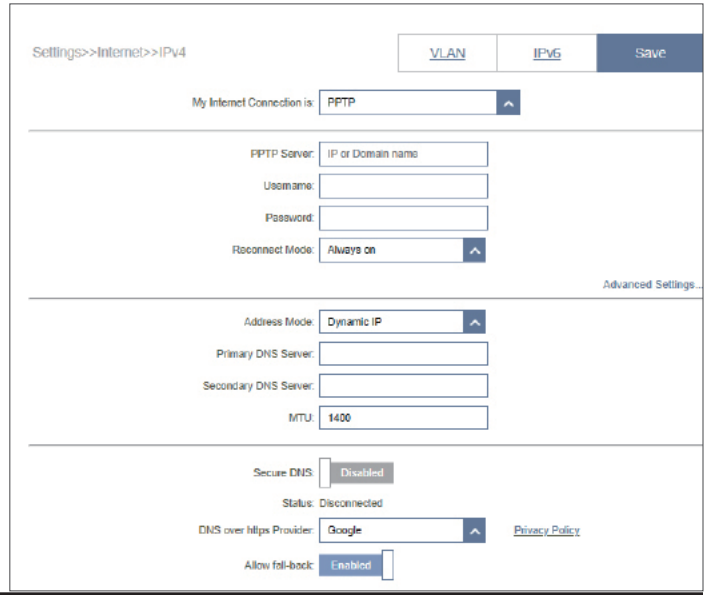
Username Enter the username provided by your ISP.

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 for the Internet connection to be maintained during inactivity. To disable this feature, select **Always on** or **Manual** as the reconnect mode.

Advanced Settings...



Address Mode: Select **Static IP** if your ISP assigned you an IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

If you select **Dynamic IP** as the Address Mode:

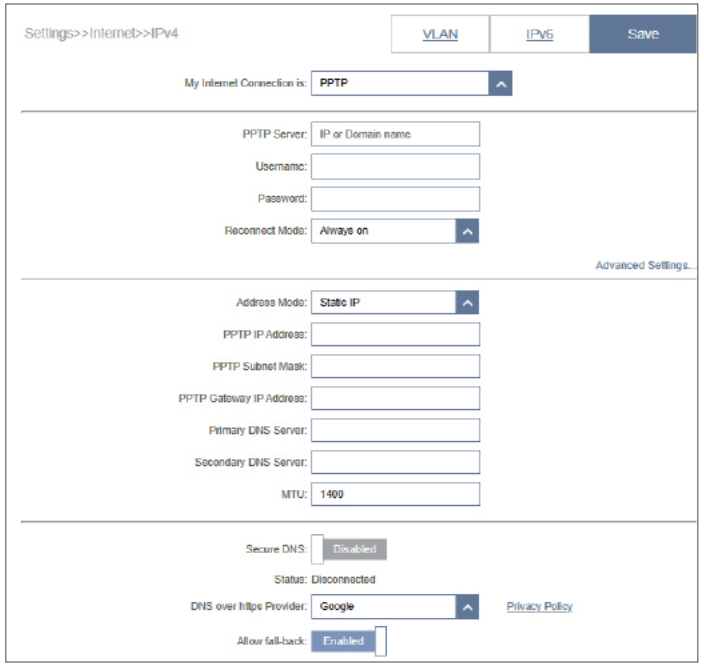
Primary DNS Server Enter the primary DNS server's IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

Secondary DNS Server Enter the secondary DNS server's IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

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

IPv4 - PPTP (continued)

If you select **Static IP** as the Address Mode:



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

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

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

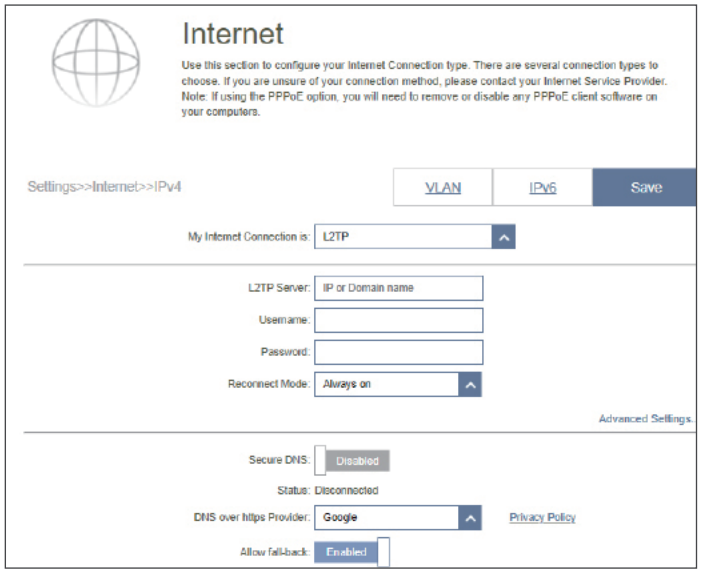
Primary DNS Server Enter the primary DNS server's IP address assigned by your ISP.

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

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

IPv4 - L2TP

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



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

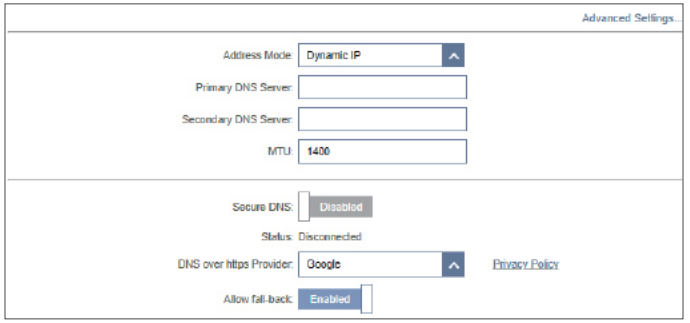
Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

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

Maximum Idle Time Configurable when **On Demand** is selected. Enter a maximum idle time (in minutes) for the Internet connection to be maintained during inactivity. To disable this feature, select **Always on** or **Manual** as the reconnect mode.

Advanced Settings...



Address Mode: Select **Static IP** if your ISP assigned you an IP address, subnet mask, gateway, and DNS server addresses. In most cases, however, select **Dynamic IP**.

If you select **Dynamic IP** as the Address Mode:

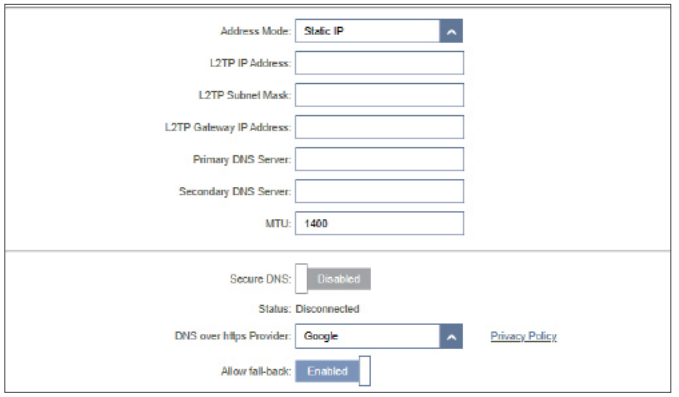
Primary DNS Server Enter the primary DNS server's IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

Secondary DNS Server Enter the secondary DNS server's IP address assigned by your ISP. This address is usually automatically obtained from your ISP.

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

IPv4 - L2TP (continued)

If you select **Static IP** as the Address Mode:



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

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

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

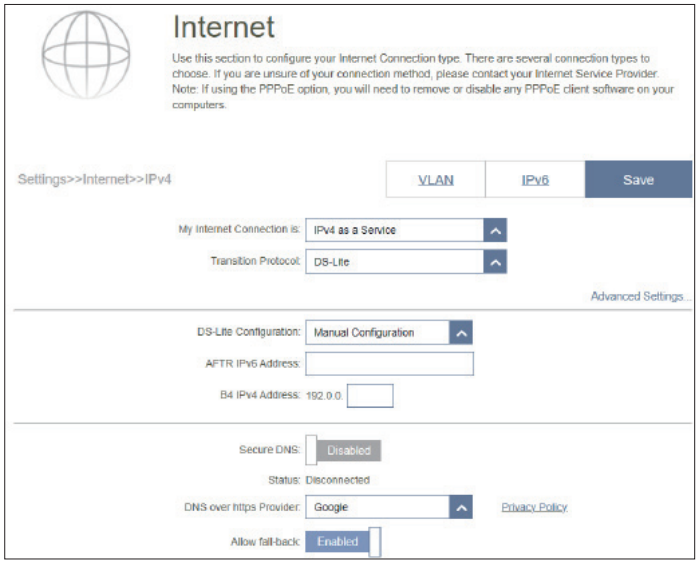
Primary DNS Server Enter the primary DNS server's IP address assigned by your ISP.

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

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

IPv4 as a Service

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



Transition Protocol Select DS-Lite or 464XLAT (CLAT) as the protocol for transition between IPv4 and IPv6 packets. The 464XLAT address translation uses CLAT (Customer-side Translator) to enable LAN IPv4 hosts to communicate with IPv4 hosts on other networks over an IPv6 network, while also allowing IPv6 clients to access IPv4 hosts.

Advanced Settings...DS-Lite

DS-Lite Configuration Select **DS-Lite DHCPv6 Option** to let the router allocate the AFTR IPv6 address automatically. Select **Manual Configuration** to enter the AFTR IPv6 address manually.

Manual Configuration

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

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

B4 IPv4 Address Enter the B4 IPv4 address value used here.

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

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

Advanced Settings...464XLAT(CLAT)

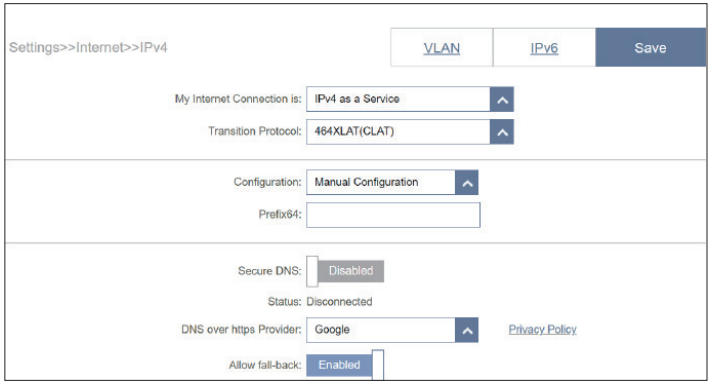
464XLAT (CLAT) Configuration Select **DS-Lite DHCPv6 Option** to let the router allocate the an IPv6 address automatically. Select **Manual Configuration** to enter the IPv6 prefix manually.

Manual Configuration

Prefix64 Enter a unique source IPv6 prefix (e.g. 2024:db9:abcd::0)to be embedded in the IPv4 source and destination addresses.

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

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



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 view the network connection details, click the **IPv4** tab. Refer to **Internet - IPv4** on **page 34.** To configure the **VLAN** connection details, click the VLAN tab. Refer to **Internet - VLAN** on **page 58.**

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

My Internet Connection Is Choose your IPv6 connection type from the drop-down menu. You will be presented with appropriate options for your connection type. Click **Advanced Settings...** to expand the list and see all of the options.

For **IPv6 - Auto Detection**, refer to **page 46**.

For **IPv6 - Static**, refer to **page 48**.

For **IPv6 - Auto Configuration (SLAAC/DHCPv6)**, refer to **page 50**.

For **IPv6 - PPPoE**, refer to **page 52**.

For **IPv6 - 6rd**, refer to **page 55**.

For **IPv6 - Local Connectivity Only**, refer to **page 57**.

IPv6 - Auto Detection

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

IPv6 DNS Settings

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

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

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

LAN IPv6 Address Settings

Enable DHCP-PD Enable or disable DHCP Prefix Delegation.

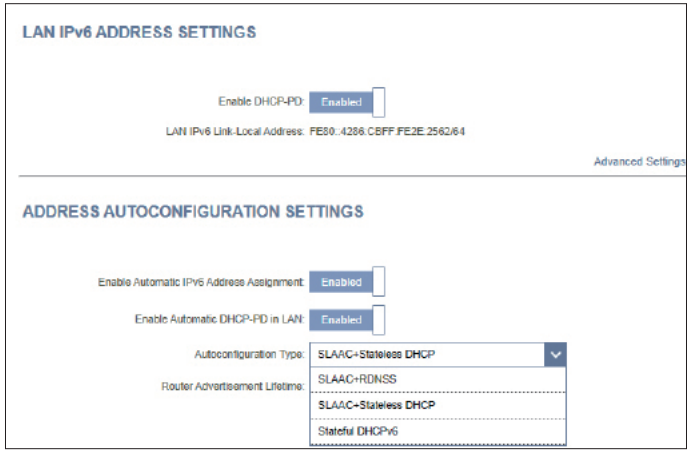
LAN IPv6 Link-Local Address Displays the router's LAN link-local address.

*If **Enable DHCP-PD** is disabled, these additional parameters are available for configuration:*

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

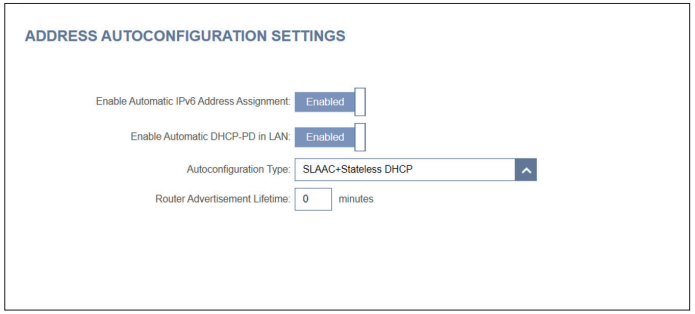


Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature.

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

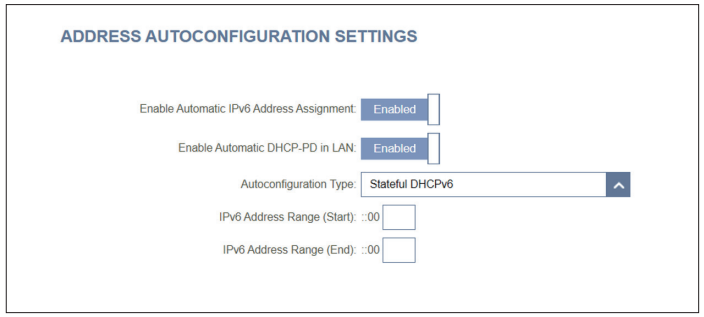
Note: *This feature requires a smaller subnet prefix than /64 (i.e. allowing for a larger address allocation), such as /63. Contact your ISP for more information.*

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



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

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



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

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

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

IPv6 - Static

Select **Static IP** if your IPv6 information is provided by your 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 use. Enabling this feature will use your local IPv6 address as the static IP. Disable this feature to manually enter your static IPv6 address and subnet prefix length.

IPv6 Address If **Use Link-Local Address** is disabled, enter the address supplied by your ISP.

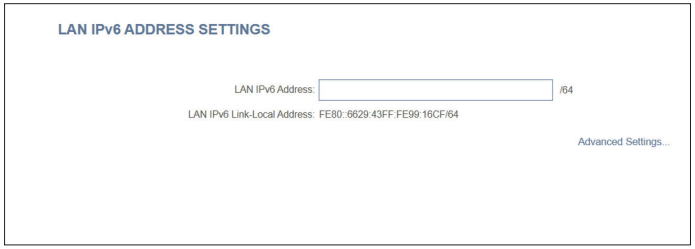
Subnet Prefix Length If **Use Link-Local Address** is disabled, enter the subnet prefix length supplied by your ISP.

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.

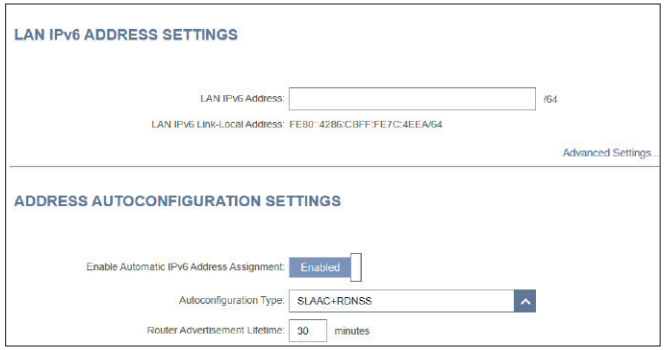
LAN IPv6 Address Settings



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

IPv6 - Static (Continued)

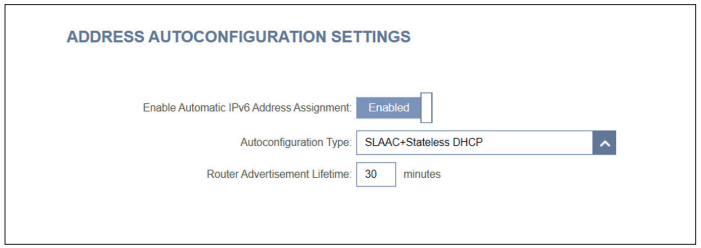
Advanced Settings... - Address Autoconfiguration Settings



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

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

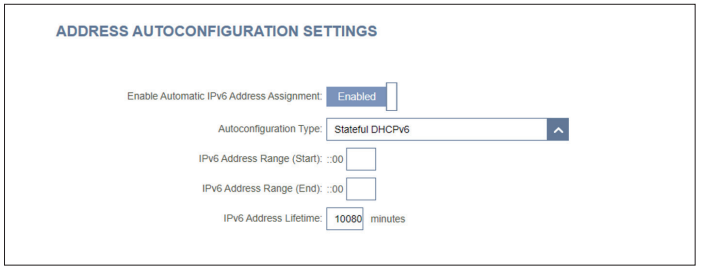
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.



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 starting IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the ending 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 - Auto Configuration (SLAAC/DHCPv6)

Select **Auto Configuration (SLAAC/DHCPv6)** if your ISP assigns your IPv6 address when your router requests one from the ISP's server. Some ISPs require you to adjust these settings before your router can connect to the IPv6 Internet. Click **Save** when you are done.

IPv6 DNS Settings

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

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

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

LAN IPv6 Address Settings

Enable DHCP-PD Enable or disable prefix delegation services.

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

If **Enable DHCP-PD** is disabled, these additional parameters are available for configuration:

LAN IPv6 Address Enter a valid LAN IPv6 address.

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

IPv6 - Auto Configuration (SLAAC/DHCPv6)

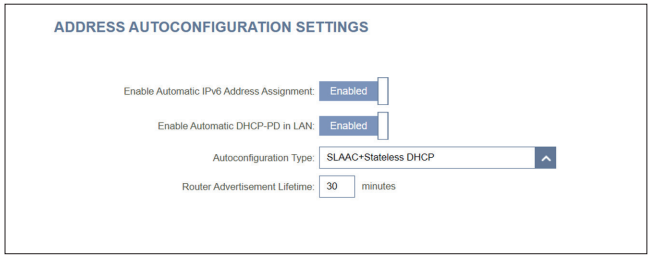
Advanced Settings... - Address Autoconfiguration Settings

Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature. Enabling this feature will present additional configuration options.

Enable Automatic DHCP-PD in LAN Enable or disable Automatic DHCP-PD in LAN for other IPv6 routers/ gateways to be connected to the LAN interface. This option is only available if **Enable Automatic DHCP-PD in LAN** is enabled.

Note: *This feature requires a smaller subnet prefix than /64 (i.e. allowing for a larger address allocation), such as /63. Contact your ISP for more information.*

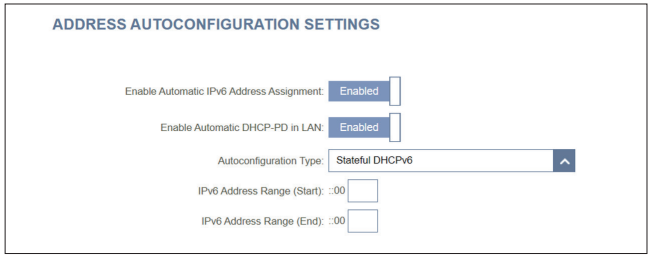
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.



If **SLAAC+RDNSS** or **SLAAC+Stateless DHCP** is selected as the Autoconfiguration Type:

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

If **Stateful DHCPv6** is selected as the Autoconfiguration Type:



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

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

IPv6 - PPPoE

Select **PPPoE** if your ISP provides and 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.

PPPoE Session Select **Create a new session** to start a new PPPoE session.

Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

Address Mode Select **Static IP** if your ISP assigned you an IP address. In most cases, select **Dynamic IP**.

IP Address If you select **Static IP** as the Address Mode, enter the IP address provided by your ISP.

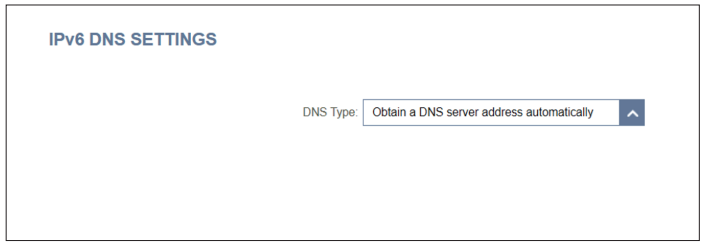
Service Name Enter the ISP service name (optional).

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

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

IPv6 - PPPoE

IPv6 DNS Settings



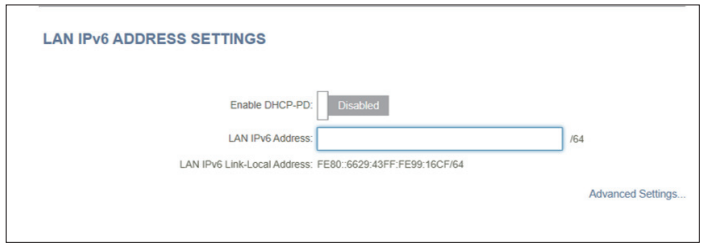
DNS Type Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

If **Use the following DNS address** is selected:

Primary DNS Server Enter the primary DNS server address.

Secondary DNS Server Enter the secondary DNS server address.

LAN IPv6 Address Settings



Enable DHCP-PD Enable or disable prefix delegation services.

