Version 1.00 | 10/02/2025

User Manual

AX3000 Wi-Fi 6 Travel Router

DBR-330

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	10/02/2025	Initial Version

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^{SM} is a service mark of Apple Inc.

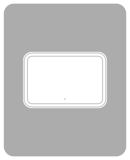
Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

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

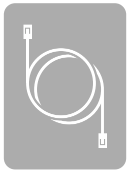
Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Table of Contents

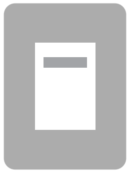
Package Contents



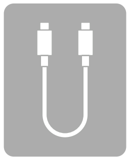
DBR-330 AX3000 Wi-Fi 6 Travel Router



Ethernet Cable (RJ45/1m)



Quick Installation Guide



USB-C to USB-C Charging Cable

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	• A D-Link DWM-222W & D501 USB adapter or an Ethernet-based LAN (10/100/1000 Mbps Ethernet) • IEEE 802.11ax/ac/n/g/b/a wireless clients
Web-Based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter or Wi-Fi interface **Browser requirements:** • Mozilla Firefox 28 or higher • Apple Safari 6 or higher • Google Chrome 28 or higher

Introduction

D-Link introduces the high-performance AX3000 Wi-Fi 6 Travel Router based on Wi-Fi 6 technology. The advanced Wi-Fi 6 delivers 3000 Mbps speed with low latency, allowing fast and reliable communication among multiple connected devices that need to process data simultaneously. This speed and reliability improvements have made possible with the Orthogonal Frequency Division Multiple Access (OFDMA) and Overlapping Basic Service Sets (OBSS) in a crowded network joined by lots of devices. In addition, the USB port allow for on-the-go connectivity to a compatible D-Link DWM-222W & D501 USB adapter.

Features

Flexibility in Network Connection
The DBR-330 offers multiple Internet connection methods to ensure high connectivity availability. Depending on your current network environment, you can connect to the Internet through the WAN port or wirelessly via cellular WAN or a Wireless Internet Service Provider (WISP).

Smooth Wireless Connectivity with AI-powered Performance
AI Wi-Fi Optimizer helps improve the overall user experience based on the network's conditions and usage data. With intelligent Wi-Fi channel tuning and beamforming technology, transmission efficiency can be much improved to attain higher speeds. Together with the decongestion and low-latency features introduced by Wi-Fi 6, bandwidth utilization can be further optimized to preserve the speed and stability of all connected devices.

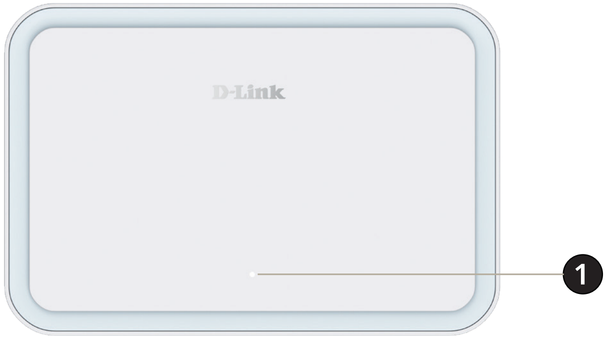
Convenient File Sharing - Join N' Share
File sharing can never be easier with the build-in Join N' Share file sharing.

Always Up-to-Date with the Latest Features
DBR-330 will automatically check for daily updates to make sure that the device is always with the latest features and the most secure firmware. For users' 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.

Secure Remote Access
Provides VPN connectivity using PPTP or L2TP, plus Site-to-Site IPSec VPN for creating virtual links between two endpoints.

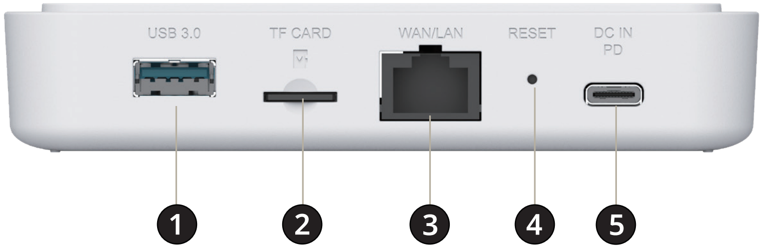
Hardware Overview

LED Indicator



	Indicator	Color	Status	Description
1	Power/Status	White	Solid	Fully powered and connected to the Internet.
		Orange	Blinking	The device cannot connect to the Internet or trying to connect to the Internet during device setup.
		Red	Blinking	Resetting to factory default or system malfunction.
			Solid	Powering on, which happens when system starts or restarts or during factory reset.

Rear Panel



1	**USB 3.0**	Store and share files in your local network. It also works with D-Link DWM-222W and D501 to provide cellular connection as a failover Internet connection.
2	**MicroSD/TF Card Slot**	Store and share files in your local network.
3	**Gigabit WAN/LAN Port**	Connect to broadband modem for Internet service or connect to Ethernet devices such as computers, switches, storage (NAS) devices, and game consoles.
4	**Reset Button**	The reset button turns the router to default settings. Insert a paperclip into the hole, wait for the LED to turn solid red, and then release.
5	**Power Connector**	Connect to a USB Type-C power input with Power Delivery (PD). It requires a minimum of 36 watts of power input.

Installation

Before You Begin

This section will guide you through the installation of your DBR-330.

- 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, make 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 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 basic guidelines:

1. Keep the number of walls and ceilings between a D-Link router and other network devices to a minimum - each wall or ceiling can reduce your router's range from 3 to 90 feet (1 to 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 to 6 feet or 1 to 2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

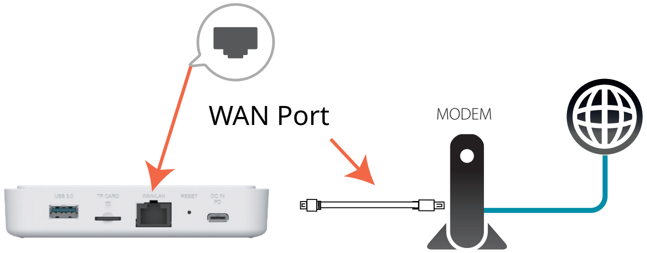
Setup

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

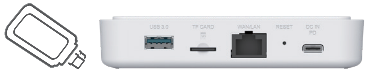
- **Hardware Setup** - This section explains how to set up your DBR-330.
- **D-Link Setup Wizard** - The wizard will launch when you log in to the router by using your PC for the first time.
- **Manual Setup** - Log in to the router for manual configuration of your router. Refer to the **Configuration** section.

Hardware Setup

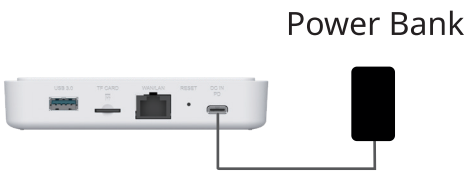
Step 1-1
Position the DBR-330 close to your Internet-connected modem. Turn off and unplug the power to your cable or DSL broadband modem. This is required. In some cases, you may need to turn it off for up to five minutes. Connect an Ethernet cable to the modem and to the WAN port of DBR-330.



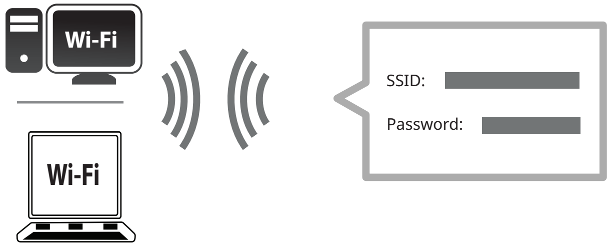
Step 1-2
You may connect to a cellular network using DWM-222W or D501. Simply plug the USB adapter into the USB 3.0 port of the DBR-330.



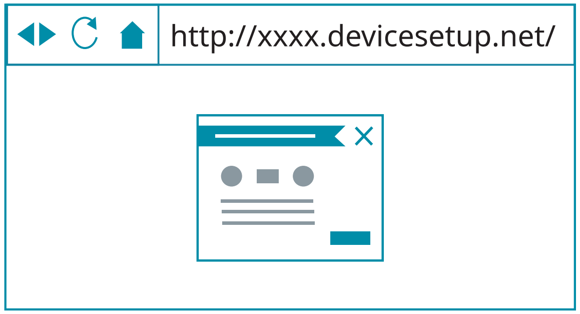
Step 2
Plug the USB Type-C connector of a power source to the DC-In (PD) port of the DBR-330. A power source must supply at least 36W power and we recommend using D-Link DPP series power bank and DCP series GaN charger. Wait for the DBR-330 to boot up.



Step 3
When the router's LED lights up white, wirelessly connect your computer to the Wi-Fi name (SSID) printed on the device label.



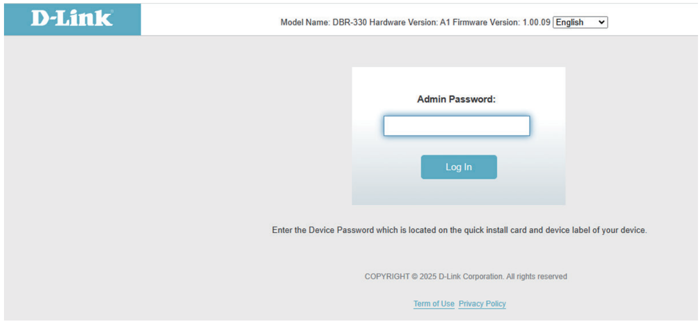
Step 4
Type ***http://xxxx.devicesetup.net/*** into a web browser and follow the on-screen instructions to complete the setup.
(xxxx represents the last 4 characters of the MAC address)



Setup Wizard

The setup wizard is designed to guide you through a step-by-step process to configure your new DBR-330 for Internet connection.

If this is your first time configuring the router, open your web browser and enter **http://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. 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.



Model Name: DBR-330 Hardware Version: A1 Firmware Version: 1.00.09

Admin Password:

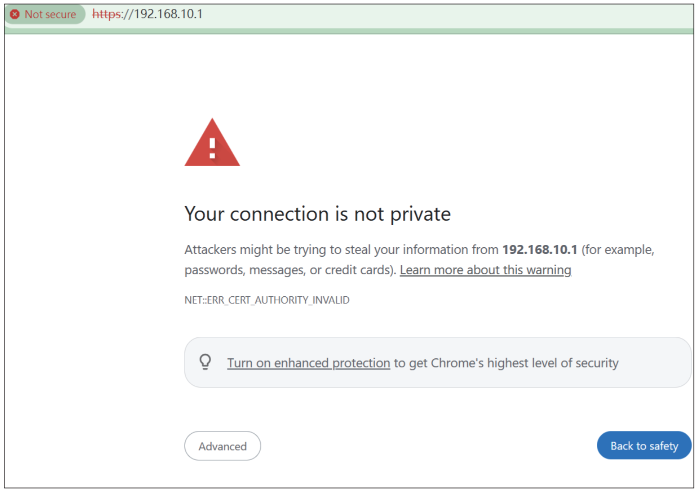
Enter the Device Password which is located on the quick install card and device label of your device.

COPYRIGHT © 2025 D-Link Corporation. All rights reserved

Term of Use Privacy Policy

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.



Your connection is not private

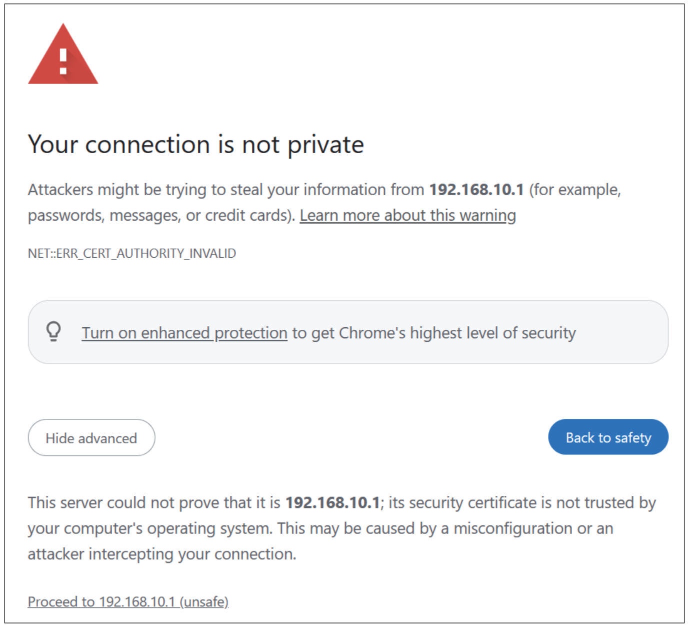
Attackers might be trying to steal your information from **192.168.10.1** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

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

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



Your connection is not private

Attackers might be trying to steal your information from **192.168.10.1** (for example, passwords, messages, or credit cards). Learn more about this warning

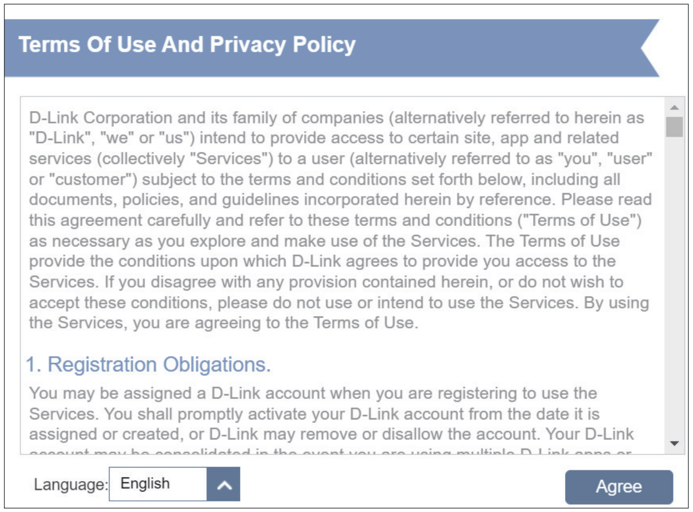
NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

This server could not prove that it is **192.168.10.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.10.1 (unsafe)

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



Terms Of Use And Privacy Policy

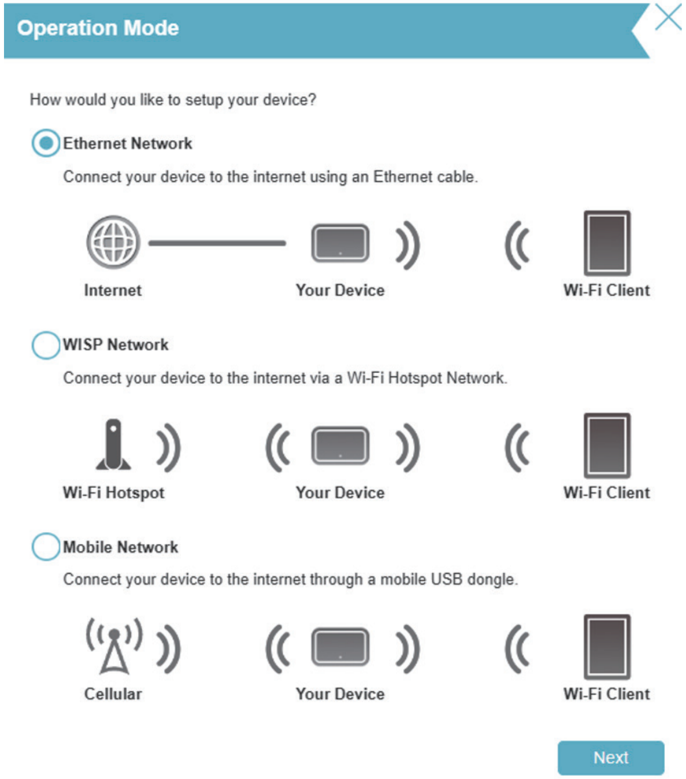
D-Link Corporation and its family of companies (alternatively referred to herein as "D-Link", "we" or "us") intend to provide access to certain site, app and related services (collectively "Services") to a user (alternatively referred to as "you", "user" or "customer") subject to the terms and conditions set forth below, including all documents, policies, and guidelines incorporated herein by reference. Please read this agreement carefully and refer to these terms and conditions ("Terms of Use") as necessary as you explore and make use of the Services. The Terms of Use provide the conditions upon which D-Link agrees to provide you access to the Services. If you disagree with any provision contained herein, or do not wish to accept these conditions, please do not use or intend to use the Services. By using the Services, you are agreeing to the Terms of Use.

1. Registration Obligations.

You may be assigned a D-Link account when you are registering to use the Services. You shall promptly activate your D-Link account from the date it is assigned or created, or D-Link may remove or disallow the account. Your D-Link

Language: English

Select the Operation Mode: Ethernet Network, WISP Network, or Mobile Network.



Operation Mode

How would you like to setup your device?

● Ethernet Network

Connect your device to the internet using an Ethernet cable.

○ WISP Network

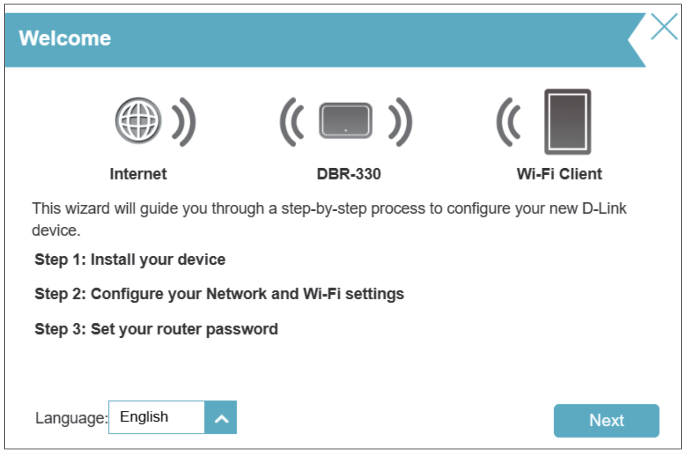
Connect your device to the internet via a Wi-Fi Hotspot Network.

○ Mobile Network

Connect your device to the internet through a mobile USB dongle.

Connect your devices as instructed depending on the selected mode.

Click **Next** to continue.



Welcome

This wizard will guide you through a step-by-step process to configure your new D-Link device.

Step 1: Install your device

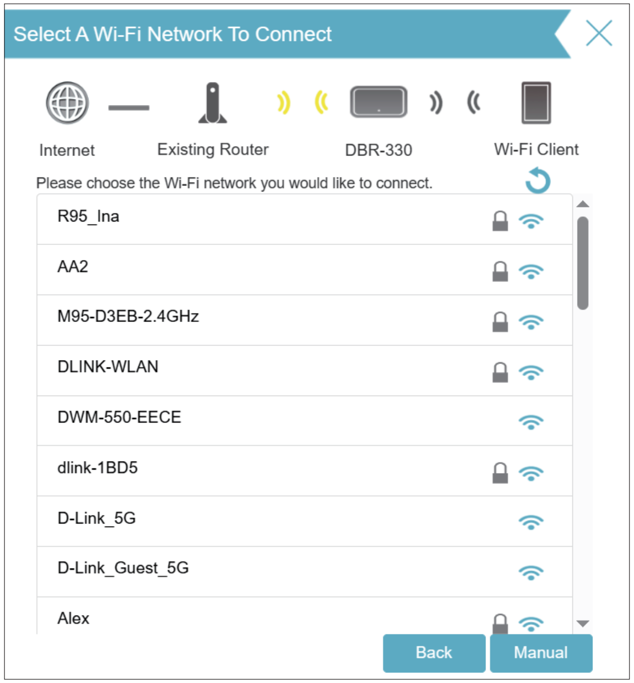
Step 2: Configure your Network and Wi-Fi settings

Step 3: Set your router password

Language: English

If the router does not detect a valid Internet connection, a list of detected wireless networks for Wi-Fi hotspot will be displayed. Select one to connect to (this information can be obtained from your ISP).

Click **Next** to continue.



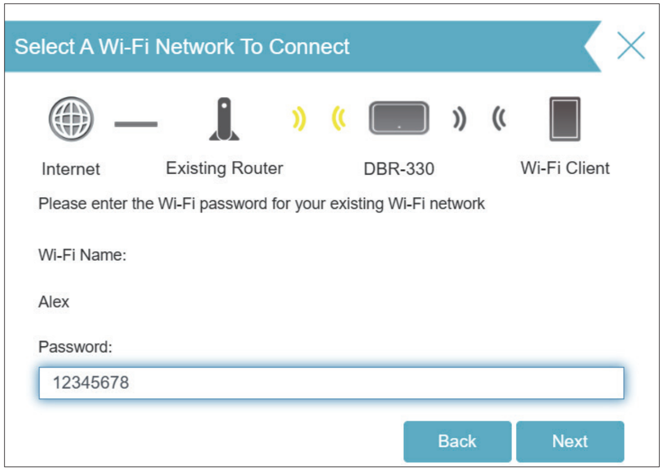
Select A Wi-Fi Network To Connect

Please choose the Wi-Fi network you would like to connect.

- R95_Ina
- AA2
- M95-D3EB-2.4GHz
- DLINK-WLAN
- DWM-550-EECE
- dlink-1BD5
- D-Link_5G
- D-Link_Guest_5G
- Alex

Enter the required password for connection.

Click **Next** to continue.



Select A Wi-Fi Network To Connect

Please enter the Wi-Fi password for your existing Wi-Fi network

Wi-Fi Name:

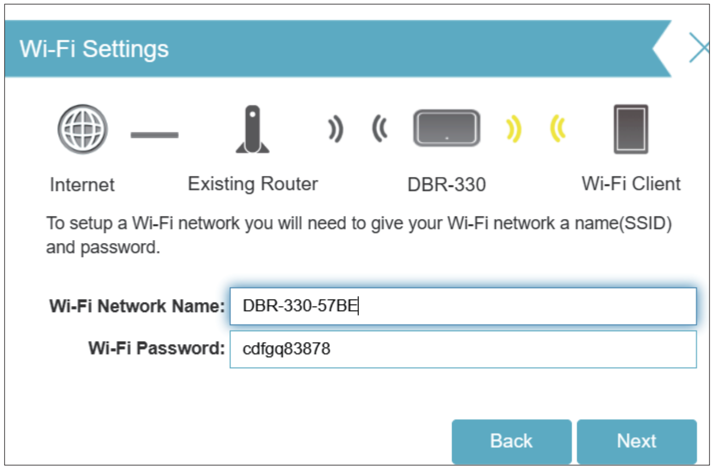
Alex

Password:

12345678

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. Your wireless clients will need to have this passphrase to be able to connect to your wireless network. The password must contain 8 to 63 characters.

Click **Next** to continue.



To setup a Wi-Fi network you will need to give your Wi-Fi network a name(SSID) and password.

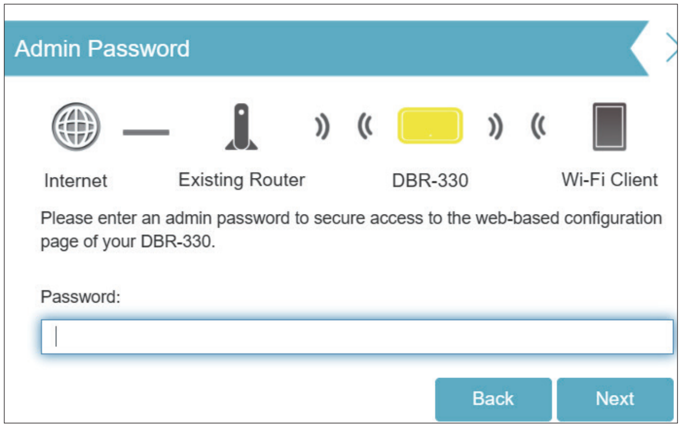
Wi-Fi Network Name: DBR-330-57BE

Wi-Fi Password: cdfgq83878

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 configuration utility.

Note: It is strongly recommended that you change the default device password. The password must contain 8 to 15 characters and include both numbers and letters.

Click **Next** to continue.



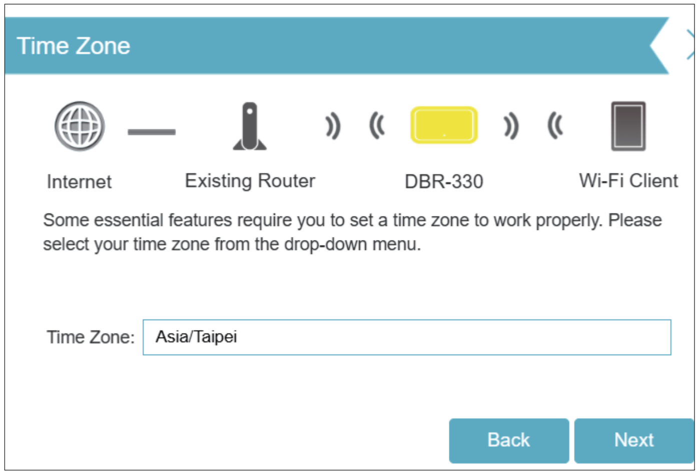
Admin Password

Please enter an admin password to secure access to the web-based configuration page of your DBR-330.

Password:

Select your time zone from the drop-down menu.

Click **Next** to continue.



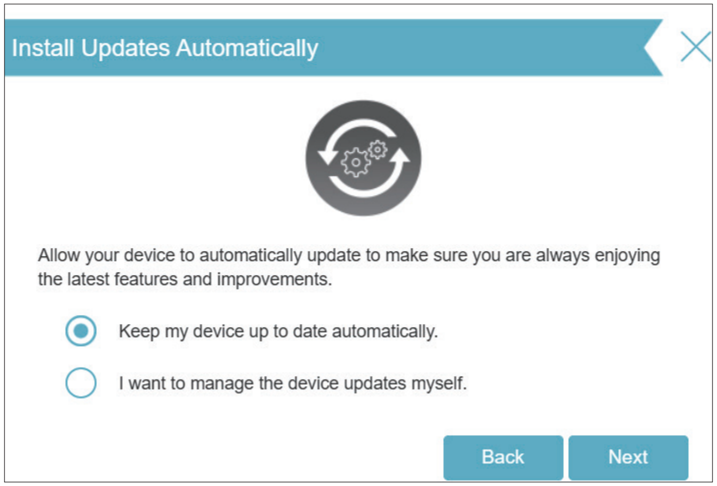
Time Zone

Some essential features require you to set a time zone to work properly. Please select your time zone from the drop-down menu.

Time Zone: Asia/Taipei

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.



