pakedge®

WR-1

Wireless Router with OvrC

User Guide

Contents

Introduction

The popularity and affordability of IP networking has driven audio/video and control networks to share the same physical wiring with computer networks. However, computer data can tolerate unpredictable latency in ways that audio-video streaming and control systems cannot. Sophisticated systems require the same robustness as an enterprise network to ensure that IP-based controls occur instantly and audio/video packets arrive in time.

> Note: If this is your first time installing this product, please read this manual in its entirety.

Customer Service and Technical Support

Pakedge is committed to providing you with exceptional support on all of our products. If you wish to speak with one of our representatives, you may contact us at:

Customer Service

- Email: customerservice@pakedge.com
- Phone: 650.385.8701

Technical Support

- Email: support@pakedge.com
- Phone: 650.385.8703
- Visit our website for up-to-date support information at www.pakedge.com.

Please be prepared to provide your product's model and serial number when contacting Pakedge Support. Your model and serial numbers are printed on a label located on the electronic housing.

Installing

For installation procedures, refer to the *Quick Start Guide* that came with the wireless router. You can also visit the Dealer Portal on our website for all the current user manuals and quick start guides.

> Note: If you install the wireless router in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room temperature. Make sure you install the equipment somewhere within the recommended temperature range.

Ensure that the unit is physically mounted away from obstructions that could interfere with the wireless signal, such as metal racks or other wireless transmitting electronic devices.

For free-standing installation, make sure that the wireless router has at least 15 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Getting to know your product

Package contents

- WR-1Wireless Router
- Power cord
- Ethernet cable
- Quick Start Guide

Front

The front panel of the wireless router has several blue LEDs. See the *Table 1* below for more information.

Table 1: LED explanation

LED	Status		Operation
Power		Blue	The wireless router is powered on
		Off	The wireless router is turned off
WAN 1	LINK/ ACT	Blue	Port is online (link established)
		Flashing Blue	Activity
		Off	No device connected
LAN 1- 4	LINK/ ACT	Blue	Port is online (link established)
		Flashing Blue	Activity
		Off	No device connected
2.4 [GHz]	LINK/ ACT	Flashing blue	Activity
		Off	No wireless connection established
5 [GHz]	LINK/ ACT	Flashing blue	Activity
		Off	No wireless connection established

Back

All connections are made at the back of the router. See Table 2 for more information.

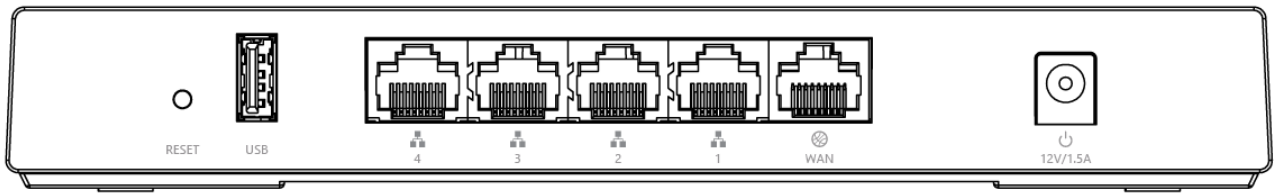


Table 2: Interface explanation

Interface	Type	Speed	Protocol	Description
Reset Button	N/A	N/A	N/A	Hold Reset button for 10 seconds to return settings to factory defaults.
USB	USB-A	Link speed up to 480 Mbps	USB 2.0	USB port used for file sharing
LAN 1-4	RJ-45	10/100/1000 Mbps	Ethernet	4-port switch connections on the internal network
WAN	RJ-45	10/100/1000 Mbps	Ethernet	WAN port used for the Internet connection from the ISP
AC power input	AC	N/A	N/A	Power input

Specifications

To view devices specifications, see the WR-1's data sheet at pkdge.com/wr1-ds.

Accessing the wireless router

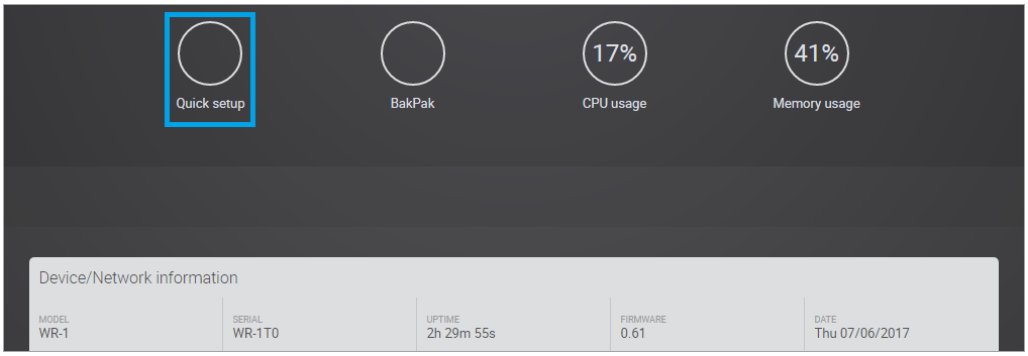
To access the wireless router's GUI:

1. Plug an Ethernet cable from the wireless router to a computer.
2. Make sure your network card is set to obtain an IP address automatically. Then open any Internet browser and go to the default IP address. **Note:** For best results, we recommend using Mozilla Firefox as your web browser. If you are using Internet Explorer, use version 9 or newer.
3. Enter the default username **admin** and the password **admin**, then click the arrow.

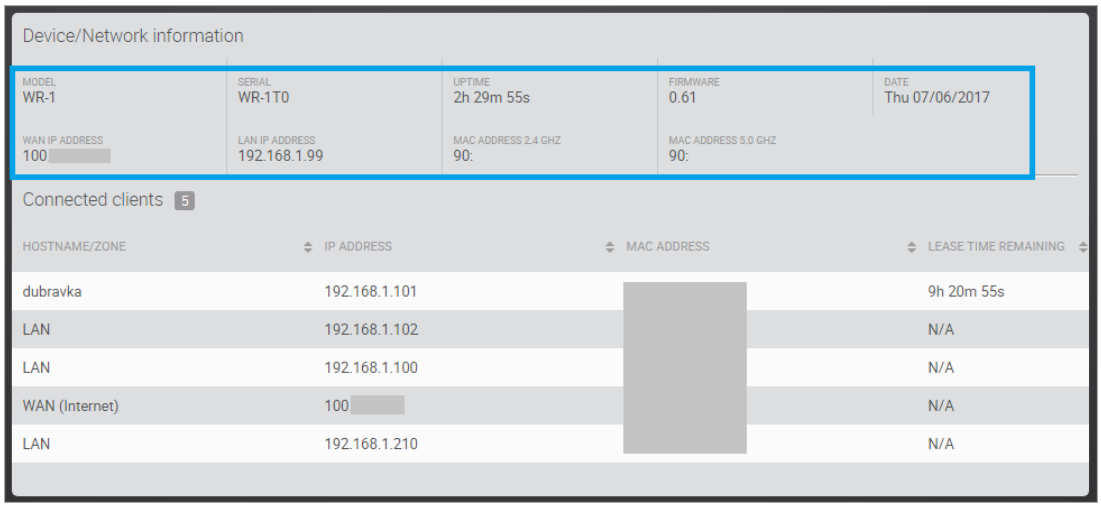
> Note: The first time you log in, you will be directed to the *Quick setup* page and will be required to update your password before proceeding to the dashboard.

Dashboard

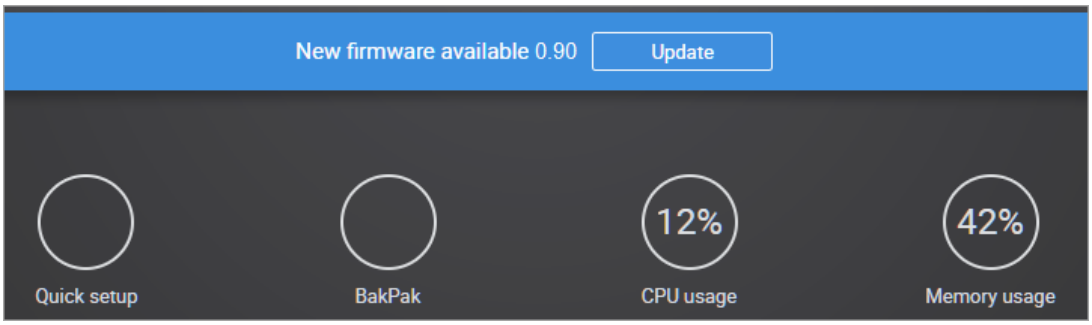
The dashboard provides a Quick setup link to help with a more efficient setup.