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

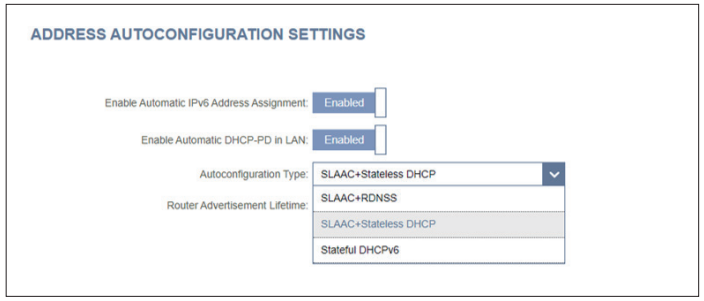
If **Enable DHCP-PD** is disabled, these additional parameters are available for configuration:

LAN IPv6 Address Enter a valid LAN IPv6 address.

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

IPv6 - PPPoE (Continued)

Advanced Settings... - Address Autoconfiguration Settings

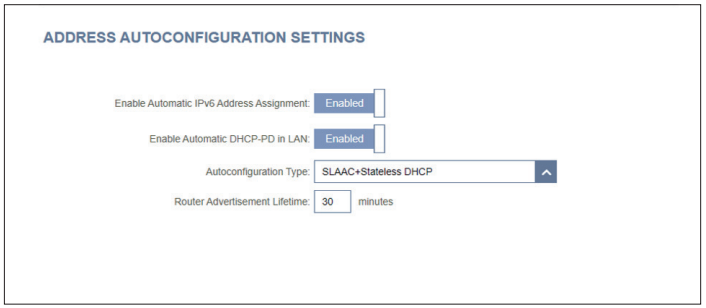


Enable Automatic IPv6 Address Assignment Enable or disable the Automatic IPv6 Address Assignment feature. Enabling this feature will present additional configuration options.

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

Note: *This feature requires a smaller subnet prefix than /64 (i.e. allowing for a larger address allocation), such as /63. Contact your ISP for more information.*

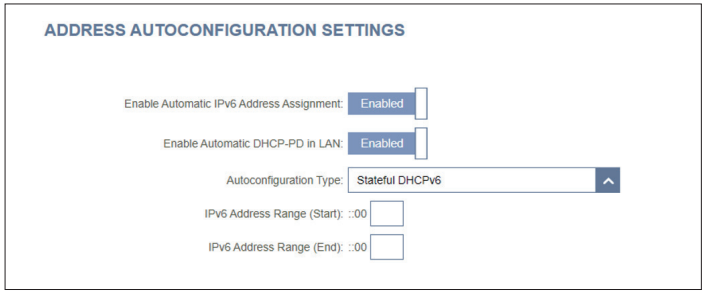
Autoconfiguration Type Select **SLAAC+RDNSS**, **SLAAC+Stateless DHCP**, or **Stateful DHCPv6**.



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

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

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

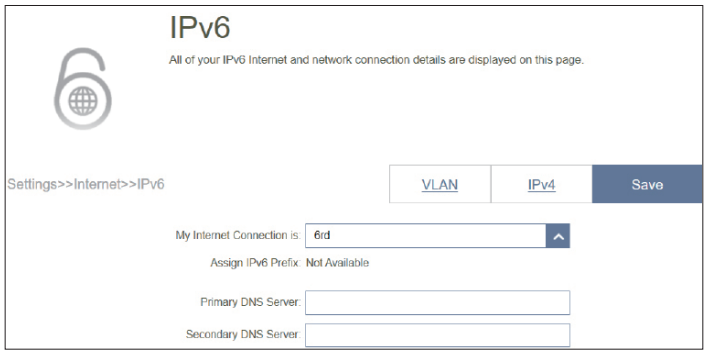


IPv6 Address Range (Start) Enter the starting IPv6 address for the DHCP server's IPv6 assignment.

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

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.

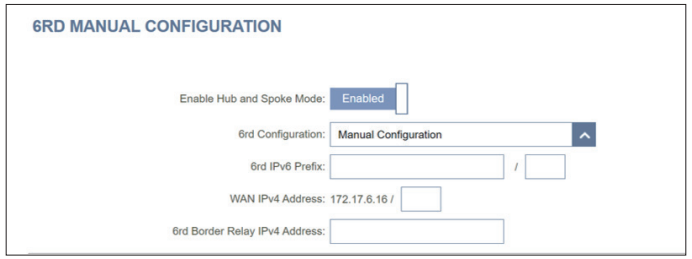


Assign IPv6 Prefix Currently unsupported.

Primary DNS Server Enter the primary DNS server address.

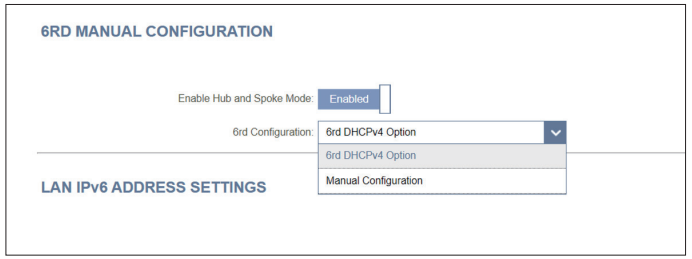
Secondary DNS Server Enter the secondary DNS server address.

6rd Manual Configuration



Enable Hub and Spoke Mode Enable this feature 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 choose **Manual Configuration** to enter the settings yourself.



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

6rd IPv6 Prefix Enter the 6rd IPv6 prefix and mask length supplied by your ISP.

WAN IPv4 Address Displays the router's IPv4 address.

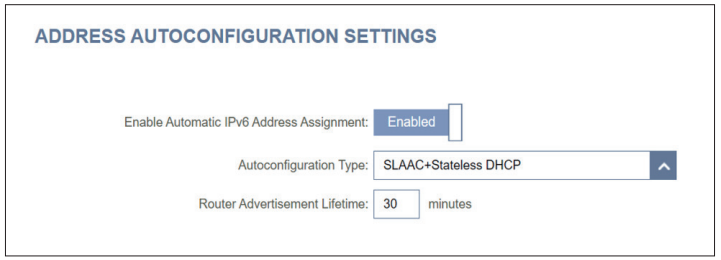
6rd Border Relay IPv4 Address Enter the 6rd border relay IPv4 address settings supplied by your ISP.

IPv6 - 6rd

LAN IPv6 Address Settings

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

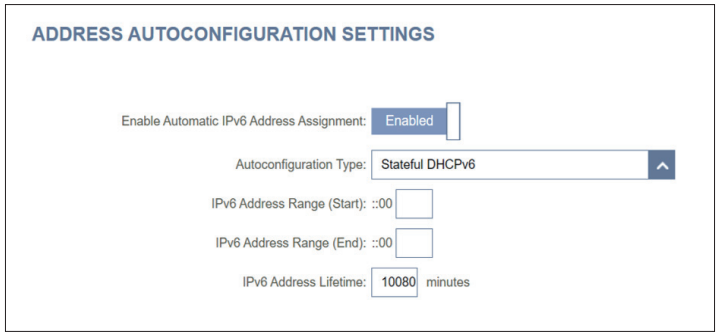
Advanced Settings... - Address Autoconfiguration Settings



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 starting IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End) Enter the ending 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.

If you select **Enable ULA** and disable **Default ULA Prefix**:

ULA Prefix Enter your own ULA prefix.

Advanced Settings - Current IPv6 ULA Settings

Current ULA Prefix Displays the current ULA prefix.

LAN IPv6 ULA Displays the LAN's IPv6 ULA.

Internet - VLAN

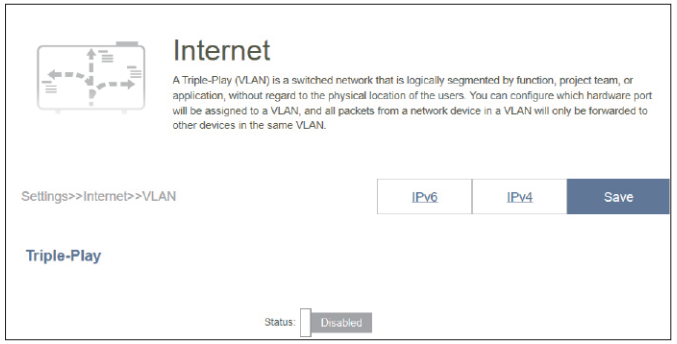
In the Settings menu on the bar at the top-left of the page, click **Internet** to see the Internet configuration options for the IPv4 connection details, then click the **VLAN** link to access the configuration options for the VLAN connection details.

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

To configure the IPv4 Internet and view network connection details, click the **IPv4** link. Refer to **IPv4** on **page 34**
To configure the IPv6 Internet and view network connection details, click the **IPv6** link. Refer to **IPv6** on **page 45**

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

Status Displays the current ULA prefix. 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.

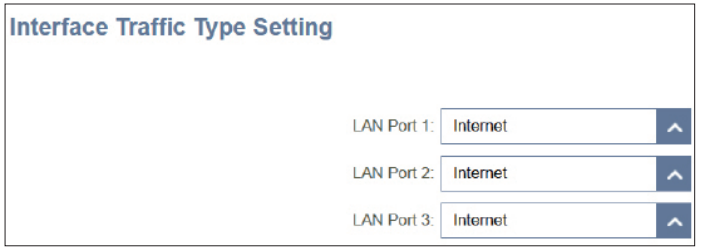
Internet VLAN ID Enter the VLAN ID for your Internet connection, as provided by your ISP.

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 (0 represents best effort and 7 represents the highest priority) takes precedence over traffic with a low priority ID tag.

Interface Traffic Type Setting



LAN Port 1-3 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

From this page you can configure your Wi-Fi settings. Click **Save** at any time to save the changes you have made on this page.

Wi-Fi Mesh

Status Enable 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 router in a mesh network topology. Hence, it enhances efficiency and reliability. The default is enabled. Enabling this will always enable the below Smart Connect feature.

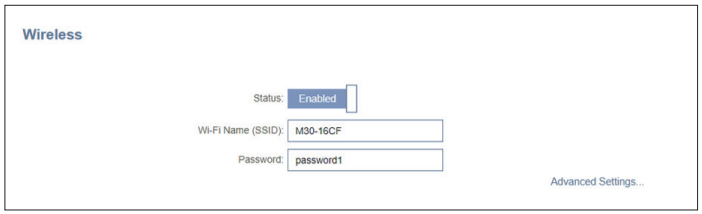
Smart Connect

Status Enable or disable the Smart Connect Feature. The Smart Connect feature presents a single wireless network. When connecting clients to the network, the clients will be automatically added to the best band, i.e. 2.4 GHz or 5 GHz according to the configured smart group of the designated bands.

Smart Group Select a different combination of bands to form a Smart Connect group.

If Smart Connect Status is Enabled:

Wireless

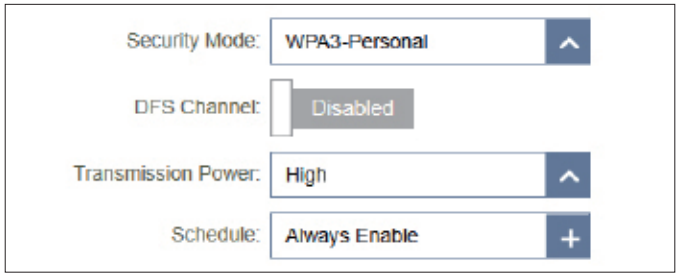


Wi-Fi Name (SSID) Enter a name for your Wi-Fi network. Up to 32 characters are allowed.

Password Create a Wi-Fi password that's 10 to 63 characters long, using a mix of letters and numbers, with no identical characters next to each other. Wireless clients will need to enter this password to successfully connect to the network.

Wireless

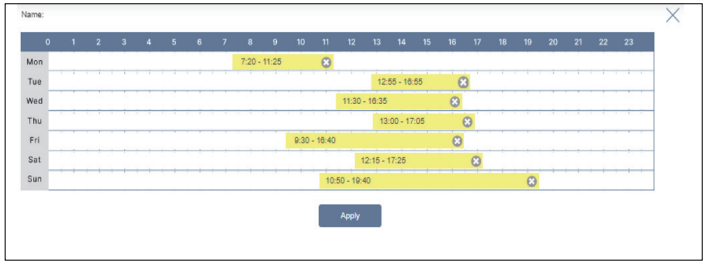
Wireless - Advanced Settings



Security Mode Choose **WPA2-Personal** (default)**, WPA2/ WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of encryption among these.Note that WPS will be disabled unless WPA2 encryption is enabled.

DFS Channel DFS (Dynamic Frequency Selection) enables you to combine additional channels to increase the channel width in 5 GHz band. Note the router must scan for radar signals before using a channel and will change channels automatically if radar signals are detected, which may cause interruption in connection.

Transmission Power Select a desired wireless transmission power: High, Medium, 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.

When Smart Connect Status is disabled, 2.4 GHz and 5 GHz configuration options become available. Please configure each band separately as instructed below.

2.4 GHz / 5 GHz

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

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

Password Create a Wi-Fi password that's 10 to 63 characters long, using a mix of letters and numbers, with no identical characters next to each other. Your Wireless clients will need to enter this password to successfully connect to the network.

2.4 GHz - Advanced Settings...

Security Mode Choose **WPA2-Personal** (default)**, WPA2/WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of encrytion among these. 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, Mix 802.11b/g,** or **802.11b only.**

Wi-Fi Channel Select a desired channel: 1-11. 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 (802.11b/g/n/ax/be) devices, or select **20 MHz** if you are using a mixed of 802.11b/g devices.

HT20/40 Coexistence Enable or disable coexistence of 20/40 MHz if Auto 20/40 MHz is selected above.

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.

5 GHz - Advanced Settings...

Security Mode Choose **WPA2-Personal** (default)**, WPA2/WPA3-Personal,** or **WPA3-Personal**. WPA3 provides the highest level of encrytion among these. Note that WPS will be disabled unless WPA2 encryption is enabled.

802.11 Mode (5 GHz) Select a desired wireless networking standard 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 **802.11a** only**.**

Wi-Fi Channel Select a desired channel: 36, 40, 44, 48, 149, 153, 157, 161, or 165. 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.

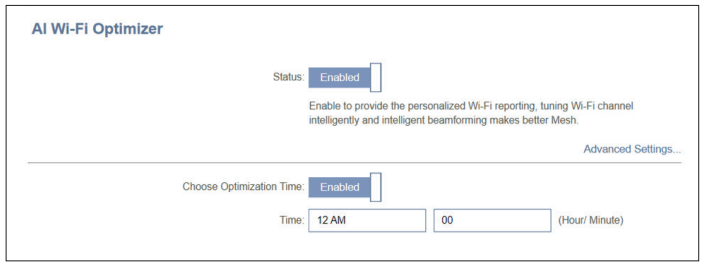
Transmission Power Select a desired wireless transmission power: High, Medium, or Low.

Channel Width (5 GHz) 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; select **20/40 MHz** if you are using 802.11n/a devices; select **20 MHz** if you are using only 802.11a devices.

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

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

AI Wi-Fi Optimizer



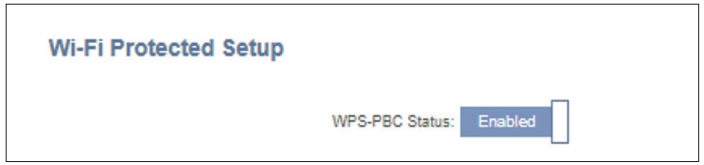
AI-powered Wi-Fi Optimizer intelligently assists with bandwidth optimization for your home or office network. It automatically adopts the "cleanest" channel coupled with the mesh beamforming technology, which in turn optimizes the overall mesh network.

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

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

Once the AI Wi-Fi optimizer is turned on, you will begin to receive weekly reports on Wi-Fi conditions through AI Assistant by clicking  *at the top right.*

Wi-Fi Protected Setup



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

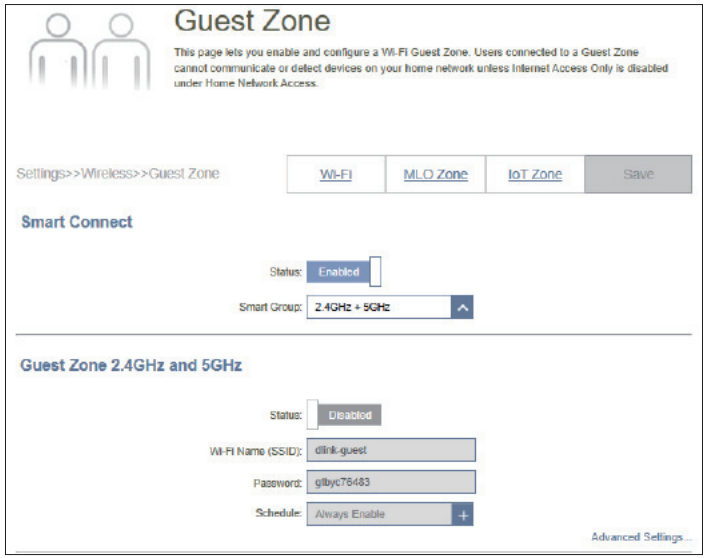
WPS-PBC Status Enable or disable WPS Push Button Configuration (PBC) functionality. Enabling this feature will allow wireless clients to connect to the Wi-Fi through an encrypted connection established through pressing the WPS button. Please refer to **WPS Button** on **page 137**.

Guest Zone

The **Guest Zone** feature will allow you to create a temporary wireless network for guests to access the Internet. This zone will be separate from your main Wi-Fi network.

In the **Settings** menu on the left side of the page, click **Wireless**, then click the **Guest Zone** link. Click **Save** at any time to save the changes you have made on this page.

If Smart Connect Status is **Enabled***, configure the following for both 2.4 and 5 GHz radio frequencies together. If it is* **Disabled***, configure the following for 2.4 GHz and 5 GHz individually.*



Wireless	
Status	Enable or disable the Guest Wi-Fi network. The default is disabled.
Wi-Fi Name (SSID)	Enter a name for your Guest wireless network.
Password	Create a password for your guest Wi-Fi network that is between 10 and 63 characters long, includes a combination of letters and numbers, and does not contain identical characters next to each other. Wireless clients will need to enter this password to successfully connect to the network. Click the eye icon to show or hide the password.
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.

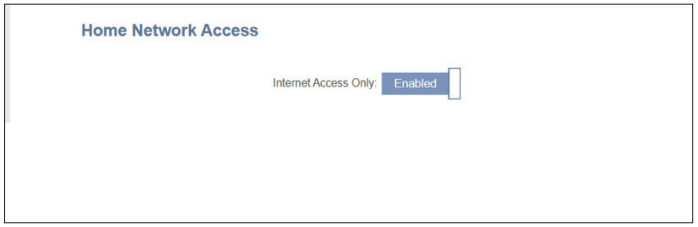
Advanced Settings

Security Mode (2.4GHz) Choose **WPA2-Personal** (default), **WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these.

Security Mode (5GHz) Choose **WPA2-Personal** (default), **WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these.

Home Network Access

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



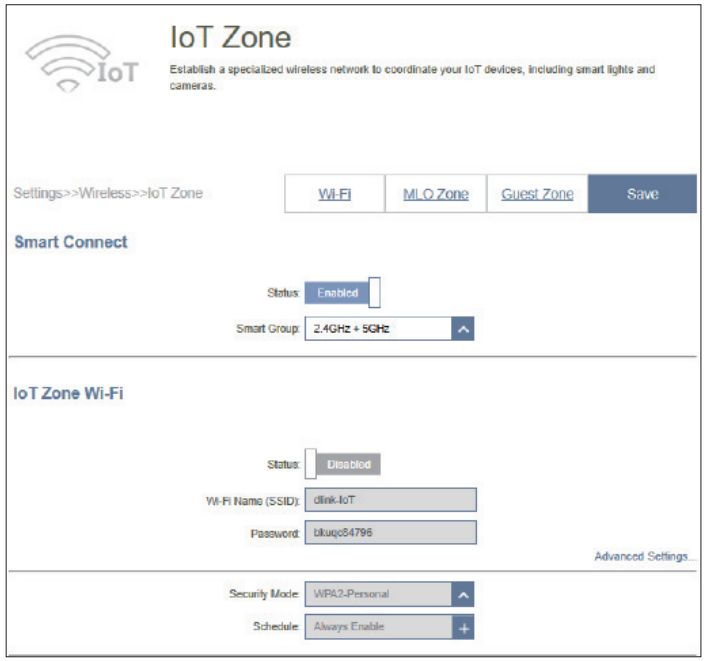
IoT Zone

The **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.

In the **Settings** menu on the left side of the page, click **Wireless**, then click the **IoT Zone** link. Click **Save** at any time to save the changes you have made on this page.

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

Wireless	
Status	Enable or disable the IoT Wi-Fi network. The default is disabled.
Wi-Fi Name (SSID)	Enter a name for your IoT wireless network.
Password	Create a password for your IoT Wi-Fi network that is between 10 and 63 characters long, includes a combination of letters and numbers, and does not contain identical characters next to each other. Wireless clients will need to enter this password to successfully connect to the network. Click the eye icon to show or hide the password.
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 (2.4GHz) Choose **WPA2-Personal** (default)**, WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these.

Security Mode (5GHz) Choose **WPA2-Personal** (default)**, WPA2/WPA3-Personal,** or **WPA3-Personal.** WPA3 provides the highest level of encryption among these.

MLO Zone

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.

In the **Settings** menu on the left side of the page, click **Wireless**, then click the **MLO Zone** link. 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

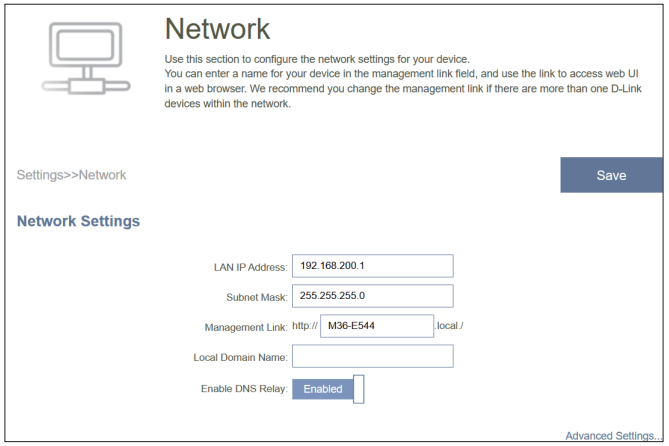
Security Mode Choose **WPA3-Personal** to authenticate and encrypt every connection attempt.