Install Updates Automatically

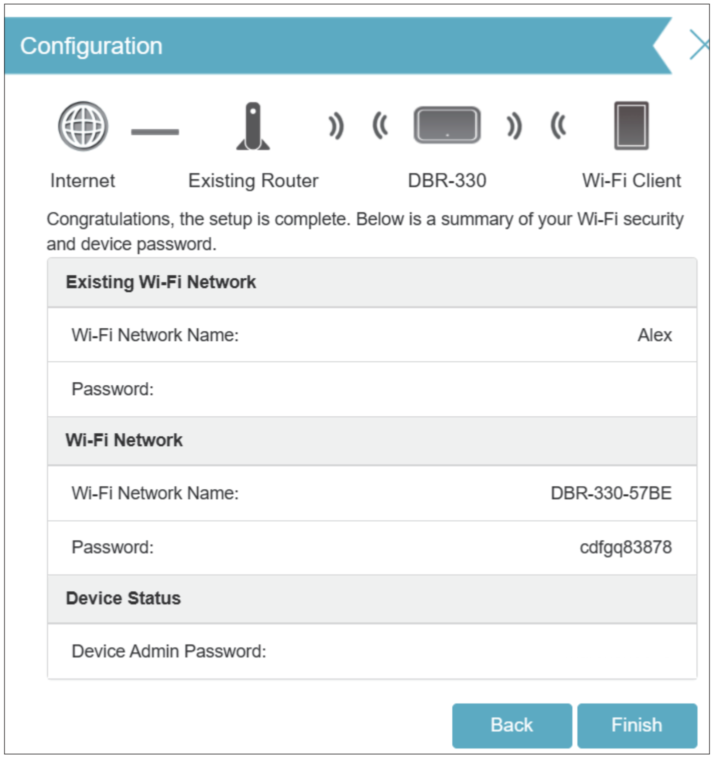
Allow your device to automatically update to make sure you are always enjoying the latest features and improvements.

● Keep my device up to date automatically.

○ I want to manage the device updates myself.

You will be presented with a summary of your settings.

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



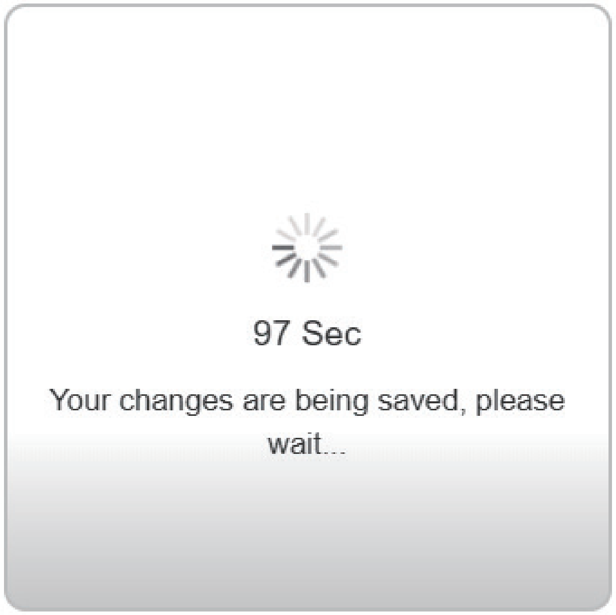
Configuration

Congratulations, the setup is complete. Below is a summary of your Wi-Fi security and device password.

Existing Wi-Fi Network	
Wi-Fi Network Name:	Alex
Password:	
Wi-Fi Network	
Wi-Fi Network Name:	DBR-330-57BE
Password:	cdfgq83878
Device Status	
Device Admin Password:	

Please wait while the device settings are being saved.

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



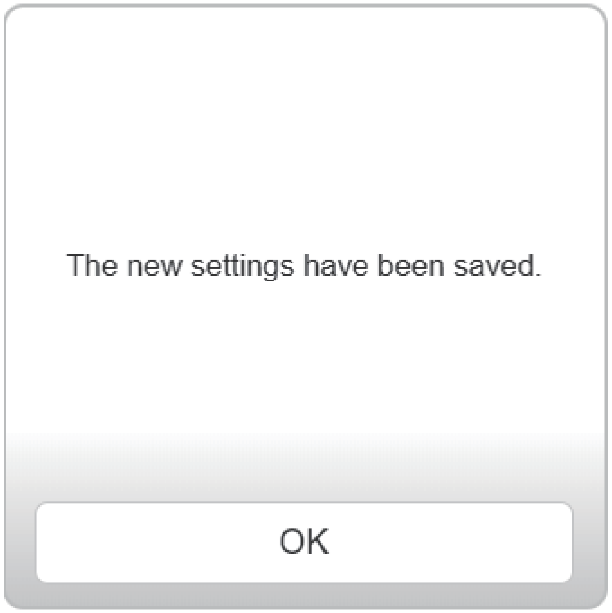
97 Sec

Your changes are being saved, please wait...

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 configuration utility by entering your Admin Password.

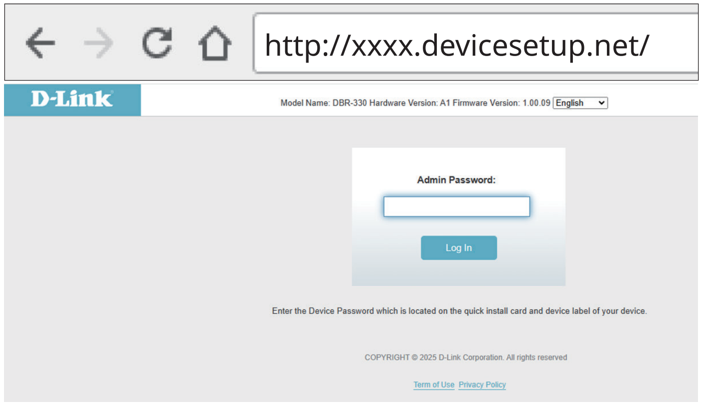


The new settings have been saved.

Configuration

Accessing the Web User 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.



http://xxxx.devicesetup.net/

Model Name: DBR-330 Hardware Version: A1 Firmware Version: 1.00.09 English

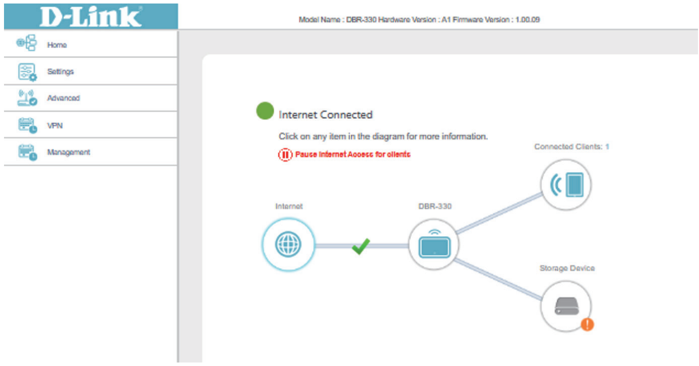
Admin Password:

Enter the Device Password which is located on the quick install card and device label of your device.

COPYRIGHT © 2025 D-Link Corporation. All rights reserved

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

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



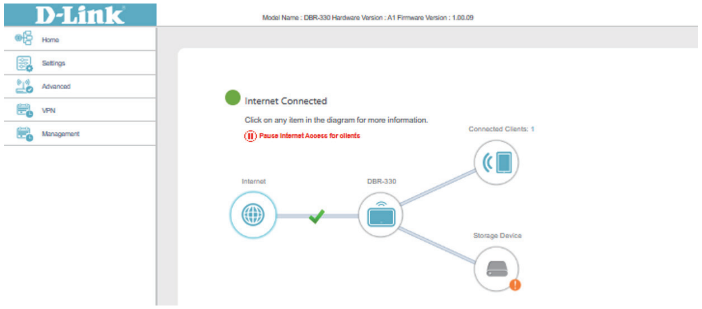
Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

Click on any item in the diagram for more information.

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.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

Click on any item in the diagram for more information.

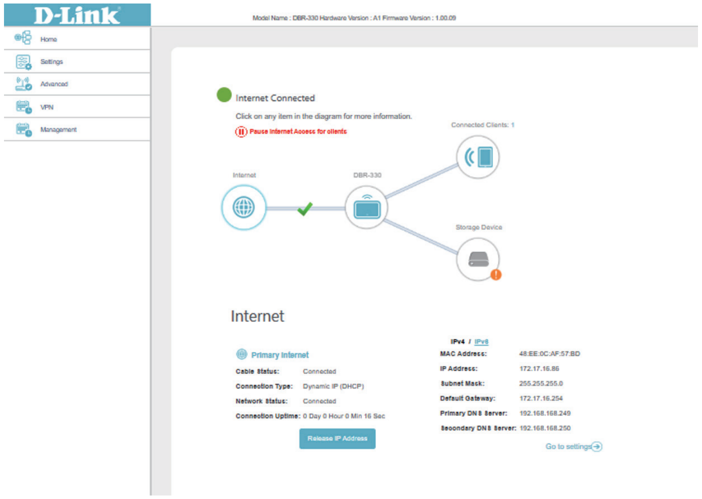
Pause Internet Access for clients

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 the **Setup Wizard** 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**.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

Click on any item in the diagram for more information.

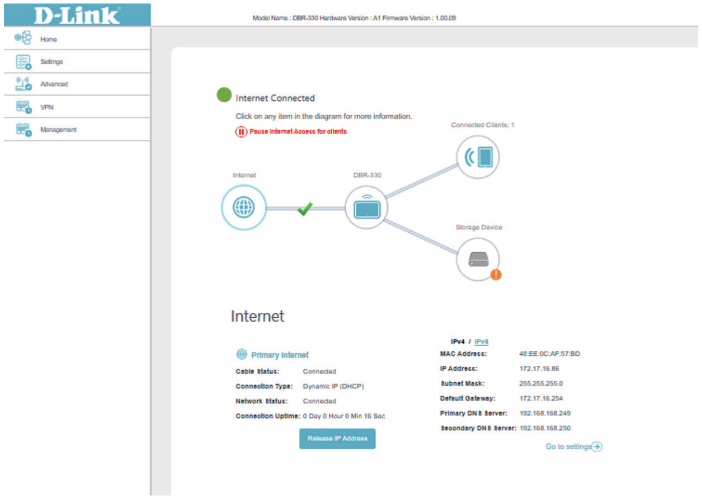
Internet

Primary Internet

Cable Status:	Connected
Connection Type:	Dynamic IP (DHCP)
Network Status:	Connected
Connection Uptime:	0 Day 0 Hour 0 Min 16 Sec

MAC Address:	48:EE:0C:AF:57:BD
IP Address:	172.17.16.86
Subnet Mask:	255.255.255.0
Default Gateway:	172.17.16.254
Primary DNS Server:	192.168.168.249
Secondary DNS Server:	192.168.168.250

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.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

Click on any item in the diagram for more information.

Internet

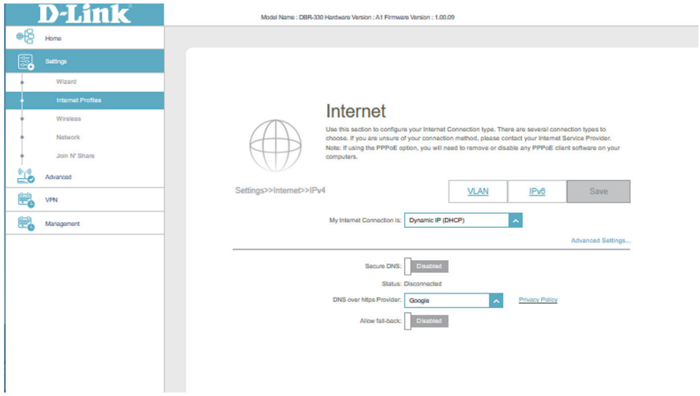
Primary Internet

Cable Status:	Connected
Connection Type:	Dynamic IP (DHCP)
Network Status:	Connected
Connection Uptime:	0 Day 0 Hour 0 Min 16 Sec

IPv4 / IPv6

MAC Address:	48:EE:0C:AF:57:BD
IP Address:	172.17.16.86
Subnet Mask:	255.255.255.0
Default Gateway:	172.17.16.254
Primary DNS Server:	192.168.168.249
Secondary DNS Server:	192.168.168.250

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



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet

Use this section to configure your Internet Connection type. There are several connection types to choose. If you are unsure of your connection method, please contact your Internet Service Provider. Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Settings>>Internet>>IPv4

My Internet Connection is: Dynamic IP (DHCP)

Secure DNS: Disabled

Status: Disconnected

DNS over https Provider: Google

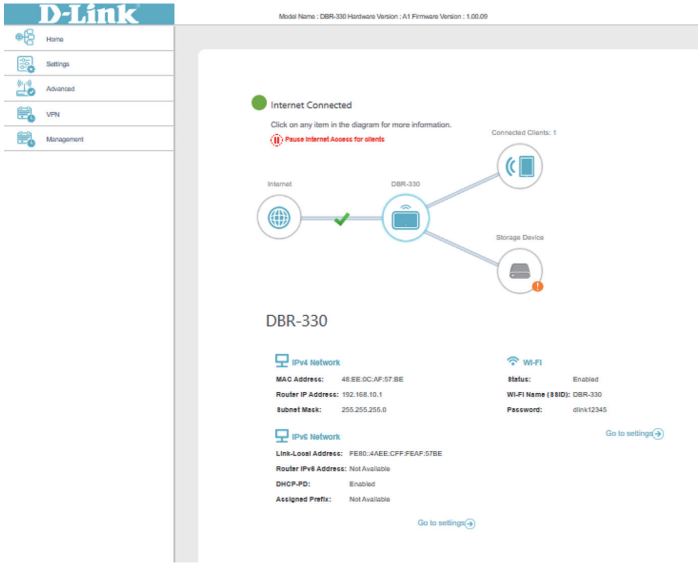
Allow fall-back: Disabled

DBR-330

Click on the **DBR-330** router 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**.

To reconfigure wireless settings, either click **Go to settings**, on the lower right, or click **Settings** on the left pane and select **Wireless**.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

Click on any item in the diagram for more information.

DBR-330

IPv4 Network

MAC Address: 48:EE:0C:AF:57:BE
Router IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0

IPv6 Network

Link-Local Address: FE80::4AEE:CFF:FEAF:57BE
Router IPv6 Address: Not Available
DHCP-PD: Enabled
Assigned Prefix: Not Available

Wi-Fi

Status: Enabled
Wi-Fi Name (SSID): DBR-330
Password: dlink12345

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.

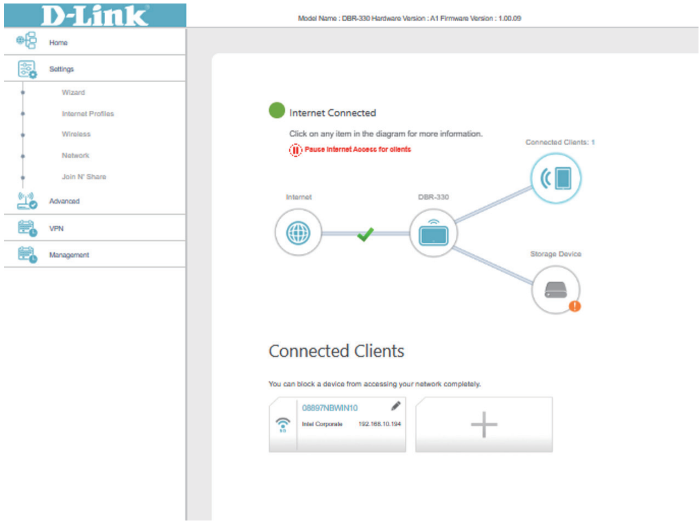
Reserve IP: Enable to reserve an IP address for this client.

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 time schedule that the rule will be enabled on. The schedule may be set to **Always Block**, or you can create your own profiles in the **Parental Control** section. Refer to **Parental Control** for more information.

Click **Save** when you are done.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

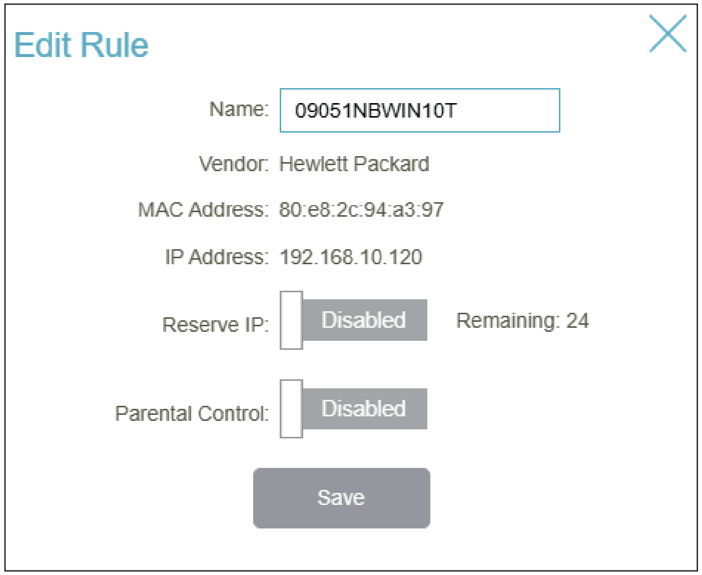
Click on any item in the diagram for more information.

Pause Internet Access for clients

Connected Clients

You can block a device from accessing your network completely.

08897NBWIN10
Intel Corporate 192.168.10.194



Edit Rule

Name:	09051NBWIN10T	
Vendor:	Hewlett Packard	
MAC Address:	80:e8:2c:94:a3:97	
IP Address:	192.168.10.120	
Reserve IP:	Disabled	Remaining: 24
Parental Control:	Disabled	

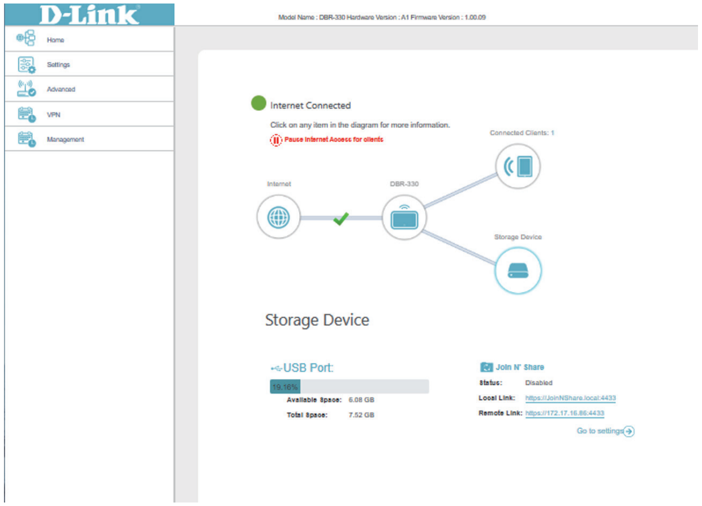
Storage Device

Click on the **Storage Device** icon to view details about the currently connected USB or TF card device as well as the Web File Access sharing settings.

If you have a USB device connected, you can see its name and how much free space it has.

To configure your USB settings, click **Go to Settings** or click **Settings > USB Sharing** to obtain more information on USB configuration.

For information on how to access your USB drive via a web browser, refer to the **Join N' Share** section.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Connected

Click on any item in the diagram for more information.

Pause Internet Access for clients

Storage Device

USB Port:

Available Space: 6.08 GB

Total Space: 7.52 GB

Join N' Share

Status: Disabled

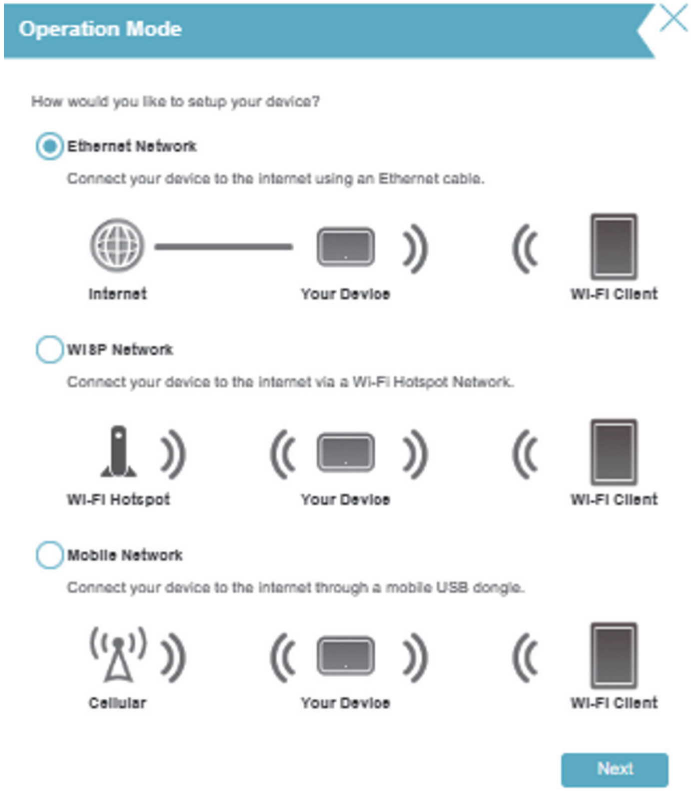
Local Link: https://JoinNShare.local:4433

Remote Link: https://172.17.16.86:4433

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** for details.

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



Operation Mode

How would you like to setup your device?

● Ethernet Network

Connect your device to the internet using an Ethernet cable.

○ WISP Network

Connect your device to the internet via a Wi-Fi Hotspot Network.

○ Mobile Network

Connect your device to the internet through a mobile USB dongle.

Internet Profiles

The Internet Profiles records the Internet connection settings of the device. From this page you can configure the failover function. When the current Internet connection is not available, the device will automatically connect using a redundant connection method used by the device previously.

Failover

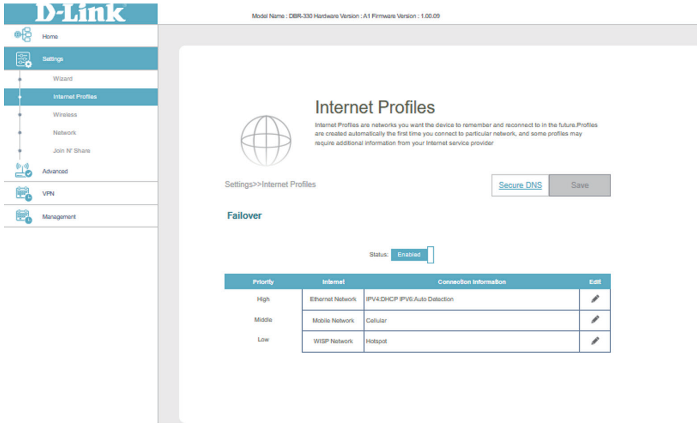
Status: Enable or disable the Failover function.

Priority: Displays the priority of the connection method.

Internet: Displays the Internet connection.

Connection Information: Displays the configured connection method, e.g. cellular or Wi-Fi.

Edit: To Edit a connection profile, click the Edit icon.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Internet Profiles

Internet Profiles are networks you want the device to remember and reconnect to in the future.Profiles are created automatically the first time you connect to particular network, and some profiles may require additional information from your Internet service provider

Settings>>Internet Profiles

Failover

Status: Enabled

Priority	Internet	Connection Information	Edit
High	Ethernet Network	IPV4:DHCP IPV6:Auto Detection	✎
Middle	Mobile Network	Cellular	✎
Low	WISP Network	Hotspot	✎

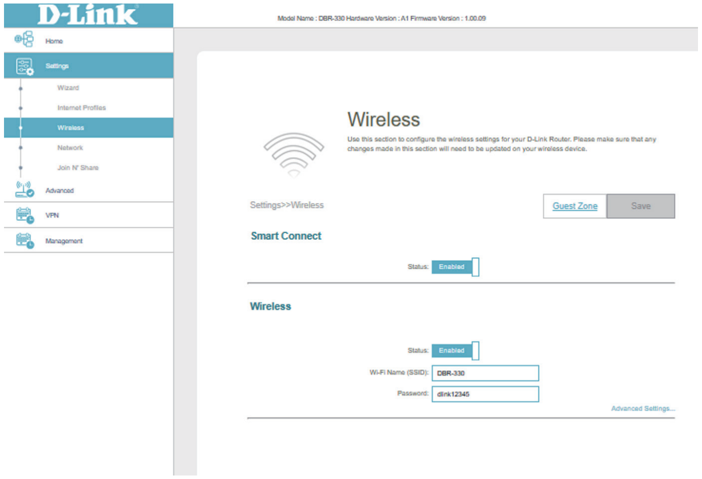
Wireless

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

Smart Connect

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

If Smart Connect Status is Enabled:



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Wireless

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

Settings>>Wireless

Smart Connect

Status: Enabled

Wireless

Status: Enabled

Wi-Fi Name (SSID): DBR-330

Password: dlink12345

Wireless

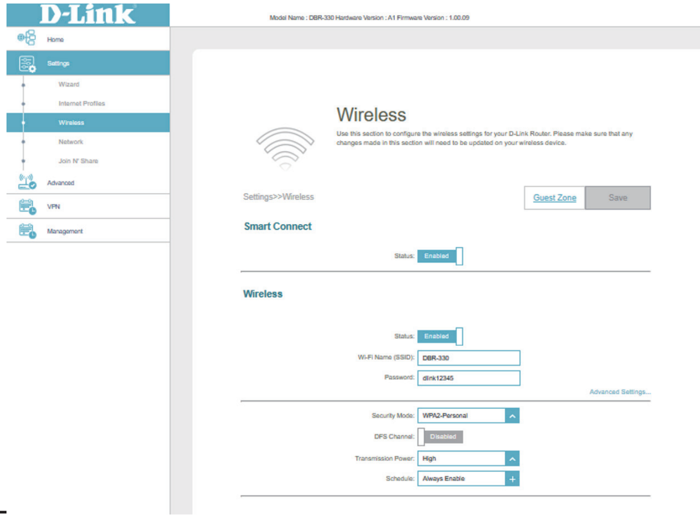
Wi-Fi Name (SSID): Enter a name for your Wi-Fi network. Up to 32 characters are allowed.

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

Wireless - Advanced Settings

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

DFS Channel: Enable Dynamic Frequency Selection (DFS) channels to use additional channel options 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.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Wireless

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

Settings>>Wireless

Smart Connect

Status: Enabled

Wireless

Status: Enabled

Wi-Fi Name (SSID): DBR-330

Password: dlink12345

Security Mode: WPA2-Personal

DFS Channel: Disabled

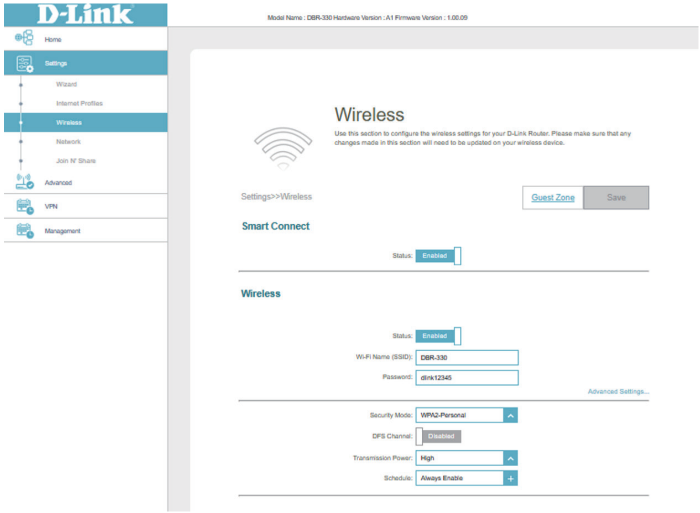
Transmission Power: High

Schedule: Always Enable

Transmission Power: Select a desired wireless transmission power. The default is high.