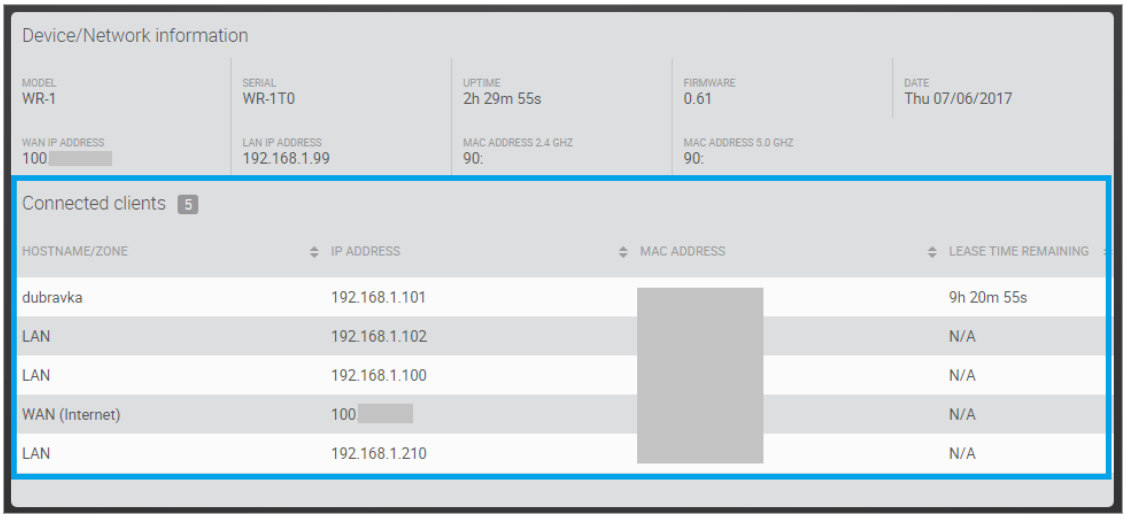
Towards the top of the page you will find information on the serial number and uptime on the wireless router as well as the CPU and memory usage.



If there is new firmware available for the wireless router, you will see a message notifying you of an option to download it.



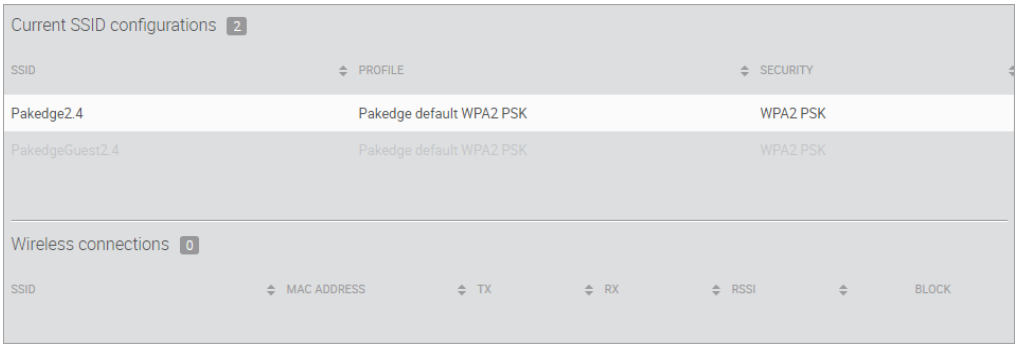
The **Connected clients** section shows the devices that have received an IP address from the wireless router. Usually devices with static IPs assigned to them will appear in this field.



Wireless LAN information summarizes the wireless configuration for the selected radio.

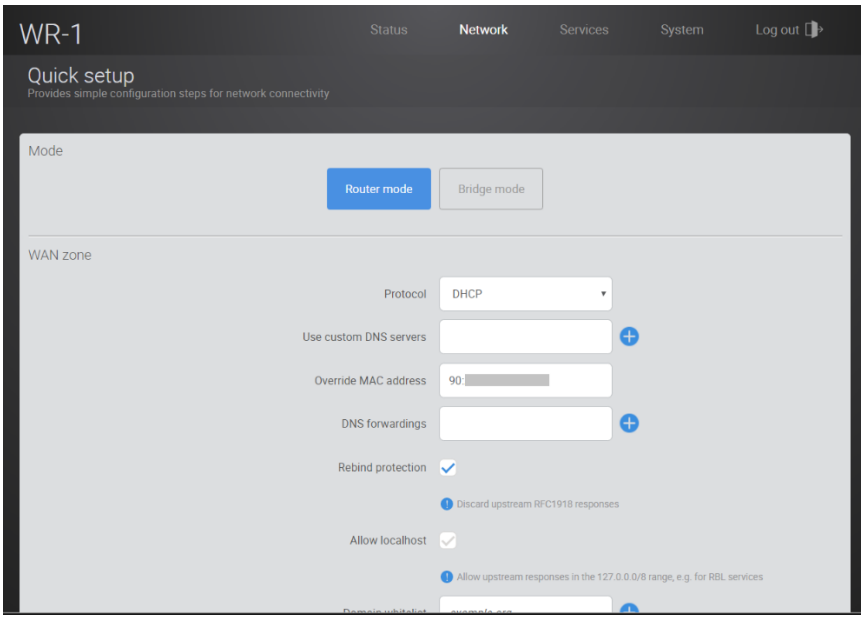
Current SSID configurations lists the SSID(s) of the wireless networks.

Wireless connections displays any wireless device that has been discovered by the wireless router on the selected network. When a device on the network transmits data, the wireless router will log its IP address.



Quick setup

The *Quick setup* link redirects to a page that walks through the key steps for setting up the wireless router in a router mode or bridge mode.



When selecting wireless router mode, the following information is required to be filled in before settings may be applied: WAN Zone, LAN Zone, and Wireless.

WAN zone

To connect to the Internet, the WAN zone must be properly configured. The wireless router supports the three main types of Internet connections:

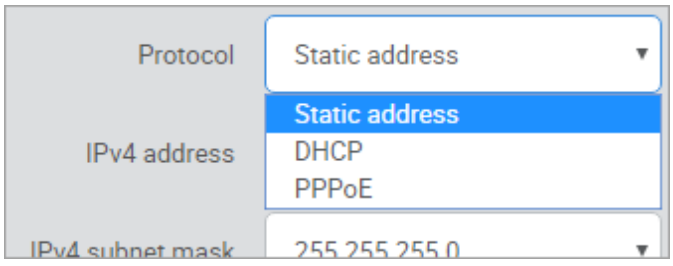
- **Static IP** (Fixed public IP address mostly used by business-class broadband services)
- **DHCP** (Typically used by cable companies and DSL basic service)
- **PPPoE** (Used by DSL companies such as AT&T)

Determine what type of Internet connection you have from your Internet service provider (ISP), and then follow one of the three instruction sets below to connect the wireless router to the Internet.

Static IP

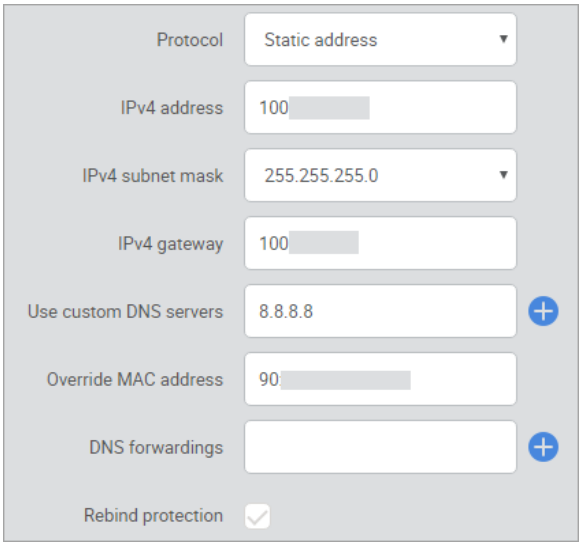
To configure the wireless router to a static IP:

1 Select Static address for the Protocol.



2. Enter the **IPv4 address, IPv4 subnet mask, IPv4 gateway,** and **DNS server** provided by your ISP. Select **Custom** from the Subnet mask drop-down menu to enter a custom subnet mask.

Click **Apply**. The wireless router now has the Static IP configured.