Note: Multi-Link Operation (MLO) enables the use of multiple bands simultaneously offered by Wi-Fi 7. To have this feature, make sure that your operating system and network adapter support Wi-Fi 7. For Windows, Wi-Fi 7 support starts in Windows 11, version 24H2. To find the version of your Windows, go to **Settings**, select **System > About,** then look for Windows edition and version under **Windows specifications.**

Network

This section allows you to change the local network settings of the router and configure the DHCP settings. In the Settings menu on the left side of the page, click **Network**. 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 **192.168.200.1**.
If you change the IP address, you will need to enter the new IP address in your browser to get back into the web management.

Subnet Mask Enter the subnet mask of the router. The default subnet mask is **255.255.255.0**.

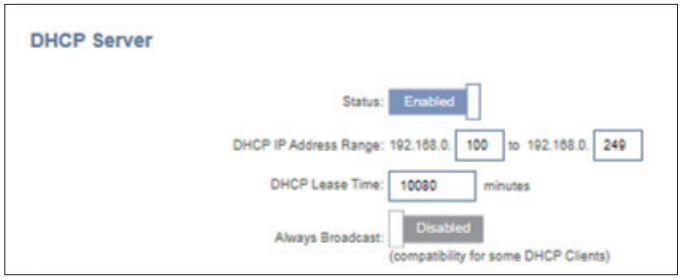
Management Link The default address to access the router's configuration is **http://M36-xxxx.local/** (where xxxx represents the last 4 digits of your router's MAC address). You can replace **M36-xxxx** with a name of your choice.

Local Domain Name Enter the domain name (optional).

Enable DNS Relay Disable to transfer the DNS server information from your ISP to your computers. If enabled, your computers will use the router's setting for a DNS server.

Network

DHCP Server



Status Enable or disable the DHCP server.

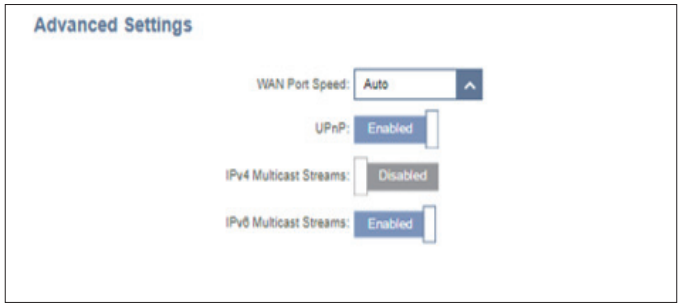
DHCP IP Address Range Enter the starting and ending IP addresses for the DHCP server's IP assignment.

Note: *If you have reserved static IP addresses for client devices, make sure the IP addresses are outside of this range or you might have an IP conflict.*

DHCP Lease Time Enter the length of time for the IP address lease in minutes. The default is 10,080 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 port speed of the Internet port to **10 Mbps**, **100 Mbps**, **1000 Mbps**, **2500 Mbps** or **Auto** (recommended).

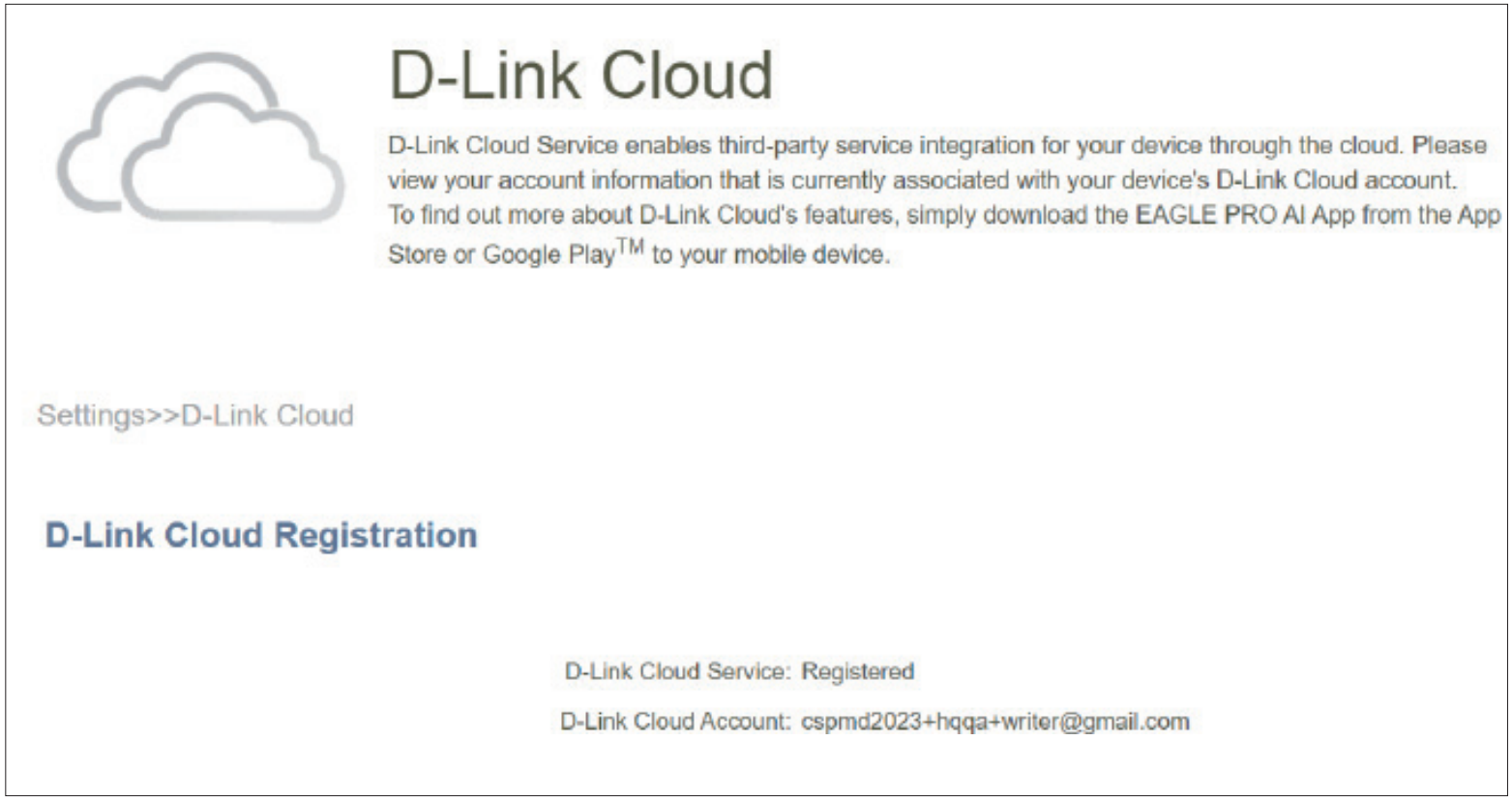
UPnP Enable or disable Universal Plug and Play (UPnP). UPnP provides compatibility with networking equipment, software, and peripherals. This is enabled by default.

IPv4 Multicast Streams Enable this to allow IPv4 multicast traffic to pass through the router from the Internet. This is enabled by default.

IPv6 Multicast Streams Enable this to allow IPv6 multicast traffic to pass through the router from the Internet. This is enabled by default.

D-Link Cloud

In the **Settings** menu on the left side of the page, click **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. Use the AQUILA PRO AI app to find out more about D-Link Cloud's features.



Operation Mode

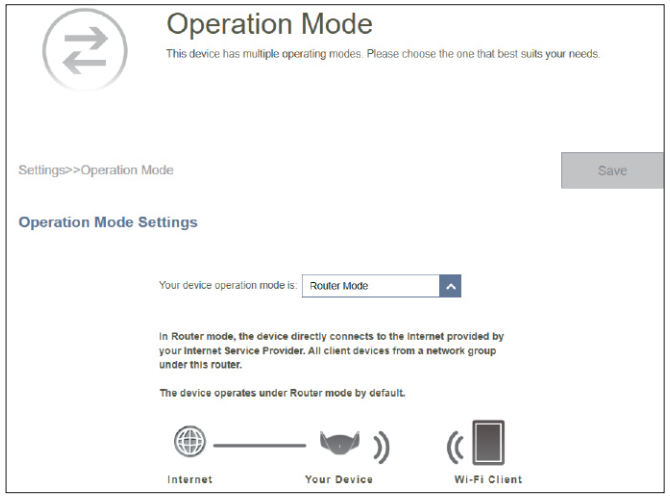
Go to **Settings > Operation Mode** to select your operation mode. Depending on your network architecture, you can configure the router to function as one of the following types of network device: router, extender, or bridge.

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

Bridge Mode: In this Mode, the router extends your existing network and improves overall Wi-Fi coverage. Under this mode, the DHCP Server, Parental Control, QoS, and Firewall settings rely on the existing router.

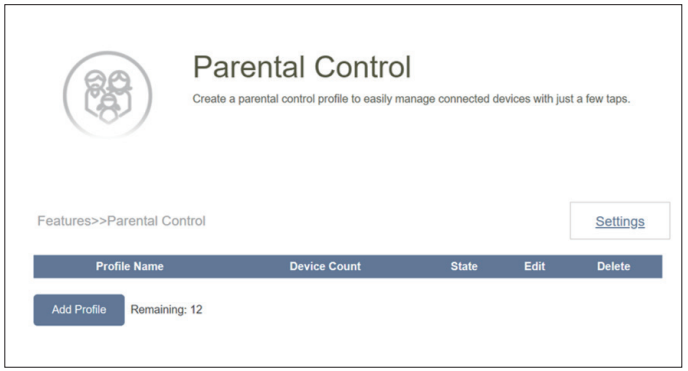
Extender Mode: In this mode, this device acts as an extender to connect your wireless devices, expanding Wi-Fi coverage. It provides connectivity between various wireless devices. This can be useful if you already have an existing wireless router. You can then manage the extender through the main router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

Operation Mode Settings	
Router Mode	Select Router Mode to run this device as a router.
Extender Mode	Select Extender Mode to run this device as an extender.
Bridge Mode	Select Bridge Mode to extend your existing network and improve overall Wi-Fi coverage. The DHCP Server, Parental Control, QoS, and Firewall settings rely on the existing 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.

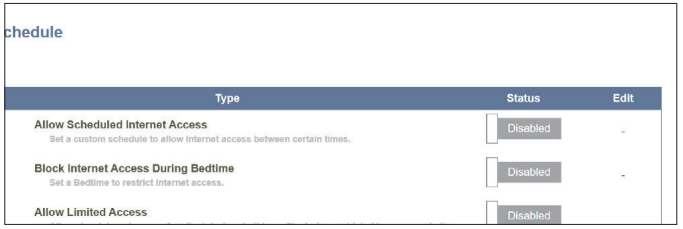
State Displays the current status of Internet accessibility, I.e. Normal, Schedule Paused, or Paused on Demand.

Edit Edit the 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:

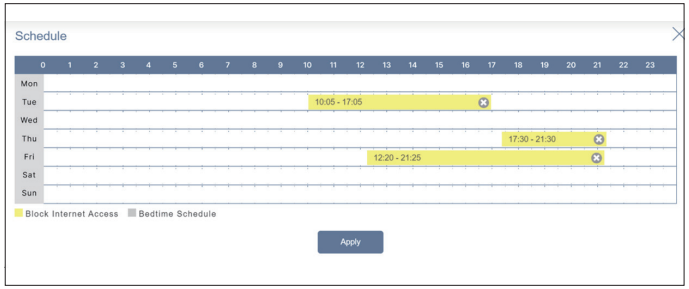


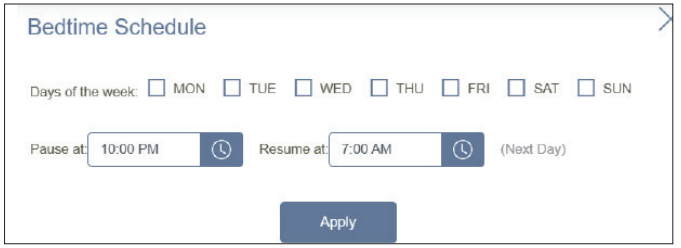
Schedule

Profile Name Enter a profile name for the schedule.

Allow Scheduled Internet Access Set a time period for the devices to be *blocked* Internet access.

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.





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 that the Bedtime schedule takes precedence over Scheduled Internet Access.

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

Click **Apply** when you are done.

Website Filter

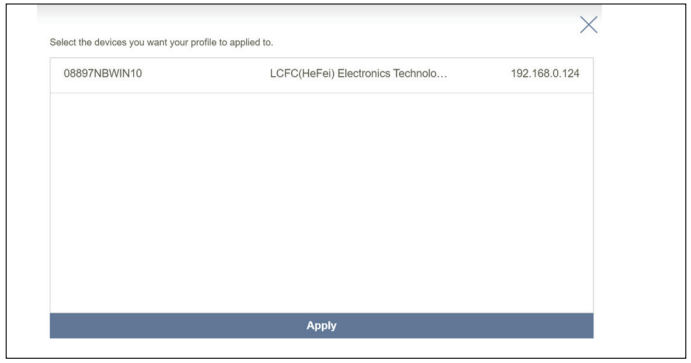
Click **Add Rule** to add a new website to be blocked:

Website Name Enter a name for the website. This blocks access to websites based on the domain names. For example, use "ABC.com" to block both "ABC.com" and "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. Re-enter the website name as above to block a specific site.

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

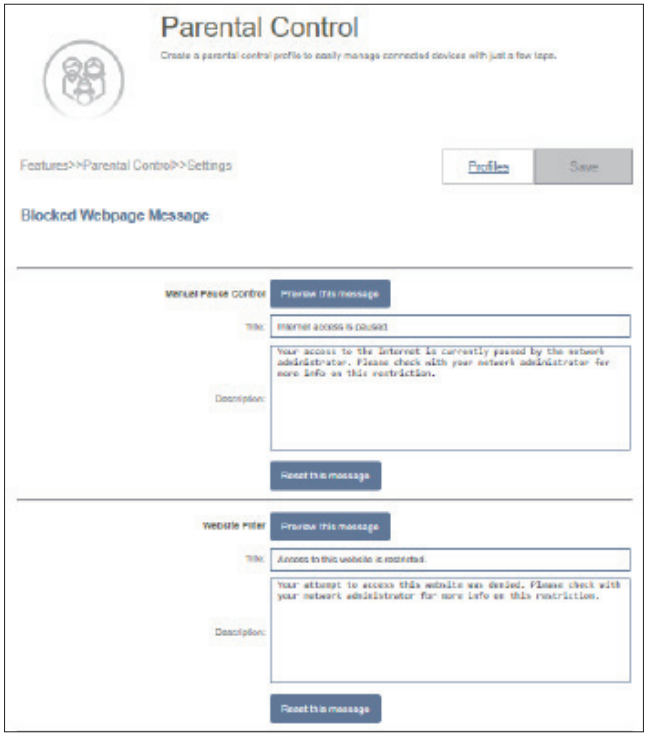
Device



Click **Add Device** to add devices to be in a defined profile. Select devices from the list of connected devices to which you want to apply the access policy to, 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 immediately **Pause for Internet Access** to specified devices of the profile.

Click **Settings** to view the messages 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**, or **Bedtime Schedule** is enabled. Edit Blocked Webpage Message and click **Save** to save the modified messages immediately.

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

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

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

Preview this message Displays the message on a new page.

QoS Engine

The **Quality of Service (QoS) Engine** allows you to prioritize particular clients over others, so that certain clients receive higher bandwidth. It also provides weekly usage reports of network bandwidth consumption.

In the **Features** tab on the left side of the page, click **QoS Engine**.

AI Traffic Optimizer Once this is turned on, you will start receiving weekly reports on bandwidth usage through AI Assistant (click at the top right to access AI Assistant).

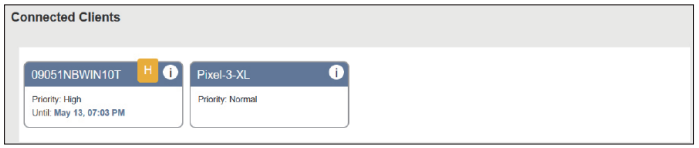
Download Speed (Mbps) Enter the maximum download speed (in Mbps) for all connected clients.

Upload Speed (Mbps) Enter the maximum upload speed (in Mbps) for all connected clients. If QoS is enabled, once this threshold is reached, traffic from higher-priority clients will be processed first, while traffic from lower-priority clients will wait until enough bandwidth becomes available.

Upload/download speeds can be obtained from your Internet Service Provider.

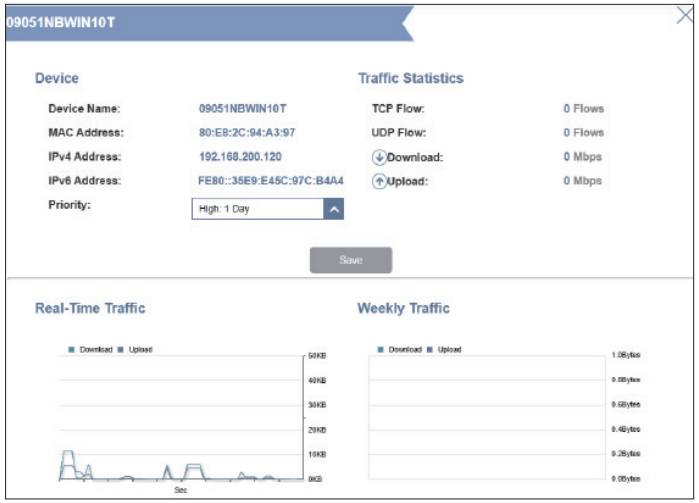
Click **Save** after filling in the above information.

QoS Engine



Under **Connected Clients**, you will see device cards representing each connected client. Click **All** to see all connected devices.

To assign a priority level to a device, enable the **AI Traffic Optimizer** first. Then click on a client to open its information page. The following information will be shown:



Device Name The name that describes the client device.

MAC Address The MAC address of the client device.

IPv4/IPv6 Address The IP address in IPv4 and IPv6 addressing mechanism of the client device.

Priority Select the priority and duration for the client device with the following categories:

Normal

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

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

Click **Save** after you have configured the **Priority**.

Traffic Statistics

The follwing traffic statistics is displayed: TCP flow, UDP flow, Download and Upload speeds (in Mbps).

Real-Time & Weekly Traffic

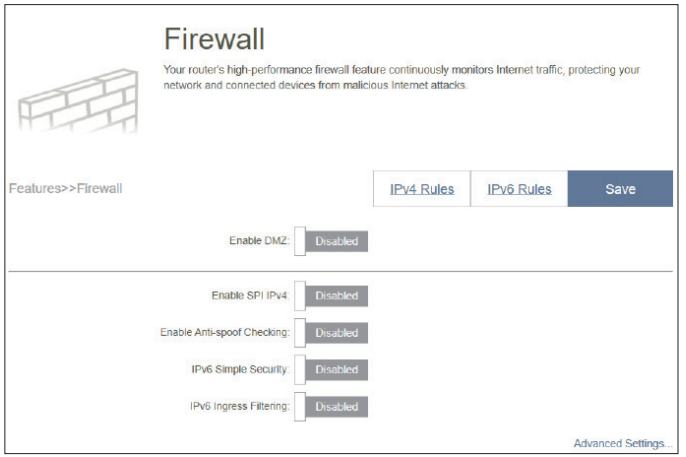
The Real-time Traffic and Weekly Traffic present real-time speed and daily data traffic for the past week respectively. If no devices are explicitly assigned with any priority, they will all be treated with equal priority.

Firewall

The integrated firewall helps protect your network from malicious attacks over the Internet. In the Features menu on the left, click **Firewall**. Click **Advanced Settings...** to expand the list and see all of the options.

To configure the IPv4 firewall rules, click the **IPv4 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on **page 82**.
To configure the IPv6 firewall rules, click the **IPv6 Rules** tab. Refer to **Firewall Settings - IPv4/IPv6 Rules** on **page 82**.

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, and is not recommended unless they are servers that must be exposed to the WAN.

DMZ IP Address If you enabled DMZ, enter the IP address of the client you wish to expose, or use the drop-down menu to quickly select it.

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

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

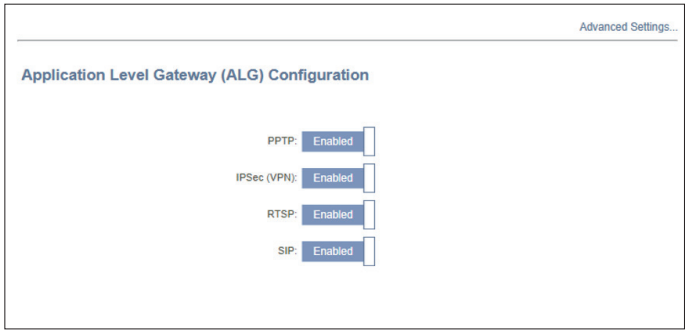
IPv6 Simple Security Enable or disable IPv6 simple security. A simple firewall configuration that denies access directly to computers behind the router.

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

Firewall

Advanced Settings...

Application Level Gateway (ALG) Configuration



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

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

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

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

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

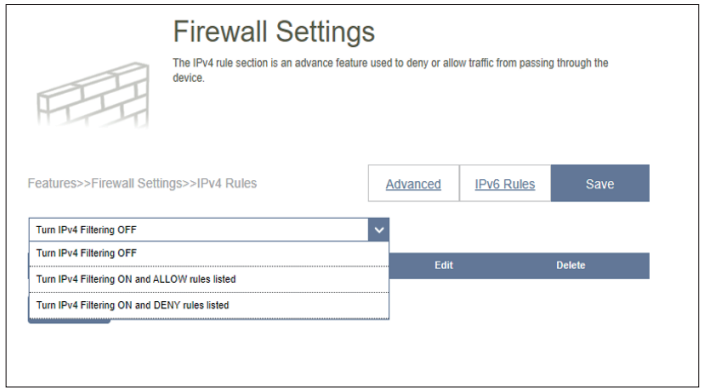
Firewall Settings - IPv4/IPv6 Rules

The IPv4/IPv6 Rules section is an advanced option that lets you configure what traffic is allowed to pass through the network. 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 80.**

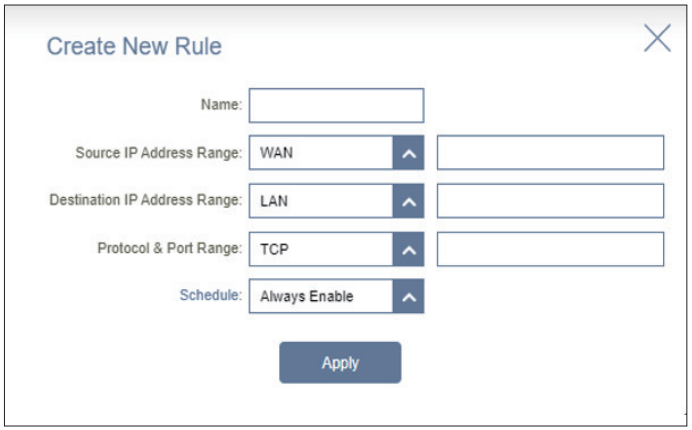
To begin, use the drop-down menu to select whether it will be an **ALLOW** or a **DENY** rule. Allow permits specific types of packets to enter or leave a network, while a DENY rule blocks specific packets from doing so. You can also choose to turn **OFF** filtering to allow all traffic to pass through unrestricted.