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.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Wireless

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

Settings>>Wireless

Smart Connect

Status: Enabled

Wireless

Status: Enabled
Wi-Fi Name (SSID): DBR-330
Password: dlink12345
Advanced Settings...

Security Mode: WPA2-Personal
DFS Channel: Disabled
Transmission Power: High
Schedule: Always Enable

When Smart Connect Status is disabled, 2.4 GHz and 5 GHz configuration options become available.

2.4 GHz Advanced Settings

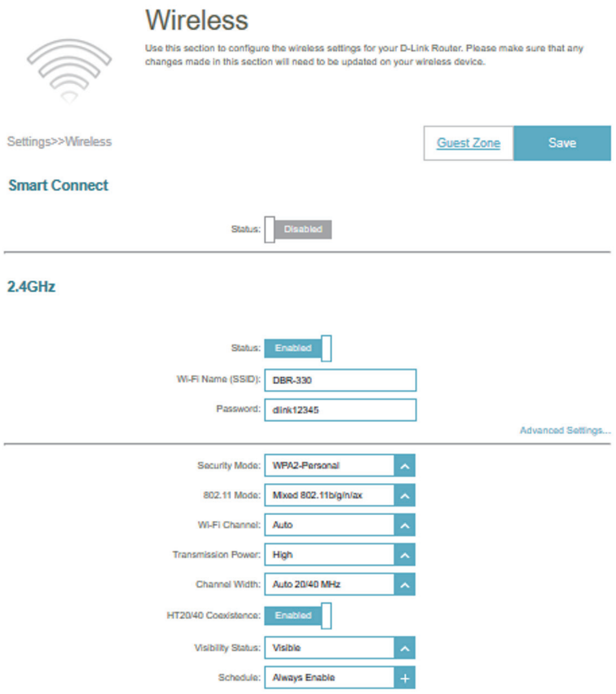
Status: Enable or disable the 2.4 GHz / 5 GHz wireless network.

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

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

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

802.11 Mode (2.4GHz): Select a desired wireless networking standard to use. The available options for the 2.4 GHz wireless network are **Mixed 802.11b/g/n/ax, Mixed 802.11b/g/n, Mixed 802.11b/g, Mixed 802.11g/n, 802.11b only, 802.11g only,** or **802.11n only.**



Wireless

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

Settings>>Wireless

Smart Connect

Status: Disabled

2.4GHz

Status: Enabled
Wi-Fi Name (SSID): DBR-330
Password: dlink12345
Advanced Settings...

Security Mode: WPA2-Personal
802.11 Mode: Mixed 802.11b/g/n/ax
Wi-Fi Channel: Auto
Transmission Power: High
Channel Width: Auto 20/40 MHz
HT20/40 Coexistence: Enabled
Visibility Status: Visible
Schedule: Always Enable

Wi-Fi Channel: Select a desired channel: 1-13. The default is **Auto** (recommended).

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

Channel Width (2.4GHz): Select **Auto 20/40 MHz** if you are using a mix of 802.11ax, 802.11n, and older standards (802.11b/g) and select **20 MHz** if you are using a mix of 802.11b/g devices.

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

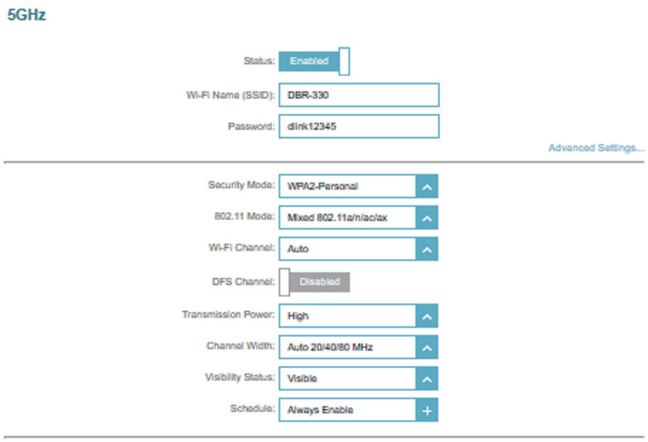
Schedule: Select the time during which the wireless network will be available. The schedule may be set to Always Enable or you can add your own schedule.
To add a schedule:
Each box represents half an hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule.

5 GHz - Advanced Settings

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

802.11 Mode (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, Mixed 802.11a/n/ac, Mixed 802.11a/n, 802.11ac only, 802.11a only,** or **802.11n only**.

Wi-Fi Channel: Select a desired channel: 36, 40, 44, or 48. The default is **Auto** (recommended).



5GHz

Status: Enabled

Wi-Fi Name (SSID): DBR-330

Password: dlink12345

Security Mode: WPA2-Personal

802.11 Mode: Mixed 802.11a/n/ac/ax

Wi-Fi Channel: Auto

DFS Channel: Disabled

Transmission Power: High

Channel Width: Auto 20/40/80 MHz

Visibility Status: Visible

Schedule: Always Enable

DFS Channel: Enable Dynamic Frequency Selection (DFS) channels to use additional channel options 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. The default is High.

Channel Width (5 GHz): Select **Auto 20/40/80/160MHz** if you are using a mix of 802.11ax, 802.11ac, 802.11n, and 802.11a devices, select **Auto 20/40 MHz** if you are using 802.11n and 802.11a devices, or select **20 MHz** if you are using 802.11a devices only. The160MHz is only available if DFS is enabled.

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.

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

Wireless

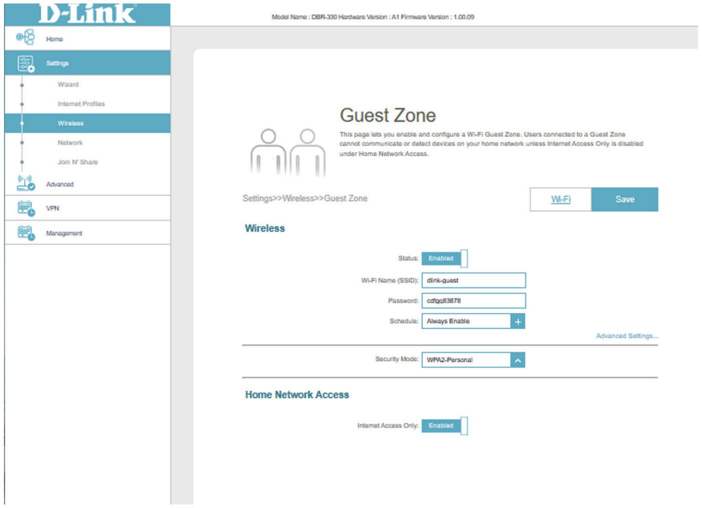
Status: Enable or disable the Guest Wi-Fi network.

Wi-Fi Name (SSID): Enter a name for your guest 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.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Guest Zone

This page lets you enable and configure a Wi-Fi Guest Zone. Users connected to a Guest Zone cannot communicate or detect devices on your home network unless Internet Access Only is disabled under Home Network Access.

Settings>>Wireless>>Guest Zone

Wireless

Status: Enabled

Wi-Fi Name (SSID): dlink-guest

Password: cdfgq83878

Schedule: Always Enable

Advanced Settings...

Security Mode: WPA2-Personal

Home Network Access

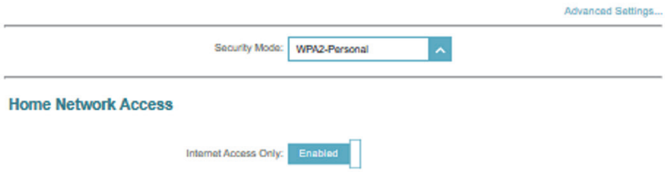
Internet Access Only: Enabled

Advanced Settings

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

Home Network Access

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



Advanced Settings...

Security Mode: WPA2-Personal

Home Network Access

Internet Access Only: Enabled

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

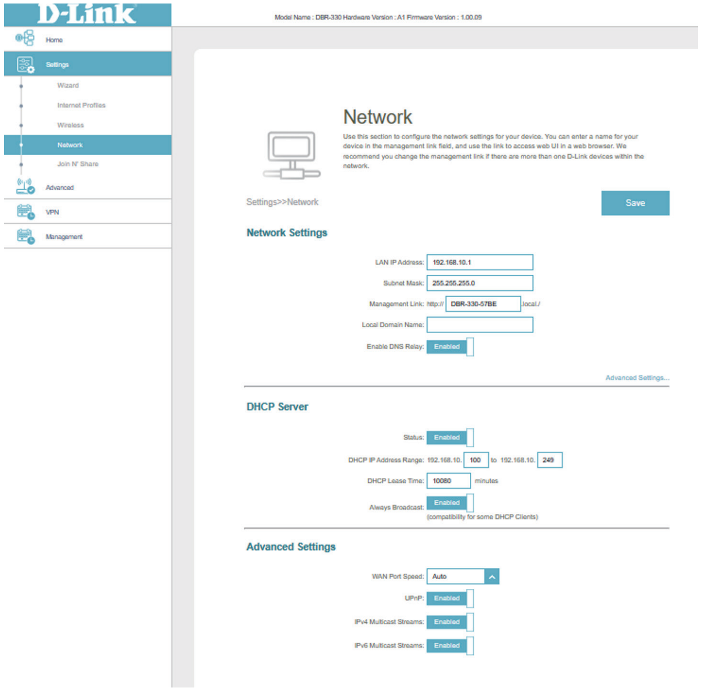
LAN IP Address: Enter the IP address of the router. The default IP address is **192.168.10.1**.
If you change the IP address, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the subnet mask 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://DBR330-xxxx.local/** (where xxxx represents the last 4 digits of your router's MAC address). You can replace **DBR330-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.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Network

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

Settings>>Network

Network Settings

LAN IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Management Link: http:// DBR-330-57BE .local/
Local Domain Name:
Enable DNS Relay: Enabled

DHCP Server

Status: Enabled
DHCP IP Address Range: 192.168.10. 100 to 192.168.10. 249
DHCP Lease Time: 10080 minutes
Always Broadcast: Enabled
(compatibility for some DHCP Clients)

Advanced Settings

WAN Port Speed: Auto
UPnP: Enabled
IPv4 Multicast Streams: Enabled
IPv6 Multicast Streams: Enabled

DHCP Server

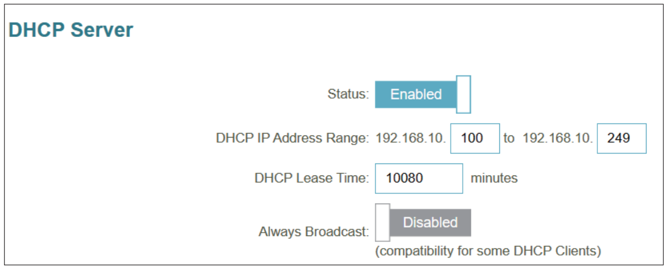
Status: Enable or disable the DHCP server.

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 10080 minutes.

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



DHCP Server

Status: Enabled

DHCP IP Address Range: 192.168.10. 100 to 192.168.10. 249

DHCP Lease Time: 10080 minutes

Always Broadcast: Disabled
(compatibility for some DHCP Clients)

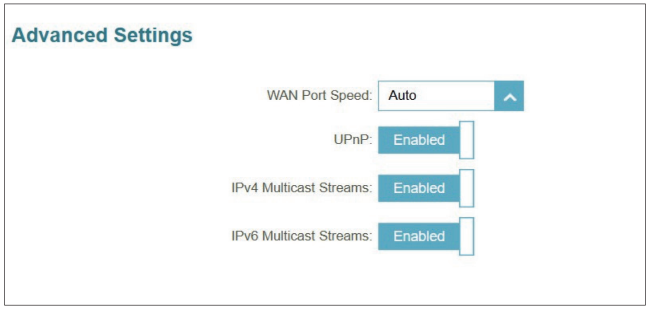
Advanced Settings...

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

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

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

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



Advanced Settings

WAN Port Speed: Auto

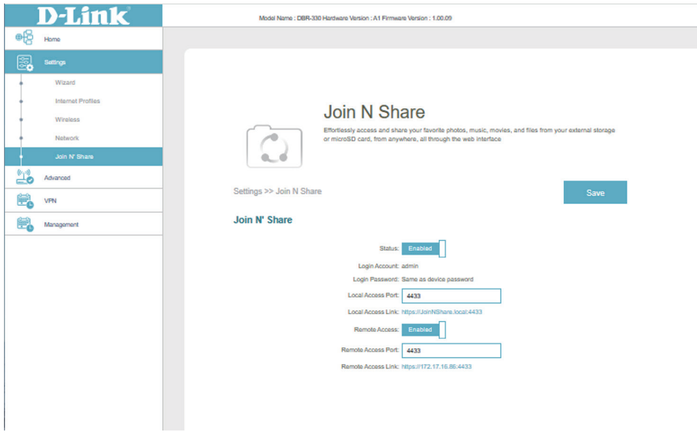
UPnP: Enabled

IPv4 Multicast Streams: Enabled

IPv6 Multicast Streams: Enabled

Join N' Share

This page allows you to set up access to files on an external USB device plugged into the router. The built-in Join N' Share web-based file sharing further allows you to perform file sharing through local and remote network. To access this page, go to **Settings > Join N' Share**.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Join N Share

Effortlessly access and share your favorite photos, music, movies, and files from your external storage or microSD card, from anywhere, all through the web interface

Settings >> Join N Share

Join N' Share

Status: Enabled
Login Account: admin
Login Password: Same as device password
Local Access Port: 4433
Local Access Link: https://JoinNShare.local:4433
Remote Access: Enabled
Remote Access Port: 4433
Remote Access Link: https://172.17.16.86:4433

Join N' Share

Status: Enable or disable file sharing. Computers and devices will be able to access the files on the USB device connected to this router through a web browser.

Local Access Port: Enable local file sharing with a designated port number.

Local Access Link: The web address for accessing the web file sharing.

Remote Access

Remote Access: Enable remote file sharing to permit file access across the Internet.

Remote Access Port: Enable remote file sharing across the Internet with a designated port number.

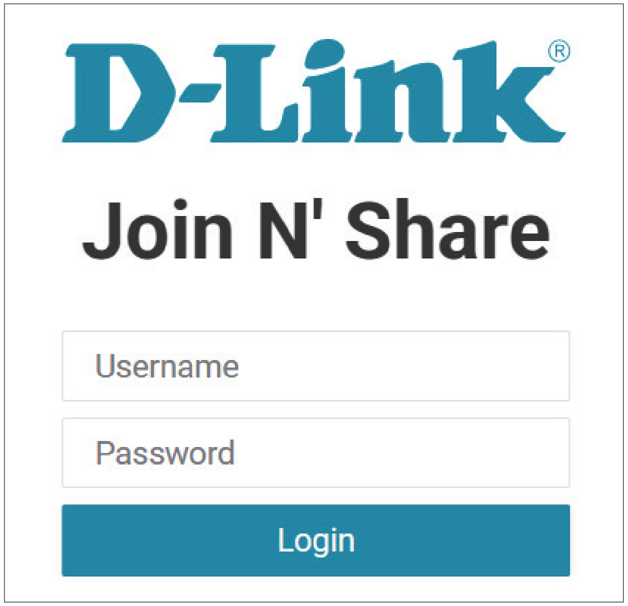
Remote Access Link: The web address for accessing the web file sharing over the Internet.

Folder: Enter the root file directory for access. Click **Browse** to select a directory of the connected external drive.

Join N' Share

This page allows you to access connected USB or TF card storage through file sharing. Simply open your browser and enter the Local Access Link displayed on the USB Sharing page above. The Join N' Share site also lets you create user accounts with different access privileges. This section explains the available features and configuration options designed to simplify file management.

To begin, enter the ***admin*** username and password configured for DBR-330.



Viewing and Accessing the Files

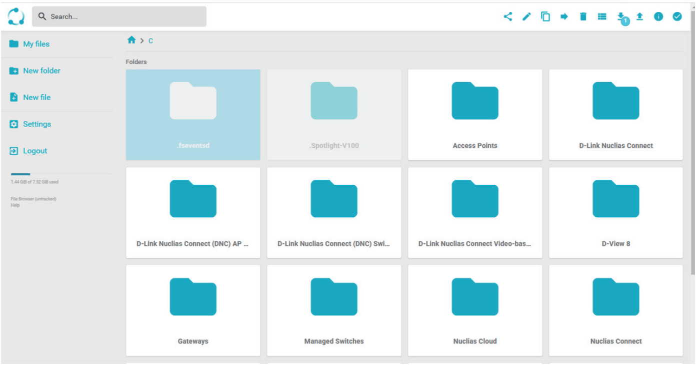
The functional buttons at the top right provide the following options to help you manage the files in the current directory.

Share: Share the selected file with a pre-configured duration and password for accessing it. Note the Share function only appears after you select an item.

Rename: Rename the selected file. Note the Rename function only appears after you select an item.

Copy: Copy the selected file to a new location. Note the Copy function only appears after you select an item.

Move file: Move the selected file to a new location. Note the Move function only appears after you select an item.



Delete: Delete the selected file. Note the Delete function only appears after you select an item.

View Mode: Change how your folders and files look and the displayed information alongside them. The following view modes are available:

Change how your folders and files look and the displayed information alongside them. The following view modes are available:

Details: Show information about your files and folders. In this view, folders show last modified date; files show file size and last modified date.

Tiles: Show icons of each item. Both files and folders display the last modified date, as well as the file size for each file.

Large icon: Show the largest available view of file and folder icons. In this view, only the name of the file or folder is displayed.

Note: Toggle the icon to switch between views.

Download: Download the selected file or folder. The number of selected items will be displayed beside the icon.

Upload: Upload files and folders from your local device.

Information: The information icon displays the file or folder information. If no items are selected, the information of the current folder will be displayed, for example, the total number of items in the current folder. If multiple items are selected and the number of items and the total size will be displayed.

Select Multiple: ✓ Select multiple items to perform the above listed functions. You can deselect an item by clicking it again.

Search: The search box is at the top left of the webpage. It allows you to search for subfolders, documents, and images in the current folder.

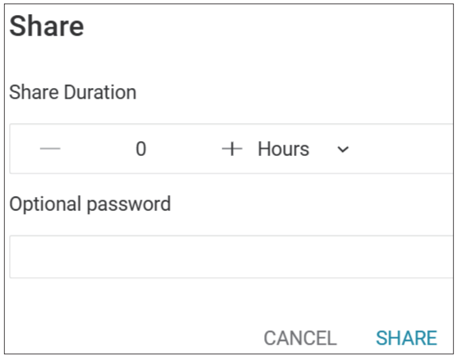
Searching files and folder contents

You can perform searches by just entering a keyword in the search box. The powerful search function will find file names and folder contents among the current folder items containing your keyword. You can refine your search by selecting the file type first: Image, Music, Video, or PDF. After typing your keyword, press the enter key. You can open your file directly to view its content if the file type is supported by your browser.

Sharing Files and Folders

File Sharing allows you to share a file or folder to anyone with a valid link.

To share a file, select the file and click < :



Share

Share Duration

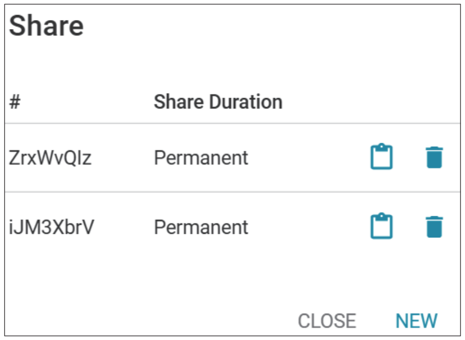
— 0 + Hours ⌄

Optional password

Share Duration: Specify the duration for which the share link will be available.

Optional password: Protect the accessibility of the share file. You can leave it blank if no password is required for file access.

Click **Share**.



Share

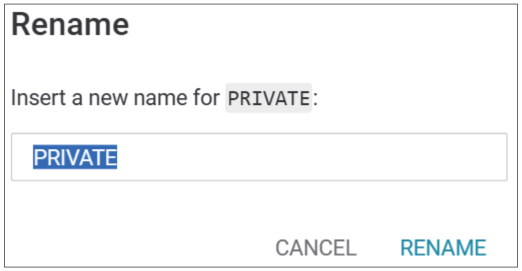
#	Share Duration
ZrxWvQlz	Permanent
iJM3XbrV	Permanent

Copy to Clipboard: Copy the share link for others to access using a browser.

Copy Download Link to Clipboard: Display the current file information and display the options to download the file to the download directory or open the file directly in the browser.

Renaming Files and Folders

Renaming a file allows you to change the name of an item.
Select the file you want to rename, click the Rename icon at the top right.
Type a new name for the file, then click **Rename**.



Insert a new name for `PRIVATE`:

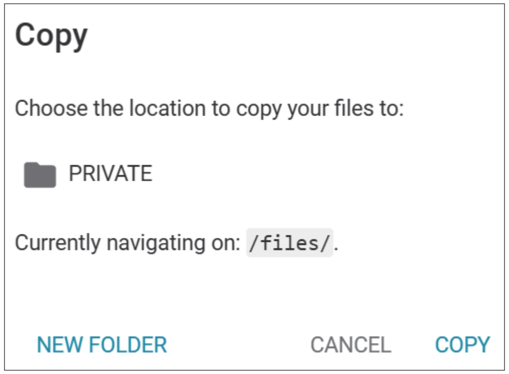
Copying Files and Folders

Copying Files and Folders allows you to replicate selected files and folders to a desired destination. Copying Files and Folders can be performed on multiple items.

To copy multiple items, select ✓ first,and select your desired files , then click ⧉ :

New Folder: Create a new folder as the destination for the selected files.

Copy: Copy the selected files and folders to the current directory.



Choose the location to copy your files to:

Currently navigating on: `/files/`.

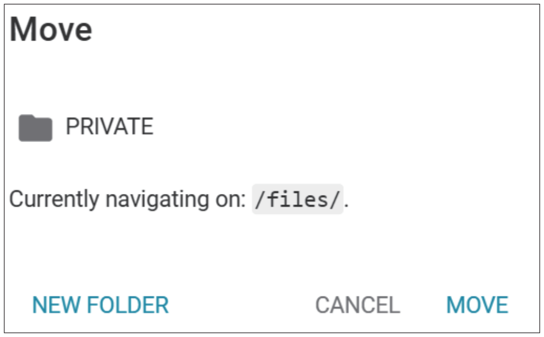
Moving Files and Folders

Moving Files allows you to change the location of files and folders. Moving Files and Folders can be performed on multiple items.

To move multiple items, select ✓ first,and select your desired files , then click ➡ :

New Folder: Create a new folder as the destination for the selected files.

Move: Move the selected files and folders to a designated directory.



Currently navigating on: `/files/`.

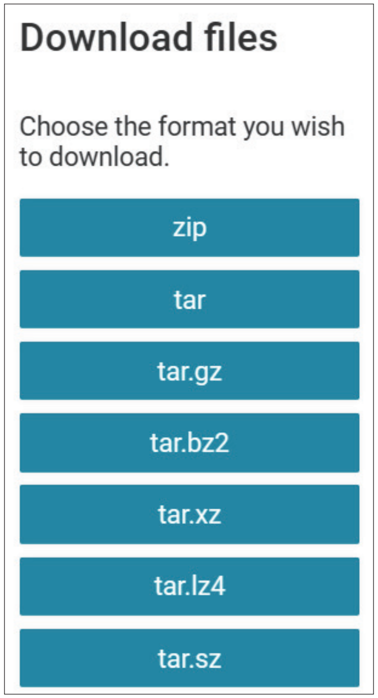
Downloading Files and Folders

Downloading Files allows you to save a copy of the files to your local drive. Downloading Files and Folders can be performed on multiple items.

To download multiple items, select ✓ first and select your desired files (the number of selected items will be shown next to the Download icon), click Download. ⬇1

Format: Select the format to zip your files to package the files as a single one.

The file will be saved to the default download directory of your browser.


Download files

Choose the format you wish to download.

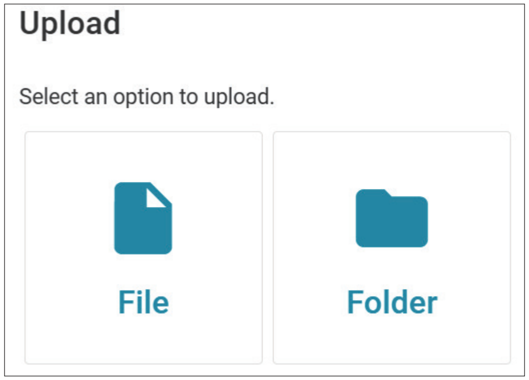
Uploading Files and Folders

Uploading Files allows you to upload a copy of the selected files from your local device.

To upload a file or folder, click ⬆.

File/Folder: Select a folder to upload all of its contents or multiple files to upload. Locate the files in your local directory. It may take a while depending on the size of the uploaded files.

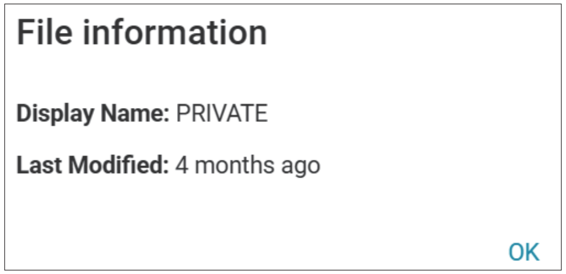
The uploaded files should be displayed in the current directory.


Upload

Select an option to upload.

Viewing File Information

Different information will be shown with respect to the file type. Without selecting a file, click Information to list the total number of files and folders under the current directory. Select a single file and click Information to display its name, size, last modified time, and related hash value such as MD5, SHA1, SHA256, and SHA512. These hash values are used for verifying the integrity of the file.



File information

Display Name: PRIVATE

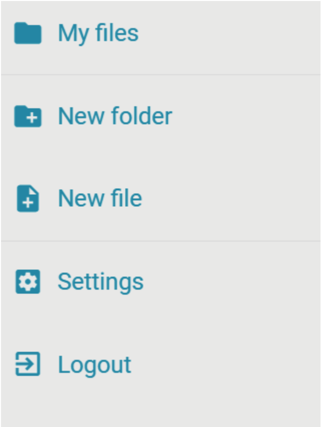
Last Modified: 4 months ago

Managing the File Structure

My files: Lists all the files in the shared directory.