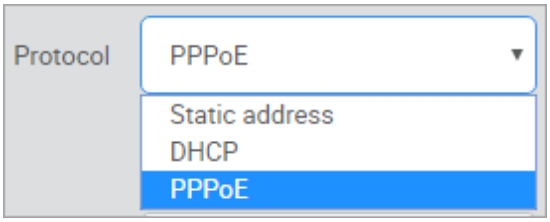
DHCP

By default, the wireless router will connect to the Internet using DHCP. If your ISP uses DHCP, you may need to reset the modem to get Internet access. If you are using a modem that has a wireless router built into it, you may have to configure DMZ settings to allow complete functionality of the wireless router.

PPPoE

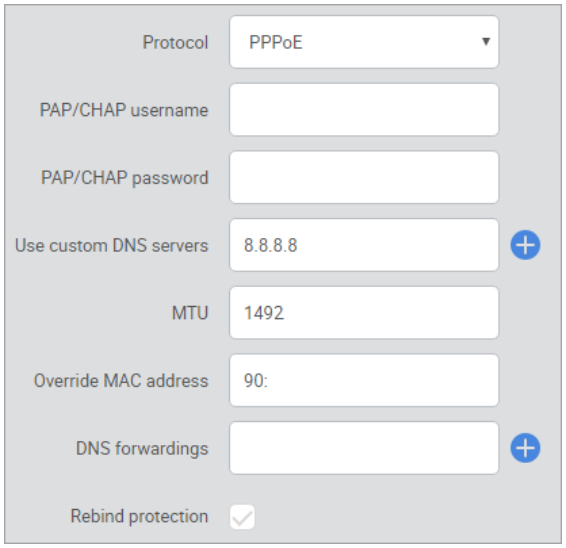
To configure the wireless router using a PPPoE connection:

1. Select **PPPoE** from the Protocol drop-down menu.



2. Enter the username that the ISP assigned under the **PAP/ CHAP username** field. Enter the password in the **PAP/ CHAP password** field. For **Use custom DNS servers**, enter the DNS server you would like to use. For example, you can use **8.8.8.8**. The wireless router is now

set up for PPPoE.



Additional WAN options

DNS forwardings

The DNS forwardings option will forward LAN DNS requests pointed to the wireless router to the specified public DNS server.

Rebind protection

This protects the WAN from receiving DNS information from any “Local” non-public IP address positioned above the wireless router in the network. If the wireless router is positioned behind another wireless router, this feature should be disabled.

Remote access

This setting only enables remote access. To configure remote access, see “Remote access”. To enable, click Enable secure web access.

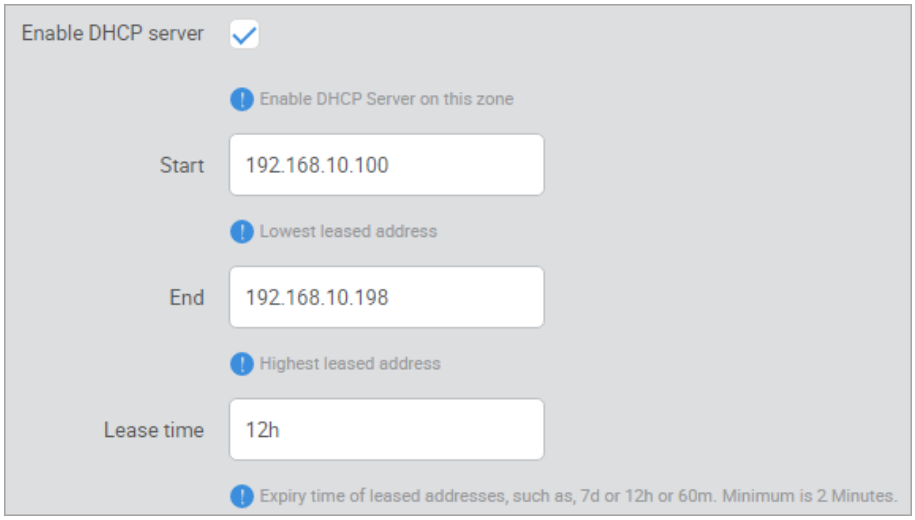
LAN zone

The default IP address of the wireless router is **192.168.1.1**.

To change the IP address of the wireless router or change the entire network address:

1. Enter the new IP address you want to use in the **IP address** field. In the following example, we change the IP address of the wireless router to **192.168.10.99**.

2. Below the *Enable DHCP Server* check box, the *Start* field indicates the first IP address that will be handed out by the wireless router. The *End* field indicates the last IP address that will be handed out.



3. The *Lease time* field allows you to view/modify DHCP IP address lease time. The following format must be used: a **D** represents days, an **H** represents hours and an **M** represents minutes. For example, if you wanted to change the lease time to be 3 days 2 hours and 30 minutes, you would set the lease time to **3D2H30M**.

Wireless

The *Wireless* menu walks you through the primary SSID configuration for the 2.4 GHz and 5.0 GHz radios.

- **Enable:** The SSID may be turned on or turned off using this toggle.
- **Wireless Name (SSID):** The SSID is the name associated with the WiFi network. An SSID cannot exceed 32 characters.
- **Encryption and Password:** This information will be associated with creating a security profile that may be applied to additional SSIDs.

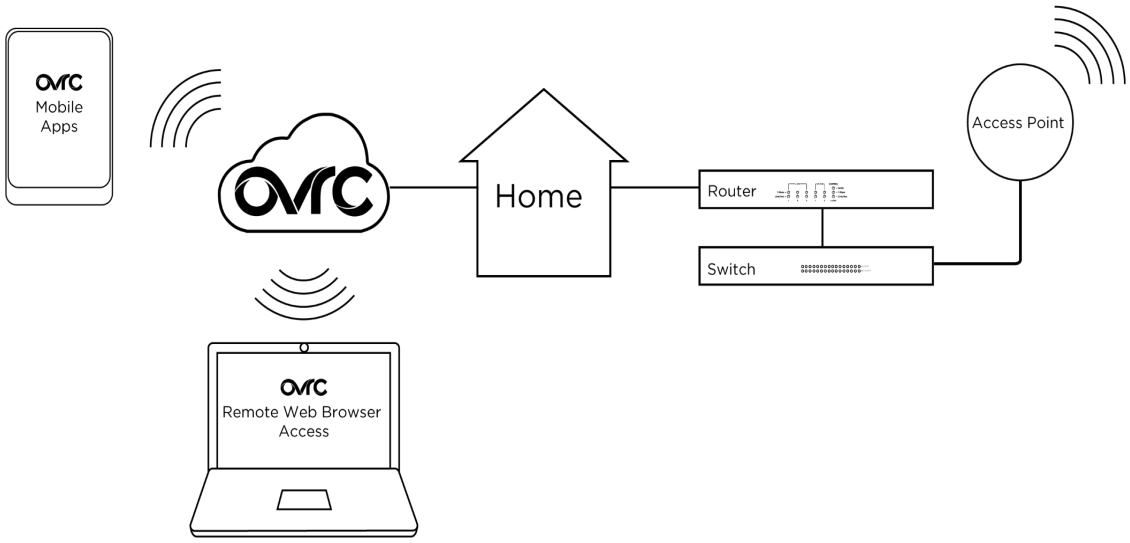
After your wireless router has been configured, click **Apply** for your changes to take effect.

> Note: When selecting *Bridge mode*, the *LAN zone* and *Wireless* information must be completed before settings can be applied.

OvrC Remote Network Management

OvrC gives you remote device management, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

To add this device to your OvrC account:



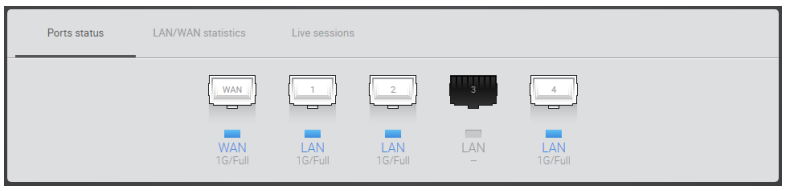
1. Connect the AP to the internet.
2. Log in to OvrC (www.ovrc.com).
3. Add the device (MAC address and serial numbers needed for authentication).

Status menu

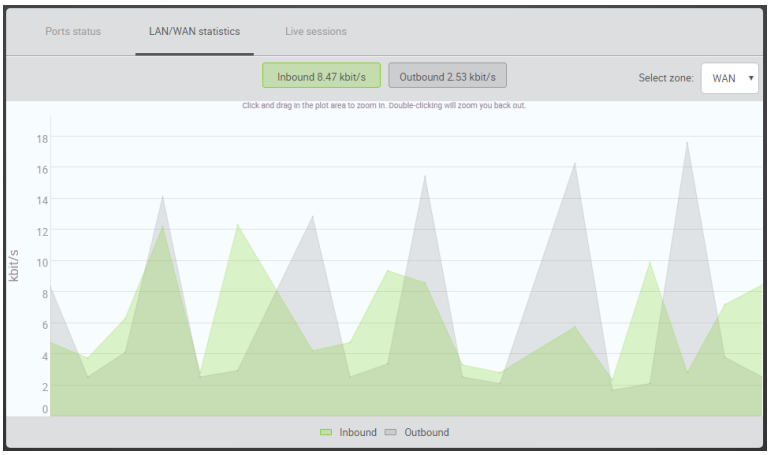
Analysis

The *Analysis* section allows you to view statistics on the wireless router.