To remove a rule, click on the trash can icon in the Delete column. To edit a rule, click on the pencil icon in the Edit column.



Firewall Settings - IPv4/IPv6 Rules

To create a new rule, click on the **Add Rule** button. Click **Save** when you are done. A maximum of 24 rules can be defined. If you edit or create a 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.

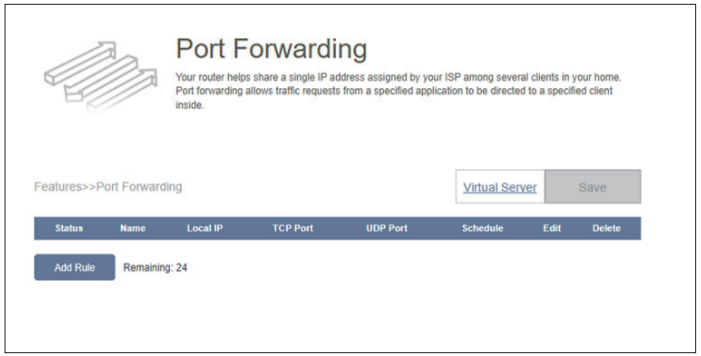
Protocol & Port Range Select a traffic protocol to allow or deny (**Any**, **TCP**, or **UDP**) and then enter a range of ports (e.g. 21-23) that the rule will apply to. Select Any to allow/deny all types of traffic regardless of the port number.

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 **Schedule** section. Refer to **Time & Schedule - Schedule** on **page 95** for more information.

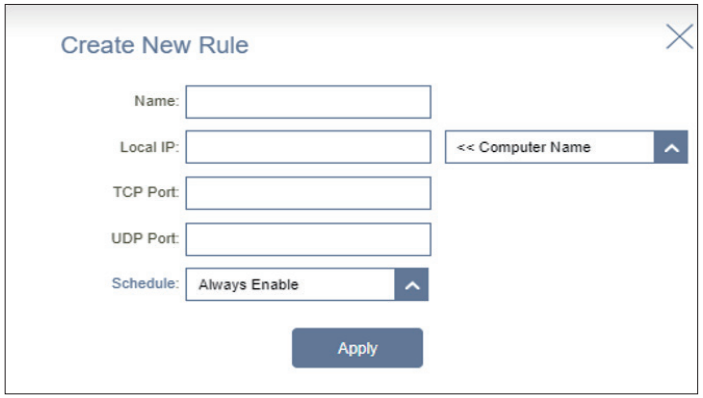
Click **Apply** when you are done.

Port Forwarding

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



In the **Features** tab on the left side of the page, click **Port Forwarding**. To remove a rule, click on its trash can icon in the Delete column. To edit a rule, click on its pencil icon in the Edit column. To create a new rule, click the **Add Rule** button. Click **Save** when you are done. If you edit or create a 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 the port will be forwarded. 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 Schedule section. Refer to Time & Schedule - Schedule on page 95 for more information.

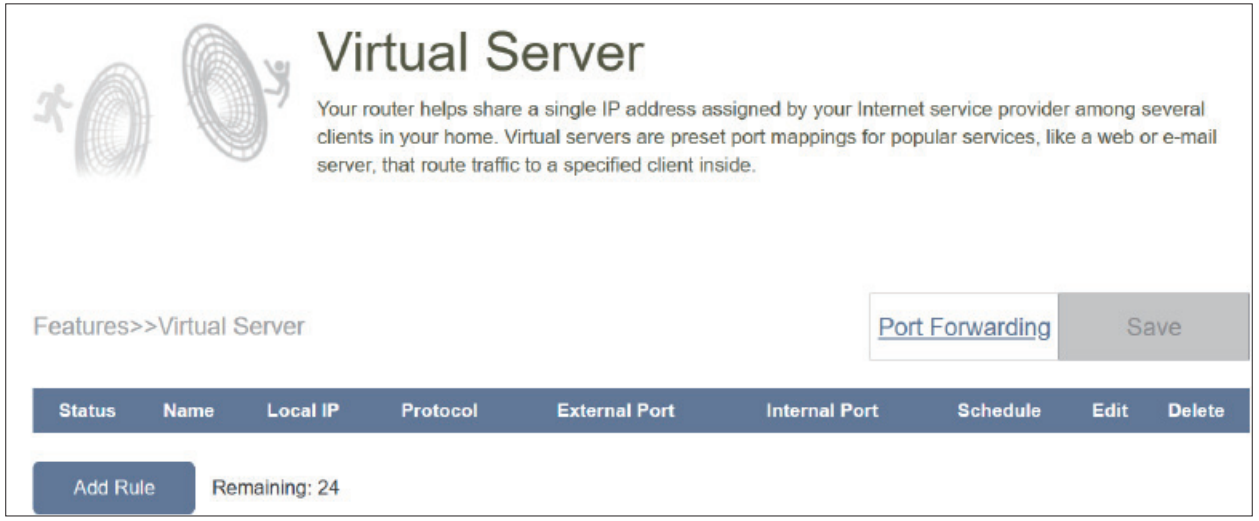
Click Apply when you are done.

Port Forwarding - Virtual Server

The virtual server allows you to specify a single public port on your router for redirection to an internal LAN IP address and Private LAN port. This might be necessary if you are hosting services behind the router.

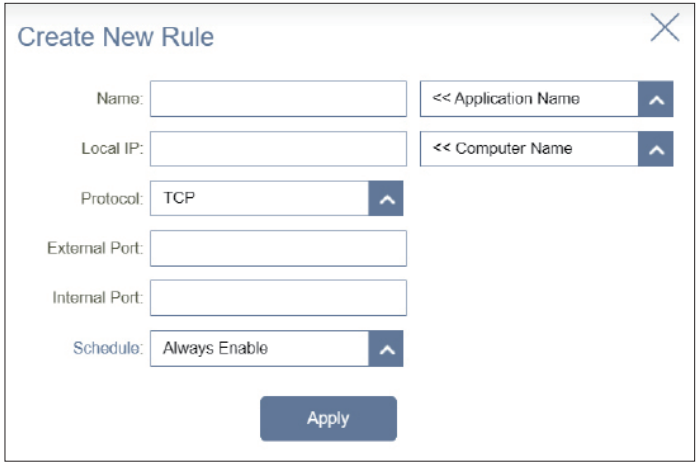
To configure the virtual server, click **Virtual Server** from the **Port Forwarding** page. To return to the main Port Forwarding page, click **Port Forwarding**.

To remove a rule, click on its trash can icon in the **Delete** column. To edit a rule, click on its pencil icon in the **Edit** column.



Port Forwarding - Virtual Server

To create a new rule, click the **Add Rules** button. Click **Apply** when you are done. If you edit or create a rule, the following options will appear:



Name Enter a name for the rule. Alternatively, select the protocol/ Application 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 to which the external port will forward. 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.

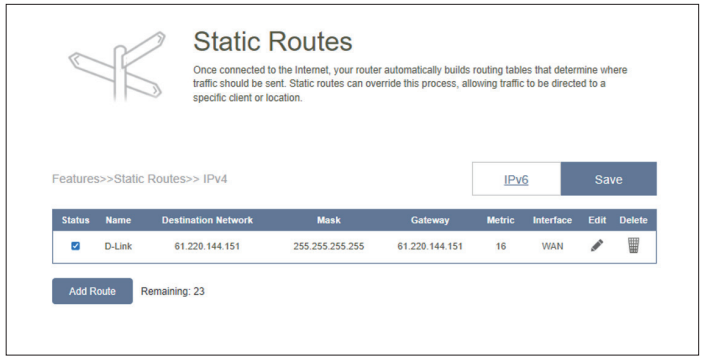
External Port If you select TCP, UDP, or Both as the protocol, enter the public port you want to forward.

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 Schedule section. Refer to Time & Schedule - Schedule on page 95 for more information.

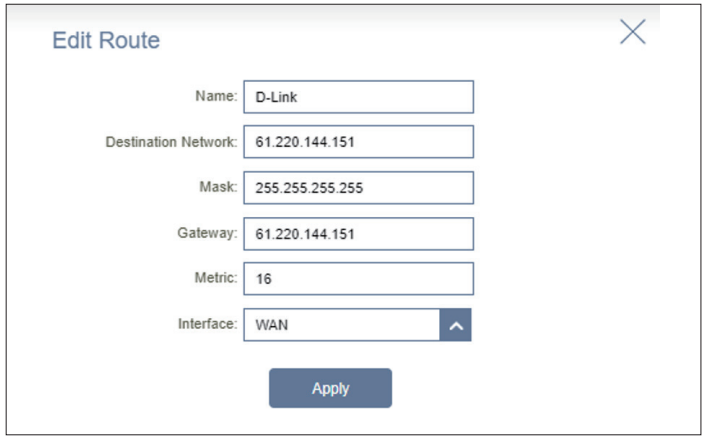
Static Routes - IPv4

The Static Routes section allows you to define custom routes to control how traffic moves around your network.



In the **Features** tab on the left side of the page, click **Static Routes**. To configure IPv6 routes, click **IPv6** and refer to **Static Routes - IPv6** on **page 88**. To return to the main **IPv4 static routes** page, click **IPv4**.

To remove a rule, click on the trash can icon in the Delete column. To edit a rule, click on the pencil icon in the Edit column. To create a new route, click the **Add Route** button. Click **Save** when you are done. If you edit or create a route, the following options will appear:



Name Enter a name for the route.

Destination Network Enter the destination IP address of this route.

Mask Enter the subnet mask of the route.

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

Metric The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 represents the lowest cost and 16 the highest cost.

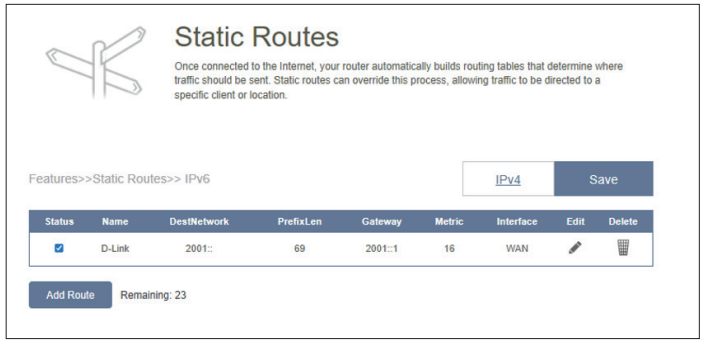
Interface Select an interface that the IP packet must use to transit out of the router when this route is in use.

Click **Apply** when you are done.

Static Routes - IPv6

To configure IPv6 routes, click **IPv6** on the **Static Routes** page. To return to the main **IPv4 static routes** page, click **IPv4**.

To remove a rule, click on the trash can icon in the Delete column. To edit a rule, click on the pencil icon in the Edit column. To create a new rule, click the **Add Rules** button. Click **Apply** when you are done. If you edit or create a rule, the following options will appear:



Name Enter a name for the route.

DestNetwork This is the IP address of the router used to reach the specified destination.

PrefixLen Enter the IPv6 address prefix length (64-128) of the packets that will take this route.

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

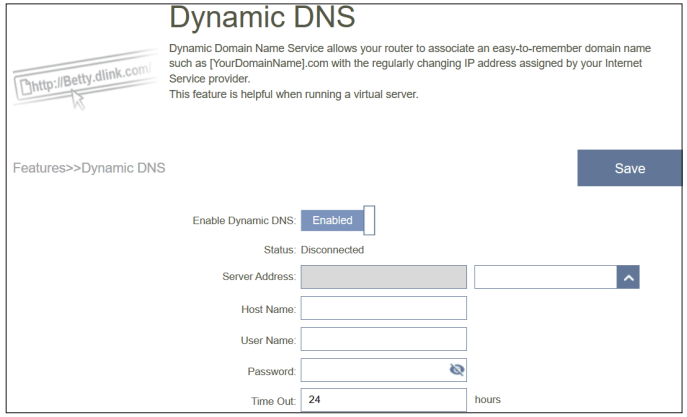
Metric The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 represents the lowest cost and 16 the highest cost.

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

Dynamic DNS

Most ISPs assign dynamic IP addresses. A dynamic DNS service provider allows users to enter their domain name in their web browser to connect to the server no matter what their IP address is. This feature is helpful when running a virtual server. Click **Save** at any time to save the changes you have made on this page.

In the **Features** tab on the left side of the page, click **Dynamic DNS**.



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 username.

Password Enter your dynamic DNS password.

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

Dynamic DNS

At the bottom of the page are the IPv6 host settings. A maximum of 10 records can be defined. To remove a record, click on its trash can icon in the Delete column. To edit a rule, click on its pencil icon in the Edit column. To create a new record, click the **Add Record** button. Click **Save** when you are done. If you edit or create a record, the following options will appear:

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

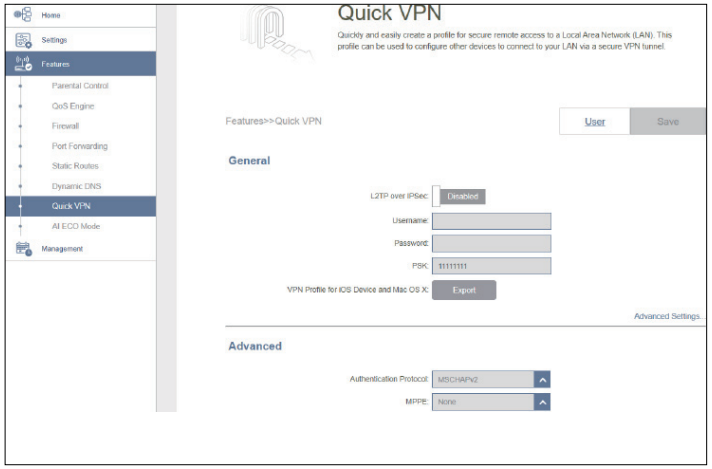
IPv6 Address Enter the IPv6 address of the dynamic DNS server. Alternatively, select the server device in the drop-down menu.

Click **Apply** when you are done.

Quick VPN

In the **Features** tab on the left side of the page, click **Quick VPN**. This page will help you configure the Quick VPN feature of your router. 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 101.** 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 between 1 and 20 characters.

Password Enter a password between 10 and 32 characters that must contain both numbers and letters.

PSK Enter a passkey between 8 and 64 characters that must contain both numbers and letters.

VPN Profile for iOS Device and MAC OS X Click export to save the VPN profile settings file for iOS devices or Mac OS X. Import the profile on iOS and Mac OS X to configure VPN client settings automatically.

Advanced Settings...

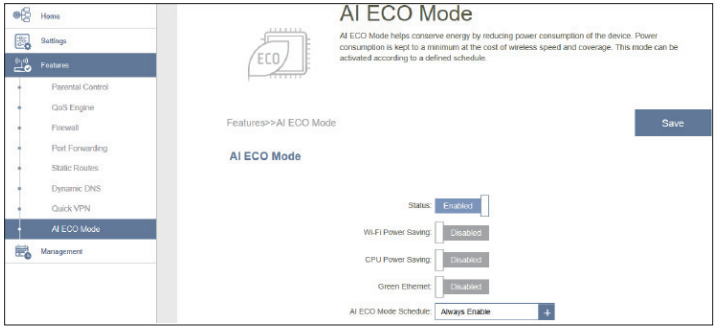
Authentication Protocol Choose an authentication protocol type: MSCHAPv2, PAP, or CHAP. MSCHAPv2 is the default.

MPPE Select encryption cipher strength: None, RC4-40, or RC4-128. None is the default.

AI ECO Mode

In the **Features** tab on the left side of the page, click **AI ECO Mode**. This page allows you to enable various power-saving features to help conserve power consumption of the router and further contribute to green environment.

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



Status Enable or disable AI ECO Mode. The mode will automatically adjust the transmission power of the wireless function as well as the power usage of other functions such as CPU compute power and green Ethernet depending on the respective activities of these functions. Enable Status to display available modes.

Wi-Fi Power Saving Enable Wi-Fi Power Saving to reduce wireless transmission power to save the overall power usage. Note that the Wi-Fi coverage or speed will also be reduced.

CPU Power Saving Enable CPU Power Saving to reduce CPU compute power to save the overall power usage. Note that the compute performance of the router will be affected.

Green Ethernet Enable Green Ethernet to reduce transmission power of the Ethernet ports when the ports are inactive or short cables are used.

Schedule Use the drop-down menu to select a time schedule during which the rule will be active. The schedule may be set to **Always Enable**, or you can create your own schedules.

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.

Management
Time & Schedule - Time

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

In the **Management** tab on the left side of the page, click **Time & Schedule**. To configure the Schedule settings, click the Schedule tab. Refer to **Time & Schedule - Schedule** on **page 95**. Click **Save** at any time to save the changes you have made on this page.

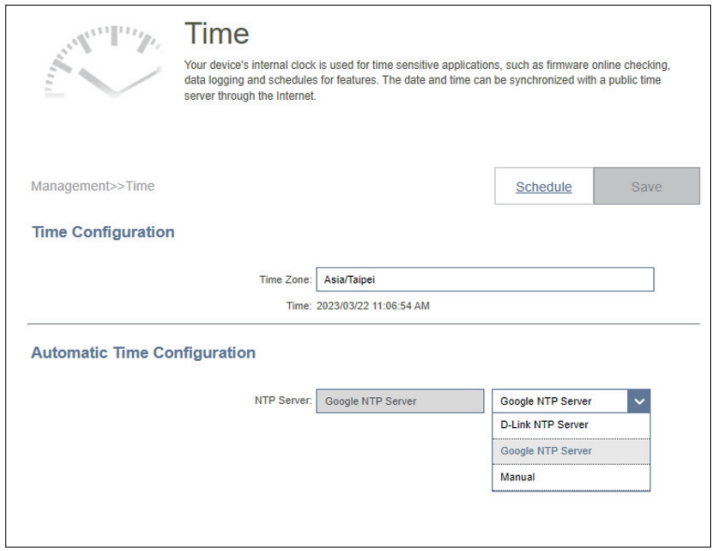
Time Configuration

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

Time Displays the current date and time of the device.

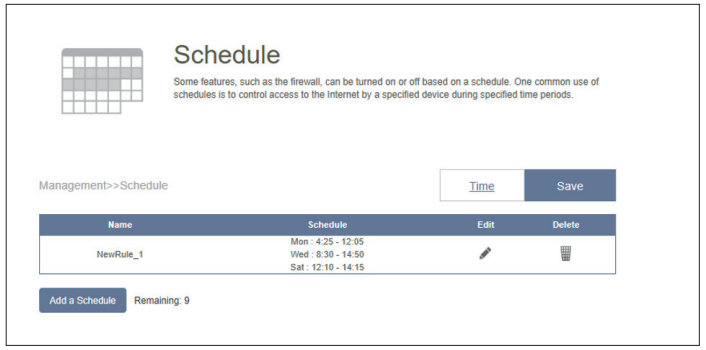
Automatic Time Configuration

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



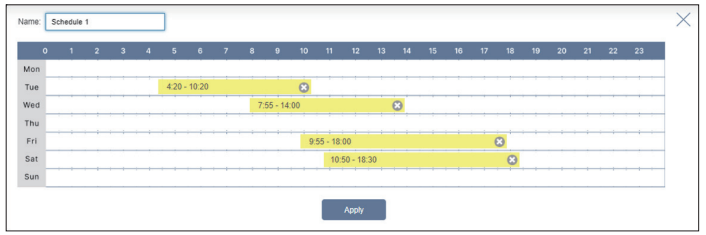
Time & Schedule - Schedule

Some functions can be controlled through a pre-configured schedule, for example, firewall settings such as IPv4/IPv6 Rules and Port Forwarding. To create, edit, or delete schedules, click **Schedule** from the **Time** page . To return to the **Time** page, click **Time**.



To remove a rule, click on the trash can icon in the Delete column. To edit a rule, click on its pencil icon in the Edit column. If you wish to create a new schedule, click the **Add a Schedule** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:

Schedule Configuration



Name Enter the name of your schedule in the **Name** field.

Schedules 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

The router keeps a running log of events. This log can be sent to a Syslog server or your email address. In the **Management** tab on the left side of the page, click **System Log**. Click **Save** at any time to save the changes you have made on this page.

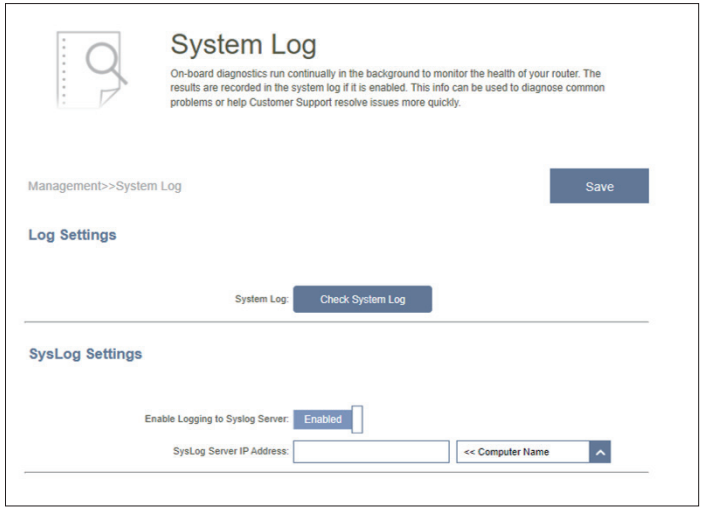
Log Settings

System Log Click the **Check System Log** to download a copy of the system log to your hard drive. You can view the log entries by opening them with any text editing applications, such as WordPad, on Windows.