New folder: Click to create a new folder under the current directory. The path of your current folder is shown at the top. It helps you navigate through the file structures. You can easily to go backward.

New file: Click to create a new file (text) under the current directory. The path is shown as breadcrumbs at the top. It helps you navigate through the file structures.



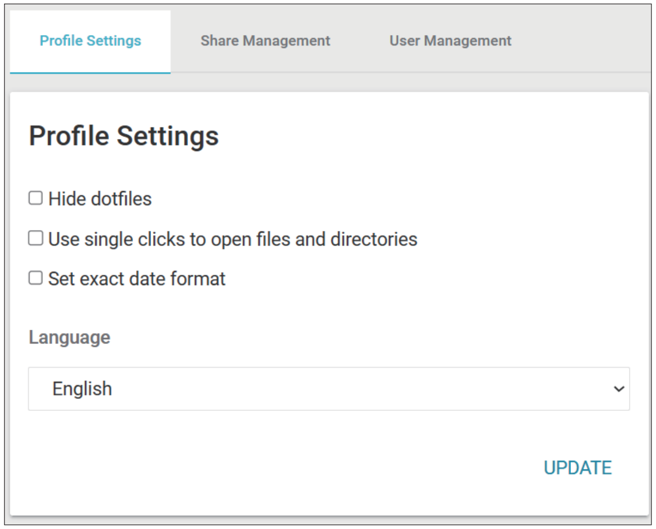
Settings

The Settings menu provides controls on how the file or folder information should be presented.

Profile Settings

Profile Settings are used for customizing the file information. The following file or folder properties can be defined.

Hide dotfiles: Dotfiles (e.g. config files of programs) will not be displayed.



Profile Settings

☐ Hide dotfiles

☐ Use single clicks to open files and directories

☐ Set exact date format

Language

English

Use single clicks to open files and directories: This permits users to open files with a single click instead of a double-click.

Set exact date format: The last modified date will be expressed as mm/dd/yyyy hh:mm AM/PM. If this option is not checked, the date will be expressed as in certain duration.

Language: Select the display language for the web.

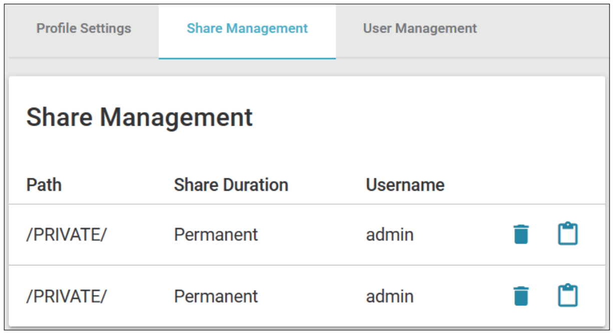
Share Management

The Share Management tab shows the sharing properties of a share folder.

Path: The path of the shared folder

Share Duration: The duration of the sharable link.

Username: The user that has been granted access to this folder.



Share Management

Path	Share Duration	Username
/PRIVATE/	Permanent	admin
/PRIVATE/	Permanent	admin

User Management

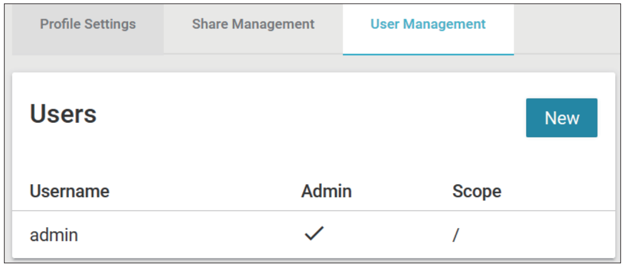
The User Management tab lists all the current users with the username and the authorized directory for access.

To create a new user, click **New**:

Username: Name the new user.

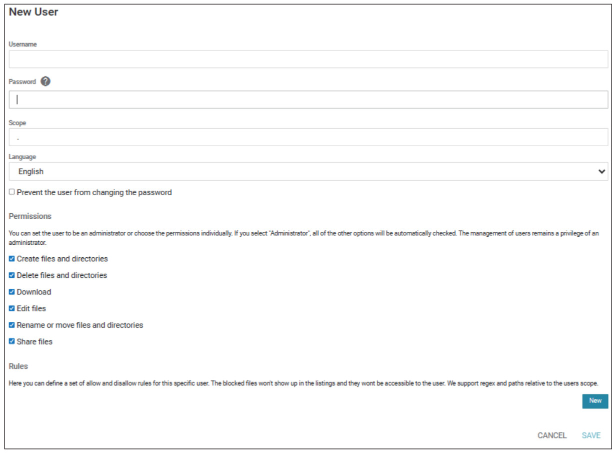
Password: Type the password of the new user. The password must be 10 to 15 characters long, include both upper- and lower-case letters and digits, and must not have identical characters in a row.

Scope: The directory permitted access. The "." means root directory, which means permitting every file and folder of the currently shared drive.



Users

Username	Admin	Scope
admin	✓	/



New User

Username

Password

Scope

.

Language

English

□ Prevent the user from changing the password

Permissions

You can set the user to be an administrator or choose the permissions individually. If you select "Administrator", all of the other options will be automatically checked. The management of users remains a privilege of an administrator.

☑ Create files and directories

☑ Delete files and directories

☑ Download

☑ Edit files

☑ Rename or move files and directories

☑ Share files

Rules

Here you can define a set of allow and disallow rules for this specific user. The blocked files won't show up in the listings and they wont be accessible to the user. We support regex and paths relative to the users scope.

Language: The language that is displayed on the web file access page.

Prevent the user from changing the password: Check this box to prevent users from changing the set password.

Permissions:
- Choose a specific permission for the user:
- Create files and directories
- Delete files and directories
- Download
- Edit files
- Rename or move files and directories
- Share files.

This user will be able to perform management functions on the shared file /folder via the control at the file access.

Rules: Rules define a set of file permissions that permit or block user's access to specific files. The regular expression (regex) is a sequence of characters that defines a search pattern to match file names for access control. For example, the expression /abc/ matches the sequence "abc" within a file name. And to match both .jpg and .png files, we can use the regex pattern: /\.(jpg|png)$/s.

User

This page allows you to set up user accounts for USB file sharing. Click **Save** at any time to save the changes you have made on this page. Click **Create User** to configure user permissions.

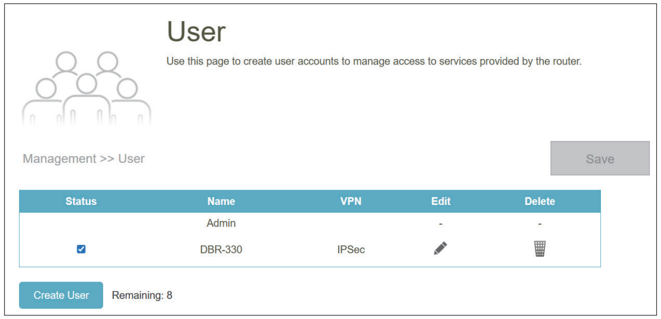
User Settings

User Name: Name a new user account.

Password: Enter a password for this user.

Status: Enable or disable the VPN function.

VPN Type: Grant the selected VPN function to the user.



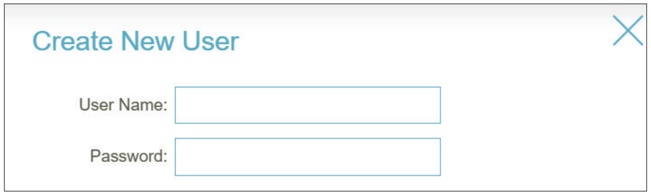
User

Use this page to create user accounts to manage access to services provided by the router.

Management >> User

Status	Name	VPN	Edit	Delete
	Admin		-	-
☑	DBR-330	IPSec	✎	🗑

Remaining: 8



Create New User

User Name:

Password:

Advanced

Parental Control

Go to **Advanced > 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. Click on **Profiles.**

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

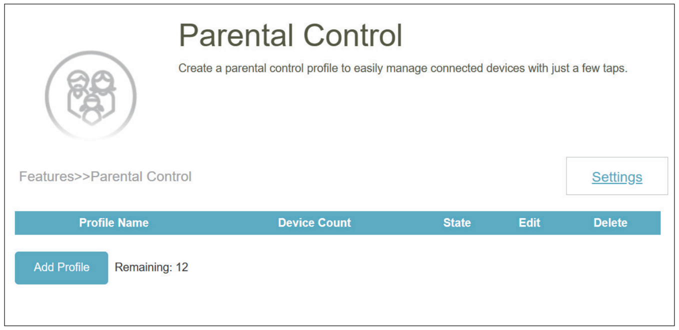
Profile Name: The name describes this profile.

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.



Parental Control

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

Features>>Parental Control

Profile Name	Device Count	State	Edit	Delete

Remaining: 12

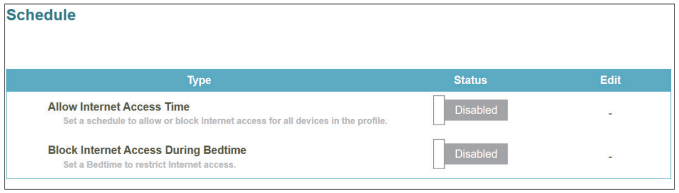
A maximum of 12 profiles can be defined. Once a profile has been set, you will start receiving weekly reports on Internet access activity of the clients through AI Assistant.

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 allowed 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.



Schedule

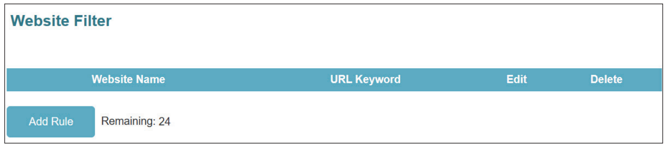
Type	Status	Edit
Allow Internet Access Time Set a schedule to allow or block Internet access for all devices in the profile.	Disabled	-
Block Internet Access During Bedtime Set a Bedtime to restrict Internet access.	Disabled	-

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.

Click **Apply** when you are done.

Website Filter



Website Filter

Website Name	URL Keyword	Edit	Delete

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

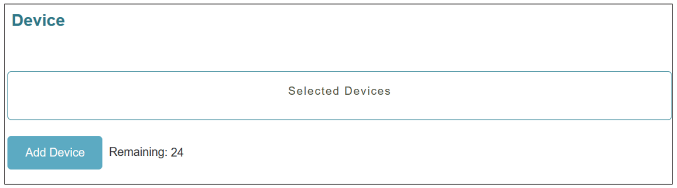
Website Name: Enter a name for the website. This blocks access to websites according to the domain names. For example, use "ABC.com" to block both "ABC.com" and "www.ABC.com".

URL Keyword: This blocks access to websites according to the keywords with matching URLs. For example, use "ABC" to block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC.

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

Device

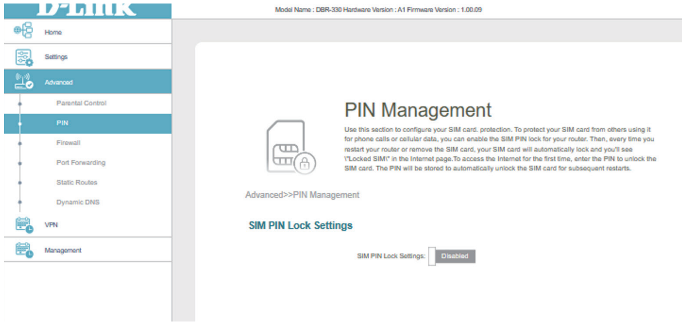
Click **Add Device** to add devices to be in a defined profile. Select devices from the list of connected devices to which you want to apply the access policy to, then click **Apply** to close the screen. Click **Save** to save your profile settings and the new profile will be added to the profile list. 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.



PIN

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

Inbox	
SIM PIN Lock Settings:	Enable or disable SIM PIN Lock.
SIM Card Status:	Displays the status of your SIM card.



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

PIN Management

Use this section to configure your SIM card. protection. To protect your SIM card from others using it for phone calls or cellular data, you can enable the SIM PIN lock for your router. Then, every time you restart your router or remove the SIM card, your SIM card will automatically lock and you'll see \"Locked SIM\" in the Internet page.To access the Internet for the first time, enter the PIN to unlock the SIM card. The PIN will be stored to automatically unlock the SIM card for subsequent restarts.

Advanced>>PIN Management

SIM PIN Lock Settings

SIM PIN Lock Settings: Disabled

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

Click **Apply** when you are done.

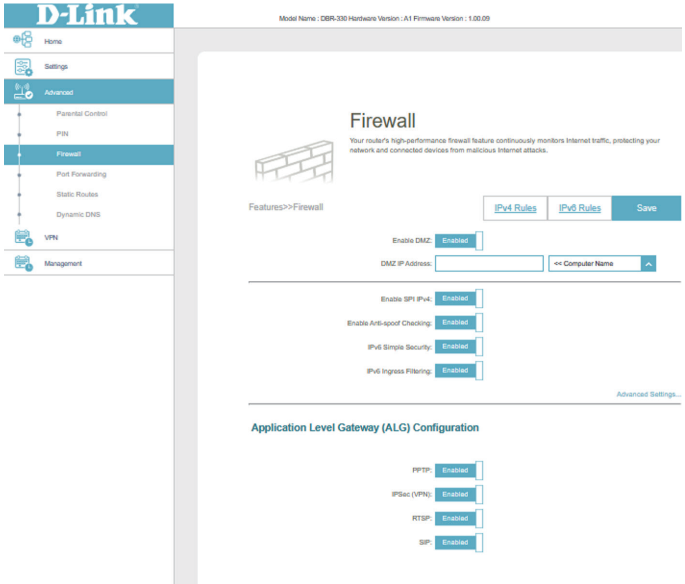
Firewall

The integrated firewall helps protect your network from malicious attacks over the Internet. In the Features menu on the bar on the top-left of the page, click **Firewall Settings**. 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.

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

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



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

Firewall

Your router's high-performance firewall feature continuously monitors Internet traffic, protecting your network and connected devices from malicious Internet attacks.

Features>>Firewall

Enable DMZ: Enabled

DMZ IP Address: << Computer Name

Enable SPI IPv4: Enabled

Enable Anti-spoof Checking: Enabled

IPv6 Simple Security: Enabled

IPv6 Ingress Filtering: Enabled

Application Level Gateway (ALG) Configuration

PPTP: Enabled

IPSec (VPN): Enabled

RTSP: Enabled

SIP: Enabled

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.

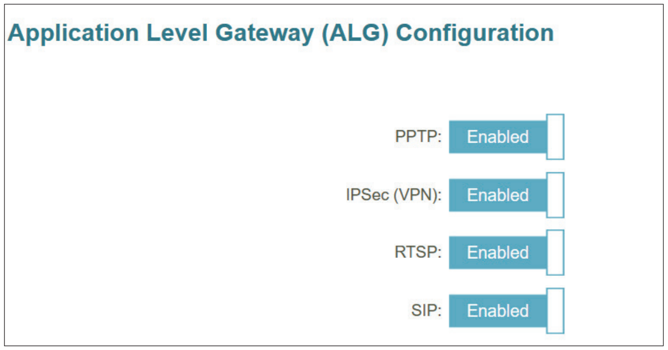
Enable Anti-Spoof Checking: Enable this feature to protect your network from certain kinds of "spoofing" attacks.

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

Advanced Settings

Application Level Gateway (ALG) Configuration



Application Level Gateway (ALG) Configuration

PPTP: Enabled

IPSec (VPN): Enabled

RTSP: Enabled

SIP: Enabled

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.

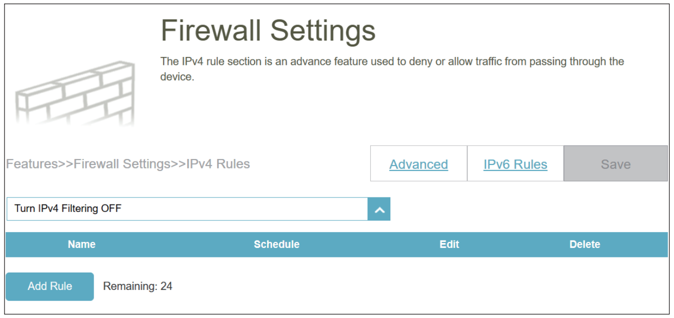
Firewall Settings - IPv4/IPv6 Rules

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 the **Firewall** section.

To begin, use the drop-down menu to select whether you want to **ALLOW** or **DENY** the rules you create. You can also choose to turn **OFF** filtering.

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

The IPv4 rule section is an advance feature used to deny or allow traffic from passing through the device.

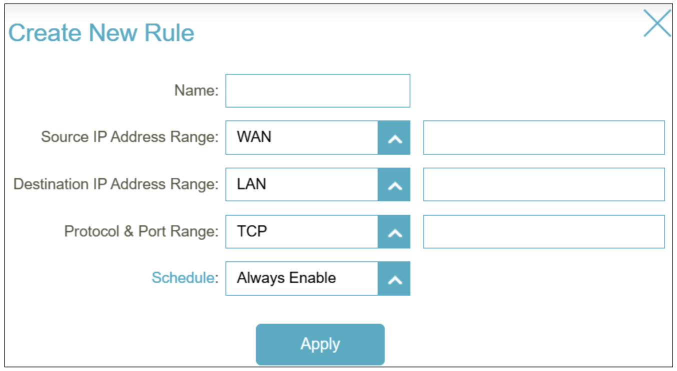
Features>>Firewall Settings>>IPv4 Rules

Turn IPv4 Filtering OFF

Name	Schedule	Edit	Delete

Remaining: 24

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:



Create New Rule

Name:

Source IP Address Range: WAN

Destination IP Address Range: LAN

Protocol & Port Range: TCP

Schedule: Always Enable

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.

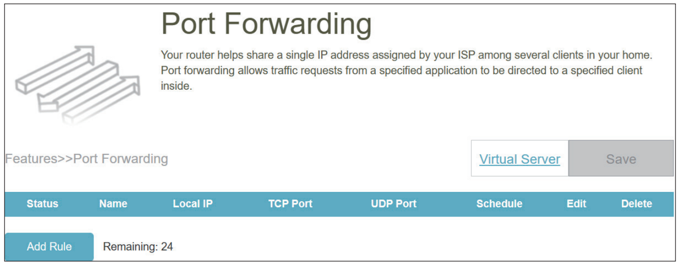
Protocol & Port Range: Select a traffic protocol to allow or deny (**Any**, **TCP**, or **UDP**) and then enter a range of ports (e.g. 21-23) that the rule will apply to. Select Any to allow/deny all types of traffic regardless of the port number.

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** 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.



Port Forwarding

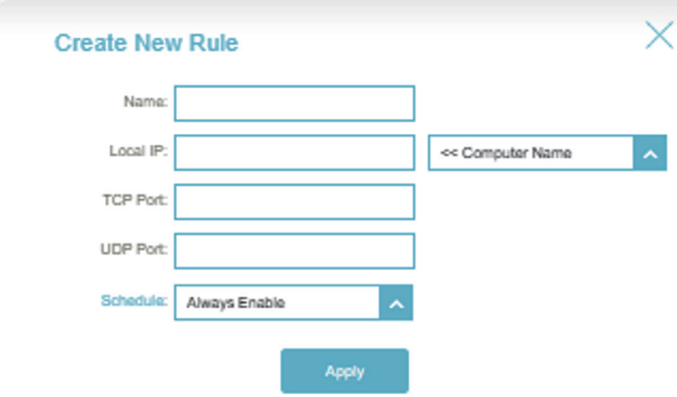
Your router helps share a single IP address assigned by your ISP among several clients in your home. Port forwarding allows traffic requests from a specified application to be directed to a specified client inside.

Features>>Port Forwarding

Status	Name	Local IP	TCP Port	UDP Port	Schedule	Edit	Delete

Remaining: 24

In the **Advanced** 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:



Create New Rule

Name:

Local IP: << Computer Name

TCP Port:

UDP Port:

Schedule: Always Enable

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** for more information.

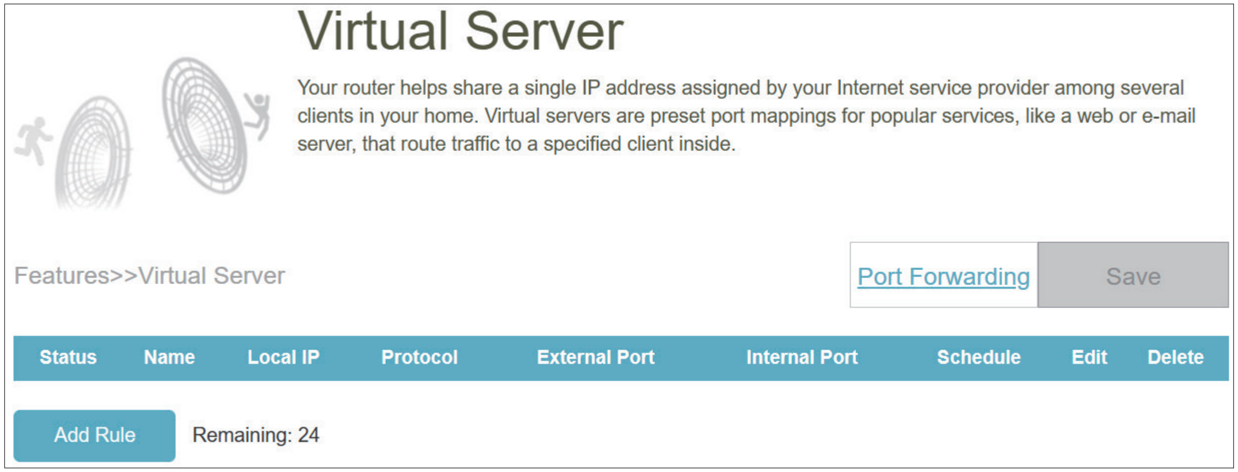
Click **Apply** when you are done.

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.



Virtual Server

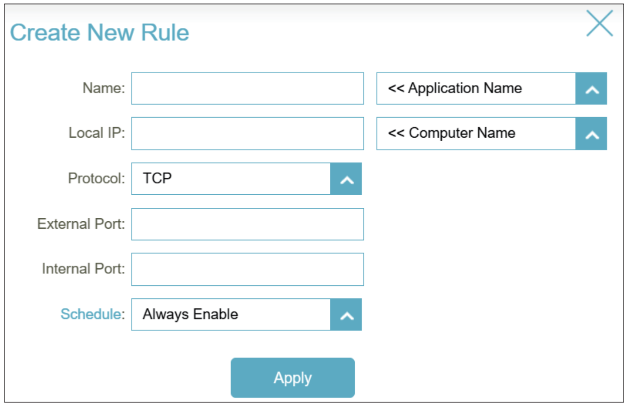
Your router helps share a single IP address assigned by your Internet service provider among several clients in your home. Virtual servers are preset port mappings for popular services, like a web or e-mail server, that route traffic to a specified client inside.

Features>>Virtual Server

Status	Name	Local IP	Protocol	External Port	Internal Port	Schedule	Edit	Delete

Remaining: 24

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:



Create New Rule

Name: << Application Name

Local IP: << Computer Name

Protocol: TCP

External Port:

Internal Port:

Schedule: Always Enable

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.

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.

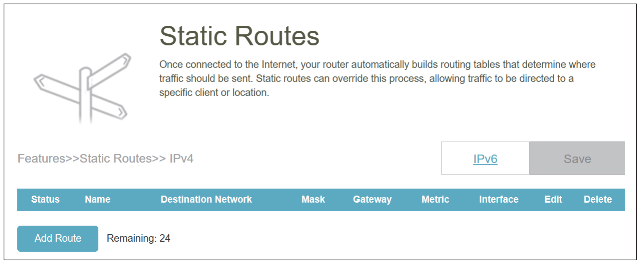
Schedule: Use the drop-down menu to select a time schedule that the rule will be enabled on. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedule** section. Refer to **Time & Schedule - Schedule** for more information.

Static Routes - IPv4

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

In the **Advanced** tab on the left side of the page, click **Static Routes**. To configure IPv6 routes, click **IPv6** and refer to **Static Routes - IPv6**. 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:



Static Routes

Once connected to the Internet, your router automatically builds routing tables that determine where traffic should be sent. Static routes can override this process, allowing traffic to be directed to a specific client or location.

Features>>Static Routes>> IPv4

Status	Name	Destination Network	Mask	Gateway	Metric	Interface	Edit	Delete

Remaining: 24

Name: Enter a name for the route.

Destination Network: Enter the destination IP address of this route.

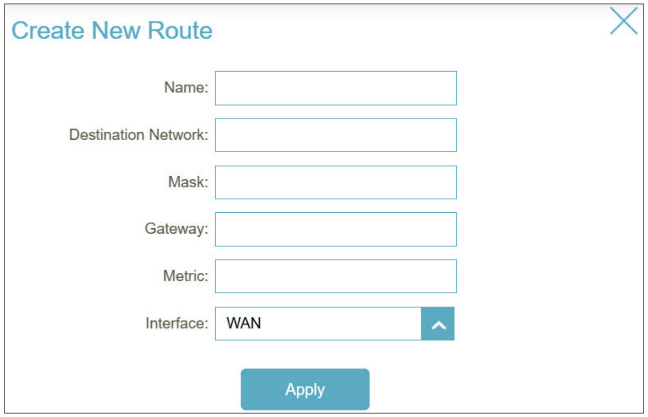
Mask: Enter the subnet mask of the route.

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

Metric: 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.



Create New Route

Name:

Destination Network:

Mask:

Gateway:

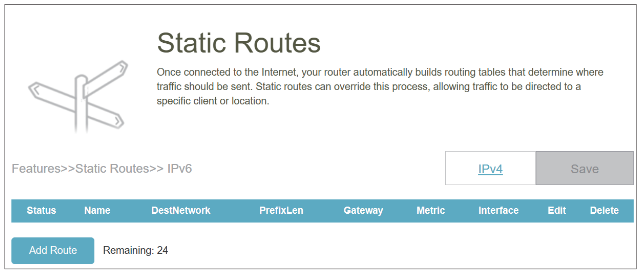
Metric:

Interface: WAN

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:



Static Routes

Once connected to the Internet, your router automatically builds routing tables that determine where traffic should be sent. Static routes can override this process, allowing traffic to be directed to a specific client or location.

Features>>Static Routes>> IPv6

Status	Name	DestNetwork	PrefixLen	Gateway	Metric	Interface	Edit	Delete

Remaining: 24

Name: Enter a name for the route.