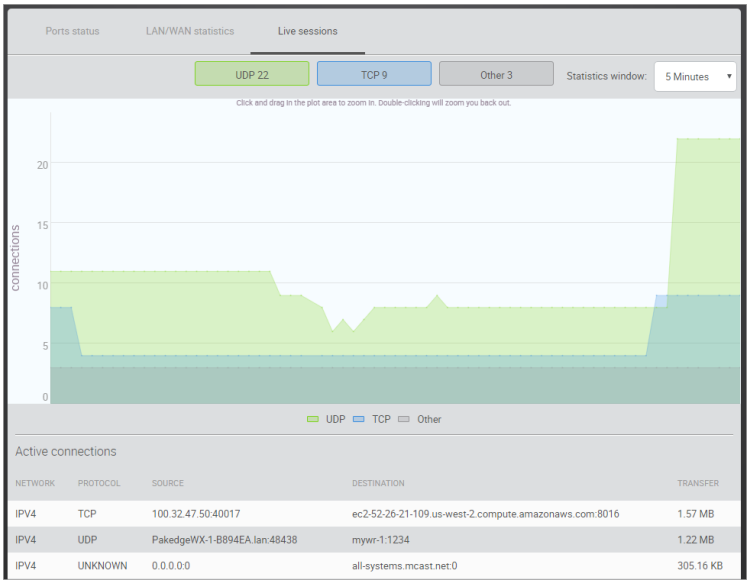
The *Port status* section displays which ports on the wireless router are currently active.



The *LAN/WAN* Statistics section displays the amount of traffic going through the LAN or WAN of the wireless router.



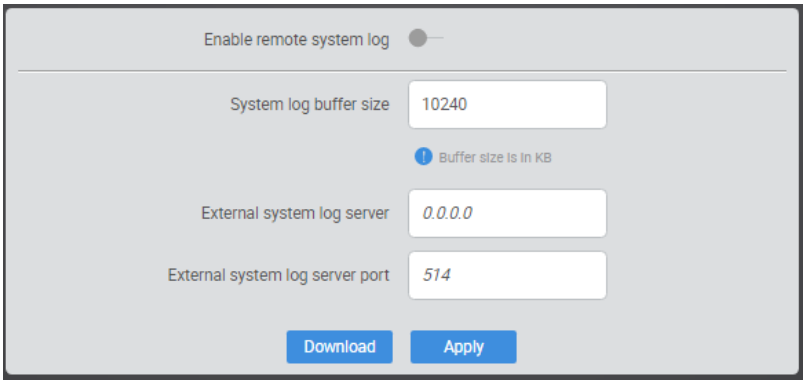
The *Live Sessions* section displays information on active connections. This information includes the protocol type, amount of data transferred, and the destination of the data.



System report

The *System report* page lets you maintain a log of system events. To enable, click the **Enable remote system log** toggle, enter the log and log server details, then click **Apply**. To download a

system log, go to this same page and click **Download**.



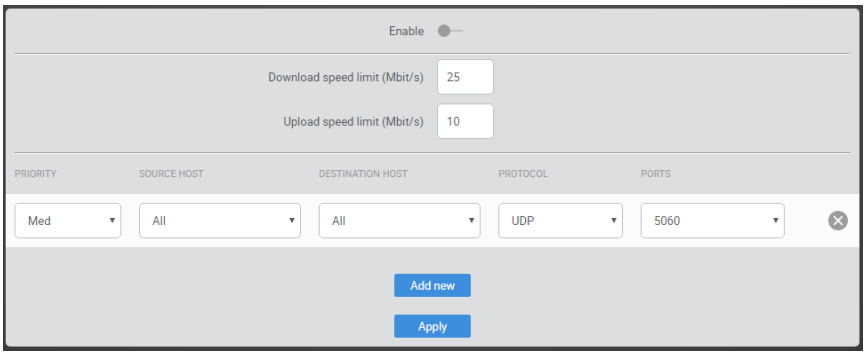
Network menu

Quality of service

Quality of service (QoS) allows you to prioritize data on the network. For example, there are certain applications which require the least amount of latency possible. You can prioritize this type of traffic so that it is sent ahead of other data that can function properly with some latency, such as ordinary web traffic.

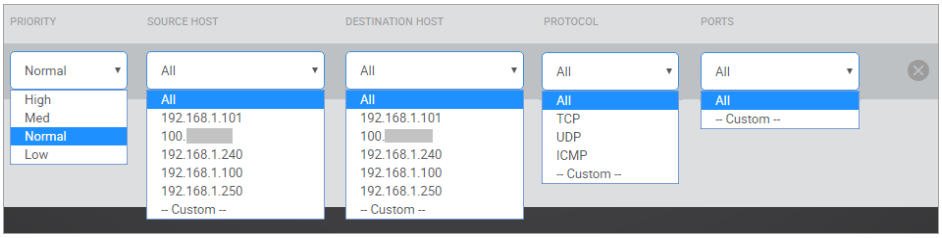
To configure QoS:

1. From the Dashboard, click **Network**, then click **Quality of service**.



2. Click the **Enable** toggle to enable QoS.
   - You can restrict download and upload speeds on this page. For example, in the image above we have set 25 Mbps as the limit for download and 10 Mbps as the limit for upload speeds. This setting will apply to all devices on the network.
   - A default rule is already defined to allow priority of Voice Over IP (VOIP) data.

3. If you want to create a new QoS policy to prioritize certain data, click **Add new** and set the following fields:



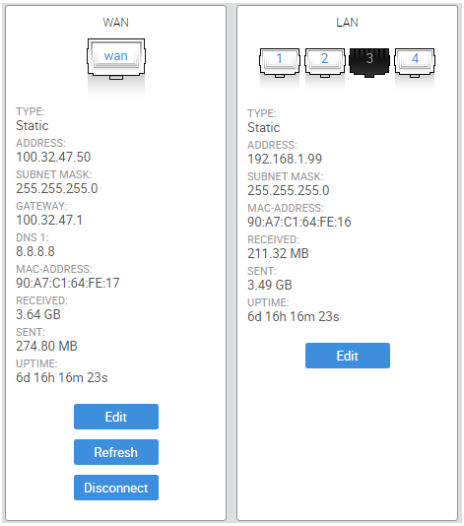
   - The *Priority* column allows you to select the priority of the data.
   - The *Source host* column allows you to define which source IP address the policy will apply to. If you select All, the policy will apply to all devices on the network. If your device is listed in the drop-down menu, you can select it. Otherwise, select custom and manually enter the IP address.
   - The *Destination host* column allows you to define which IP destination address the policy will apply to. If you select All, the policy will apply to any IP address on the Internet.
   - The *Protocol* column allows you to select whether the data that you are prioritizing is TCP or UDP. If you are unsure, you can simply select All, which will use both.

- The *Ports* column allows you to select which ports the data you are prioritizing uses. Click the drop-down menu and select Custom. You can then enter the port number that your application uses.

4. For example, we will prioritize the data of a computer on the network. For the **Priority** select **High**. Enter **192.168.1.34** as the IP address of the computer for the **Source host**. For the **Destination host**, select **All**; this will ensure that the policy will apply no matter what destination on the Internet the computer goes to. For Protocol select All. This means the policy will apply to TCP and UDP data. **Ports** is also set to **All**.
5. Click **Apply** to finalize the settings. By default, a rule is defined to allow priority of Voice Over IP (VOIP) data.

Network zones

The *Network* zones section displays the WAN and LAN network settings.



To change any of these settings, click **Edit**.