SysLog Settings

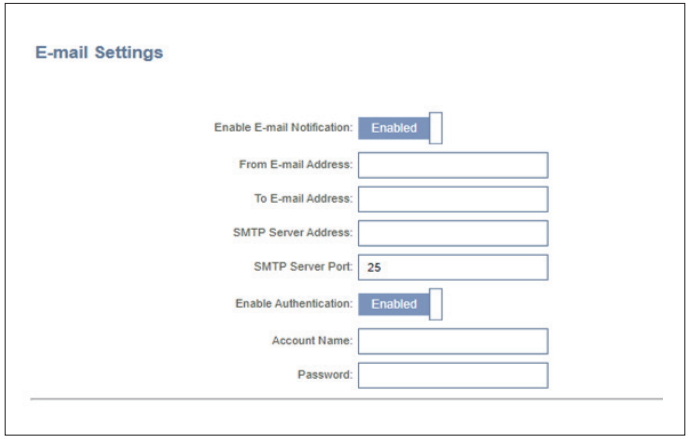
Enable Logging to Syslog Server Enable this function to send the router's logs to a SysLog Server.

Syslog Server IP Address If **Enable Logging to Syslog Server** is **Enabled**, enter the IP address of the Syslog server. Or, select from the drop-down menu for IP address auto-population if the Syslog server is connected to the router.



System Log

Email Settings



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

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.

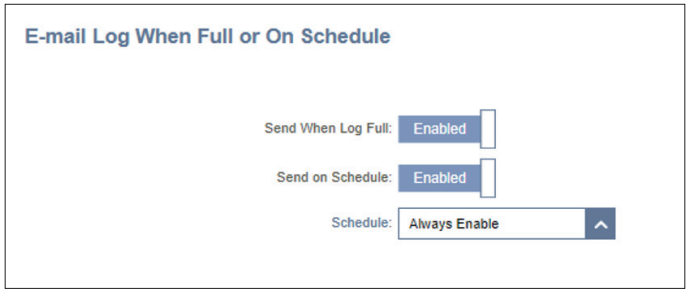
SMTP Server Port Enter your SMTP server port. The default is 25.

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.

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 **Schedule** section. Refer to **Time & Schedule - Schedule** on **page 95** for more information.

System Admin
Admin

This page allows you to change the administrator (Admin) password and enable the HTTPS server. In the **Management** tab on the left side of the page, click **System Admin**. 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 adhere to the following rule:

- Contain 10 to 15 characters
- Contain both numbers and letters
- Not contain two identical letters or digits in a row

Advanced Settings - Administration

Enable HTTPS Management Enable router management using an encrypted HTTP connection. It is enabled by default.

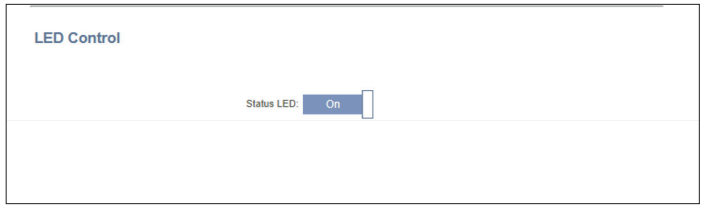
Enable HTTPS Remote Management Enable remote management over the Internet. Turn on the **Use HTTPS** option below if encrypted communication should be enforced.

Remote Admin Port The port number used for accessing the device's web management interface. The default port number is **8081.**

Use HTTPS If you enabled **Use HTTPS**, you must enter https:// at the beginning of the address for secure remote access.

Admin

LED Control

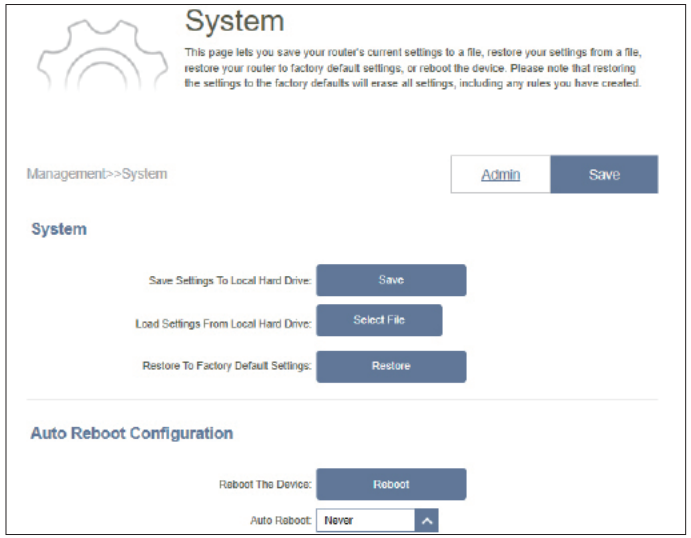


Status LED Choose to enable or disable the status LED indicator on the router and other mesh point(s). When disabled, the LED will no longer light up solid white during normal operation and will instead turn off.

The LED will still light up with the corresponding color and mode in any of the following circumstances:

System

This page allows you to backup, restore configuration settings or restore settings from a previous backup, reset, and set up a reboot schedule for the device. On the **System Admin** page, click **System**. Click **Save** at any time to save the changes you have made on this page.

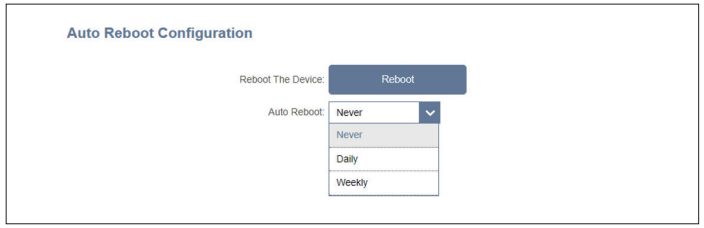


System

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 Click **Restore** to restore all configuration settings back to the settings that were in effect at the time the device was shipped from the factory. Any settings that have not been saved will be lost, including rules that you have created.



Auto Reboot Configuration

Reboot the Device Click **Reboot** to reboot the device immediately.

Auto Reboot Use the drop-down menu to select a schedule for the device to automatically reboot. The schedule may be set to **Never**, **Daily**, or **Weekly**. You may set a specific hour and minute for daily reboot or choose a day and time for weekly reboot.

User

The User section is used to create, manage, and delete user accounts that have access to certain router services. In the **Management** tab on the left side of the page, click **User**.

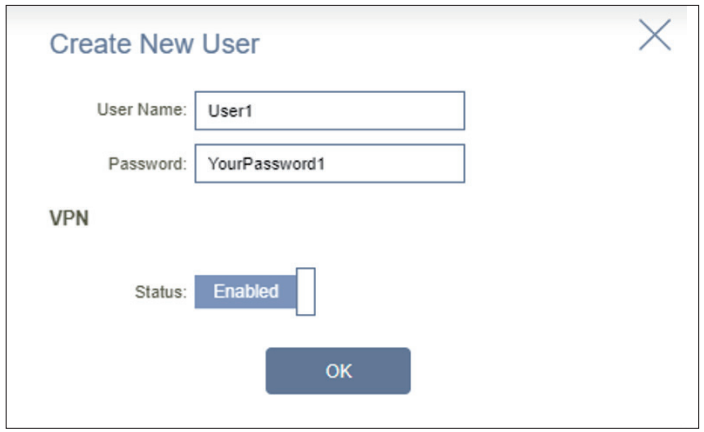
Click **Save** at any time to save the changes you have made on this page.

To remove a user, click on the trash can icon in the **Delete** column. To edit a user, click on the pencil icon in the **Edit** column.

To create a new user, click the **Create User** button.

User Name Enter a username for the new user account.

Password Enter a password for the new user account.



VPN

Status Enable or disable VPN functionality for this user.
If enabled, you can use **Export VPN Profile** to export VPN configuration profile for quick connection setup.

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

Upgrade

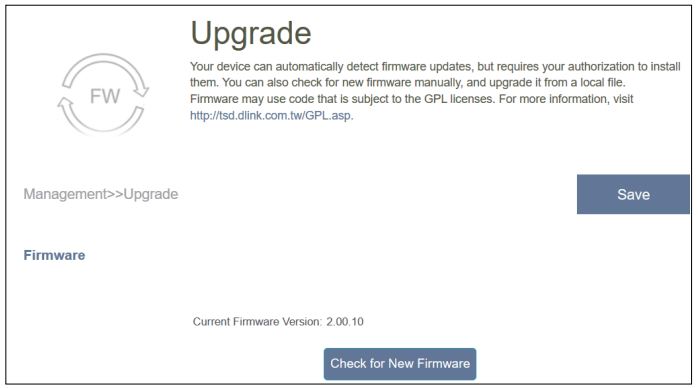
This page allows you to upgrade the router's firmware, either automatically or manually. To manually upgrade the firmware, you must first download the latest firmware file from **http://support.dlink.com**.

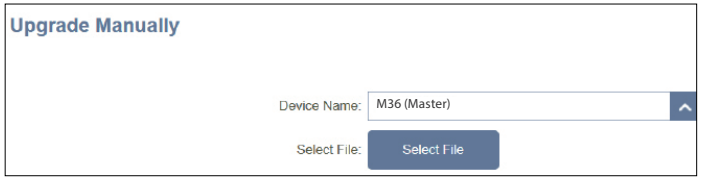
In the **Management** tab on the left side of the page, click **Upgrade**. Click **Save** at any time to save the changes you have made on this page.

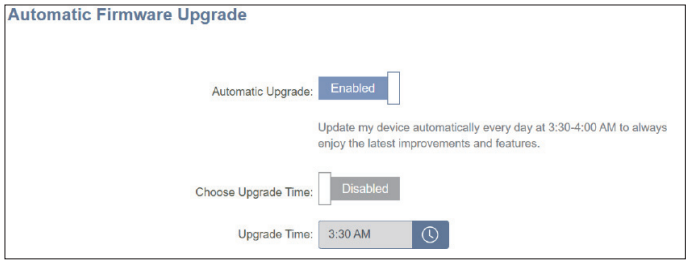
Firmware Information	
Master	Displays the name of the master router.
Firmware Version	Displays the current firmware version of the router.
Check for New Firmware	Click this button to prompt the router to automatically check for a new firmware version. If a newer version is found, click **Upgrade Firmware** to download and install the new firmware.

Advanced Settings... Upgrade Manually	
Device Name	Select a device in the mesh network for manual update.
Select File	Click the **Select File** button and browse your computer to locate the firmware file you want to install. With the file selected, click **Upload** to begin the upgrade process.

Automatic Firmware Update	
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's automatic firmware upgrade 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

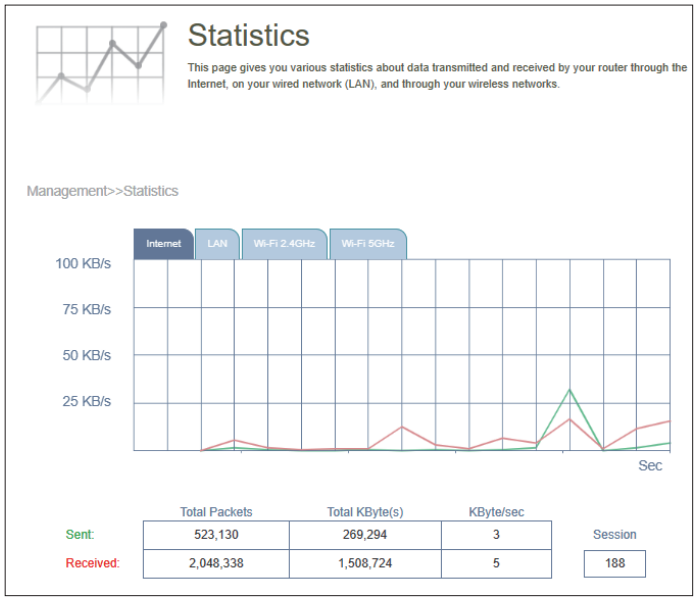
On the **Statistics** page, you can view the amount of packets that pass through your Internet and LAN interfaces as well as the traffic from Wi-Fi 2.4 GHz and Wi-Fi 5 GHz networks.

In the **Management** tab on the left side of the page, click **Statistics**.

Router

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 once the device is rebooted.



AQUILA PRO AI

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

AI Wi-Fi Optimizer: Enable this feature to always connect to the cleanest Wi-Fi Channel with enhanced transmission efficacy using the breakthrough beamforming technology, and receive weekly Wi-Fi usage on individual devices and bandwidth utilization reports for continual Wi-Fi environment improvements.

AI Traffic Optimizer: The intelligent QoS engine controls the traffic flow intelligently by automatically prioritizing traffic accordingly to improve the overall user experience.

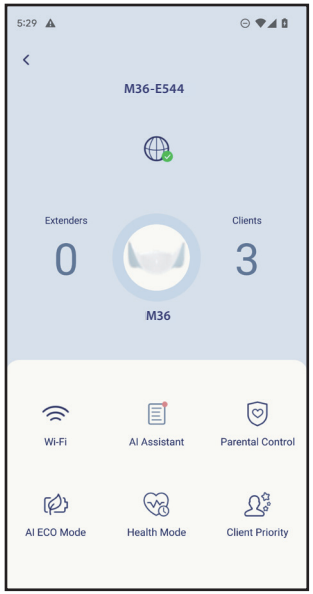
AI Assistant: The Message Center offers weekly insights into bandwidth usage and lets you manage the activity of high-traffic clients during nighttime. It also logs all enhancements made by the AI-assisted Wi-Fi Optimizer, keeping you informed about the wireless environment.

AI ECO Mode: The AI ECO Mode can be scheduled to automatically save power during specified time periods. It optimizes power consumption in three key areas: Wi-Fi power, CPU performance, and Green Ethernet.

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

AI Wi-Fi Optimizer:

From the home screen of the selected device, tap **Wi-Fi**. At the bottom of the screen, tap **AI Wi-Fi Optimizer**. Tap the slider and check if your **AI Wi-Fi Optimizer** is enabled as default. Your wireless connection will automatically adopt an interference-free channel and you will receive weekly Wi-Fi environment report every Monday at 8 AM local time.

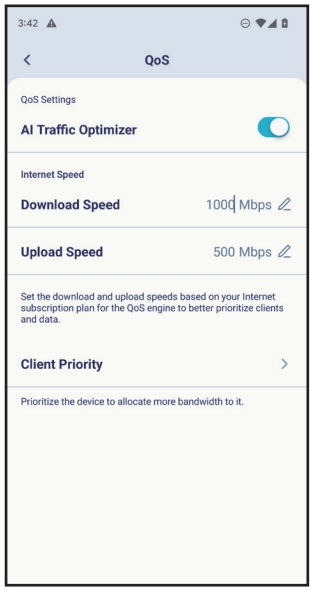


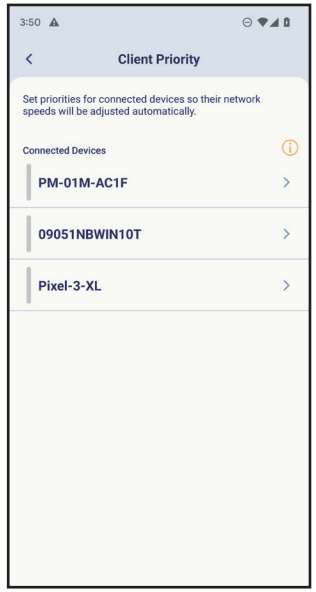
AI Traffic Optimizer:

From the home screen, tap the main router, then scroll down **Device Info** and go to **Settings,** and tap **QoS**. There, slide the toggle on for **AI Traffic Optimizer.**

Before you start the AI Traffic Optimizer, you can input the download and upload speeds to assist the QoS engine in distributing the bandwidth to prioritized clients.

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

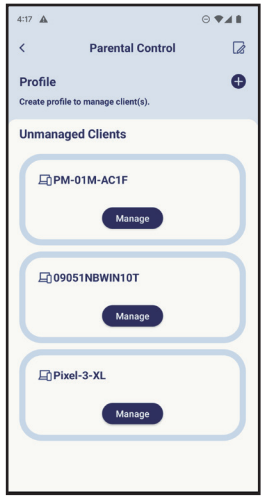


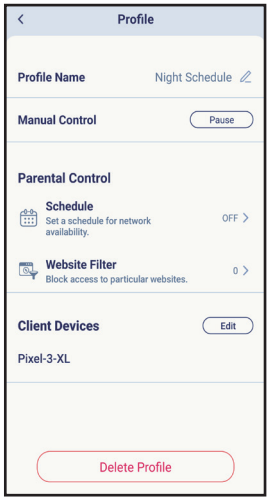


AI Parental Control:

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 continue configuring Internet schedules and website filters.
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.



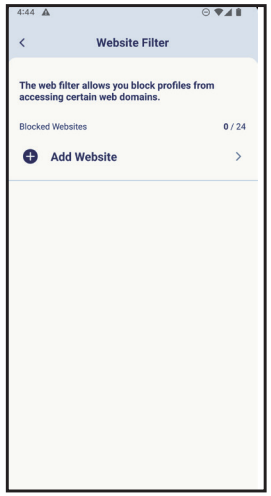


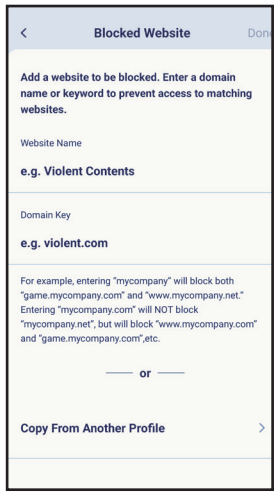
Schedule

You can set a custom schedule and/or bedtime schedules to restrict Internet access during the defined days and time periods. For bedtime scheduling, select days of the week with restricted time periods. Up to 2 bedtime schedules can be defined. For custom scheduling, tap on a cell (or time slot) and drag to the desired end time slot. You can long-press on a cell to define the time periods more precisely in 5-minute intervals.

Website Filter

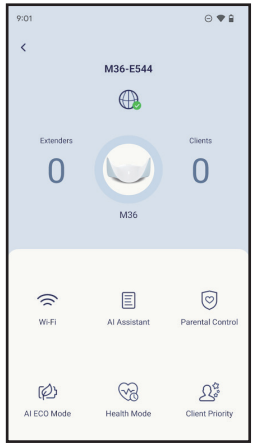
You can also block specific websites. To do this, tap **Website Filter**, tap **Add Website**, then enter a website name and the domain key. For example, violent and violent.com. The Website Name can be used to block websites containing the specified keyword (for example, "violent" will block ABC.violent.com and www.violent.net, etc.). The domain key can be used to block websites with a specific domain name (for example, "violent.com" will block both www.violent.com and ABC.violent.com as well as other subdomains). Then tap **Add** in the upper right corner.

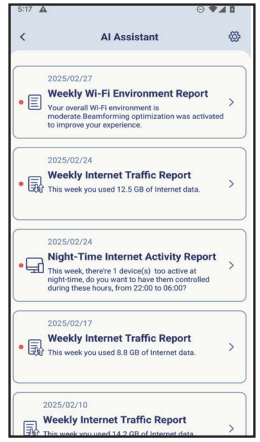


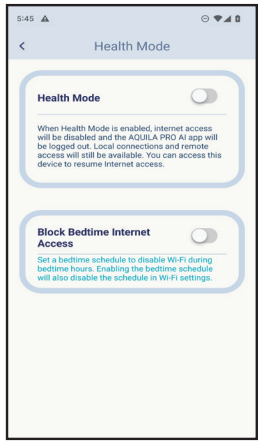


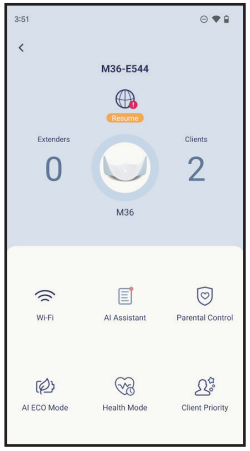
AI Assistant:

Tap **AI Assistant** to display the weekly report on bandwidth consumption. The weekly report also gives information on the number of times the system performs traffic management automatically when congestion occurs, and provides qualitative rating on your Wi-Fi environment. Furthermore, the **Nighttime Internet Activity** informs you about the overly active Internet access during nighttime. The app enables you to proactively improve sleep quality by restricting Internet access during nighttime. Tap **Health Mode** to disable Internet access for all client connections immediately or to set the bedtime during which Internet access will be blocked. Note these settings in Health Mode prevail over Wi-Fi Schedules. When Health Mode is enabled, you can still log in to the device and resume Internet access anytime (tap the Internet icon with the exclamation mark (!) on the Home screen of the main device).









AI ECO Mode:

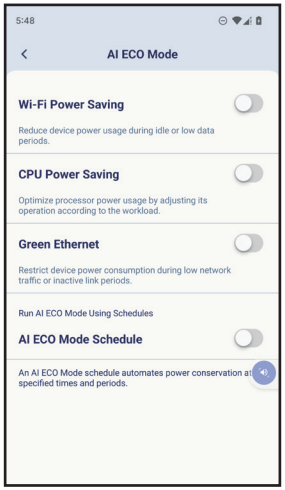
Tap **AI ECO Mode** to access power-saving features that help you save energy and extend product lifespan. You can turn on the following mechanisms individually:

Wi-Fi Power Saving: Reduce power usage when the wireless network is idle or transmitting minimal data.

CPU Power Saving: Optimize CPU power consumption based on workload.

Green Ethernet: Lower power consumption when Ethernet ports are inactive or transmitting low amounts of data.

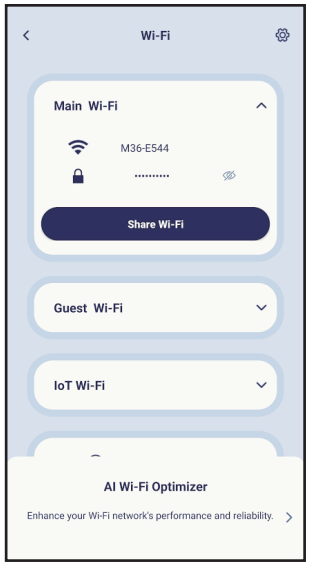
AI ECO Mode Schedule: Enable AI ECO Mode according to a predefined schedule. To set a schedule, tap on a cell (or time slot) and drag to the desired end time slot. For more precise control, long-press a cell to adjust the time in 5-minute intervals.