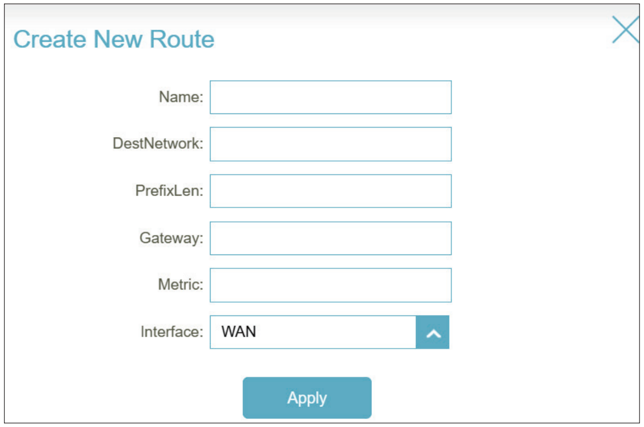
DestNetwork: This is the IP address of the router used to reach the specified destination.

PrefixLen: Enter the IPv6 address prefix length of the packets that will take this route.

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

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.



Create New Route

Name:

DestNetwork:

PrefixLen:

Gateway:

Metric:

Interface: WAN

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 **Advanced** 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.

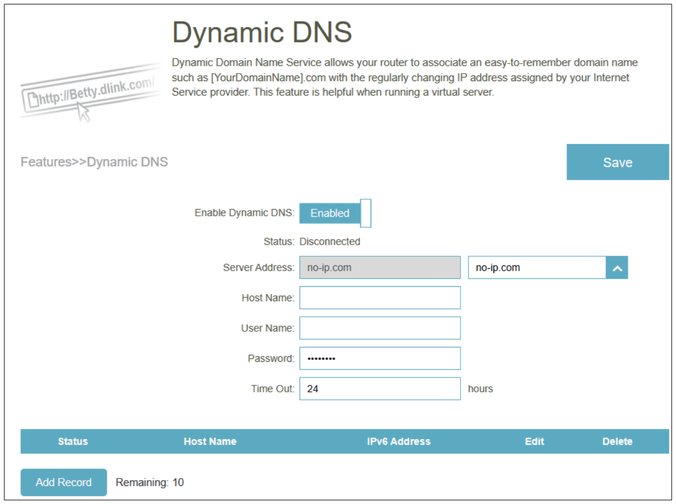
Server Address: Select a Dynamic DNS server from the drop-down menu.

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

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

Features>>Dynamic DNS

Enable Dynamic DNS:	Enabled
Status:	Disconnected
Server Address:	no-ip.com no-ip.com
Host Name:	
User Name:	
Password:	••••••••
Time Out:	24 hours

Status	Host Name	IPv6 Address	Edit	Delete

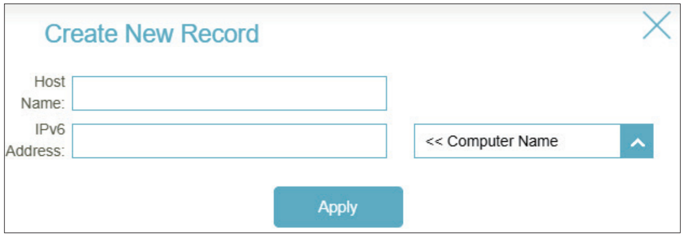
Remaining: 10

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.



Create New Record

Host Name:

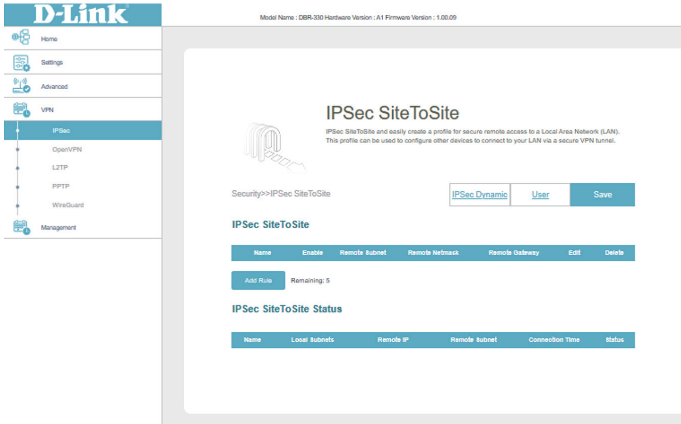
IPv6 Address:

VPN

IPSec

IPSec facilitates VPN communications with security capabilities. This page allows you to create an IPSec tunnel between two sites and set parameters for authentication method and encryption algorithm. To create user accounts with VPN privilege, go to **Management > User**.

Click **Add Rule** and configure the following to set up an IPSec profile for VPN connections:



Model Name : DBR-330 Hardware Version : A1 Firmware Version : 1.00.09

IPSec SiteToSite

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

Security>>IPSec SiteToSite

IPSec SiteToSite

Name	Enable	Remote Subnet	Remote Netmask	Remote Gateway	Edit	Delete

Remaining: 5

IPSec SiteToSite Status

Name	Local Subnets	Remote IP	Remote Subnet	Connection Time	Status

IPSec: Enable the IPSec function.

Connection Name: Name this IPSec connection.

Encap Mode: Select Tunnel for the encapsulation mode.

Encap Protocol: Select ESP for the encapsulation protocol.

IKEver: Select the IKE (Internet Key Exchange) version used for setting up secure connections

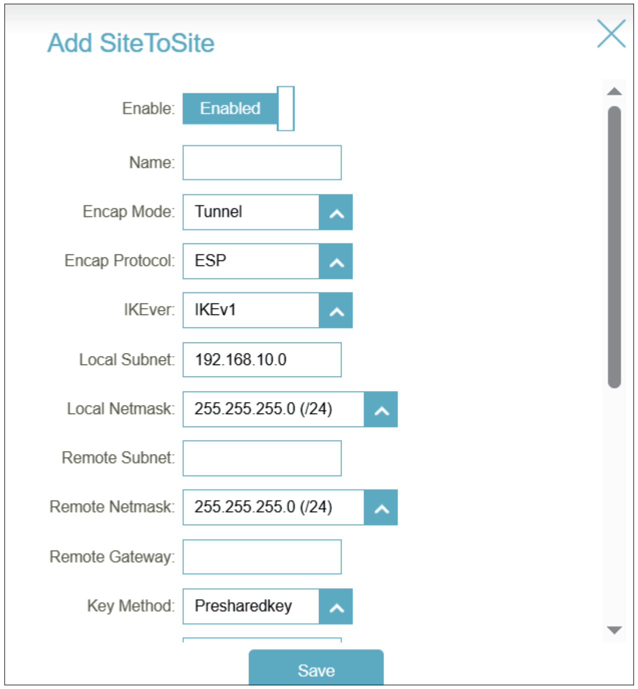
Local Subnet: Enter **IP Subnet** to specify local subnetwork.

Local Netmask: Enter the subnet mask for the local subnet.

Remote Subnet: Enter the subnet of the remote peer.

Remote Netmask: Enter the subnet mask for the remote subnet.

Remote Gateway: Enter the IP address of the remote device that can use this tunnel.



Add SiteToSite

Enable: Enabled

Name:

Encap Mode: Tunnel

Encap Protocol: ESP

IKEver: IKEv1

Local Subnet: 192.168.10.0

Local Netmask: 255.255.255.0 (/24)

Remote Subnet:

Remote Netmask: 255.255.255.0 (/24)

Remote Gateway:

Key Method: Presharedkey

Key Method: Select pre-shared key and enter the key below.

Pre-Shared Key: Enter a pre-shared key to authenticate a remote peer. Up to 16 characters including symbols can be entered. Both local and remote device of the VPN tunnel must use the same pre-shared Key.

Local ID Type: Select the ID format and specify the Local ID below: Username, FQDN, User_FQDN, Key_ID _ASCII, Key_ ID_HEX

Local ID: Enter the Local ID.

Remote ID Type: Select the ID format and specify the Remote ID below: Username, FQDN, User_FQDN, Key_ID _ASCII, Key_ ID_HEX

Remote ID: Enable or disable NAT traversal for the negotiation of an IPSec VPN connection. It allows IPSec VPN traffic to pass if NAT is used on the gateways.

Negotiation Mode: Select **Main** or **Aggressive** mode. The Main mode sends first two messages for negotiating the encryption and authentication method.

Auth Mode: Select the authentication mode: Client or None. If client is selected, enter the username and password below.

Username/ Password: Enter the Username and Password for client authentication.

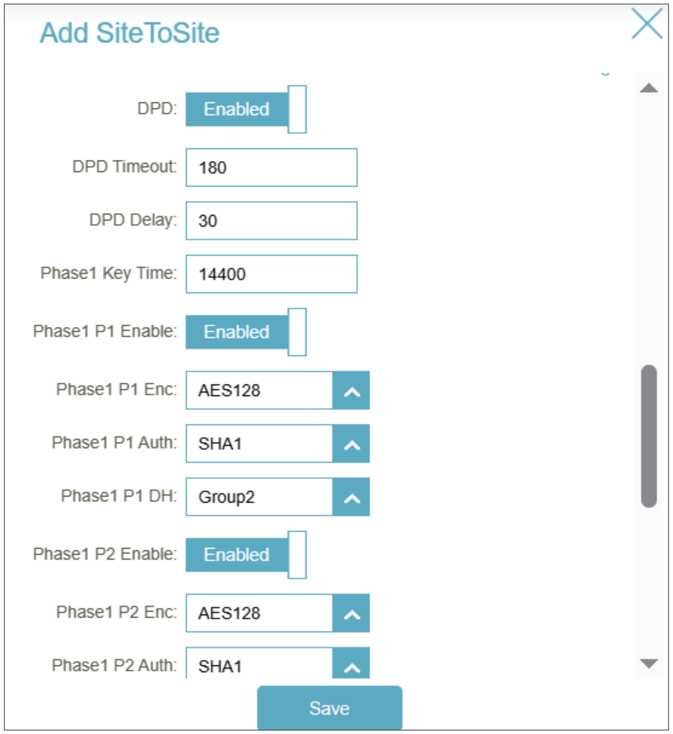
Advanced Settings

DPD: Enable Dead Peer Detection to detect if the remote peer is connected.

DPD Timeout: The time it must elapse before declaring a peer dead.

DPD Delay: The time the system must wait before sending DPD messages to its peer to check whether the peer is alive.

Key Exchange Phase 1



Add SiteToSite

DPD: Enabled

DPD Timeout: 180

DPD Delay: 30

Phase1 Key Time: 14400

Phase1 P1 Enable: Enabled

Phase1 P1 Enc: AES128

Phase1 P1 Auth: SHA1

Phase1 P1 DH: Group2

Phase1 P2 Enable: Enabled

Phase1 P2 Enc: AES128

Phase1 P2 Auth: SHA1

Phase1 Key Time: Enter the valid time for the key in seconds.

Phase1 P1/P2 Enable: Enable the P1 and P2 key exchange process.

Encryption Algorithm: Select encryption method as the algorithm for encrypting data packets. The options are **3DES, AES-128, AES-192** or **AES-256**.

Authentication Algorithm: The authentication algorithm validates data packets. Select **SHA1** or **SHA256**. Both local and remote device of the VPN tunnel must use the same authentication algorithm.

Phase1 P1/P2 DH: The Diffie-Hellman key exchange protocol offers different prime key Lengths in groups. Group 2 , 5 , and 14 has key size 1024 bit, 1536 bit and 2048 bit respectively.

Key Exchange Phase 2

Phase2 Key Time: Enter the valid time for the key in seconds.

Phase2 P1/P2 Enable: Enable the P1 and P2 key exchange process.

Encryption Algorithm: Select encryption method as the algorithm for encrypting data packets. The options are **3DES, AES-128, AES-192** or **AES-256**.

Authentication Algorithm: The authentication algorithm validates data packets. Select **SHA1** or **SHA256**. Both local and remote device of the VPN tunnel must use the same authentication algorithm.

Phase2 PFS: Enable or disable Perfect Forward Secrecy.

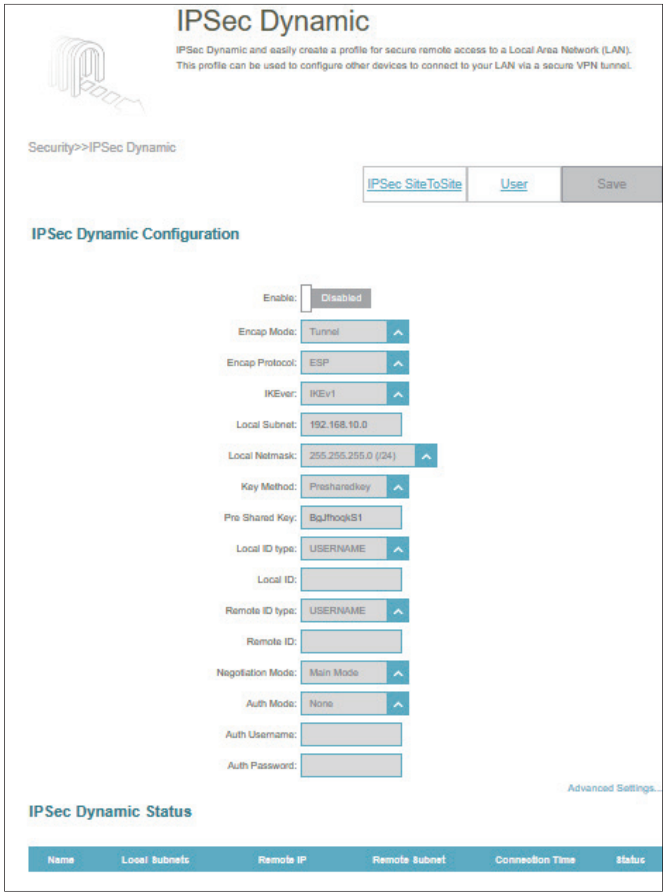
Key Life Time: Enter the amount of time that a key is active in Phase 2. Then select the unit: **Seconds, Minutes** or **Hours**.

Click **Save** when you are done. You can create up to 7 IPSec profiles.

IPSec Dynamic

The system's IPSec function supports VPN communications using dynamic IP addreses. Use the IPSec Dynamic to set up tunnels dynamically. To create user accounts with VPN privilege, go to **Management > User**.

Click **Enable** and configure the following to set up dynamic IPSec for VPN connections:



IPSec Dynamic

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

Security>>IPSec Dynamic

IPSec Dynamic Configuration

Enable:	Disabled
Encap Mode:	Tunnel
Encap Protocol:	ESP
IKEver:	IKEv1
Local Subnet:	192.168.10.0
Local Netmask:	255.255.255.0 (/24)
Key Method:	Presharedkey
Pre Shared Key:	BgJfhoqkS1
Local ID type:	USERNAME
Local ID:	
Remote ID type:	USERNAME
Remote ID:	
Negotiation Mode:	Main Mode
Auth Mode:	None
Auth Username:	
Auth Password:	

IPSec Dynamic Status

Name	Local Subnets	Remote IP	Remote Subnet	Connection Time	Status

IPSec: Enable the IPSec function.

Encap Mode: Select Tunnel for the encapsulation mode.

Encap Protocol: Select ESP for the encapsulation protocol.

IKEver: Select the IKE (Internet Key Exchange) version used for setting up secure connections.

Local Subnet: Enter IP Subnet to specify local subnetwork.

Local Netmask: Enter the subnet mask for the local subnet.

Key Method: Select Pre-shared key and enter the pre-shared key below.

PreShared Key: Enter the pre-shared key.

Local ID Type: Select the ID format and specify the Local ID below: Username, FQDN, User_FQDN, Key_ID _ASCII, Key_ ID_HEX.

Local ID: Enter the Local ID.

Remote ID Type: Select the ID format and specify the Local ID below: Username, FQDN, User_FQDN, Key_ID _ASCII, Key_ ID_HEX.

Remote ID: Enter the Remote ID.

Negotiation Mode: Select **Main** or **Aggressive** mode. The Main mode sends first two messages for negotiating the encryption and authentication method. In general, Aggressive mode is faster than the Main mode but offers less protection against authentication security.

Auth Mode: Select the authentication mode: Client or None. If client is selected, enter the username and password below.

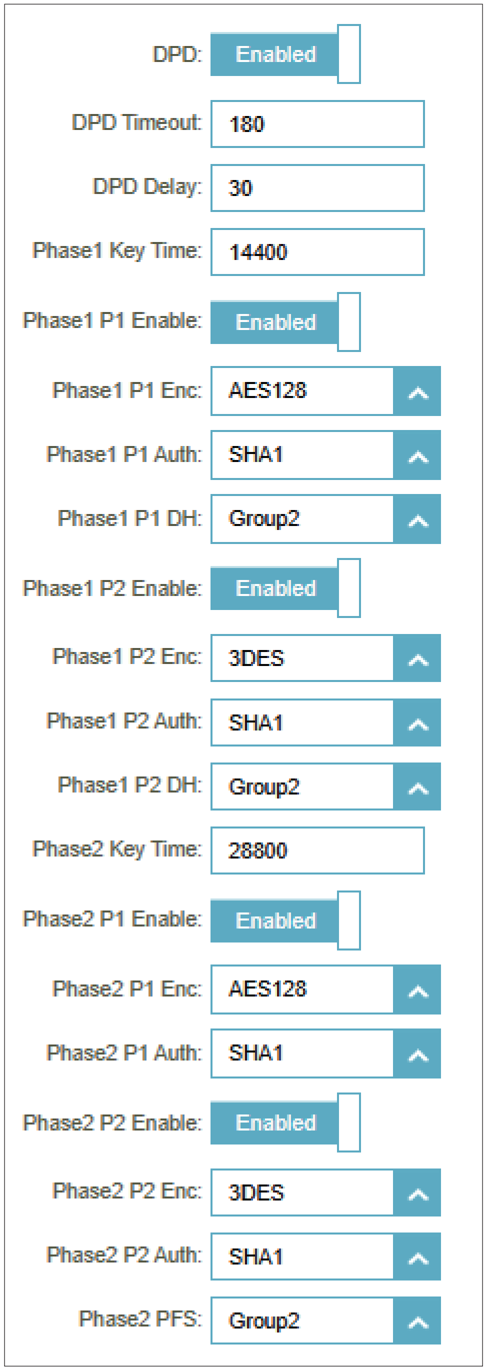
Username/ Password: Enter the Username and Password for client authentication.

Advanced Settings

DPD: Enable Dead Peer Detection to detect if the remote peer is connected.

DPD Timeout: The time it must elapse before declaring a peer dead.

DPD Delay: The time the system must wait before sending DPD messages to its peer to check whether the peer is alive.



DPD:	Enabled
DPD Timeout:	180
DPD Delay:	30
Phase1 Key Time:	14400
Phase1 P1 Enable:	Enabled
Phase1 P1 Enc:	AES128
Phase1 P1 Auth:	SHA1
Phase1 P1 DH:	Group2
Phase1 P2 Enable:	Enabled
Phase1 P2 Enc:	3DES
Phase1 P2 Auth:	SHA1
Phase1 P2 DH:	Group2
Phase2 Key Time:	28800
Phase2 P1 Enable:	Enabled
Phase2 P1 Enc:	AES128
Phase2 P1 Auth:	SHA1
Phase2 P2 Enable:	Enabled
Phase2 P2 Enc:	3DES
Phase2 P2 Auth:	SHA1
Phase2 PFS:	Group2

Key Exchange Phase 1

Phase1 Key Time: Enter the valid time for the key in seconds.

Phase1 P1/P2 Enable: Enable the P1 and P2 key exchange process.

Encryption Algorithm: Select encryption method as the algorithm for encrypting data packets. The options are **3DES, AES-128, AES-192** or **AES-256**.

Authentication Algorithm: The authentication algorithm validates data packets. Select **SHA1** or **SHA256**. Both local and remote device of the VPN tunnel must use the same authentication algorithm.

Phase1 P1/P2 DH: The Diffie-Hellman key exchange protocol offers different prime key lengths in groups. Group 2, 5, and 14 has key size 1024 bit, 1536 bit and 2048 bit, respectively.

Key Exchange Phase 2

Phase2 Key Time: Enter the valid time for the key in seconds.

Phase2 P1/P2 Enable: Enable the P1 and P2 key exchange process.

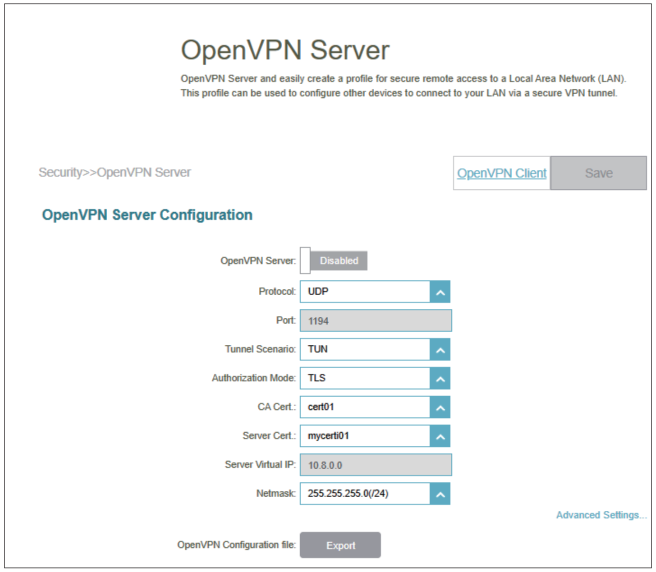
Encryption Algorithm: Select encryption method as the algorithm for encrypting data packets. The options are **3DES, AES-128, AES-192** or **AES-256**.

Authentication Algorithm: The authentication algorithm validates data packets. Select **SHA1** or **SHA256**. Both local and remote device of the VPN tunnel must use the same authentication algorithm.

Phase2 PFS: Enable or disable Perfect Forward Secrecy. It generates a new key with DH exchange in Phase 2 to improve the security of IPSec data communication.

OpenVPN

In the **VPN** tab on the left side of the page, click **OpenVPN**. This page will help you configure the **OpenVPN Server** feature of your router. Before proceeding, ensure that your Internet connection is working properly. We recommend configuring Dynamic DNS before proceeding with OpenVPN 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 Client settings, click the **OpenVPN Client** tab. Click **Save** at any time to save the changes you have made on this page.



OpenVPN Server

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

Security>>OpenVPN Server

OpenVPN Server Configuration

OpenVPN Server: Disabled
Protocol: UDP
Port: 1194
Tunnel Scenario: TUN
Authorization Mode: TLS
CA Cert.: cert01
Server Cert.: mycerti01
Server Virtual IP: 10.8.0.0
Netmask: 255.255.255.0(/24)

OpenVPN Configuration file:

OpenVPN Server: Enable or disable the OpenVPN server.

Protocol: Select the communication protocol: TCP or UDP.

Port: Enter the TCP or UDP port to be used for OpenVPN. The default is TCP 4430 or UDP 1194.

Tunnel Scenario: Select TUN or TAP. TUN can be used in network layer 3 for IP routing while TAP works in network layer 2 for Ethernet bridging.

Authorization Mode: Select either TLS or Static Key. If TLS is selected, enter the Server Virtual Ip and Netmask. If Static key is selected, enter **Local Endpoint**, **Remote Endpoint IP addresses, and Static Key** below.

Local/Remote Endpoint IP Address: Enter the Local and Remote Endpoint IP addresses if Static Key is selected for authorization in TUN tunneling scenario.

Server Virtual IP/ Netmask: Enter a virtual IP address and netmask for the server if TLS is selected above in TUN tunneling scenario.

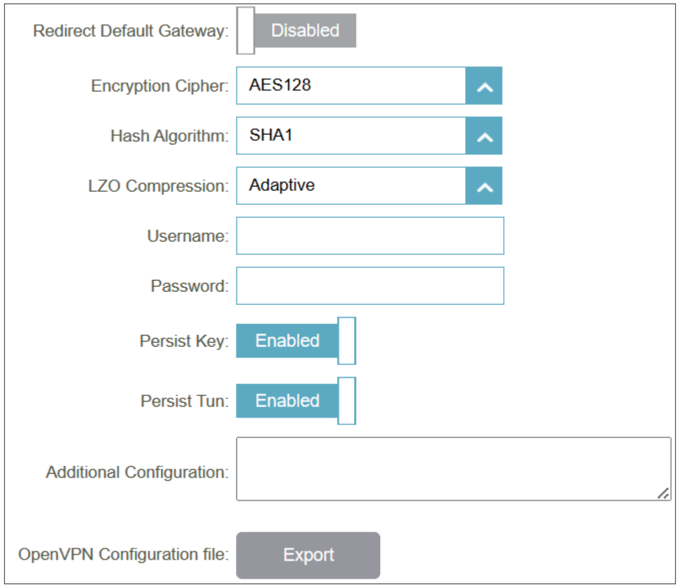
DHCP-Proxy Mode: Enable or disable DHCP proxy if TAP is selected for tunneling.

IP Pool: Enter the start and end IP address for DHCP IP assignment.

Gateway: Enter the gateway's IP address.

Netmask: Enter the netmask of the above IP address.

Advanced Settings



Redirect Default Gateway: Disabled

Encryption Cipher: AES128

Hash Algorithm: SHA1

LZO Compression: Adaptive

Username:

Password:

Persist Key: Enabled

Persist Tun: Enabled

Additional Configuration:

OpenVPN Configuration file: Export

Redirect Default Gateway: Enable or disable gateway redirection.

Encryption Cipher: Select encryption cipher strength: **AES 128, AES 192 or AES 256.**

Hash Algorithm: Select the hashing algorithm: SHA1, MD4, SHA2-256 or SHA2-512.

LZO Compression: Enable or disable LZO compression to compress packets.

Username/ Password: Enter the username and password

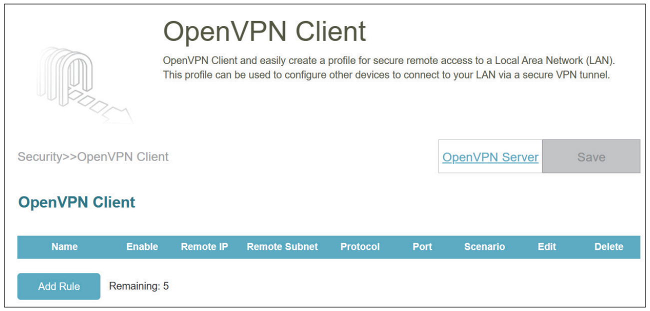
Persist Key: Enable the Persist Key. Enabling this to keep the private key and credentials in memory during reconnection.

Persist Tun: Enable the Persist Tun. Enabling this to keep the virtual network interface open when connection restarts or renegotiates.

Additional Configuration: Enter configuration setting here.

Export: Export the OpenVPN configuration file.