Changing WAN settings

The wireless router supports the three main types of Internet connections:

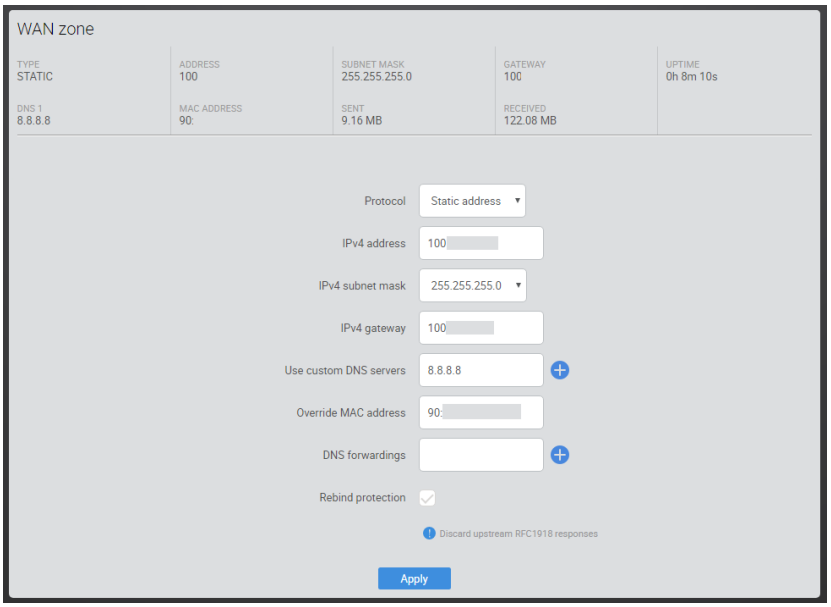
- **Static address** (fixed public IP address mostly used by business class broadband services)
- **DHCP** (typically used by cable companies and DSL basic service)
- **PPPoE** (used by DSL companies such as AT&T)

Determine what type of Internet connection you have from your Internet service provider (ISP), and then follow one of the three instruction sets below to connect the wireless router to the Internet.

Static IP

To configure the wireless router to a static IP address:

1 In the *Network zones* section, under *WAN*, click **Edit**. The *WAN zone* edit screen opens.



2. For *Protocol*, select **Static Address**.
3. Enter the **IP address, Subnet mask, Default gateway,** and **DNS server** provided by your ISP.
4. Click **Apply**. The wireless router is now configured for static IP.

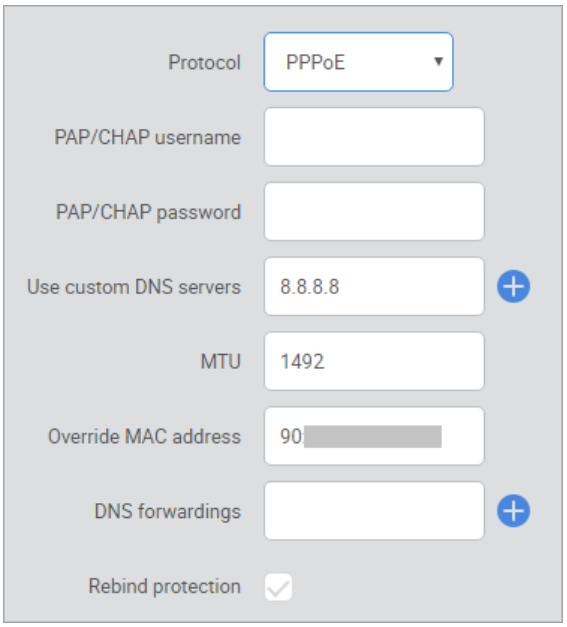
DHCP

By default, the wireless router will connect to the Internet using DHCP. If your ISP uses DHCP, you may need to restart the modem to get Internet access. If you are using a modem that has a wireless router built into it, you may have to configure DMZ settings to allow complete functionality of the wireless router.

PPPoE

To configure the wireless router using a PPPoE connection:

1. In the *Network zones* section, under *WAN*, click **Edit**. The *WAN zone edit* screen opens.
2. Select **PPPoE** from the *Protocol* drop down menu. The available fields change.



3. Enter the username that the ISP assigned under the **PAP/ CHAP username** field. Enter the password in the **PAP/ CHAP password** field. For the **Use custom DNS servers**, enter the DNS server you would like to use. For example, you can use 8.8.8.8. Click **Apply** when finished. The wireless router is now set up for PPPoE.

Additional WAN options

DNS forwarding

The DNS forwarding option will forward LAN DNS requests pointed to the wireless router to the specified public DNS server.

Rebind protection

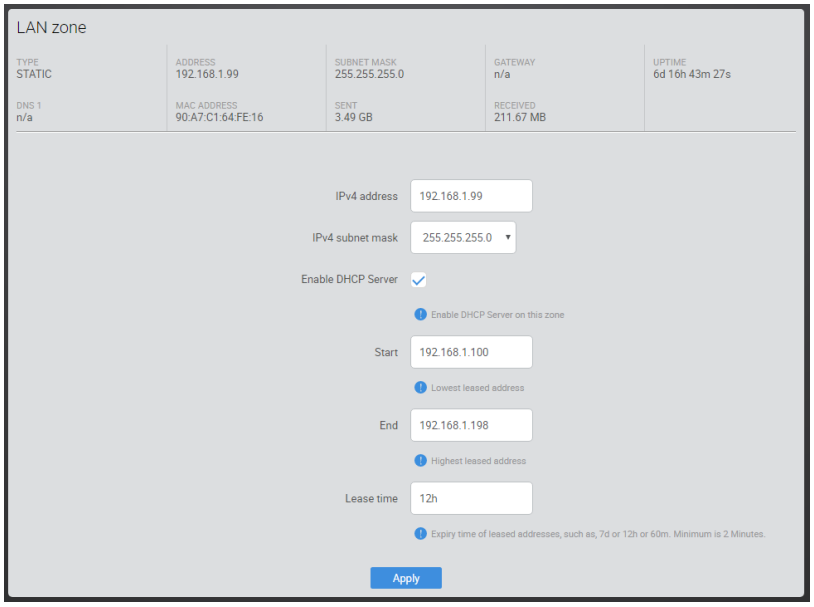
This function protects the WAN from receiving DNS information from any “Local” non-public IP address positioned above the wireless router in the network. If the wireless router is positioned behind another wireless router, this feature should be disabled.

Changing the IP address of the LAN zone

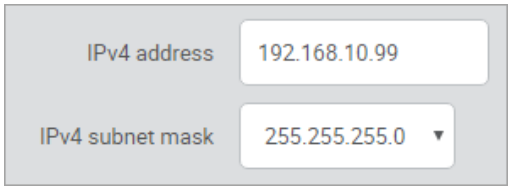
The default IP address of the wireless router is **192.168.1.1**.

To change the IP address of the wireless router or change the entire network address:

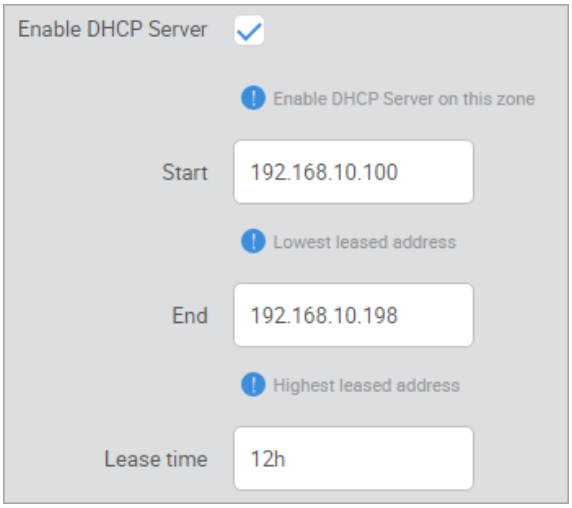
1. In the *Network zones* section, under *LAN*, click **Edit**. The *LAN zone* edit screen opens.



2. Click **Edit**.
3. Enter the new IP address you want to use in the **IPv4 address** field. In the following example, we change the IP address of the wireless router to **192.168.10.99**.



4. In the *DHCP Server* section, the *Start* field indicates the first IP address that will be handed out by the wireless router. The *End* field indicates the last IP address that will be handed out.
5. The **Lease time** field allows you to view/modify DHCP IP address lease time. The following format must be used: A **D** represents days, an **H** represents hours and an **M** represents minutes. For example, if you wanted to change the lease time to be 3 days 2 hours and 30 minutes, you would set the lease time to **3D2H30M**.