Other Features

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:



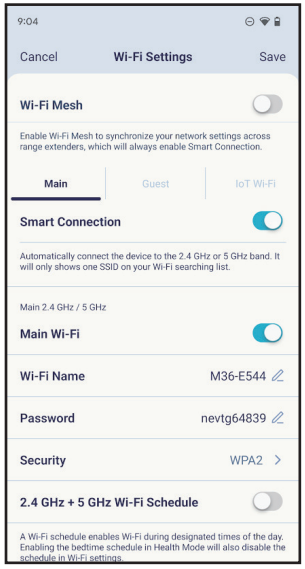
Main Wi-Fi: The primary Wi-Fi used by trusted devices such as computers, NAS, mobile devices for works and leisure.

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 or editing utilities installed on your phone with other devices.



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

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

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, or WPA2. It is recommended that you use the strongest security protocol - WPA3.

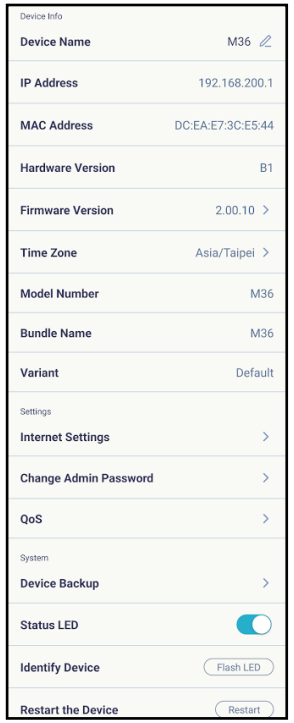
Wi-Fi Schedule: Select the time during which the wireless network will be available.

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

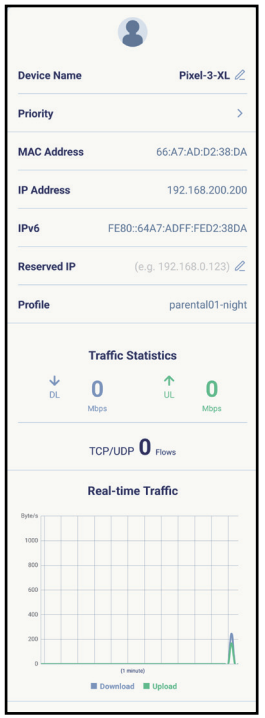
After changing the configurations on this page, click **Save** at the top right.

Device Information and Settings

From **Home**, tap the device (**main router)** in the mesh network topology to view its information and settings: name (modifiable), IP and MAC address, hardware and firmware version (firmware update), time zone (modifiable), 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: Device Backup, Status LED On/Off, identfy Device, and Restart the Device.

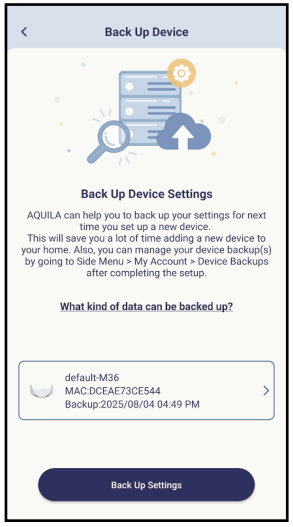


Device Backup: Help you save your current settings to expedite device configuration when installing new devices. The following settings will be saved to your account: Wi-Fi Settings, Internet Settings including WAN and VLAN configuration, Firmware Update Settings, and Operation Mode. Tap **Back Up Settings** to save a copy of your current device configuration and accept Terms and Conditions to continue. You can manage your backups later by deleting them.



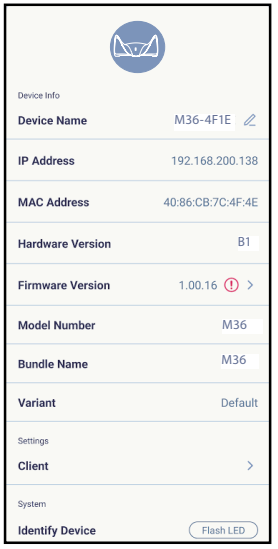
Client Information and Statistics

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, priority, and parental control profile. It also displays real-time traffic statistics in MB/s as well as weekly traffic in MB/d for both download and upload data transmissions. The Priority function allows you to assign a High/Low priority for this device with duration parameters: Always, 1 Day, 4 Hours, 2 Hours, 1 Hour.



Extender Information

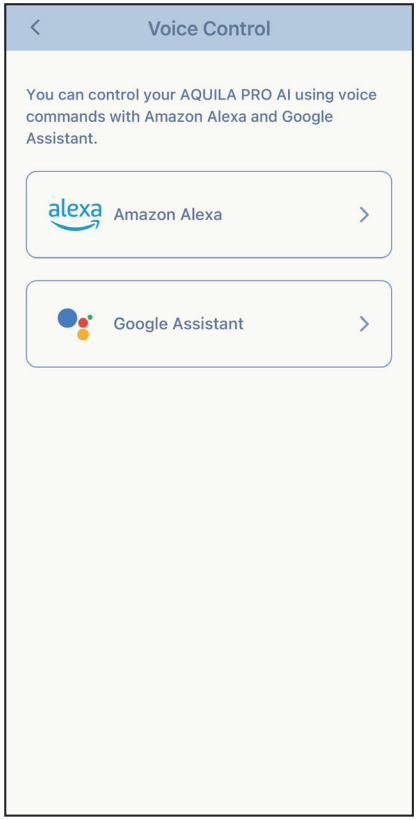
From **Home**, tap **device (Extenders)** in the mesh network topology to view the extenders currently connected with the following information: name, IP and MAC address, and hardware and firmware version. Tap **Clients** to view its currently connected clients. You can also identify the device by breathing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



Voice Control

With M36, you can give commands to your router's functionality with Amazon Alexa and Google Assistant. The voice control function lets you easily manage your network with voice commands. Features include enabling and disabling your Wi-Fi guest zone without having to go into the UI, rebooting your router and checking for its firmware upgrades. In order to use third party services to control and manage your device, please register your device with D-Link Cloud Service.

This section will go through how to set up and link your Amazon Alexa or the Google Assistant to your D-Link Cloud Service.



works with Google Home

Compatible with Alexa

Register a D-Link Cloud Service Account

Google Home Setup

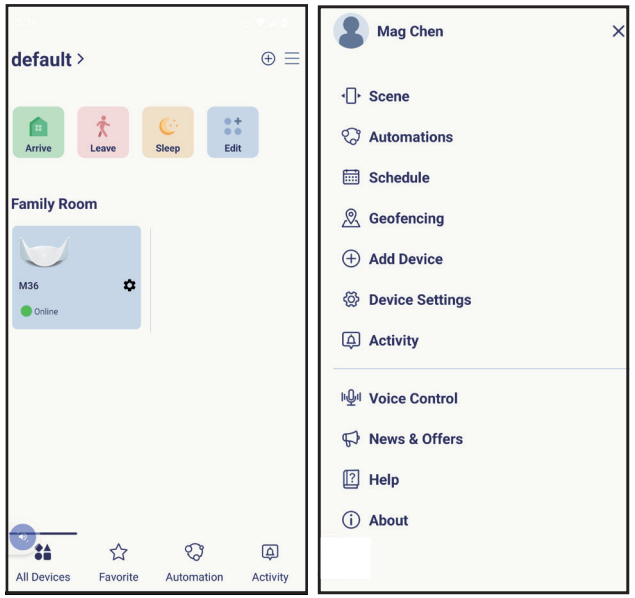
In order to use third-party apps to control and manage your device, you will first need to download Google Home app and link your D-Link account with apps such as Google Assistant.

Step 1

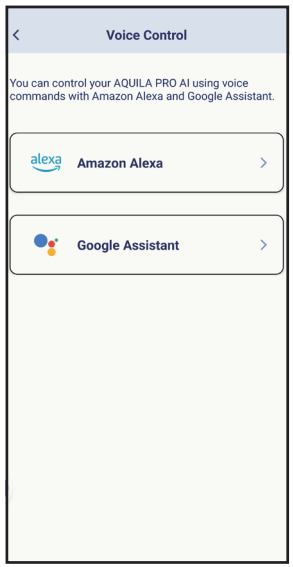
Download and launch the **AQUILA PRO AI** app.

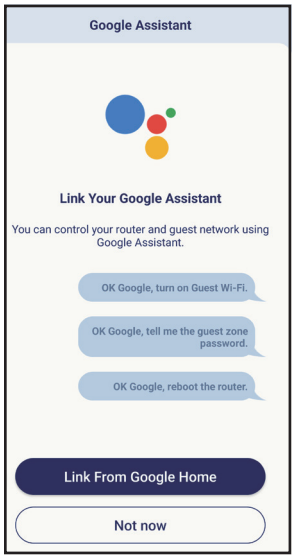
Step 2

Sign in your AQUILA PRO AI app and tap ☰ to access the side menu.
Tap **Voice Control** on the lower left.

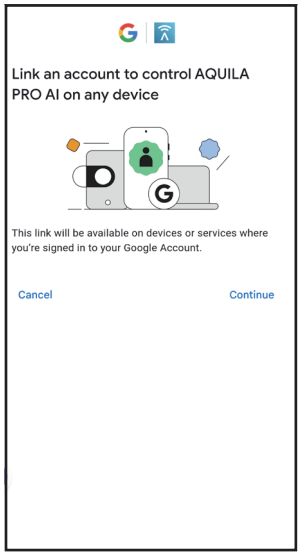


Step 3
Tap **Google Assistant** and select **Link From Google Home** on the next page.



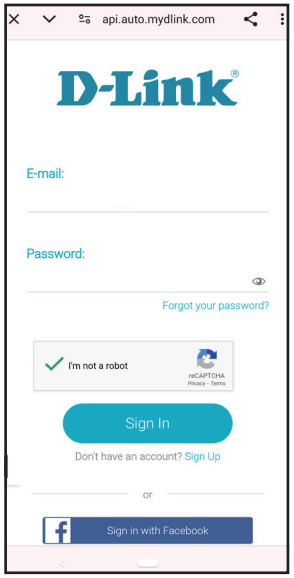


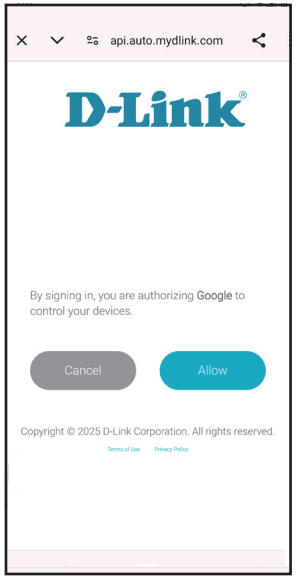
Step 4
You will be prompted with a window for linking an account to control AQUILA PRO AI on any device. Tap **Continue** to link a device.



Step 5

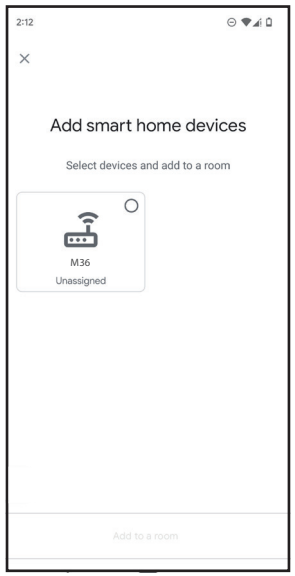
Sign in to your D-Link account and tap **Allow** to allow your router to be linked with Google Home.



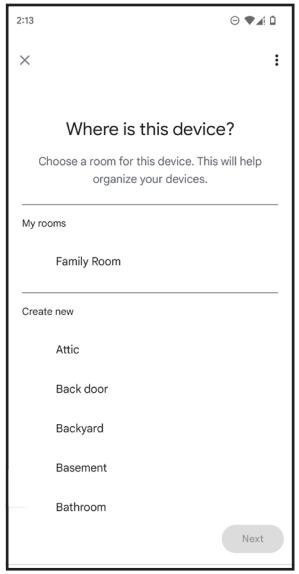


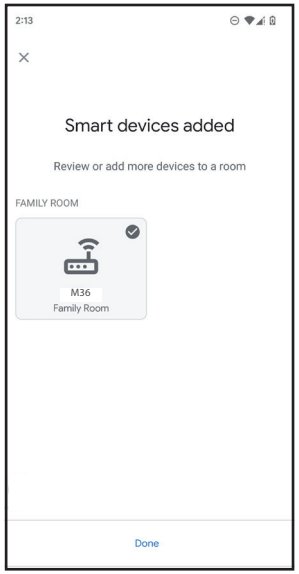
Step 6

Choose your device to add it to your smart home.

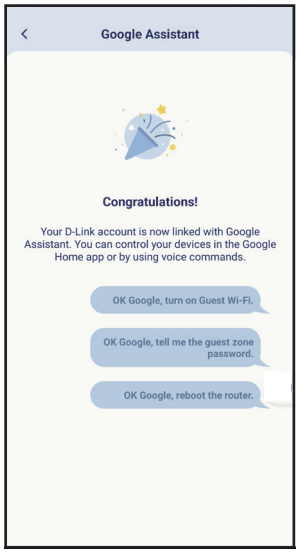


Step 7
Choose a location for your device. Then click **Done** to finish adding M36 to Google Home.





Step 8
Your device is now successfully linked with Google Home.



Amazon Alexa Setup

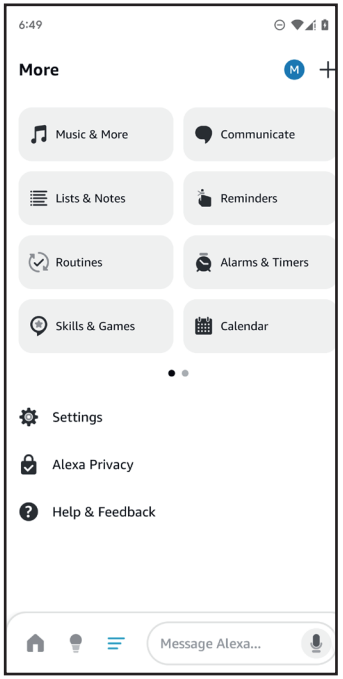
You will need the Amazon Alexa app, an Amazon account, an Amazon Alexa device and a D-Link Cloud Service account to use this feature.

Note: *The screenshots may be different depending on your mobile device's OS version. The following steps show the Android interface. If you are using an iOS device, the appearance may be different from that of the screenshots, but the process is the same.*

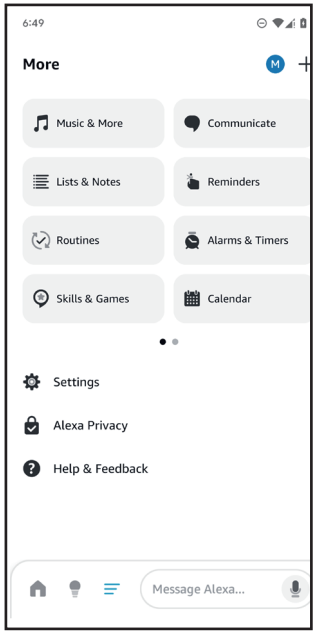
Step 1
Download and launch the **Amazon Alexa** app.

Amazon Alexa

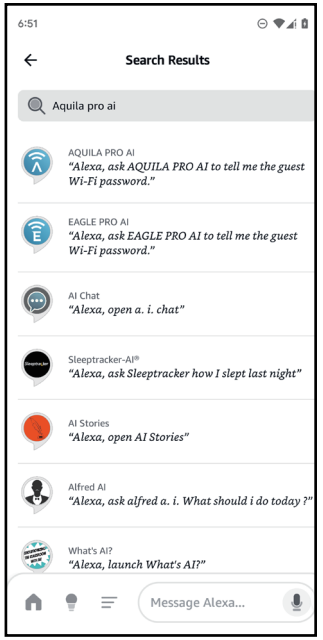
Step 2
Tap **More** at the bottom of the home screen.



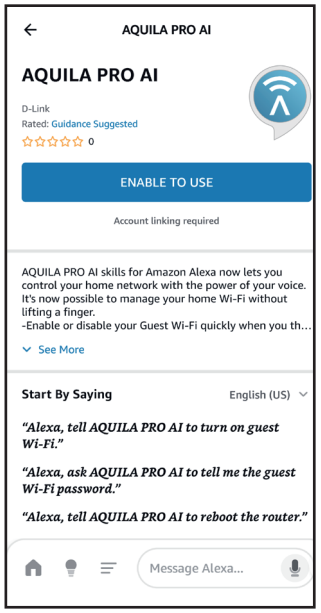
Step 3
Tap on **Skills & Games**.



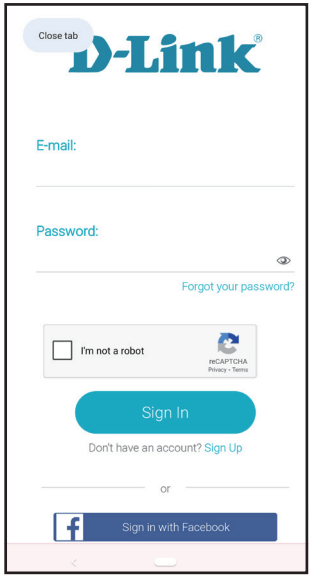
Step 4
Search for "AQUILA PRO AI". Tap on the search result.



Step 5
Tap **Enable To Use** to link the skill.

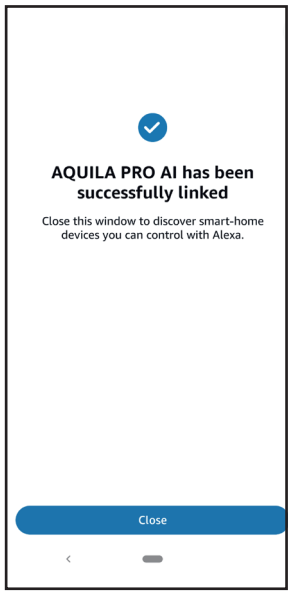


Step 6
Sign in using your D-Link account details.



Step 7

Congratulations! Your D-Link account has been successfully linked as a skill for your Amazon device. See the next page for **Amazon Alexa Voice Commands on page 119**and the tasks that you can ask your Amazon Alexa to perform.



Amazon Alexa Voice Commands

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

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

If using an Alexa speaker, start your command with one of the following:
1. "Alexa, ask AQUILA PRO AI to." Then command Alexa by saying, " Alexa, ask AQUILA PRO AI to enable my guest Wi-Fi."
2. "Alexa, talk to AQUILA PRO AI" and wait for Alexa to respond. Then say your command.

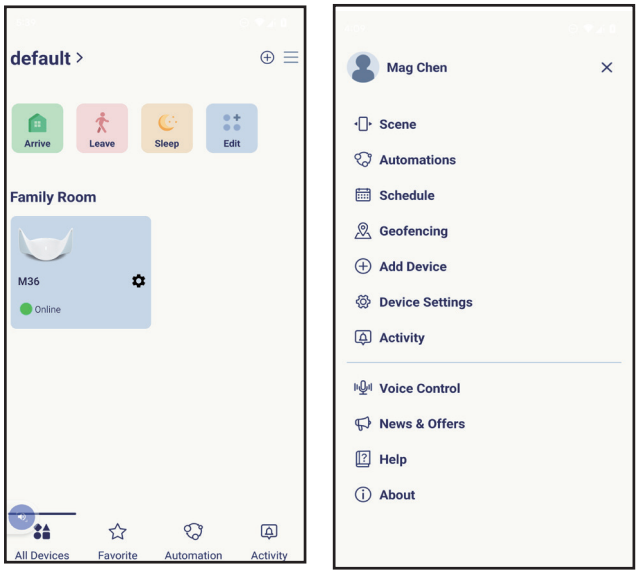
Google Assistant Setup

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

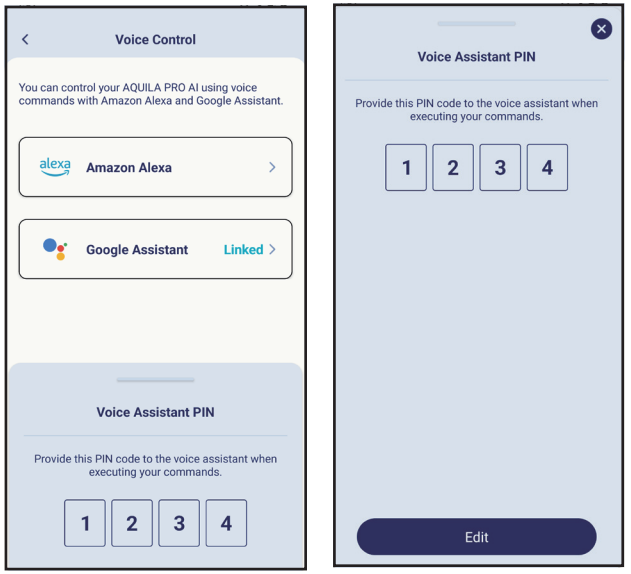
Note: *The screenshots may be different depending on your mobile device's OS version.*

Step 1

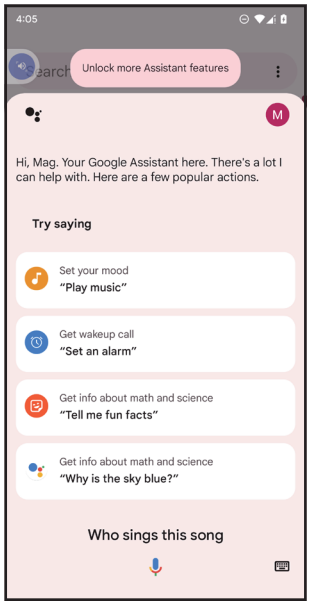
Launch the **AQUILA PRO AI** app and sign in with your account. Tap More in the top right corner of the page to access the side menu. Then, tap **Voice Control**.



Step 2
Enter **Voice Assistant PIN** to customize the pin code.



Step 3
Launch the **Google Assistant** app. You can enter your command by voice or text and provide the PIN code when prompted. Refer to the next page for **Google Assistant Voice Commands** and tasks that you can ask your Google Assistant to perform.



Google Assistant Voice Commands

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

Task	Command
Check guest Wi-Fi status.	“Is my guest Wi-Fi enabled?"
Check Wi-Fi status.	“Is my Wi-Fi enabled?"
Check guest Wi-Fi SSID.	“What is my guest Wi-Fi SSID?"
Check Wi-Fi SSID.	“What is my Wi-Fi SSID?"
Enable the guest Wi-Fi.	“Enable my guest Wi-Fi.”
Disable the guest Wi-Fi.	“Disable my guest Wi-Fi.”
Find out the guest Wi-Fi password.	“What is my guest Wi-Fi password?”
Reboot the router.	“Reboot my router."
Update the router.	“Update my router's software.”
Notes: 1. Only supported on Nest Hub with screen display. 2. Network can be substituted for Wi-Fi.	