In the **VPN** tab on the left side of the page, click **OpenVPN**. This page will help you configure the OpenVPN client feature of your router. Click **Add Rule** to add a new client setting. Click **Save** at any time to save the changes you have made on this page.



OpenVPN Client

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

Security>>OpenVPN Client

OpenVPN Client

Name	Enable	Remote IP	Remote Subnet	Protocol	Port	Scenario	Edit	Delete

Remaining: 5

OpenVPN Client: Enable or disable the OpenVPN client function.

Name: Enter a name for this client configuration.

Protocol: Select the communication protocol: TCP or UDP.

Port: Enter the TCP or UDP port to be used for OpenVPN. he default is TCP 4430 or UDP 1194.

Tunnel Scenario: Select TUN or TAP. TUN can be used in network layer 3 for IP routing while TAP works in network layer 2 for Ethernet bridging.

Remote IP: Enter the IP Address of the remote end.

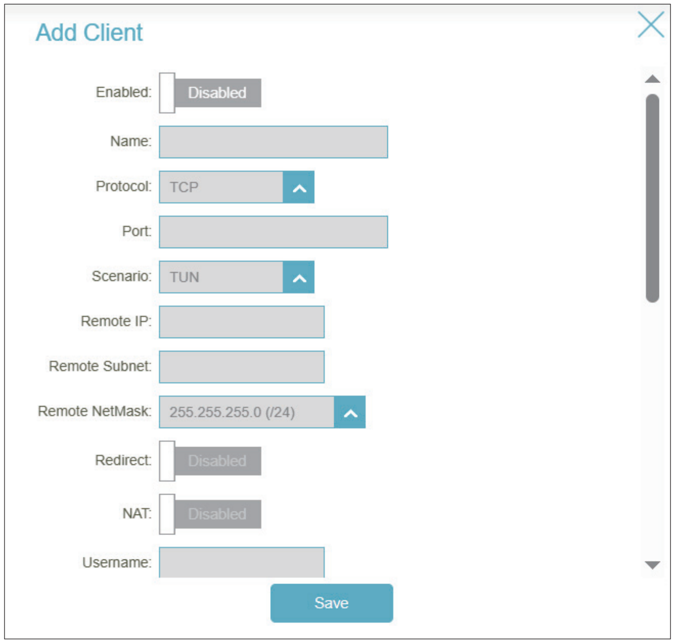
Remote Subnet: Enter the IP subnet of the remote site.

Remote NetMask: Enter the subnet mask of the remote subnet.

Redirect: Enable or disable gateway redirection.

NAT: Enable or disable Network Address Translation (NAT).

Username/ Password: Enter the Username and Password.



Add Client

Enabled: Disabled

Name:

Protocol: TCP

Port:

Scenario: TUN

Remote IP:

Remote Subnet:

Remote NetMask: 255.255.255.0 (/24)

Redirect: Disabled

NAT: Disabled

Username:

Authorization Mode: Select either TLS or Static Key. If TLS is selected, select the CA and Server certificate. Go to **Features > Certificates** to obtain configured certificates. If Static key is selected, enter both **Local Endpoint** and **Remote Endpoint IP addresses** below.

CA Certificate/ Client Certificate/ Client Key: Select the CA and Client certificate and the Client key if TLS is selected for authorization.

Local/Remote Endpoint IP Address: Enter the Local and Remote Endpoint IP addresses if Static Key is selected for authorization in TUN tunneling scenario.

Encryption Cipher: Select encryption cipher strength: **AES 128, AES 192 or AES 256.**

Hash Algorithm: Select the hashing algorithm: SHA1, MD4, SHA2-256 or SHA2-512.

LZO Compression: Enable or disable LZO compression to compress packets.

Persist Key: Enable the Persist Key. Enabling this to keep the private key and credentials in memory during reconnection.

Persist Tun: Enable the Persist Tun. Enabling this to keep the virtual network interface open when connection restarts or renegotiates.

Additional Configuration: Enter configuration setting here.

Click **Save** to close the configuration screen.

L2TP

VPN connections use Layer 2 Tunneling Protocol (L2TP) to build tunnels. The L2TP Server page allows you to configure L2TP Server parameters to facilitate VPN connections. Click **Save** at any time to save the changes you have made on this page.

L2TP Server: Enable or disable the L2TP server function.

L2TP Over IPsec: Enable or disable IPsec security for L2TP.

PSK: If IPsec is enabled, enter the passkey.

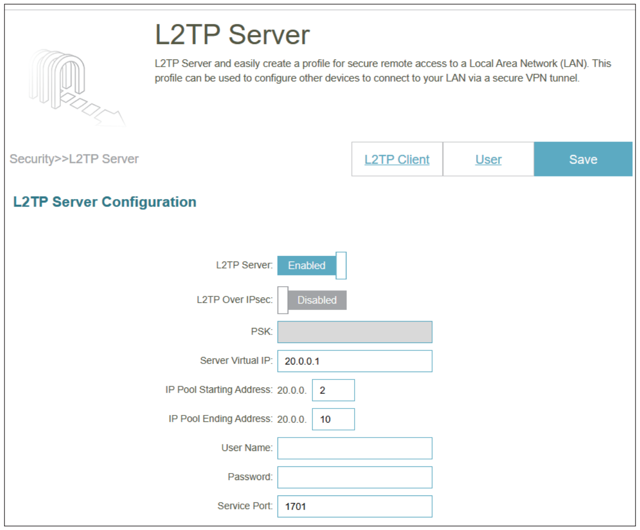
Server Virtual IP: Enter the IP address of the virtual server.

IP Pool Starting Address: Enter the starting IP Address for the IP address assignment.

IP Pool Ending Address: Enter the ending IP Address for the IP address assignment.

Username/Password: Enter the Username and Password.

Service Port: Enter the port number for service communications. The default is 1701.



L2TP Server

L2TP Server and easily create a profile for secure remote access to a Local Area Network (LAN). This profile can be used to configure other devices to connect to your LAN via a secure VPN tunnel.

Security>>L2TP Server

L2TP Server Configuration

L2TP Server: Enabled

L2TP Over IPsec: Disabled

PSK:

Server Virtual IP: 20.0.0.1

IP Pool Starting Address: 20.0.0. 2

IP Pool Ending Address: 20.0.0. 10

User Name:

Password:

Service Port: 1701

Advanced Settings

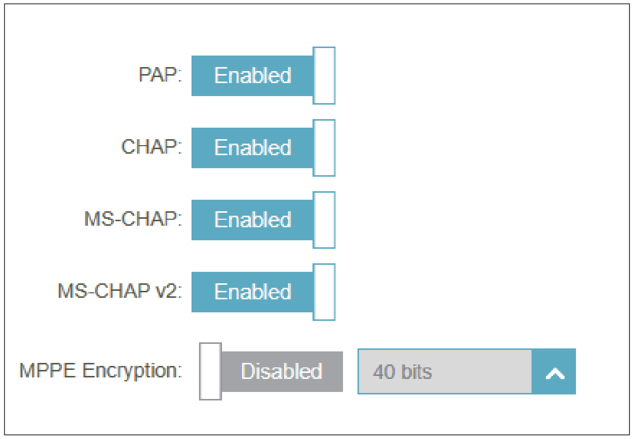
PAP: Enable or disable the PAP authentication protocol type.

CHAP: Enable or disable the CHAP authentication protocol type.

MS-CHAP: Enable or disable the MS-CHAP authentication protocol type.

MS-CHAP v2: Enable or disable the MS-CHAP v2 authentication protocol type.

MPPE Encryption: Enable or disable the MPPE Encryption and select encryption cipher strength: 40 or 128 bits if it enabled.



PAP: Enabled

CHAP: Enabled

MS-CHAP: Enabled

MS-CHAP v2: Enabled

MPPE Encryption: Disabled 40 bits

VPN connections use Layer 2 Tunneling Protocol (L2TP) to build tunnels. The L2TP Server page allows you to configure the L2TP client feature of the router to connect to a remote L2TP server. Click **Save** at any time to save the changes you have made on this page.

L2TP Client: Enable or disable the L2TP client function.

Tunnel Name: Enter a name for the tunnel.

L2TP Over IPsec: Enable or disable IPsec security for L2TP.

PSK: If IPsec is enabled, enter the passkey.

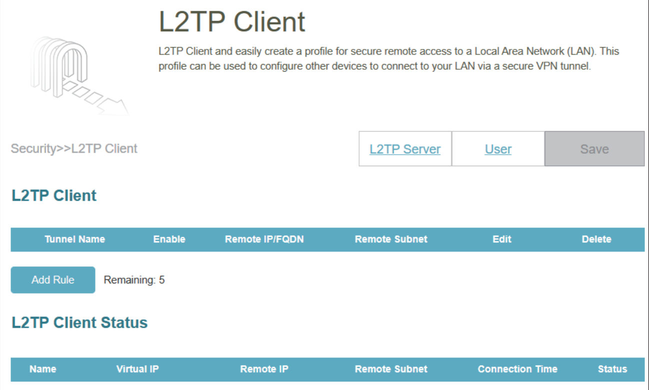
Service Port: Enter the port number for service communications. The default is 1701.

Remote IP/FQDN: Enter the Internet address of the virtual server.

MTU: Enter the Maximum Transmission Unit.

Username/ Password: Enter the Username and Password.

Remote Subnet: Enter the subnet of the remote end.



L2TP Client

L2TP Client and easily create a profile for secure remote access to a Local Area Network (LAN). This profile can be used to configure other devices to connect to your LAN via a secure VPN tunnel.

Security>>L2TP Client

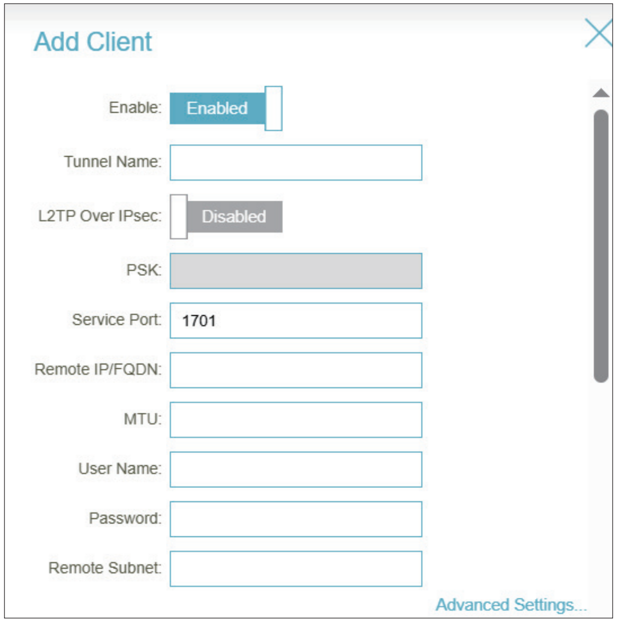
L2TP Client

Tunnel Name	Enable	Remote IP/FQDN	Remote Subnet	Edit	Delete

Remaining: 5

L2TP Client Status

Name	Virtual IP	Remote IP	Remote Subnet	Connection Time	Status



Add Client

Enable:	Enabled
Tunnel Name:	
L2TP Over IPsec:	Disabled
PSK:	
Service Port:	1701
Remote IP/FQDN:	
MTU:	
User Name:	
Password:	
Remote Subnet:	

Advanced Settings

PAP: Enable or disable the PAP authentication protocol type.

CHAP: Enable or disable the CHAP authentication protocol type.

MS-CHAP Enable or disable the MS-CHAP authentication protocol type.

MS-CHAP v2: Enable or disable the MS-CHAP v2 authentication protocol type.

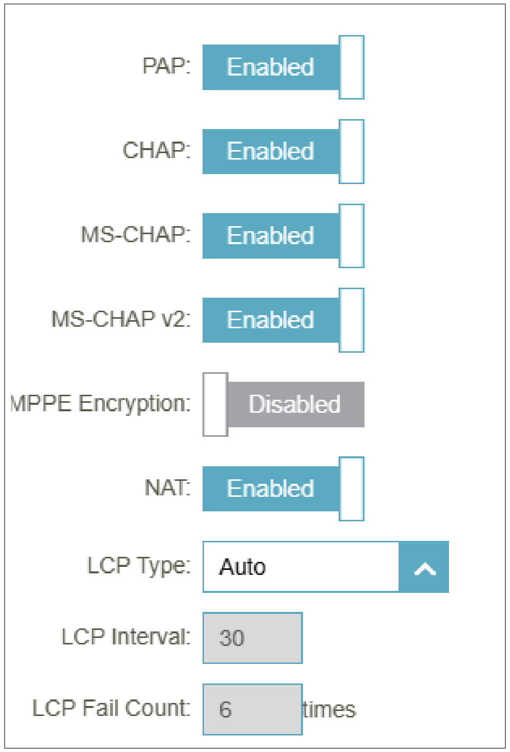
MPPE Encryption: Enable or disable the MPPE Encryption and select encryption cipher strength: 40 or 128 bits if it enabled.

NAT: Enable or disable the NAT function.

LCP Type: Select the Link Control Protocol (LCP) Type: Auto, Manual, or Disable.

LCP Interval: Enter the time interval between LCP Echo-Request messages to determine if a connection is alive if manual LCP type is selected. The default is 30.

LCP Fall Count: Enter the maximum number of allowed LCP connection failures before a connection is declared down if manual LCP type is selected. The default is 6.



PAP: Enabled

CHAP: Enabled

MS-CHAP: Enabled

MS-CHAP v2: Enabled

MPPE Encryption: Disabled

NAT: Enabled

LCP Type: Auto

LCP Interval: 30

LCP Fail Count: 6 times

PPTP

PPTP is another tunnelling technology for VPN. It differs from L2TP in many aspects, including security and connection speed. Click **Save** at any time to save the changes you have made on this page.

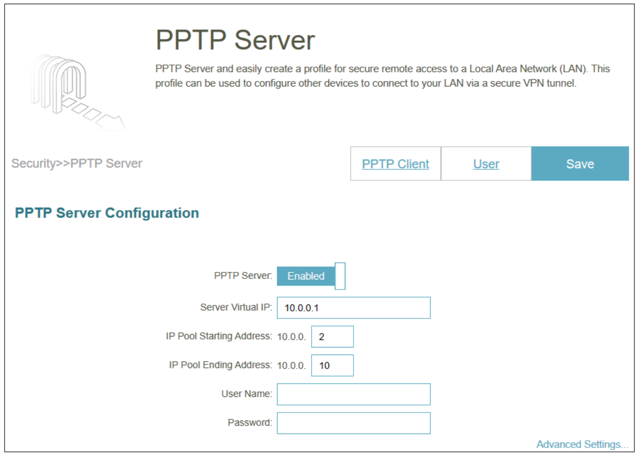
PPTP Server: Enable or disable the PPTP server function.

Server Virtual IP: Enter a name for the tunnel.

IP Pool Starting Address: Enter the starting IP Address for the IP address assignment.

IP Pool Ending Address: Enter the ending IP Address for the IP address assignment.

Username/ Password: Enter the Username and Password.



PPTP Server

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

PPTP Server Configuration

PPTP Server: Enabled

Server Virtual IP: 10.0.0.1

IP Pool Starting Address: 10.0.0. 2

IP Pool Ending Address: 10.0.0. 10

User Name:

Password:

Advanced Settings...

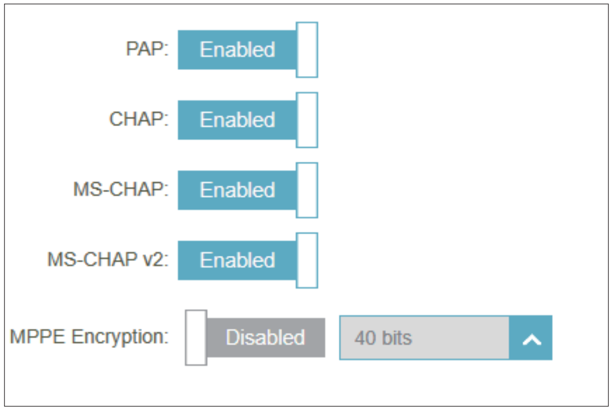
PAP: Enable or disable the PAP authentication protocol type.

CHAP: Enable or disable the CHAP authentication protocol type.

MS-CHAP Enable or disable the MS-CHAP authentication protocol type.

MS-CHAP v2: Enable or disable the MS-CHAP v2 authentication protocol type.

MPPE Encryption: Enable or disable the MPPE Encryption and select encryption cipher strength: 40 or 128 bits if it enabled.



PAP: Enabled

CHAP: Enabled

MS-CHAP: Enabled

MS-CHAP v2: Enabled

MPPE Encryption: Disabled 40 bits

PPTP is another tunnelling technology for VPN. It differs from L2TP in many aspects, including security and connection speed. The Client page allows you to configure PPTP client features for connection to a remote PPTP server. Click **Save** at any time to save the changes you have made on this page.

PPTP Client: Enable or disable the L2TP client function.

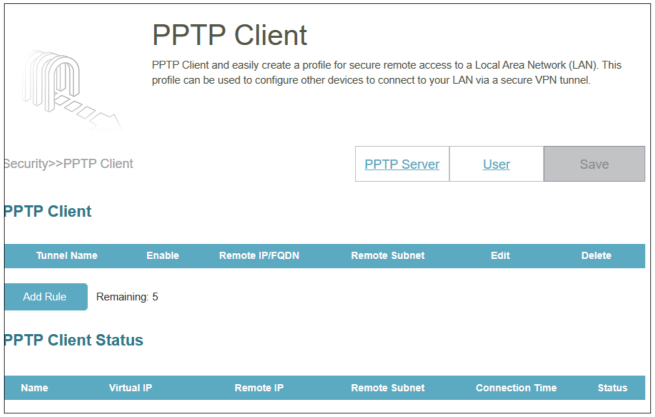
Tunnel Name: Enter a name for the tunnel.

Remote IP/FQDN: Enter the Internet address of the virtual server.

MTU: Enter the Maximum Transmission Unit.

Username/ Password: Enter the Username and Password.

Remote Subnet: Enter the subnet of the remote end.



PPTP Client

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

Security>>PPTP Client

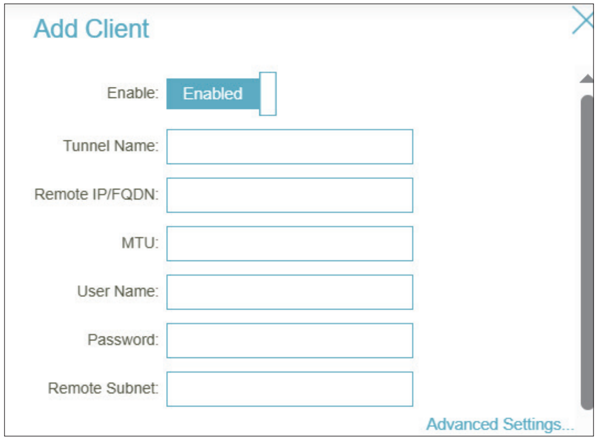
PPTP Client

Tunnel Name	Enable	Remote IP/FQDN	Remote Subnet	Edit	Delete

Remaining: 5

PPTP Client Status

Name	Virtual IP	Remote IP	Remote Subnet	Connection Time	Status



Add Client

Enable: Enabled

Tunnel Name:

Remote IP/FQDN:

MTU:

User Name:

Password:

Remote Subnet:

WireGuard

WireGuard is a more recent and secure protocol designed to support simple and yet efficient VPN connections. This page allows you to configure WireGuard server functions. Click **Save** at any time to save the changes you have made on this page.

Server Configuration

WireGuard Server: Enable or disable the WireGuard server function.

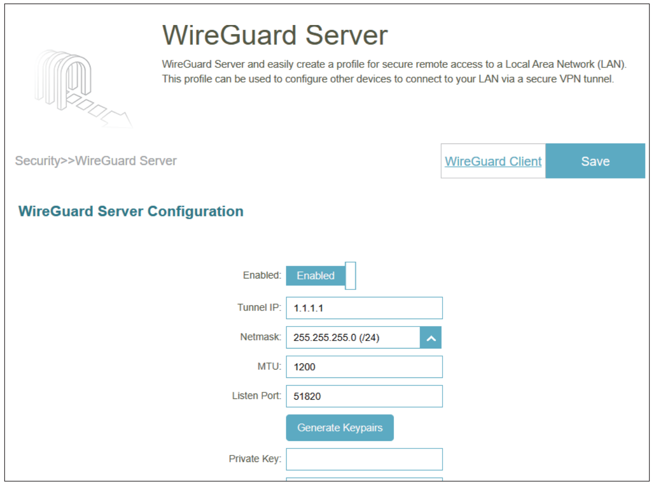
Tunnel IP: Enter the IP address for the tunnel.

Netmask: Enter the subnet mask of the tunnel IP address.

MTU: Enter the Maximum Transmission Unit.

Listen Port: Enter the port number of WireGuard communication.

Public Key/ Private Key: Click **Generate Keypairs** to obtain a public and a private key for connection authentication.



WireGuard Server

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

WireGuard Server Configuration

Enabled: Enabled

Tunnel IP: 1.1.1.1

Netmask: 255.255.255.0 (/24)

MTU: 1200

Listen Port: 51820

Private Key:

Peer Configuration

Enabled: Enable or disable the connection of the remote peer.

Peer IP: Enter the IP address of the remote peer

NetMask: Select the subnet mask of the remote peer's IP address.

Private Key: The Private Key required for connection authentication.

Public Key: The Public Key required for connection authentication.

Preshared Key: Enable or disable Preshared key. Then enter the Preshared Key if enabled.

Allowed IP: Enter the IP subnetworks that would be allowed for data transmission using this peer connection.

WireGuard is a more recent and secure protocol designed to support simple and yet efficient VPN connections. The Client page allows you to configure the client feature for connection to a WireGuard server. Click **Save** at any time to save the changes you have made on this page.

WireGuard Client: Enable or disable the WireGuard client function.

Name: Enter a name for the tunnel.

Tunnel IP: Enter the IP Address for the tunnel.

Netmask: Enter the subnet mask for the above tunnel IP address.

MTU: Enter the Maximum Transmission Unit.

Private Key: Enter the private key required for authentication.

Preshared Key: Enter the preshared key required for authentication.

Remote IP: Enter the IP address of the remote end of the VPN connection.

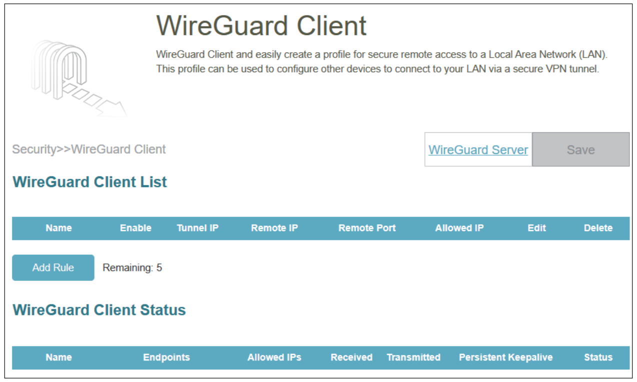
Remote Port: Enter the port of the remote end of the VPN connection.

Remote Public Key: Enter the public key used by the remote end for authentication.

Keep Alive Enabled: Enter the ending IP Address for the IP address assignment.

Keep Alive Time: Specify the duration of inactivity after which the connection will be terminated.

Allowed IP: Enter the IP subnetworks that should use this tunnel for data transmission.



WireGuard Client

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

Security>>WireGuard Client

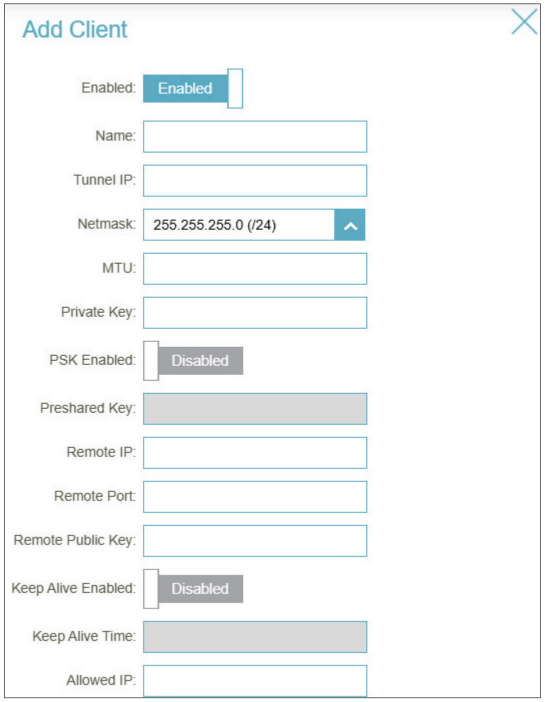
WireGuard Client List

Name	Enable	Tunnel IP	Remote IP	Remote Port	Allowed IP	Edit	Delete

Remaining: 5

WireGuard Client Status

Name	Endpoints	Allowed IPs	Received	Transmitted	Persistent Keepalive	Status



Add Client

Enabled:	Enabled
Name:	
Tunnel IP:	
Netmask:	255.255.255.0 (/24)
MTU:	
Private Key:	
PSK Enabled:	Disabled
Preshared Key:	
Remote IP:	
Remote Port:	
Remote Public Key:	
Keep Alive Enabled:	Disabled
Keep Alive Time:	
Allowed IP:	

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

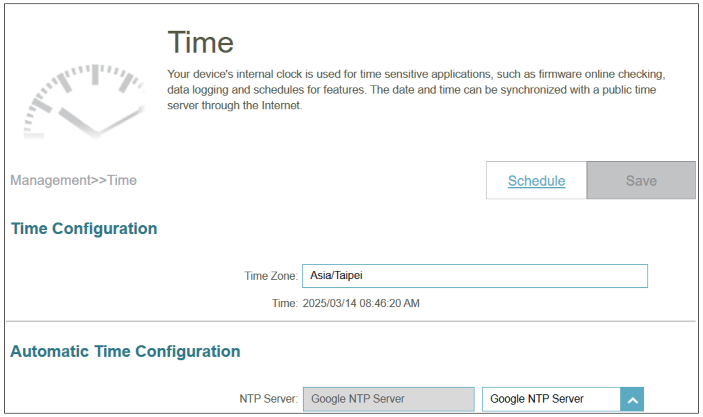
Time Configuration

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 your router: D-Link NTP Server or Google NTP Server.
Choose Manual to set the NTP server's IP address or domain name.



Time

Your device's internal clock is used for time sensitive applications, such as firmware online checking, data logging and schedules for features. The date and time can be synchronized with a public time server through the Internet.