6. Click **Apply** to finalize your settings.

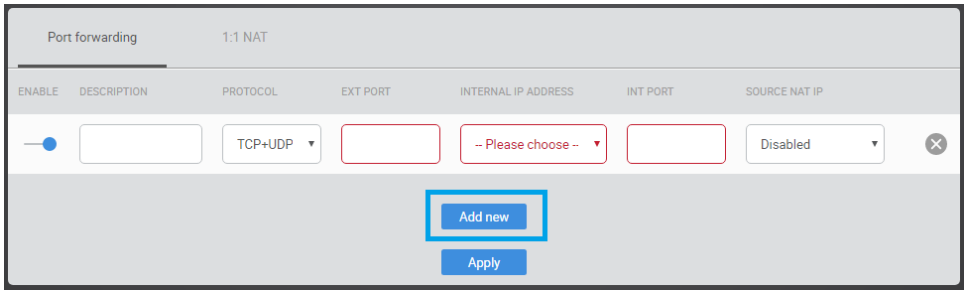
NAT

Port forwarding

Port forwarding allows services inside the network to be available from the Internet. For example, if you have an IP camera on your network, port forwarding would allow you to remotely view the camera.

To configure port forwarding:

1. From the Dashboard, click **Network**, then click **NAT**.
2. As an example, we will forward TCP port 80 to an IP camera on the IP address 192.168.150. Click **Add new**.



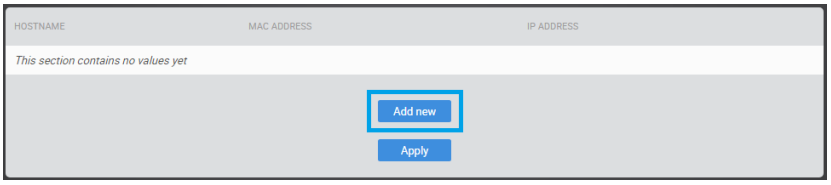
3. For the *Description*, enter IP Camera. For the *Protocol*, select **TCP**. Enter **80** for the *Ext port*. For the *Internal IP address*, select Custom and enter **192.168.150**. Enter **80** as the int port. For *Source NAT IP*, select **Disabled**. Click **Apply**.

DHCP reservation

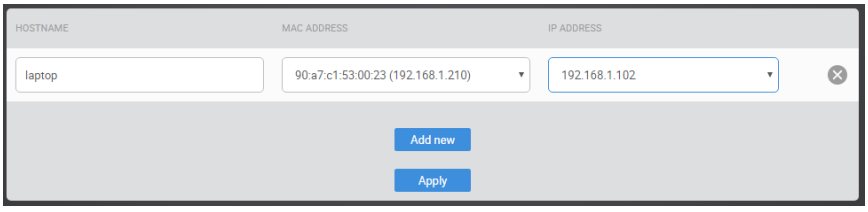
DHCP reservation allows the wireless router to continually assign the same IP address to a device.

To create a DHCP reservation:

1. From the dashboard, click **Network**, then click **DHCP Reservation**.
2. Click **Add new**.



3. For the *Hostname* field, type a name. For the *MAC-address* field, select the device you would like to make a reservation for. You can also manually enter the MAC address of the device. When entering the MAC address, use colons. For example, **aa:bb:cc:dd:ee:ff**.
   In the *IP address* field, select custom and enter the IP address that you would like to assign to the device.



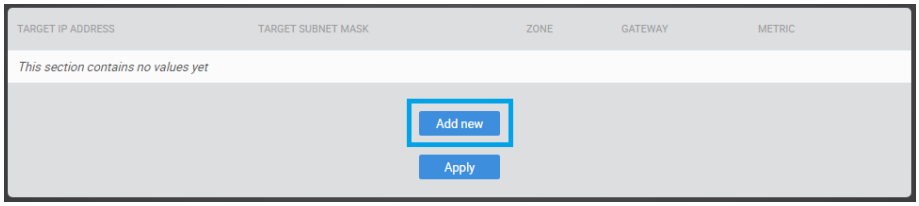
4. Click **Apply** when finished. You may need to restart the network card of your device for it to receive the new IP address.

Static routes

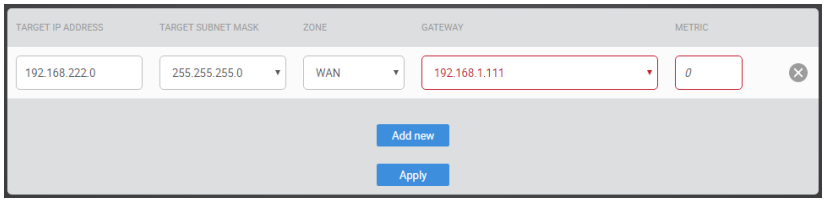
Static routes allow the manual forwarding of traffic to networks that are not a part of the wireless router internal routable networks.

To create a static route:

1. From the dashboard, click **Network**, then click **Static routes**.
   - For our example, we will be forwarding traffic destined for the unknown network (**192.168.222.0 / 24**) to the IP address of the gateway device which has knowledge of that network (**192.168.1.111**).
2. Click **Add new**.



   - **Target IP Address** is the network that must be accessed and is not directly known by the wireless router (**192.168.222.0**).
   - **Target Subnet mask** is the subnet mask of that network (**255.255.255.0**).
   - **Zone** should match the network zone that gateway traffic will be forwarded to.
   - **Gateway** is the IP address traffic should be forwarded to in order to reach that new network (**192.168.1.111**).
     An example of this would be the WAN IP address of a second router connecting to the LAN of the wireless router. In order to reach the second router's LAN, a static route must be added to inform the wireless router of the gateway IP that has direct knowledge of this new network.
   - **Metric** can be changed to indicate precedence between two similar routes. If the higher precedence route is not accessible, then the lower metric route will be taken.



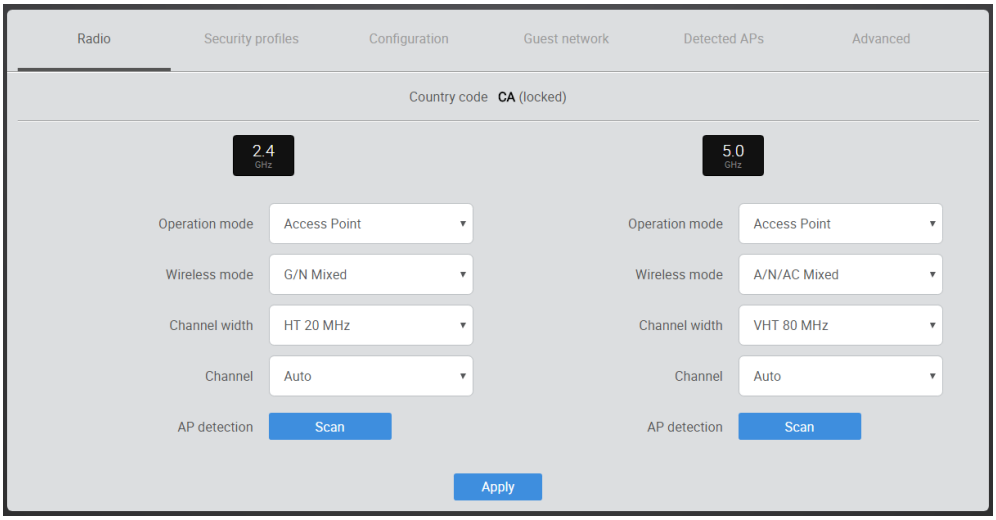
3. After the information has been entered, click **Apply**.

Wireless

The Wireless menu walks you through configuring all wireless settings. (The default wireless password is **pakedgewireless**).

Radio

1. From the dashboard, click **Network**, then click **Wireless**. The *Wireless Radio Settings* screen opens at the *Radio* tab.
2. Click **Apply** after making any changes.



- **Operation mode:** Both the 2.4 and the 5 GHz bands have the following operating modes:
  - Access point: Standard mode of operation. Allows a wireless connection to the LAN.
  - WDS root access point: The access point with this mode set will be the “root” device that access points configured with *WDS repeater* and *WDS bridge* will connect to.
- **Wireless mode:** Select the setting that corresponds to the type of wireless clients connected to your network: **B-Only, G-Only, B/G-Mixed, N-Only, N/G-Mixed,** or **B/G/N-Mixed** (on 2.4 GHz) or **A-Only, N-Only, N/A-Mixed, AC-Only, AC/N-Mixed,** or **A/AC/N-Mixed** (on 5 GHz). If you aren’t sure which types of clients will access the wireless networks, we recommend selecting **B/G/N-Mixed** on 2.4 GHz and **A/AC/N-Mixed** on 5 GHz for best performance.

> *Note:* When set to a mixed mode, all devices connected to the wireless network will use the mode that is compatible for all devices. For example, if you have the 2.4 GHz radio set to **B/G/N Mixed** and all connected devices use G, the speeds will slow accordingly.

- **Channel width:** By default, the *Channel Mode* is set to **HT 20 MHz** (when using 2.4 GHz) and **HT 80 MHz** (when using 5 GHz). Selecting the HT 40 MHz channel mode on 2.4 GHz will allow for greater speeds, but at the risk of also increasing interference.