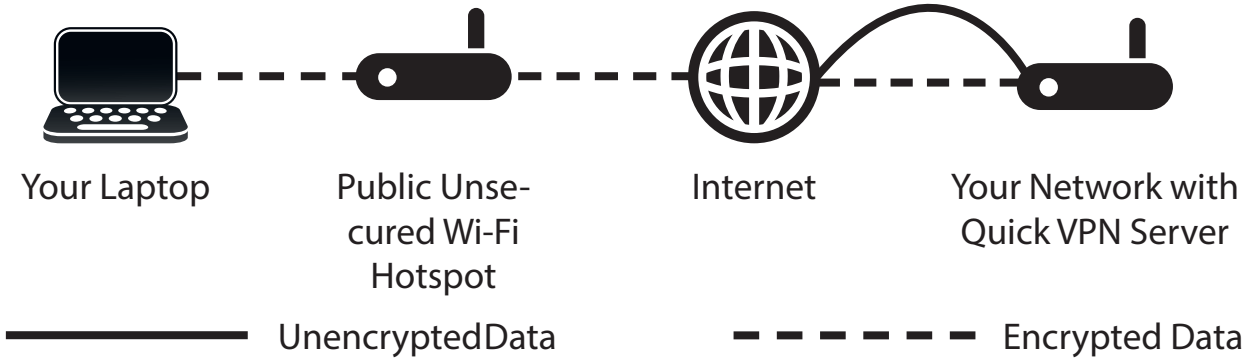
If using a Google Home speaker, start your command by saying "Hey Google.” or "OK Google."

Quick VPN

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

Without Quick VPN

With Quick VPN



Important Information

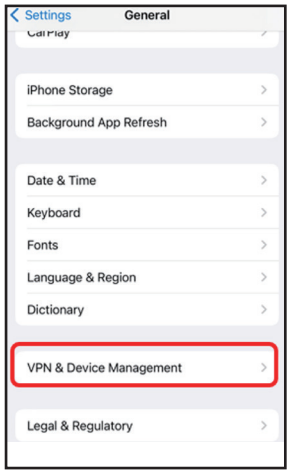
The following instructions explain and help you configure your D-Link Quick VPN enabled router and devices to create a Virtual Private Network (VPN). This feature is intended for advanced users who wish to connect remotely and use their router's Internet connection with an extra layer of security while using untrusted networks. Configure a Quick VPN Server on your router or gateway 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. 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 but not limited to Internet conditions, local and remote network Wi-Fi and WAN bandwidth limitations, and increased latency. This may negatively affect real-time voice and video communication.
- Quick VPN supports up to five concurrent VPN client sessions using the same login and password. Quick VPN uses L2TP/IPsec with MSCHAPv2, PAP, or CHAP authentication.
- You device may warn you of your information being intercepted, and you may ignore this warning since you are in control of the Quick VPN server.
- 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 and are sure you are not violating any network access rules, try to contact your ISP or network administrator.
- Devices connected via Quick VPN are assigned with 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 that 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 91** 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.

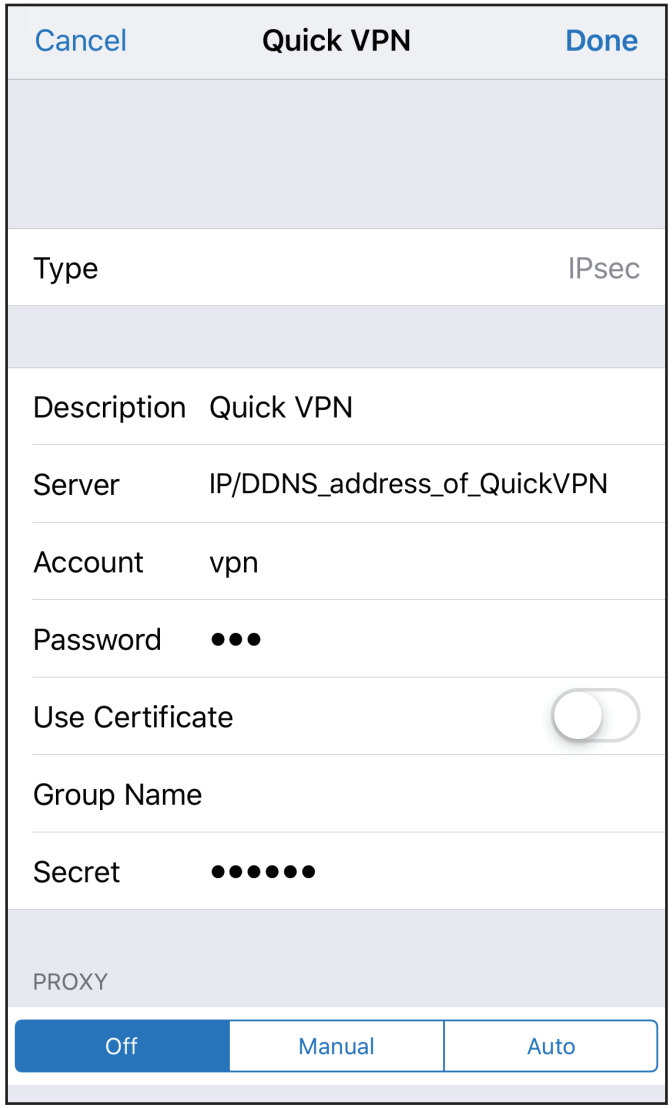
Account: Enter the Username used to authenticate login to the VPN server.

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

Secret: Enter your Passkey (PSK).

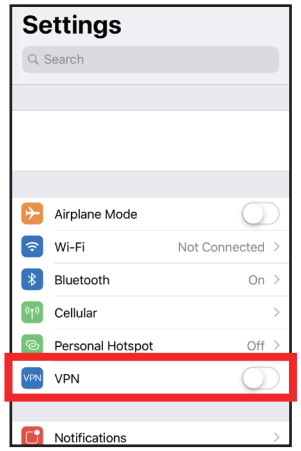
Tap **Done** at the top right corner of the page to finish adding the configuration.

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

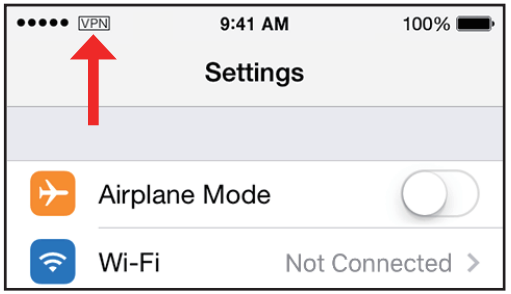


Connect or Disconnect

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



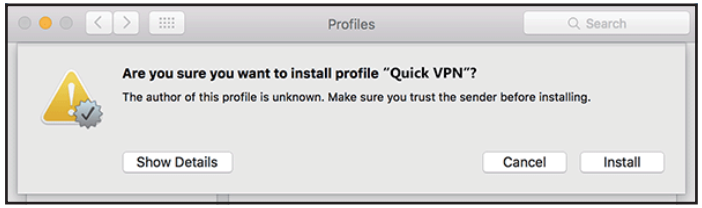
The VPN icon will appear in the notification area at the top of your screen indicating that your device is currently connected to the Quick VPN server.



Mac OS X
VPN Setup Instructions

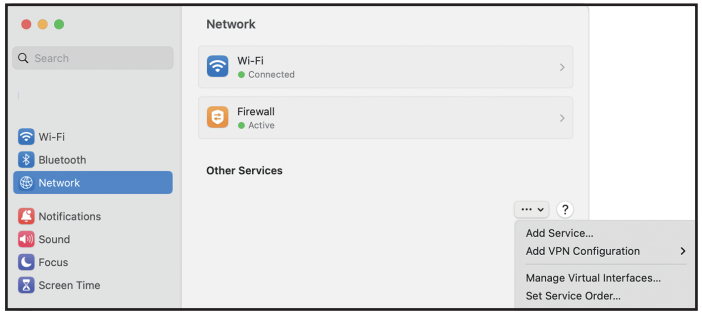
This section provides Quick VPN setup instructions for OS X using the **Export** Profile function. Refer to **Quick VPN** on **page 91** for your router's setup instructions.

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



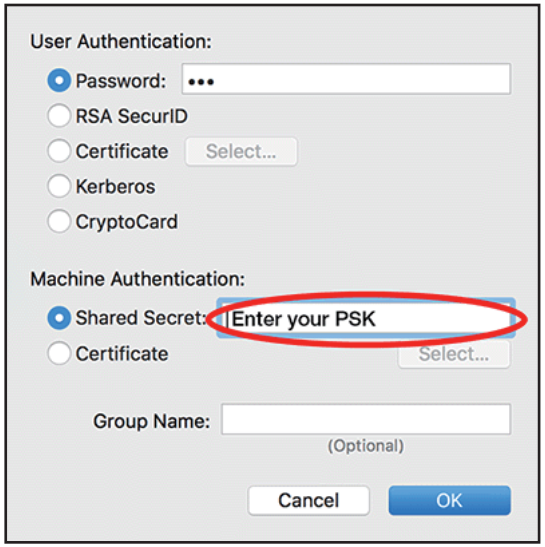
Enter your user account password when prompted. Close the **Profiles** dialogue.

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

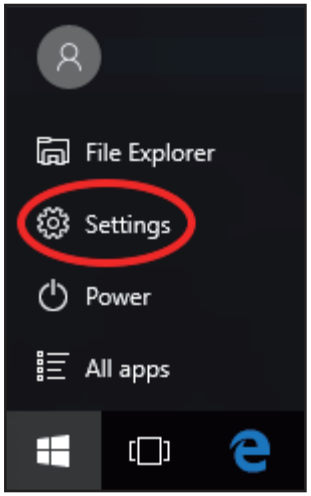
This section provides Quick VPN setup instructions for Windows 11/10. Refer to **Quick VPN** on **page 91** for your router's setup instructions.

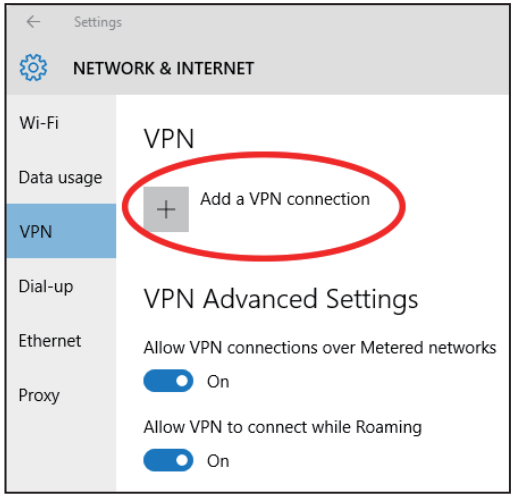
This section provides Quick VPN setup instructions for Windows 11/10.

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**.

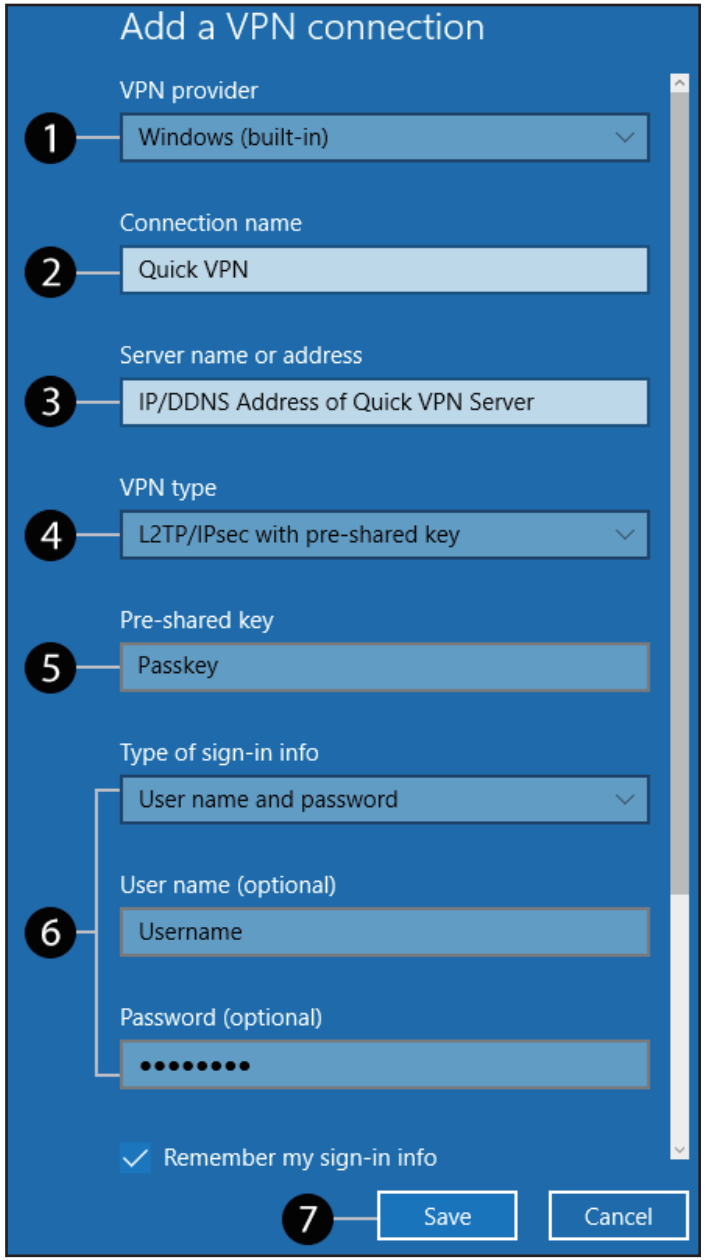




1. Select **Windows (built-in)** from the **VPN Provider** drop down menu.
2. Create a name for your VPN connection.
3. Enter your **IP/DDNS address** of your Quick VPN server.
4. Select **L2TP/IPSec with pre-shared key** from **VPN type**.
5. Enter the **Passkey.**
6. Select **User name and password**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

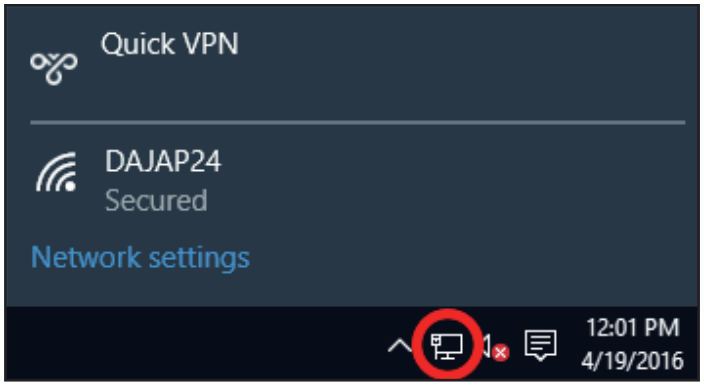
   If you would like windows to remember your sign-in information, enter your **User name, Password,** and select **Remember my sign-in info**
7. Choose **Save**.

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



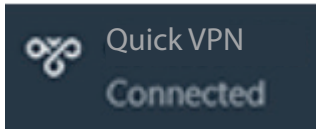
Connect or Disconnect

To connect to or disconnect from your Quick VPN server:



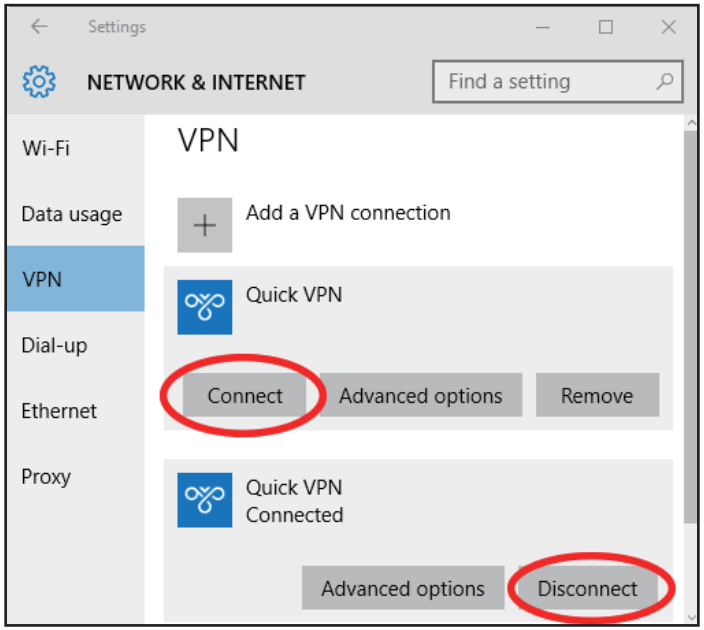
On **Windows 10**:

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**:

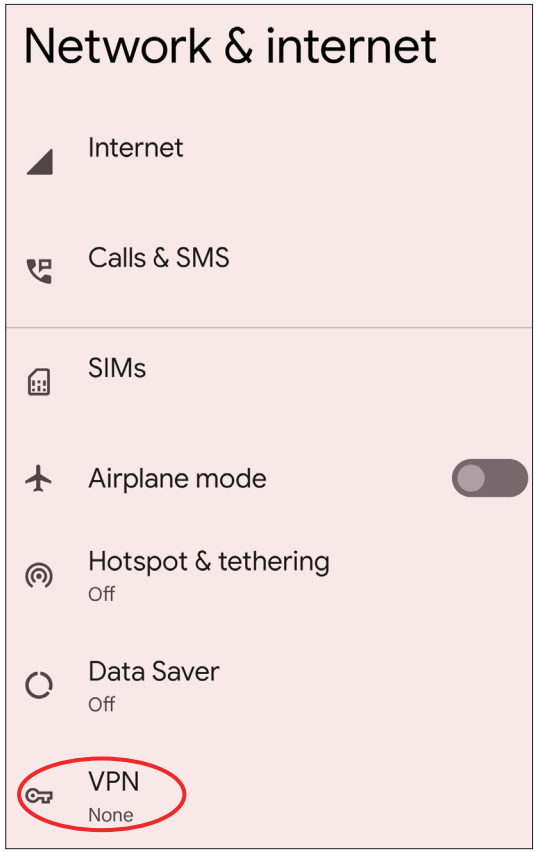
Click on the **Network, Volume, Battery** icon. .
Select the Connect or disconnect of your Quick VPN connection.
A blue shield appears when you are connected to a VPN.

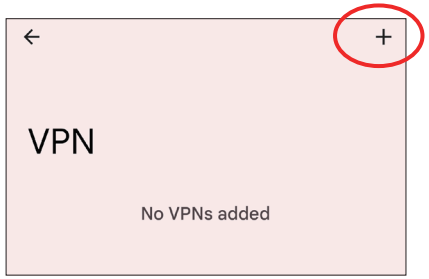


Android
VPN Setup Instructions

This section provides Quick VPN setup instructions for Android devices. Your device's screens may vary. Refer to **Quick VPN** on **page 91** for your router's setup instructions.

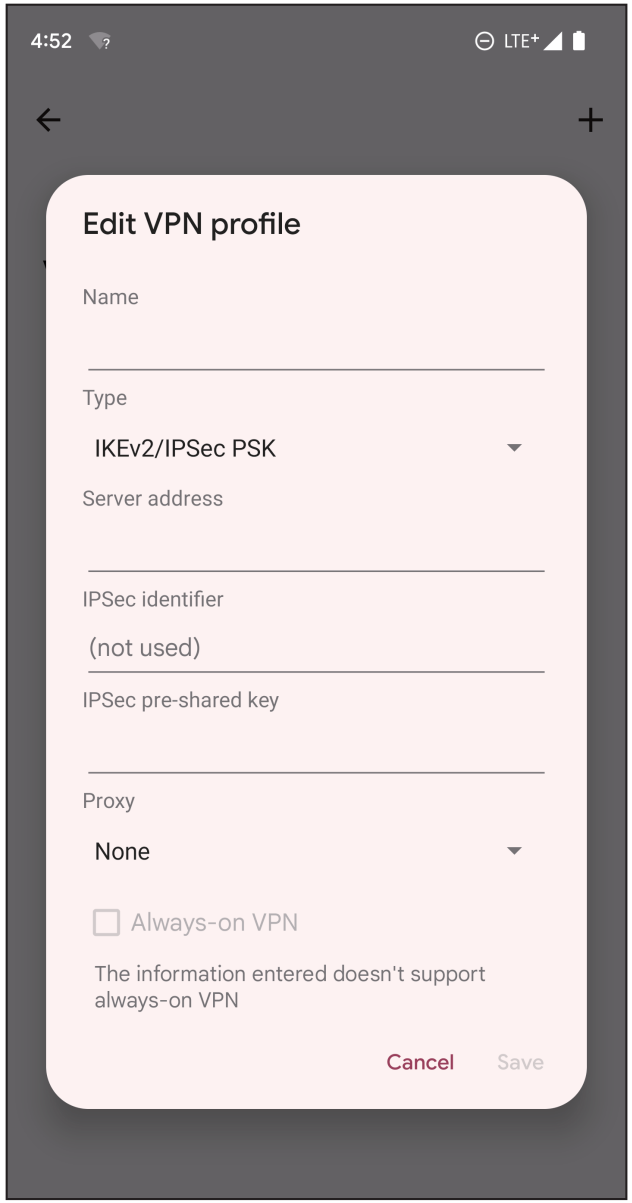
Go to **Network & Internet** > **VPN** > **+**





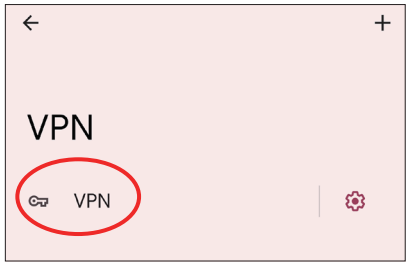
1. Enter a name for your VPN connection.
2. Select **L2TP/IPSec PSK** for **Type.**
3. Enter the **IP/DDNS address** of your Quick VPN server.
4. Enter your **Passkey** in **IPSec pre-shared key** field.
5. Choose **Save**.