Management>>Time

Time Configuration

Time Zone: Asia/Taipei

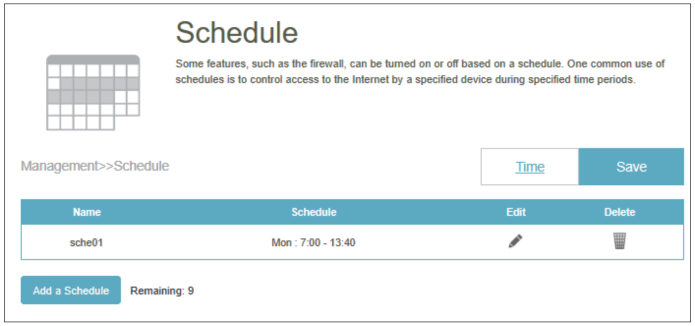
Time: 2025/03/14 08:46:20 AM

Automatic Time Configuration

NTP Server: Google NTP Server | Google NTP Server

Time & Schedule - Schedule

Some functions, for example, Port Forwarding and scheduled system log emailing , can be controlled through a pre-configured schedule. To create, edit, or delete schedules, click **Schedule** from the **Time** page . To return to the **Time** page, click **Time**.



Schedule

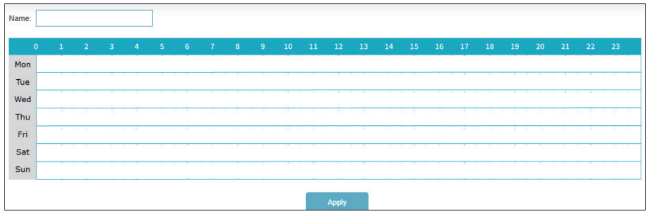
Some features, such as the firewall, can be turned on or off based on a schedule. One common use of schedules is to control access to the Internet by a specified device during specified time periods.

Management>>Schedule

Name	Schedule	Edit	Delete
sche01	Mon : 7:00 - 13:40	✎	🗑

Remaining: 9

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



First, enter a name for your schedule in the **Name** field.

Then, set up your schedule. Each box represents half an hour, with the time at the top of each column and the day of the week to the left of each row. To add a time period to the schedule, simply click on the starting hour and drag to the ending hour. 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 at the end of the highlighted section.

Click **Apply** when you are done.

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.

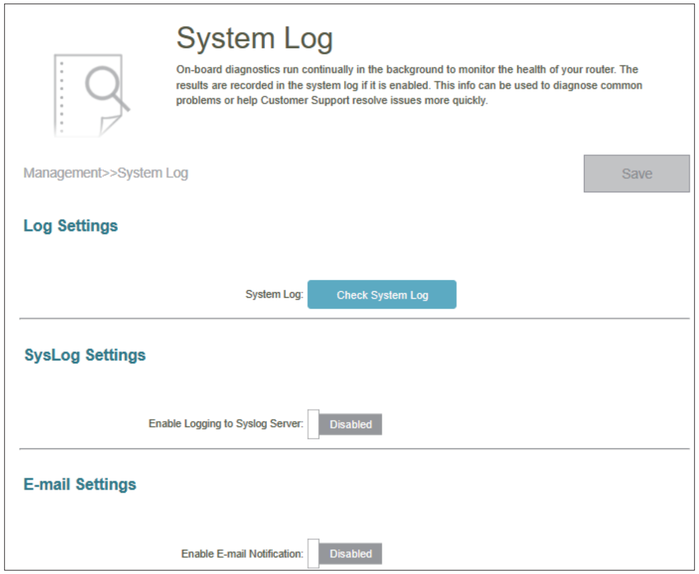
Log Settings

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

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

Management>>System Log

Log Settings

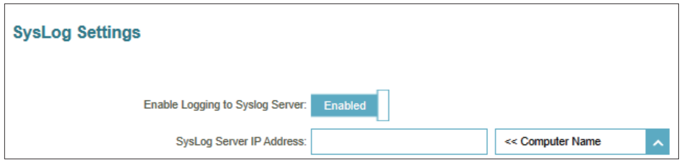
System Log:

SysLog Settings

Enable Logging to Syslog Server: Disabled

E-mail Settings

Enable E-mail Notification: Disabled



SysLog Settings

Enable Logging to Syslog Server: Enabled

SysLog Server IP Address:

Email Settings

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

If E-mail notification is Enabled:

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.

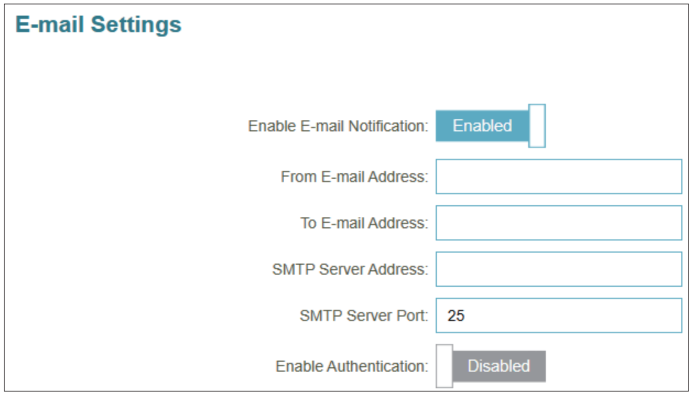
SMTP Server Address: Enter your SMTP server address.

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 Settings

Enable E-mail Notification: Enabled

From E-mail Address:

To E-mail Address:

SMTP Server Address:

SMTP Server Port: 25

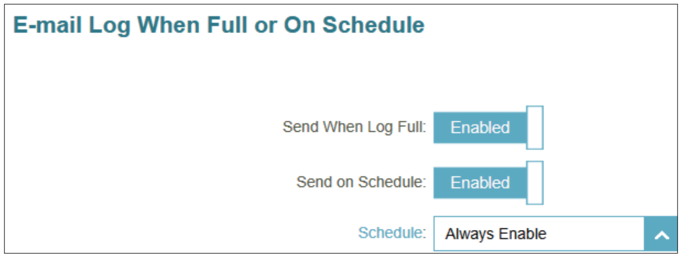
Enable Authentication: Disabled

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** for more information.



E-mail Log When Full or On Schedule

Send When Log Full: Enabled

Send on Schedule: Enabled

Schedule: Always Enable

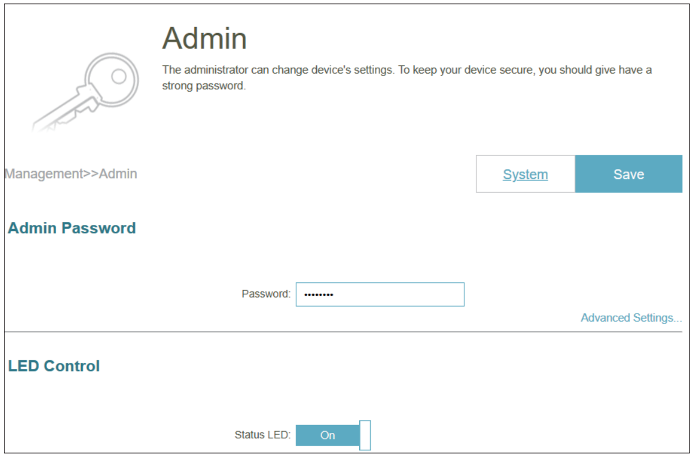
System Admin

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.



Admin

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

Management>>Admin

Admin Password

Password: ••••••••

LED Control

Status LED: On

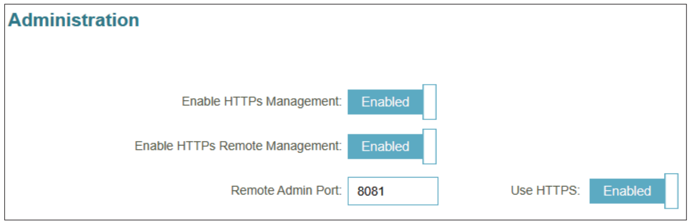
Advanced Settings - Administration

Enable HTTPS Management: Enable **HTTPS Management** to connect to the extender securely.

Enable HTTPS Remote Management: Enable **HTTPS Remote Management** over the Internet using encrypted HTTP connection.

Remote Admin Port: The port number is used in the URL to access the web configuration page. The default port number is **8081.**

Note: If you enabled **Use HTTPS** and wish to access the router remotely and securely, you must enter https:// at the beginning of the address.



Administration

Enable HTTPs Management: Enabled

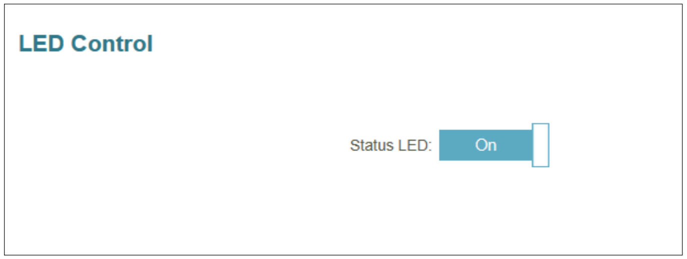
Enable HTTPs Remote Management: Enabled

Remote Admin Port: 8081

Use HTTPS: Enabled

LED Control

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



LED Control

Status LED: On

System

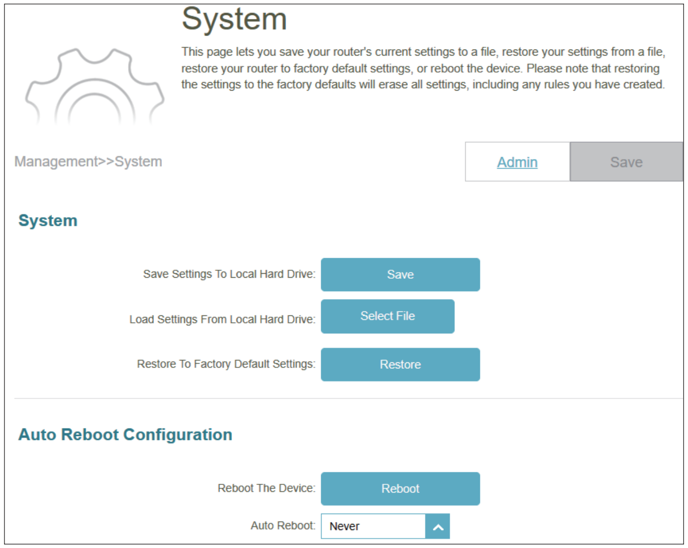
This page allows you to backup, restore configuration settings or restore settings from a previous backup, reset, and set up a reboot schedule for the device. On the **System Admin** page, click **System**. Click **Save** at any time to save the changes you have made on this page.

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.



System

This page lets you save your router's current settings to a file, restore your settings from a file, restore your router to factory default settings, or reboot the device. Please note that restoring the settings to the factory defaults will erase all settings, including any rules you have created.

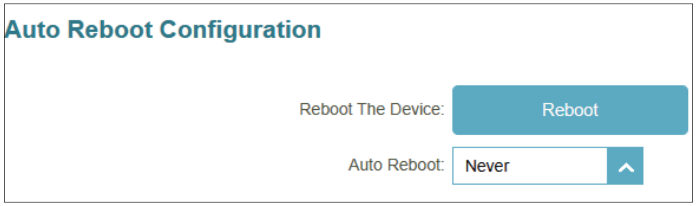
Auto Reboot: Never

Management>>System
Admin
Save
System
Save Settings To Local Hard Drive:
Save
Load Settings From Local Hard Drive:
Select File
Restore To Factory Default Settings:
Restore
Auto Reboot Configuration
Reboot The Device:
Reboot

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 day and hour and minute of a day for automatic reboot.

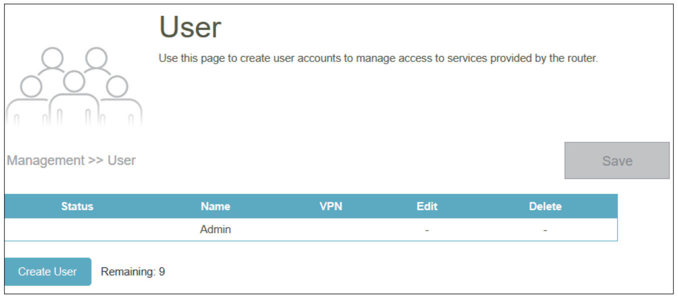


Auto Reboot: Never

User

The User section is used to create, manage, and delete user accounts that have access to certain router service such as VPN functions in the **Security** tab. 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.



User

Use this page to create user accounts to manage access to services provided by the router.

Management >> User

Status	Name	VPN	Edit	Delete
	Admin		-	-

Remaining: 9

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.

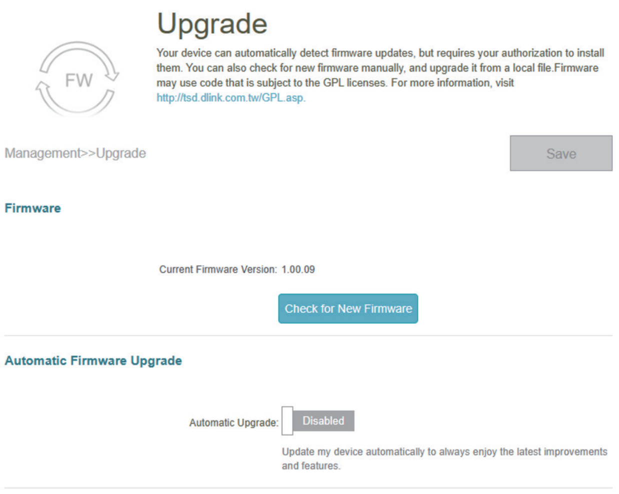
Status Enable or disable VPN functionality for this user.

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.



Upgrade

Your device can automatically detect firmware updates, but requires your authorization to install them. You can also check for new firmware manually, and upgrade it from a local file.Firmware may use code that is subject to the GPL licenses. For more information, visit http://tsd.dlink.com.tw/GPL.asp.

Management>>Upgrade

Firmware

Current Firmware Version: 1.00.09

Automatic Firmware Upgrade

Automatic Upgrade: Disabled

Update my device automatically to always enjoy the latest improvements and features.

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 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 Upgrade

Automatic Upgrade: If enabled, the router will automatically upgrade to the newest firmware. The system will automatically upgrade to the latest firmware every day at 3:30-4:00 AM.

Choose Upgrade Time: Enable this function to set the router'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

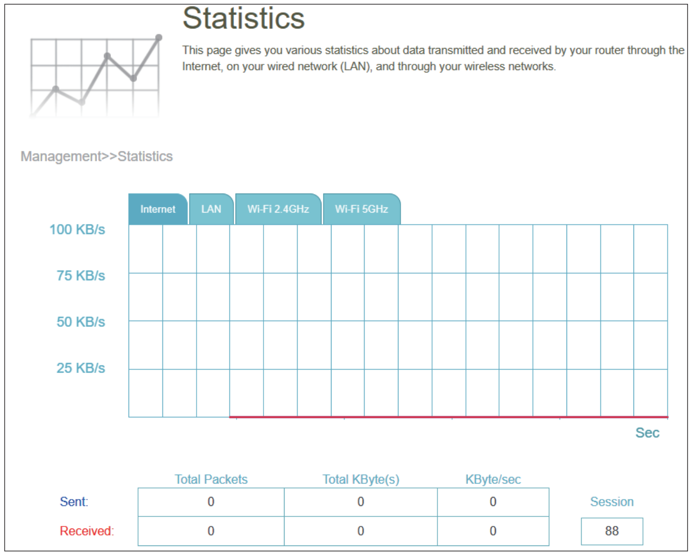
On the **Statistics** page, you can view the amount of packets that pass through your Internet and LAN interfaces as well as the traffic from Wi-Fi 2.4 GHz and Wi-Fi 5 GHz networks.

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 if the device is rebooted.



Statistics

This page gives you various statistics about data transmitted and received by your router through the Internet, on your wired network (LAN), and through your wireless networks.

Management>>Statistics

	Total Packets	Total KByte(s)	KByte/sec	Session
Sent:	0	0	0	
Received:	0	0	0	88

Join N’ Share App Setup

The Join N’ Share app allows you to access your shared files in a breeze.

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

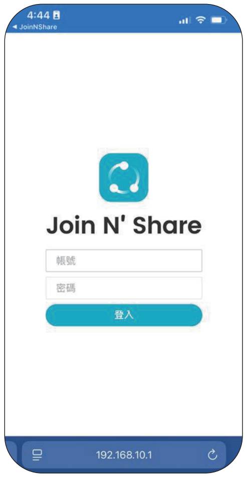
Step 1

Search and install the free **Join N’ Share** app available on the App Store or on Google Play.

NOTE: Enter the device's admin password to log in.

Step 2

Launch the Join N’ Share app from the home screen of your device.

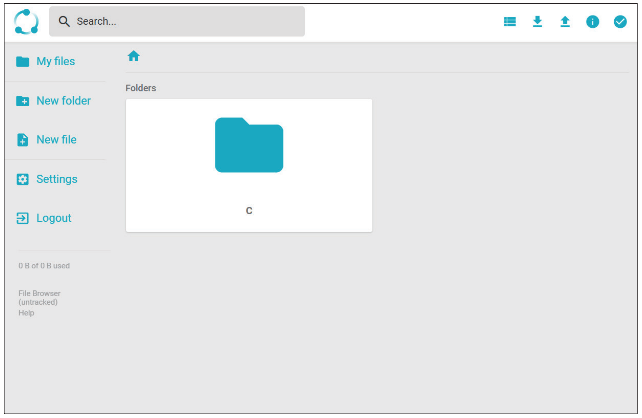


Step 3

Sign in on the app using the device's admin password.

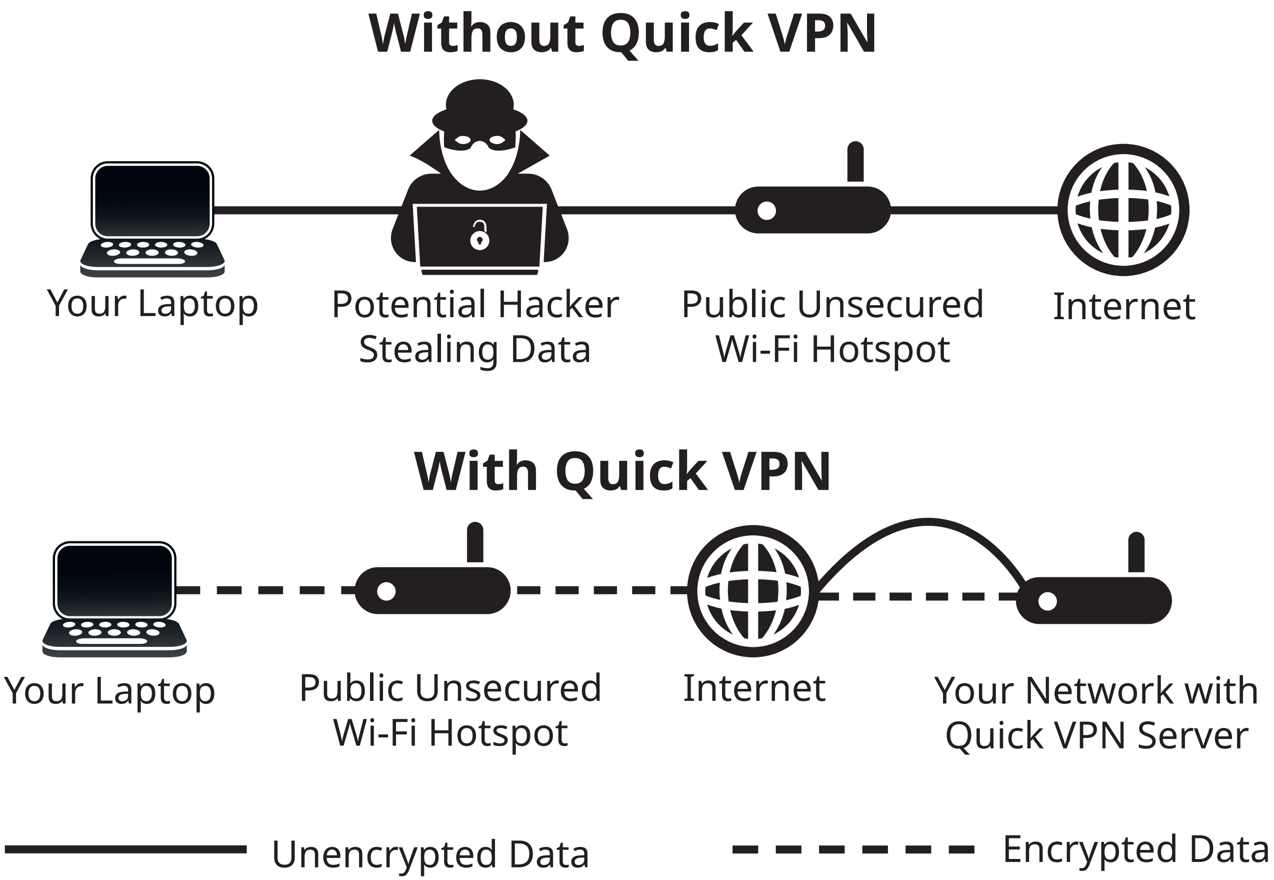
Easy File Management & Seamless Sharing

You can now access and share files online locally with the app or remotely with a browser. Create, edit, and upload files at your finger tips from any device with advanced security protection and access control.
Refer to **Join N' Share** for detailed feature explanation and operation instructions.



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
Your Laptop
Potential Hacker Stealing Data
Public Unsecured Wi-Fi Hotspot
Internet
With Quick VPN
Your Laptop
Public Unsecured Wi-Fi Hotspot
Internet
Your Network with Quick VPN Server
Unencrypted Data
Encrypted Data

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.

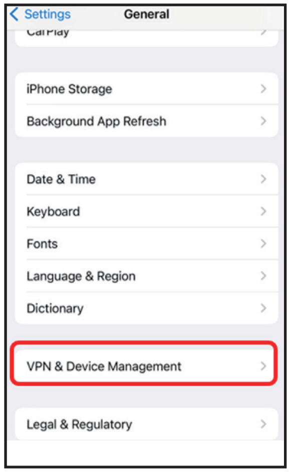
- Quick VPN only provides an added layer of security against specific types of snooping attacks and does not guarantee complete data integrity or protection. Only traffic in the tunnel between your router and device will be encrypted, WAN traffic will leave your D-Link Quick VPN enabled router unencrypted.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

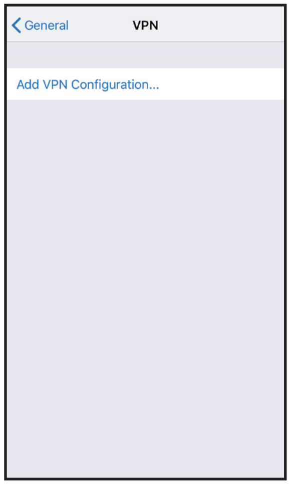
VPN Setup Instructions

This section provides Quick VPN setup instructions for iOS devices. Refer to **Quick VPN** for your router's set-up instructions.

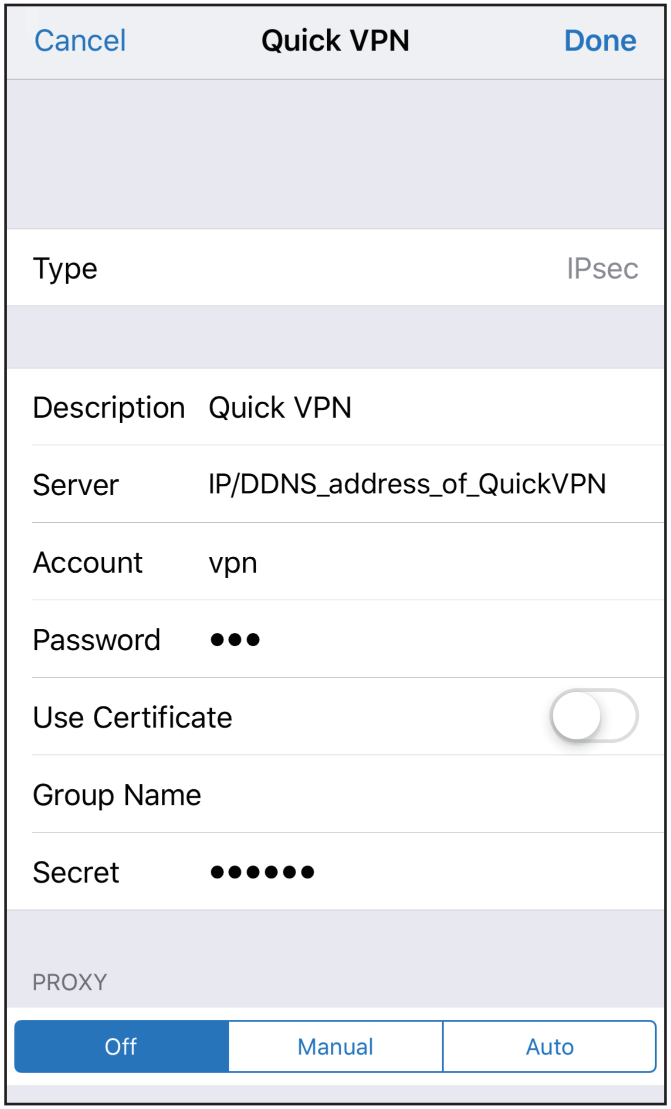
Go into **Settings** on your compatible iOS device.
Scroll to and tap **General**.
Scroll to and tap **VPN & Device Management**.



Tap **Add VPN Configuration...**



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



Type IPsec

Description Quick VPN

Server IP/DDNS_address_of_QuickVPN

Account vpn

Password •••

Use Certificate ○

Group Name

Secret ••••••

PROXY

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.

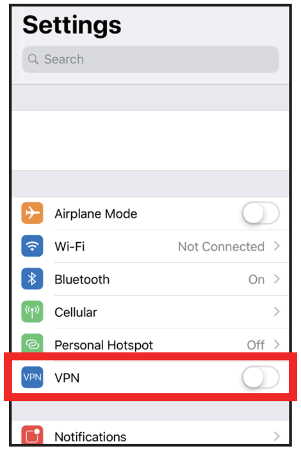
Secret: Enter your Passkey (PSK).

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/Disconnect

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


Settings

Search

Airplane Mode

Wi-Fi Not Connected

Bluetooth On

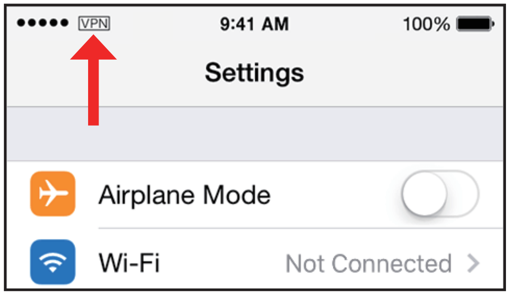
Cellular

Personal Hotspot Off

VPN

Notifications

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.