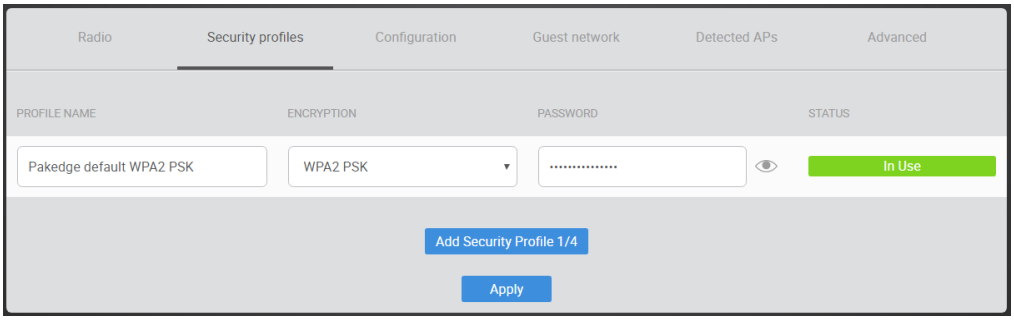
> *Example*: When using the 20 MHz channel width on the 2.4 GHz band, channel 6 would bleed into channels 4, 5, 7, and 8, giving you three non-overlapping channels (1, 6, and 11). When using 40 MHz channel width on the 2.4 GHz radio, channel 6 would bleed into channels 2, 3, 4, 5, 7, 8, 9, and 10.

- **Channel:** Using the default setting (**Auto**), the wireless router automatically selects the channel with best performance for the wireless network. This automatic scan occurs only after a reboot or restoration of factory default settings. To select a channel manually, click the drop-down list and select a channel. The channel options available depend on the country code that's selected.
- **AP detection:** Click **Scan** to perform an automatic site survey. A new window will open and display the site survey utility. The wireless router will scan the frequency for devices currently broadcasting their SSID and then display them in the table.
- **Country code:** Selecting your country is required for proper functionality of this device and may be required by law. After selecting your country and clicking **Apply**, the Country Code feature will lock. To regain access to Country Code, the access point must have factory defaults restored.

Security profiles

Under the *Security profiles* tab, you will be able to configure security profiles that can be used when creating SSIDs under the *Configuration* tab.

1. From the dashboard, click **Network**, then **Wireless**, then the **Security profiles** tab. Click **Apply** after making any changes.



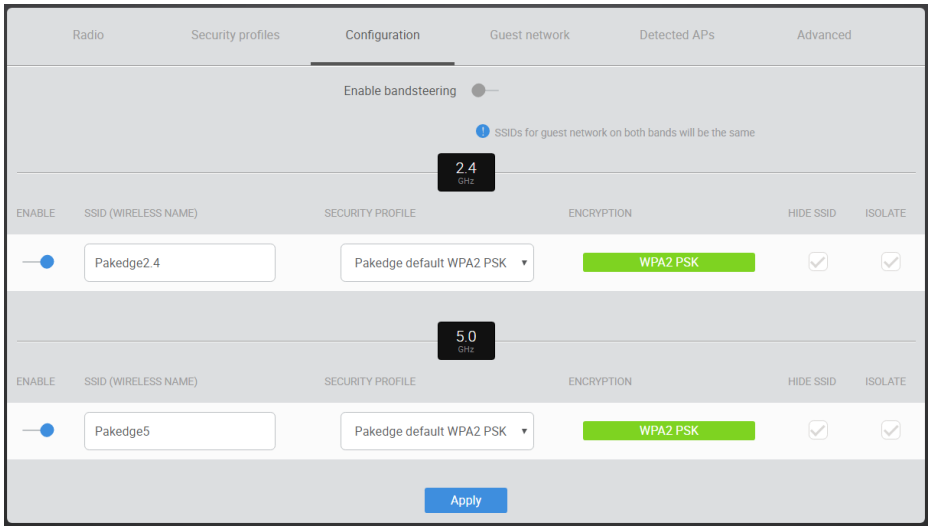
2. **Profile Name:** Create a name for the security profile.
3. **Encryption:** Select an encryption type for your security profile:
   - **No encryption:** This will leave your profile without security (not recommended).
   - **WPA PSK:** Password must be at least eight characters long. This is a legacy encryption protocol (not recommended).
   - **WPA2 PSK:** Password must be at least eight characters long. AES-only encryption. (Recommended)
   - **WPA/WPA2 PSK:** Password must be at least eight characters long. This feature is also known as Mixed Mode and uses TKIP encryption.

> Note: Passwords may contain only numbers and letters. Special characters are not allowed. Examples of special characters: (!@#$%:;^&*). Default password is **pakedgewireless**.

Configuration

To configure SSIDs for both the 2.4 GHz and 5 GHz bands, go to the Configuration tab. The WR-1 can set up one SSID per band.

1. From the dashboard, click **Network, Wireless,** then the **Configuration** tab. Click **Apply** after making any changes.



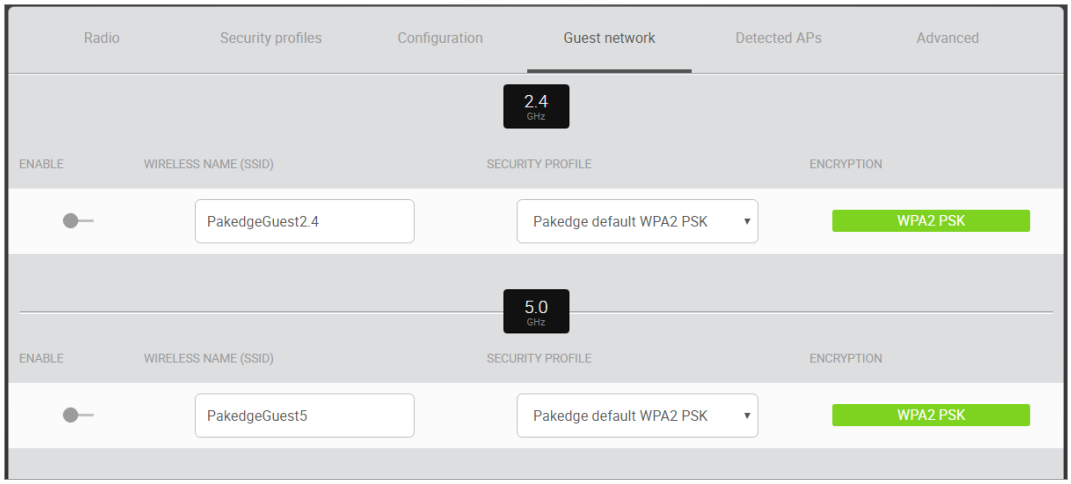
- **Enable band steering:** Band steering steers 5 GHz-capable clients to that frequency. By enabling this, the 2.4 GHz SSID and settings will be copied to the 5 GHz band.
- **Enable:** Use this toggle to turn the SSID on or off.
- **SSID** (wireless name): The SSID is the name associated with the WiFi network. An SSID cannot exceed 32 characters.
- **Security profile**: The profiles created under the *Security profiles* tab may be applied to the SSID here.
- **Encryption**: Displays the encryption method that the selected security profile uses.
- **Hide SSID**: Prevents the SSID name from being broadcast. The SSID will still be available for client access, provided the SSID is turned on. This is not a security feature.
- **Isolate**: This feature is also called “station separation,” and it prevents clients on the same SSID from being able to access other clients on the network.

Guest network settings

The guest network acts as its own network and has access to only the Internet. Each access point’s guest network is independent from the guest networks of other access points.

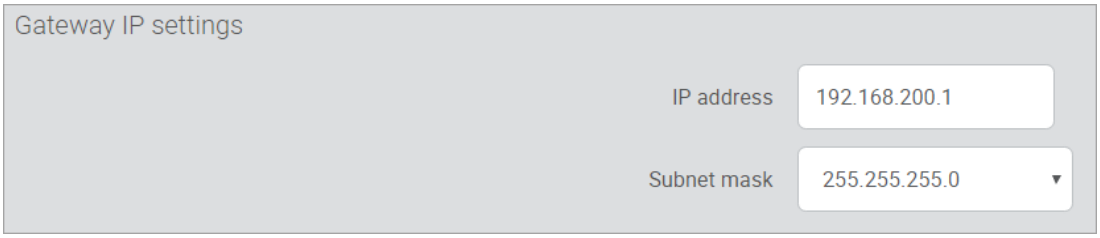
To enable the guest network for each band, select enable. By default, the guest network names are **PakedgeGuest2**.4 and **PakedgeGuest5**, and the IP scheme is set to **192.168.200.X**. You can change the SSID, IP address, subnet, starting IP address, and ending IP address. After changes are complete, click **Apply** to save them.