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

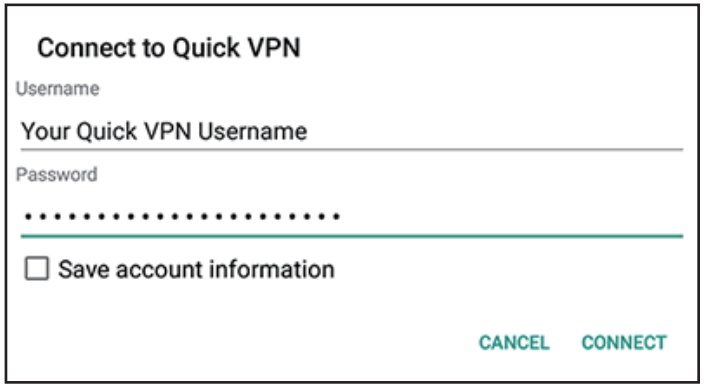


Connect or Disconnect

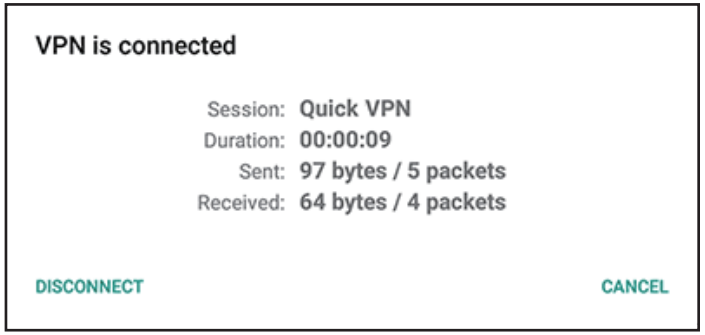
To connect to or disconnect from your Quick VPN server, go to **Network & Internet** > **VPN** and select the **Quick VPN** connection you created.



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



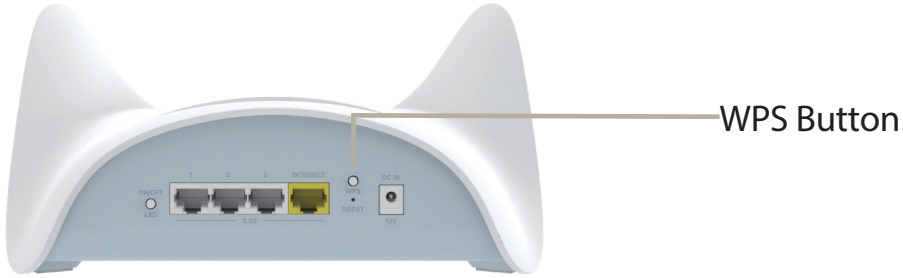
To disconnect, select **DISCONNECT**.



Connect to a Wireless Client
WPS Button

The easiest way to connect your wireless devices to your Wi-Fi network is through 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 that you can press to connect to the router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. After consulting your device's manual, follow the steps below:

Step 1 - Press the WPS button on the router for about 2 seconds. The LED on the top will start to breathe white.



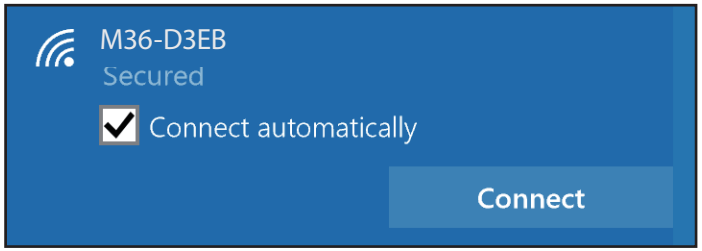
Step 2 - Within 120 seconds, press the WPS button on your wireless device (or launch the software utility and start the WPS process).

Step 3 - Allow up to 1 minute for your connection to be configured. Once the LED stops breathing, you will be connected and your wireless connection will be encrypted with WPA2.

Windows® 11/10

When connecting to the M36 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 initial configuration.

Note: To enjoy the advancements offered by Wi-Fi 7, please make sure that your operating system and wireless network adapter support Wi-Fi 7. Windows adds support for Wi-Fi 7 starting with Windows 11, version 24H2.

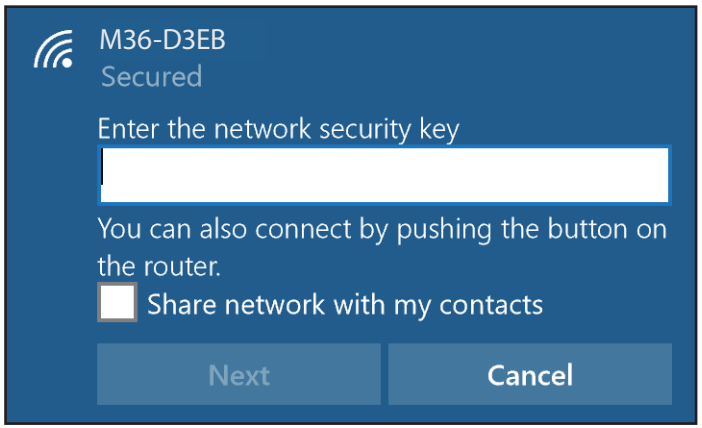


To join an existing network, locate the wireless network icon (or on Windows 10 or on Windows 11) in the taskbar. For Windows 11, select **Manage Wi-Fi connections**. Then It will display a list of wireless networks which are within your computer's range. Select a desired network by clicking on its SSID.

Or you can set up a wireless networking by visiting the Network Settings page:

On In Windows 10, select **Start** , then select **Settings** > **Network & Internet** > **Status** > **Network and Sharing Center**.

On Windows 11, select **Start**, type **control panel**, then select **Control Panel** > **Network and Internet** > **Network and Sharing Center**.



Then select **Set up a new connection or network** and follow the wizard.

To ensure automatic connection to the router when your device next detects the SSID, check the **Connect Automatically** check box.

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

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 any problems.

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

When entering the IP address of the D-Link router (**192.168.200.1** 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:

  - 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 how to disable or configure it.

- Configure your Internet settings:

  - Go to **Start** > **Settings** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**. Click the **Internet Options** under **See Also** at the bottom left. From the **Security** tab, click the **Default Level** button to reset the selected zone to default settings.
  - Click the **Connections** tab. Click the **LAN Settings** button. Make sure nothing is checked. Click **OK**.
  - Close your web browser (if opened) and re-open 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 for about 30 seconds and try to access the configuration. If you have multiple computers, try connecting using a different computer.

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

If you forget 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 for about 2-3 seconds (see **M36 Rear Panel on page 6**). Release the button and the router will go through its reboot process. Wait for about 30 seconds to access the router. The default IP address is **192.168.200.1**. When logging in, use the default device password printed on the label on the bottom of the device.

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 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. The latest W-Fi 6 generation is introduced to cope with continued increase in the number of devices demanding higher bandwidth and lower latency for responsive, multimedia-rich content.

Wireless LANs are used increasingly in both home and office environments, and at public areas such as airports, coffee shops, and universities. Innovative ways to utilize WLAN technology is 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. 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 for sensors to collect data for cloud-based applications through an Internet connection supplied through the wired LAN. A wireless router or gateway is a device used to provide this link.

What is Wireless?

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

Why D-Link Wireless?

D-Link is a worldwide leader and also award-winning designer, developer, and manufacturer of networking products. We deliver the performance you need at an affordable price, and offer all the products you need to build your network.

How does wireless technology work?

Wireless technology works just as how cordless phones work: through radio signals, data is transmitted from one point A to point B. But there are restrictions for wireless technology: how you can access the netwosrk. 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 less than those of WLAN, and WPAN in turn does not comsume 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.

Technical Advancements of Wi-Fi 7

Over these years, Wi-Fi, a collection of wireless networking protocols based on IEEE 802.11 standard, has improved continually.

The router supports Wi-Fi 7 to achieve higher reliability and lower latency. Here are some features in Wi-Fi 7 that stand out and improve over the previous wireless generations:

- 4096-QAM: The higher order Quadrature Amplitude Modulation significantly increases data throughput and capacity to more than double that of Wi-Fi 6.
- Multi Link Operation (MLO): Two channels from the same or different bands can be combined to increase the throughput and reduce latency and interference.
- Enhanced MU-MIMO (Multi-User, Multiple Input Multiple Output): Up to 16×16 MIMO configuration, doubling MIMO configuration in Wi-Fi 6
- Improved Target Wake Time (TWT): Target Wake Time (TWT) allows battery-powered devices to conserve energy by optimizing sleep and wake schedules.

These technical innovations allow for higher speeds, much less latency, more efficient communication with multiple devices simultaneously.

You have probably noticed that more and more household devices support Wi-Fi connectivity, including televisions and home surveillance equipment. As the number of wireless and IoT devices rapidly increases, Wi-Fi 7 brings improved performance for wider-range operation and tackles the problems of resource contention. It improves communication efficiency among multiple devices transmitting data at the same time to achieve better overall bandwidth utilization.

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 set up, but if you're configuring 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 configure 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 and 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 may operate on the same frequency.

Wireless Encryption
Don't let your next-door neighbors or intruders connect to your wireless network. Encrypt your wireless network by turning on the router's WPA security feature. Refer to the product manual for detailed information on how to set it up.

Wireless Security

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

- WPA2-Personal (Wi-Fi Protected Access Pre-Shared Key)
- WPA3-Personal (Wi-Fi Protected Access 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.

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.

WPA3 has the strongest encryption 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

- 3 x 2.5 Gigabit Ethernet LAN port
- 1 x 2.5 Gigabit Ethernet WAN port
- 1 x WPS Button
- 1 x Reset Button
- 1 x Power Connector
- 1 x LED on/off Button

Standards

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

Antenna Types

- 2 x 2.4 GHz internal antennas[1,2,3]
- 2 x 5 GHz internal antennas[1,2,3]

Security

- WPA2™ - Personal
- WPA3™ - Personal

WAN Connection Type

- Static IP
- Dynamic IP
- PPPoE
- PPTP
- L2TP
- DS-Lite
- 802.1p & 802.1q VLAN tagging and priority bit

Power

- 12 V / 1.5 A

Temperature

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

Humidity

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

Certifications

- FCC
- CE
- IC

Dimensions

- 192.65 x 171.42 x 92.96 mm (7.58 x 6.75 x 3.66 in)

Weight

- 557 g (19.65 oz)

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

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

FCC regulations restrict the operation of this device to indoor use only.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

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 & your body.

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.

D-Link Systems, Inc.

14420 Myford Rd. Suite 100. Irvine, CA 92606

+1 714 885 6333

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 bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;

(iii) 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

(iv) the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) shall be clearly indicated.

(v) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment :

(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 les bandes de 5250 à 5 350 MHz et de 5470 à 5725 MHz doit être conforme à la limite de la p.i.r.e;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 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;

(iv) les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3), doivent être clairement indiqués.

(v) 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 5250-5350 MHz et 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 40 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 40 cm de distance entre la source de rayonnement et votre corps.

IC Notice

Operation shall be limited to indoor use only.

Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

leur utilisation doit être limitée à l'intérieur seulement;

leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite, sauf à bord d'un gros aéronef volant à plus de 3 048 m (10 000 pi) d'altitude.

以下警語適用台灣地區
依據 低功率電波輻射性電機管理辦法

第十二條: 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條: 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

1.使用此產品時應避免影響附近雷達系統之操作。

「電磁波曝露量MPE標準值1mW/cm^2，本產品使用時建議應距離人體 22 cm」

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/cedoc.
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/cedoc.
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/cedoc 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/cedoc
English	D-Link hereby declares that this product, accessories, and software are in compliance with directive 2014/53/EU. More information about EU Declaration of Conformity please visit www.dlink.com/cedoc
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/cedoc.
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/cedoc.
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit, ces accessoires et ce logiciel sont conformes aux directives 2014/53/UE.Le texte complet de la déclaration de conformité de l'UE et le icroprogramme du produit sont disponibles au téléchargement sur la page des produits à www.dlink.com/cedoc.
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/cedoc.

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/cedoc.
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/cedoc.
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/cedoc.
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/cedoc.
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/cedoc 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/cedoc.
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/cedoc.
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/cedoc.
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/cedoc.
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/cedoc.

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/cedoc.
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/cedoc.

Warning Statement:

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

For EU/EFTA and UK(NI), this product can be used in the listed countries.

AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES
FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV
MT	NL	NO	PL	PT	RO	SE	SI	SK	TR	UK(NI)

This product can be used in the UK

UK

D-Link European Headquarter

D-Link (Europe) Ltd
3rd Floor, 166 College Road, Harrow, HA1 1BH, United Kingdom
www.dlink.com

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

A. LOW POWER INDOOR (LPI) WI-FI 6E DEVICES:

THE DEVICE IS RESTRICTED TO INDOOR USE ONLY WHEN OPERATING IN THE 5945 TO 6425 MHZ FREQUENCY RANGE IN BELGIUM (BE), BULGARIA (BG), CYPRUS (CY), CZECH REPUBLIC (CZ), ESTONIA (EE), FRANCE (FR), ICELAND (IS), IRELAND (IE), LITHUANIA (LT), GERMANY (DE), NETHERLANDS (NL), SPAIN (ES).

- 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, 5 GHz or all.

Technology	Frequency	Max. Output Power (EIRP)
5 GHz	5.15 – 5.25 GHz	200 mW
	5.25 – 5.35 GHz	200 mW
	5.47 – 5.725 GHz	1 W
2.4 GHz	2.4 – 2.4835 GHz	100 mW

NOTICE OF BLUETOOTH USAGE IN THE EUROPEAN COMMUNITY

- Devices that support Bluetooth are intended for use in all EU member states and EFTA countries.

Technology	Frequency	Max. Output Power (ERP)
Bluetooth 2.4GHz	2.4 – 2.4835 GHz	100 mW (20 dBm)

CE EMI CLASS A WARNING (only for class A product)

This equipment is compliant with Class A of EN 55032. In a residential environment this equipment may cause radio interference.

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, die 5 GHz unterstützen, unterstützen die Funktionen DFS (Dynamic Frequency Selection/Dynamische Frequenzauswahl) und TPC (Transmit Power Control/Regelung der Sendeleistung bei Funksystemen mit mobilen Teilnehmern), die bei dem Betrieb in 5 GHz innerhalb der Europäischen Gemeinschaft erforderlich sind.
- Bitte lesen Sie das Produkthandbuch oder das Datenblatt um zu erfahren, ob Ihr Produkt 2,4 GHz, 5 GHz einzeln oder kombiniert verwendet.

Technologie	Frequenz	Max. Ausgangsleistung (EIRP)
5 GHz	5,15-5,25 GHz	200 mW
	5,25-5,35 GHz	200 mW
	5,47-5,725 GHz	1 W
2,4 GHz	2,4-2,4835 GHz	100 mW

HINWEISE ZUR VERWENDUNG VON BLUETOOTH IN DER EUROPÄISCHEN GEMEINSCHAFT

- Geräte, die 2,4 GHz unterstützen, sind für die Verwendung in allen EU-Mitgliedstaaten und in EFTA-Staaten vorgesehen.

Technologie	Frequenz	Max. Ausgangsleistung (EIRP)
Bluetooth 2,4 GHz	2,4-2,4835 GHz	100 mW (20 dBm)

Gebrauchshinweise:

- Überprüfen Sie im Produkthandbuch oder im Datenblatt, ob Ihr Produkt Bluetooth Wirless nutzt, sowie die Betriebsfrequenzbänder und die maximale Funkfrequenzleistung Ihres Produkts.

WARNUNG ZUR CE EMI KLASSE A (gilt nur für Produkte der Klasse A)

Dieses Gerät entspricht Klasse A der EN 55032. In einer Wohngebäudeumgebung kann dieses Gerät Funkstörungen verursachen.

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.
- Veuillez consulter le manuel ou la fiche technique du produit pour vérifier si votre produit utilise 2,4 GHz, 5 GHz ou tous.

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.

Technologie	Fréquence	Puissance de sortie max. (EIRP)
5 GHz	5,15-5,25 GHz	200 mW
	5,25-5,35 GHz	200 mW
	5,47-5,725 GHz	1 W
2,4 GHz	2,4-2,4835 GHz	100 mW

AVIS D'UTILISATION DE BLUETOOTH DANS LA COMMUNAUTÉ EUROPÉENNE

- Les appareils compatibles Bluetooth sont conçus pour une utilisation dans tous les États membres de l'UE et les pays de l'AELE.

Technologie	Fréquence	Puissance de sortie max. (EIRP)
Bluetooth 2,4 GHz	2,4-2,4835 GHz	100 mW (20 dBm)

Notes d'utilisation :

- Veuillez vous reporter au manuel ou à la fiche technique du produit pour vérifier si votre produit utilise la technologie sans fil Bluetooth et ses bandes de fréquences de fonctionnement applicables et la puissance RF maximale de votre produit.

AVERTISSEMENT CE EMI CLASSE A (uniquement pour les produits de classe A)

Cet équipement est conforme à la classe A de la norme EN 55032. Dans un environnement résidentiel, cet équipement peut provoquer des interférences radio.

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 prodotsto 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.
- Consultare il manuale del prodotto o la scheda tecnica per verificare se il prodotto utilizza 2,4 GHz, 5 GHz o tutti.

Tecnologia	Frequenza	Potenza massima in uscita (EIRP)
5 GHz	5.15 – 5.25 GHz	200 mW
	5.25 – 5.35 GHz	200 mW
	5.47 – 5.725 GHz	1 W
2.4 GHz	2.4 – 2.4835 GHz	100 mW

NOTA D'USO DEL BLUETOOTH NELLA COMUNITÀ EUROPEA

- I dispositivi che supportano il Bluetooth sono concepiti per l'uso in tutti gli stati membri dell'UE e nei paesi EFTA.

Tecnologia	Frequenza	Potenza massima in uscita (EIRP)
Bluetooth 2.4GHz	2.4 – 2.4835 GHz	100 mW (20 dBm)

Note d'uso:

- Consultare il manuale del prodotto o la scheda dati per verificare se il prodotto usa Bluetooth wireless, le relative bande di frequenza operativa e la potenza RF massima del prodotto.

CE EMI CLASSE A AVVISO (solo per prodotti di classe A)

La presente apparecchiatura è conforme alla Classe A di EN 55032. In ambienti residenziali, questa apparecchiatura potrebbe causare interferenze radio.

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 producthandleiding of datasheet om te controleren of uw product 2,4 GHz, 5 GHz of alle frequenties gebruikt.

Technologie	Frequentie	Max. uitgangsvermogen (EIRP)
5 GHz	5,15-5,25 GHz	200 mW
	5,25-5,35 GHz	200 mW
	5,47-5,725 GHz	1 W
2,4 GHz	2,4-2,4835 GHz	100 mW

OPMERKING OVER HET GEBRUIK VAN BLUETOOTH IN DE EUROPESE GEMEENSCHAP

- Apparaten die Bluetooth ondersteunen zijn bedoeld voor gebruik in alle EU-lidstaten en EVA-landen

Technologie	Frequentie	Max. uitgangsvermogen (EIRP)
Bluetooth 2,4 GHz	2,4-2,4835 GHz	100 mW (20 dBm)

Gebruiksopmerkingen:

- Raadpleeg de handleiding of het gegevensblad van het product om te weten of uw product draadloos Bluetooth gebruikt. In deze documentatie worden ook de gebruikte frequentieband(en) en het maximum RF-vermogen van uw product vermeld.

CE EMI KLASSE A-WAARSCHUWING (alleen voor klasse A-producten)

Dit apparaat voldoet aan Klasse A van EN 55032. Dit apparaat kan in een woonomgeving radio-interferentie veroorzaken.

SAFETY INSTRUCTIONS

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

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

SICHERHEITSVORSCHRIFTEN

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

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

CONSIGNES DE SÉCURITÉ

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

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

INSTRUCCIONES DE SEGURIDAD

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

- La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej.,

tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.

- No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
- No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
- No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
- Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
- Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa.

ISTRUZIONI PER LA SICUREZZA

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

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

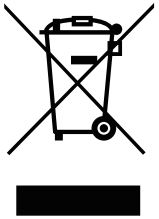
VEILIGHEIDSINFORMATIE

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

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

Disposing and Recycling Your Product

ENGLISH **EN**



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

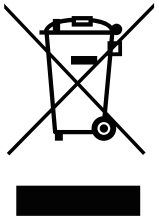
D-Link and the Environment

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

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

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

DEUTSCH **DE**



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

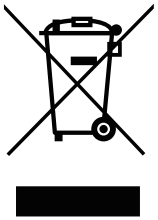
D-Link und die Umwelt

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

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

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

FRANÇAIS FR



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

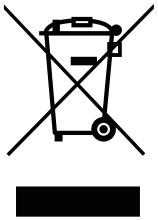
D-Link et l'environnement

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

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

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

ESPAÑOL ES



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

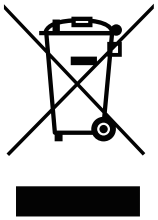
D-Link y el medio ambiente

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

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

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

ITALIANO IT



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

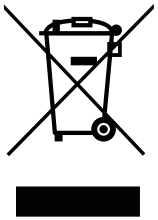
D-Link e l'ambiente

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

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

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

NEDERLANDS NL



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

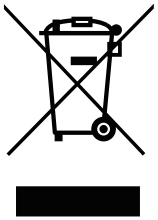
D-Link en het milieu

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

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

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

POLSKI PL



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

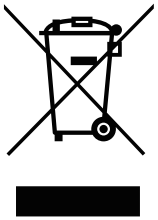
D-Link i środowisko

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

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

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

ČESKY CZ



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

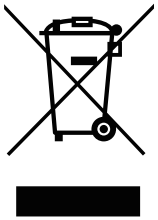
D-Link a životní prostředí

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

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

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

MAGYAR **HU**



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

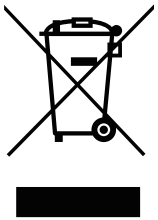
A D-Link és a környezet

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

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

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

NORSK **NO**



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

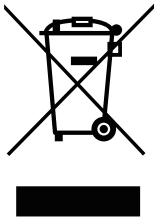
D-Link og miljøet

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

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

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

DANSK DK



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

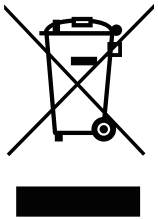
D-Link og miljøet

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

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

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

SUOMI FI



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

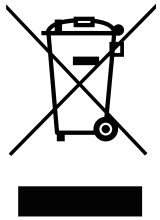
D-Link ja ympäristö

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

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

Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta **www.dlinkgreen.com**.

SVENSKA SE



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

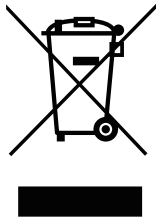
D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar **www.dlinkgreen.com**.

PORTUGUÊS PT



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

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite **www.dlinkgreen.com**.