●●●●● VPN 9:41 AM 100%

Settings

Airplane Mode

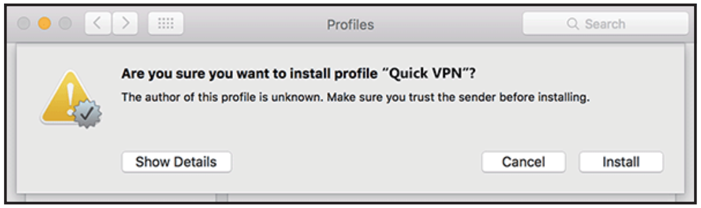
Wi-Fi Not Connected

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** for your router's setup instructions.

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

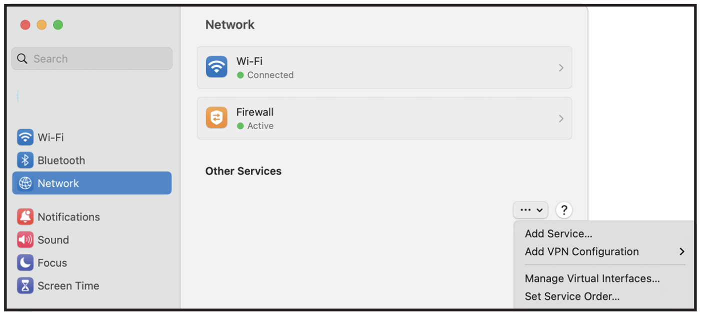


Are you sure you want to install profile “Quick VPN”?

The author of this profile is unknown. Make sure you trust the sender before installing.

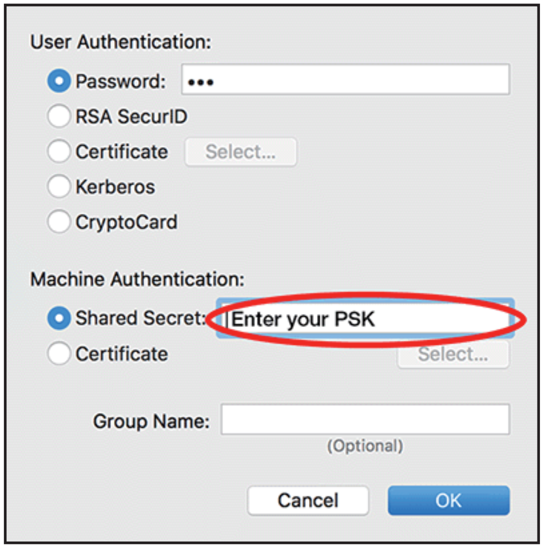
Enter your user account password when prompted. Close the **Profiles** dialogue.

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**.



User Authentication:

● Password: •••

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

Machine Authentication:

● Shared Secret: Enter your PSK

○ Certificate

Group Name:

(Optional)

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

Connect/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

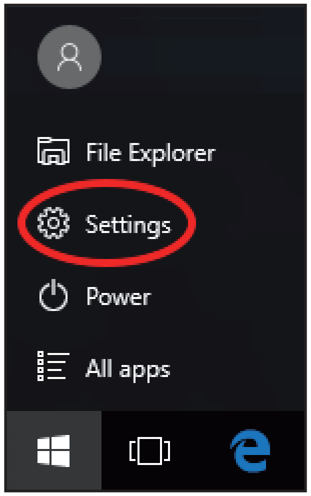
This section provides Quick VPN setup instructions for Windows 11/10. Refer to **Quick VPN** for your router's setup instructions.

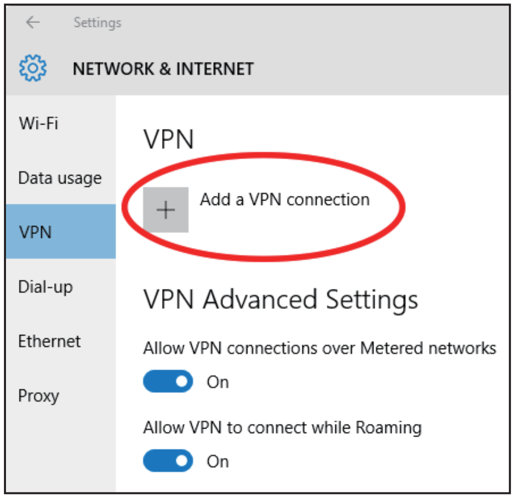
This section provides Quick VPN setup instructions for Windows 11/10.

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**.





VPN

Add a VPN connection

VPN Advanced Settings

Allow VPN connections over Metered networks

On

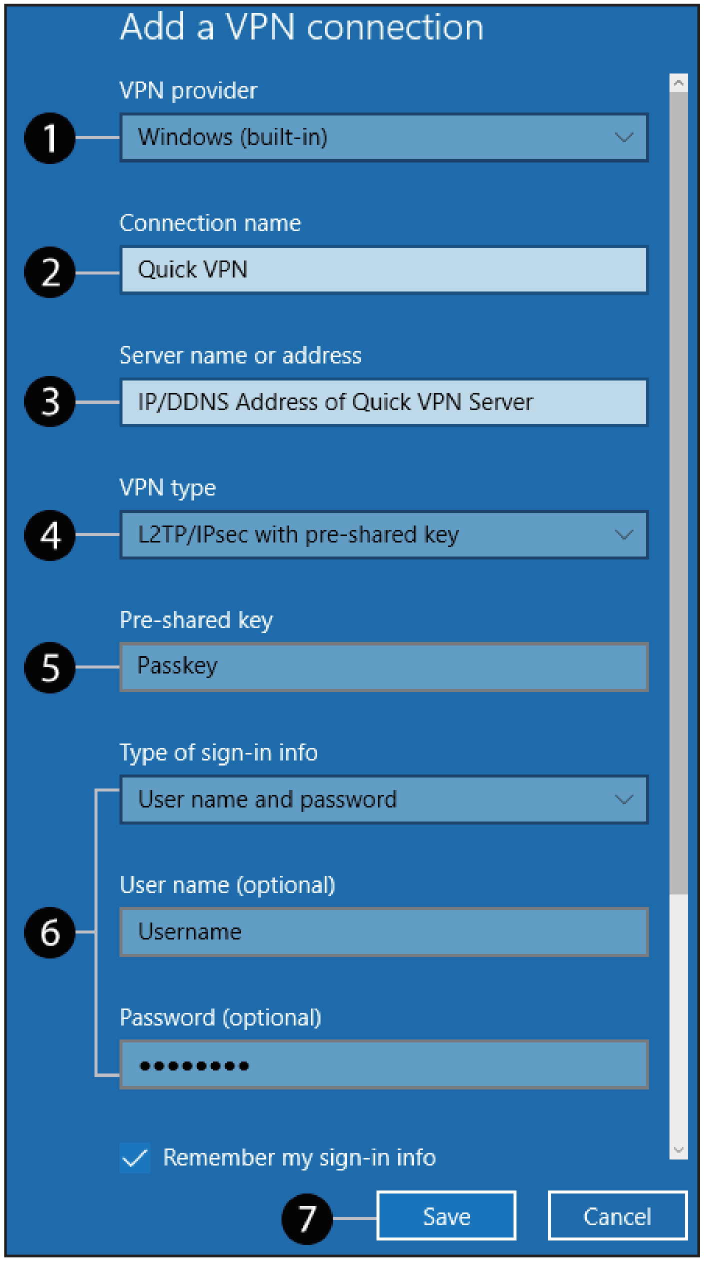
Allow VPN to connect while Roaming

On

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.



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: Quick VPN

Server name or address: IP/DDNS Address of Quick VPN Server

VPN type: L2TP/IPsec with pre-shared key

Pre-shared key: Passkey

Type of sign-in info: User name and password

User name (optional): Username

Password (optional): ••••••••

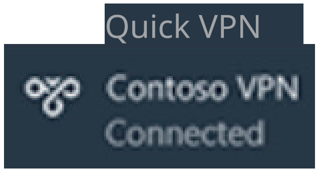
☑ Remember my sign-in info

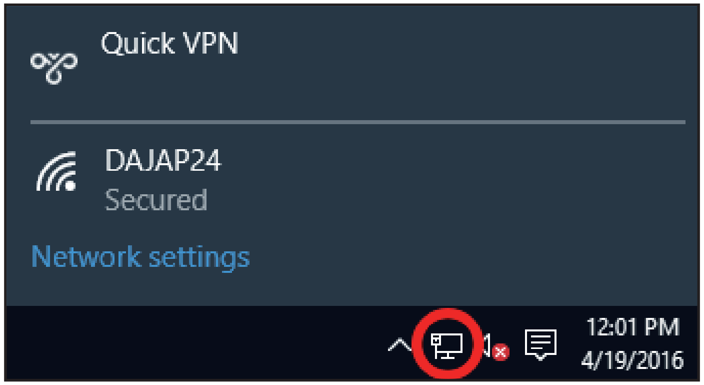
Connect/Disconnect

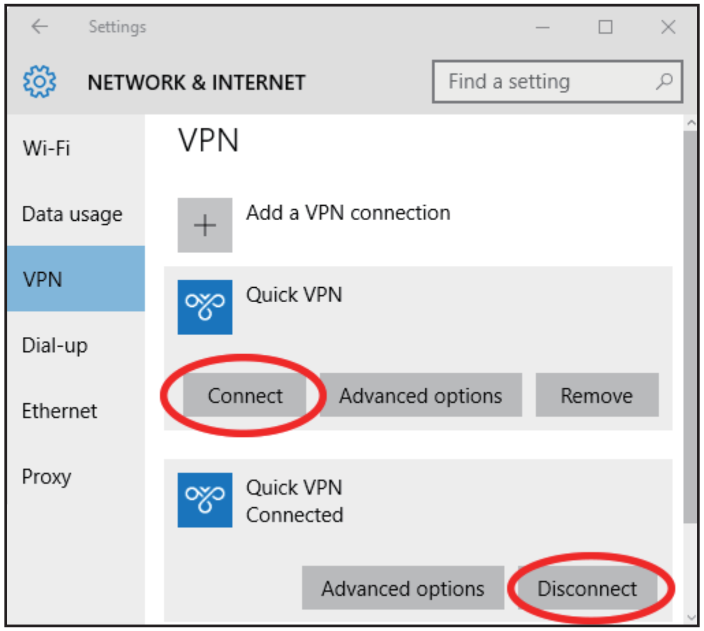
To connect to or disconnect from your Quick VPN server:

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.

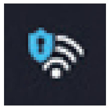






On **Windows 11**:

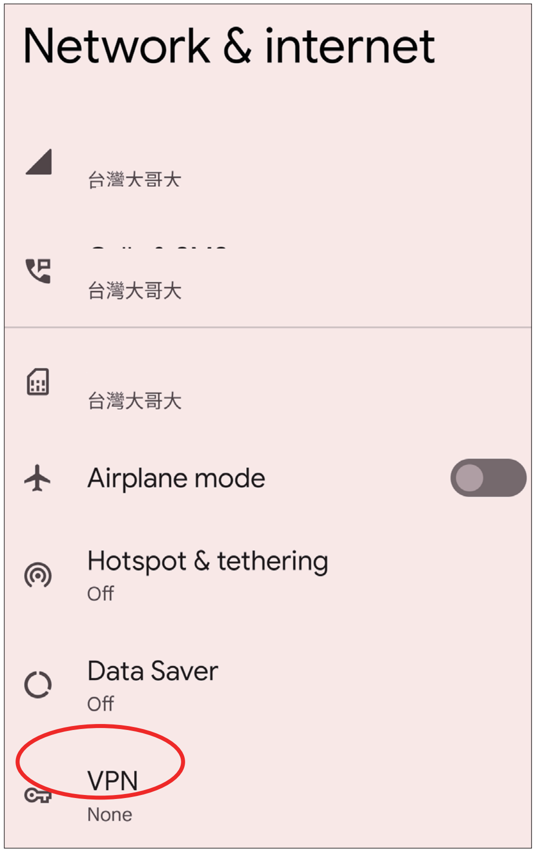
Click on the **Network, Volume, Battery** icon. . Select the Connect or disconnect of your Quick VPN connection. A blue shield appears when you are connected to a VPN.



Android
VPN Setup Instructions

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

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



Network & internet

台灣大哥大

台灣大哥大

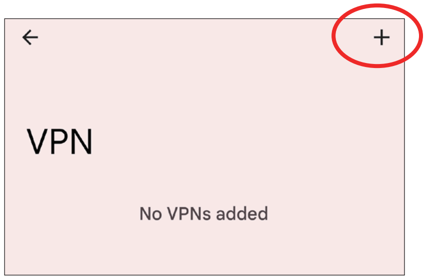
台灣大哥大

Airplane mode

Hotspot & tethering
Off

Data Saver
Off

VPN
None

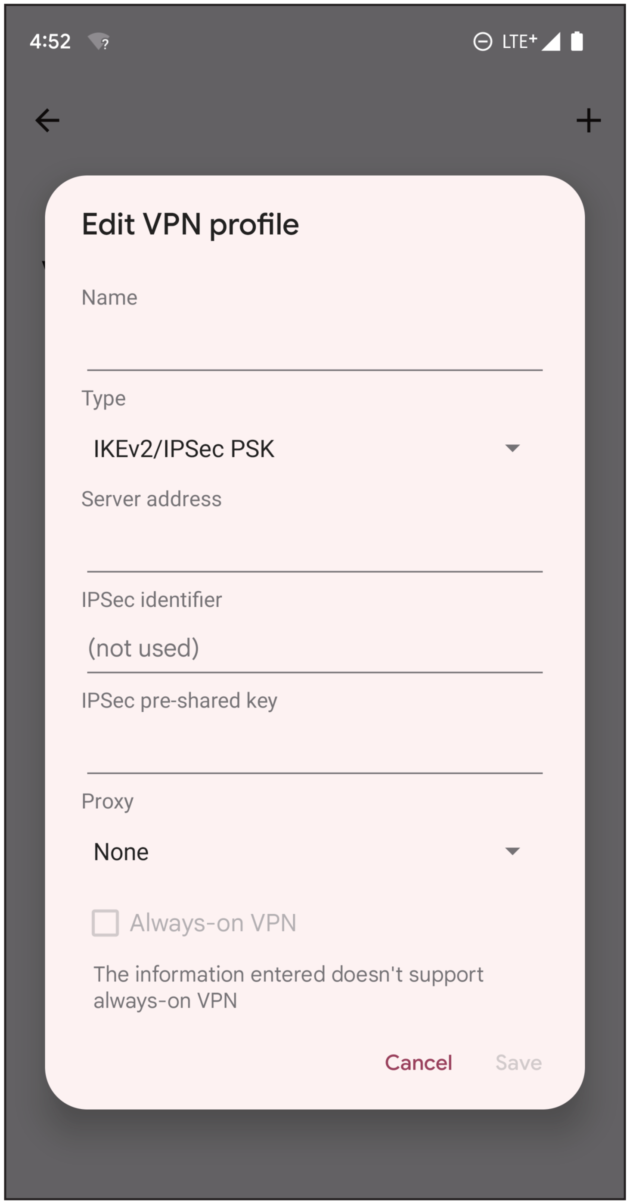


VPN

No VPNs added

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.



4:52

Edit VPN profile

Name

Type

IKEv2/IPSec PSK

Server address

IPSec identifier

(not used)

IPSec pre-shared key

Proxy

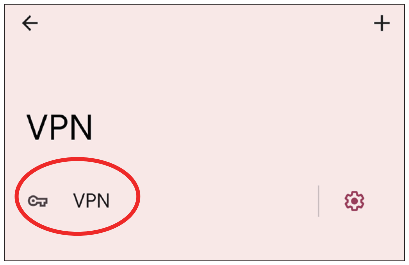
None

□ Always-on VPN

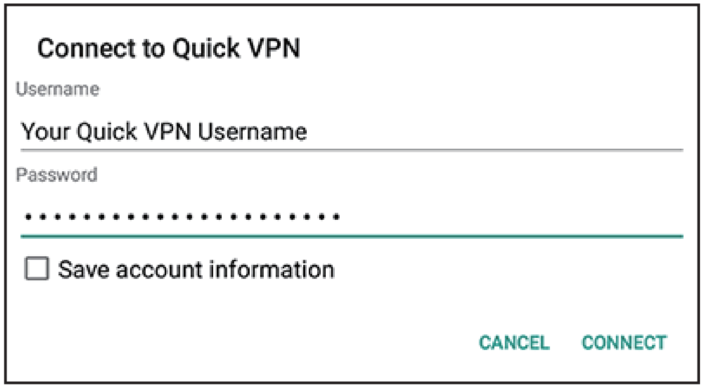
The information entered doesn't support always-on VPN

Connect/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**.


Connect to Quick VPN

Username

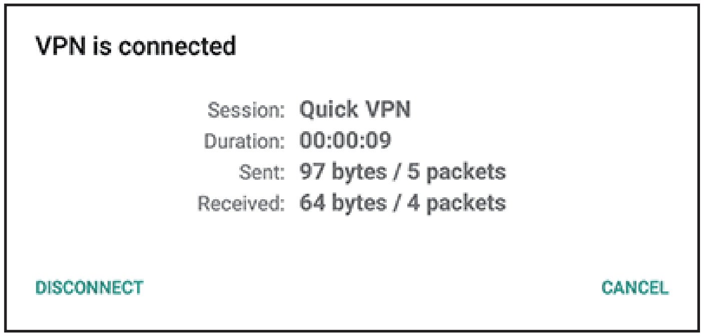
Your Quick VPN Username

Password

••••••••••••••••••••••

□ Save account information

To disconnect, select **DISCONNECT**.


VPN is connected

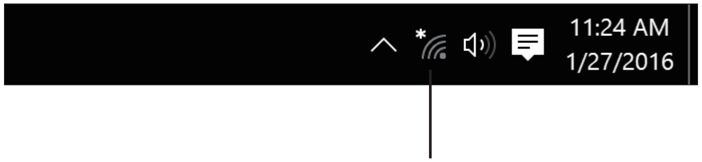
Session: Quick VPN
Duration: 00:00:09
Sent: 97 bytes / 5 packets
Received: 64 bytes / 4 packets

Windows® 11/10

When connecting to the DBR-330 wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise, refer to the product label on the bottom of the device for the default Wi-Fi network SSID and password or enter the Wi-Fi credentials set during the product configuration.

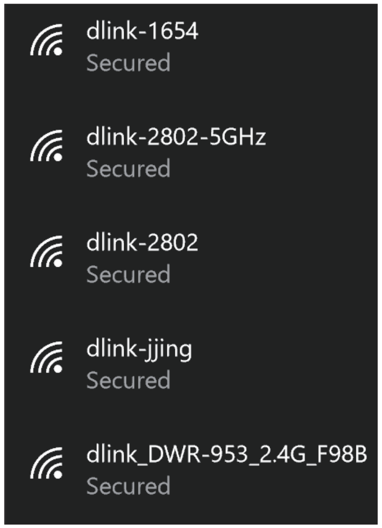
Note: To enjoy the benefits offered by Wi-Fi 6 and WPA3, please make sure that your operating system and wireless network adapter support Wi-Fi 6.

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



Wireless Icon

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



dlink-1654
Secured

dlink-2802-5GHz
Secured

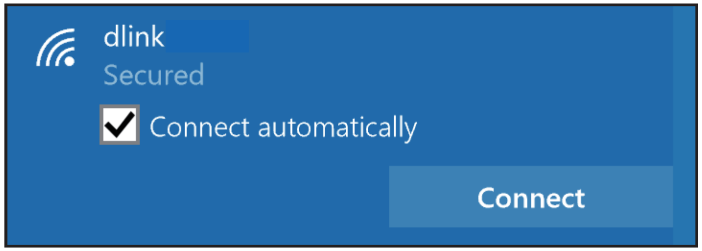
dlink-2802
Secured

dlink-jjing
Secured

dlink_DWR-953_2.4G_F98B
Secured

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

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

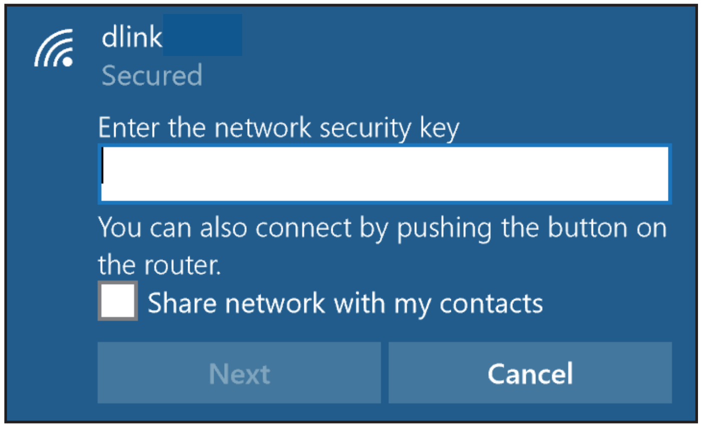


dlink [redacted]

Secured

☑ Connect automatically

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



dlink [redacted]

Secured

Enter the network security key

You can also connect by pushing the button on the router.

□ Share network with my contacts

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 configuration utility?

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.

- 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 forgot my password?

If you forgot your password, you must reset your router. This process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the recessed button down for 2 seconds. 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 product label.

Wireless Basics

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

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of through wires. Wireless LANs are used increasingly in both home and office environments, and 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. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards do.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

What is Wireless?

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

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 transmited from one point A to point B. But there are restrictions for wireless technology: how you can access the network. You must be within the range of a wireless network area to be able to connect your computer. There are, basically, two different types of wireless networks: Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

Compared to WLAN, both the speed and wireless operation range of WPAN are 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.

Who uses wireless?

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

Home uses/benefits

- Gives everyone at home broadband access
- Web surfing, email and instant message checking, etc.
- Gets rid of the cables around your house
- Simple and easy to use

Small office and home office uses/benefits

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

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.

Another way to reduce wireless resource contention is to separate the use of radio frequency and channel by allocating devices accordingly. Advanced Wi-Fi devices supporting the 5 GHz band should use this band instead of 2.4 GHz, which can be used to accommodate legacy devices and Bluetooth. Enable **Smart Connect** to manage band selection automatically when connecting to devices. The same principle applies to automatic channel selection. This option enables the system to select the cleanest channel for your network. You can also turn on the AI-powered Wi-Fi Optimizer and Mesh to have the system tune the Wi-Fi environment automatically according to the present network condition and receive personalized weekly Wi-Fi reports.

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 latest WPA3 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 some of the following types of security protocols:

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

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles keys using a hashing algorithm and by adding an integrity-checking feature to ensure that the keys have not been tampered. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication through the Extensible Authentication Protocol (EAP), which is generally missing in WEP. WEP regulates access to a wireless network based on a computer’s hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK/WPA3-SAE uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

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

WPA3 has the strongest encryption among these with an increased cryptographic capability and the requirements of the Protected Management Frames (PMFs) to facilitate protection from snooping attack.

Technical Specifications

Device Interfaces

- 1 x Gigabit Ethernet LAN/WAN port (auto-switch between LAN and WAN)
- 1 x USB Type-C with Power Delivery (PD) for power input
- 1 x USB Type-A
- 1 x MicroSD/TF card slot (CLASS 6 / CLASS 10 / UHS- I)
- 1 x Reset button

Wi-Fi Access Point[2,3]

- IEEE 802.11ax/ac/n/a (5 GHz)
- IEEE 802.11ax/n/g/b (2.4 GHz)

Wi-Fi Data Rate[1,2,3]

- 3000 Mbps (5 GHz up to 2403 Mbps / 2.4 GHz up to 574 Mbps)

Antenna

- 2 x Wi-Fi 2.4 GHz internal antennas
- 3 x Wi-Fi 5 GHz internal antennas

Indicators

- Power status
- Internet status

Wireless Encryption

- WPA™ Personal
- WPA2™ Personal
- WPA3™ Personal
- None

Dimensions (L x W x H)

- 120 x 82 x 23.5 mm (4.72 x 3.23 x 0.93 in)

Power Input

- 36 W (minimum required)

Weight

- 122 g (4.3 oz)

Operating Temperature

- 0 to 40 °C (32 to 104 °F)

Storage Temperature

- -20 to 65 °C (-4 to 149 °F)

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

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

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

Regulatory 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 5.15-5.25 GHz 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.

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.

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 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations

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

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

European Community Declaration of Conformity:

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

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

Svenska[Swedish]	D-Link Corporation försäkrar härmed att denna produkt, tillbehör och programvara överensstämmer med direktiv 2014/53/EU. Hela texten med EU-försäkran om överensstämmelse och produkt-firmware kan hämtas från produktsidan på www.dlink.com.
Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisyfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á www.dlink.com.
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på www.dlink.com.

Warning Statement:

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

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

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

Usage Notes:

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

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

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

Gebrauchshinweise:

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

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

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

Notes d'utilisation:

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

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

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

Notas de uso:

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

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

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

Note per l'uso

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

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

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

Gebruiksaanwijzingen:

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

SAFETY INSTRUCTIONS

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

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

SICHERHEITSVORSCHRIFTEN

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

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

CONSIGNES DE SÉCURITÉ

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

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

INSTRUCCIONES DE SEGURIDAD

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

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

ISTRUZIONI PER LA SICUREZZA

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

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

VEILIGHEIDSINFORMATIE

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

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

Disposing and Recycling Your Product

ENGLISH EN

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

D-Link and the Environment

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

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

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

DEUTSCH DE

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

D-Link und die Umwelt

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

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

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

FRANÇAIS FR

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

D-Link et l’environnement

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

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

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

ESPAÑOL ES

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

D-Link y el medio ambiente

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

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

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

ITALIANO IT

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

D-Link e l'ambiente

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

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

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

NEDERLANDS NL

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

D-Link en het milieu

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

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

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

POLSKI PL

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

D-Link i środowisko

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

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

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

ČESKY CZ

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

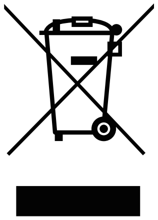
D-Link a životní prostředí

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

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

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

MAGYAR HU



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

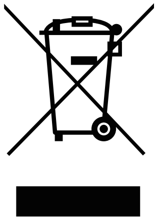
A D-Link és a környezet

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

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

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

NORSK NO



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

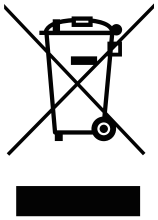
D-Link og miljøet

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

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

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

DANSK DK



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

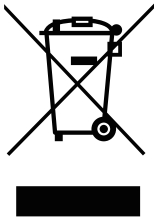
D-Link og miljøet

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

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

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

SUOMI FI



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

D-Link ja ympäristö

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

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

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

SVENSKA SE

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

D-Link och miljön

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

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

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

PORTUGUÊS PT

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

A D-Link e o ambiente

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

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

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