1. From the dashboard, click **Network**, then **Wireless**, then the **Guest network** tab. Click **Apply** after making any changes.



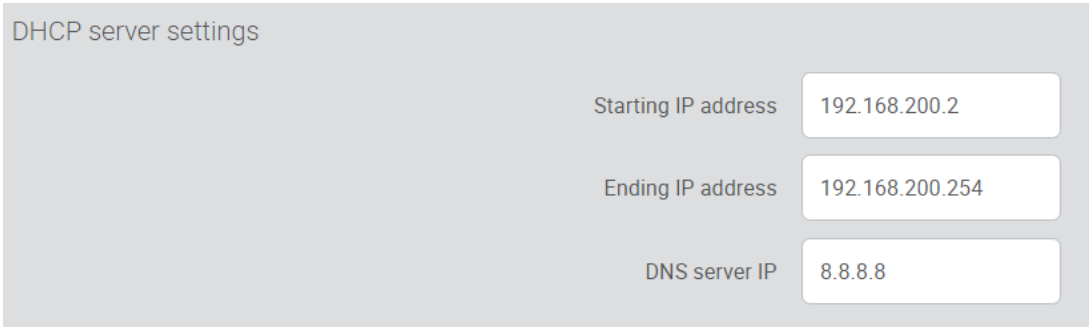
- **Enable:** Use this toggle to turn the guest network on or off.
- **Wireless name** (SSID): Enter the guest network's SSID here.
- **Security profile:** The profiles created under the *Security profiles* tab may be applied to the SSID here.
- **Encryption:** Displays the encryption method that the selected security profile uses.

Gateway IP settings (manual)



- **IP address**: Enter in the IP address the access point will be used on.
- **Subnet mask**: Select the class of the guest network. 255.255.255.0 is the standard setting and is selected by default.

DHCP settings (manual)

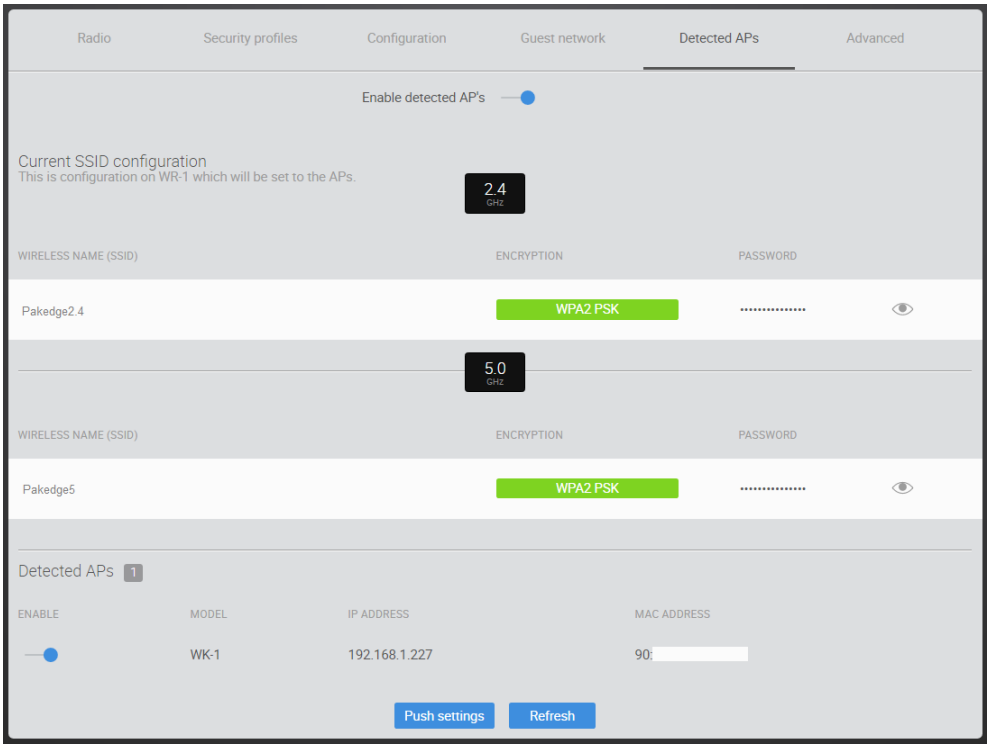


- **Starting IP address**: This is the beginning of the DHCP range used on the guest network. If you have multiple access points, you can give them the same DHCP range because the guest network of each access point will be independent of one another.
- **Ending IP address**: This is the last IP address available on the DHCP range.
- **DNS server IP**: The DNS Server IP can be set to an external DNS or to the wireless router's IP address if the wireless router provides a DNS server.

Detected APs

When enabled, the *Detected APs* tab will display the current SSID configuration and allow for up to two access points to be detected. After they're detected, the wireless router will be able to push not only the displayed SSID configuration, but also all settings from the *Configuration* and *Guest network* tabs to those Pakedge access points on the network (available only on access point firmware version 120 or higher).

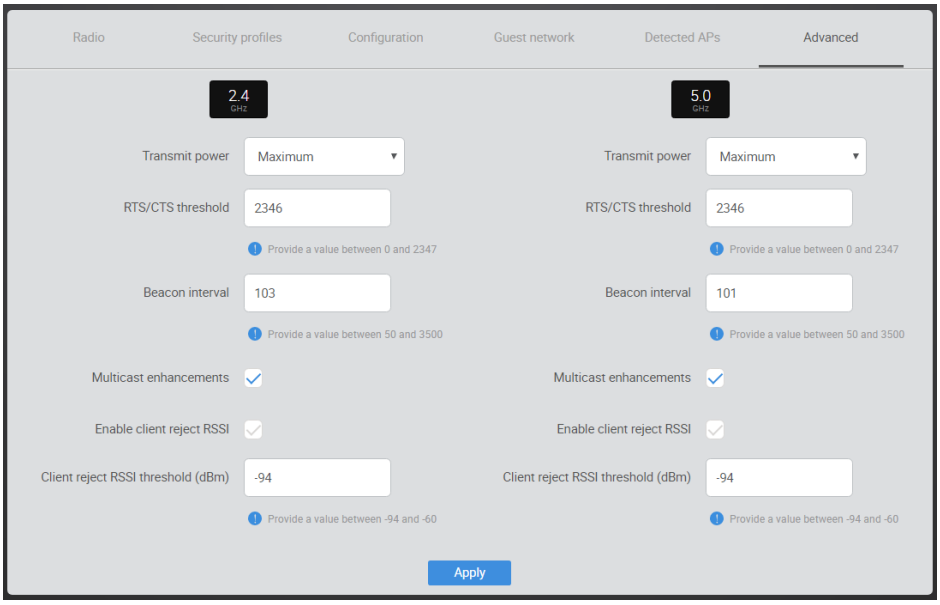
1. From the dashboard, click **Network**, then **Wireless**, then the **Detected APs** tab. Click **Push settings** after making any changes.



2. If there are no APs listed below the *Detected APs* section, click **Refresh**.
3. After the APs have been detected, use the Enable toggle to enable/ disable the settings to be pushed to particular access points.

Advanced

1. From the dashboard, click **Network**, then **Wireless**, then the **Advanced** tab. Click **Apply** after making any changes.



- **Transmit power:** The power depends on the distance of the devices in your wireless network. From the drop-down list, select the desired power. You can use this feature to limit the coverage area of the wireless network.
  - 1dBm (1mW) – 30 dBm (1000 mW): These are static power settings. The access point will broadcast at the selected power level.
  - Maximum: This setting will broadcast at the maximum allowed mW for the channel selected if Obey Regulatory Power is checked. If Obey Regulatory Power is not checked, then the maximum 30 dBm (1000 mW) will be broadcast.
- **RTS/ CTS threshold:** Enter the packet size threshold for RTS/ CTS (Request to Send/ Clear to Send) to occur. The primary reason for implementing this function is to minimize the collision between hidden stations, which occurs when access points and wireless users are spread out in a location and there is a high occurrence of retransmissions on the wireless LAN. Default setting is 2347.
- **Beacon interval:** Adjusting Beacon Interval will allow clients to sleep longer. Clients have to wake up for every beacon, so this setting tells your client how many milliseconds it can sleep for (e.g., if BP = 100 your stations are allowed to sleep for up to 100 ms).
- **Multicast enhancements:** This converts multicast to unicast to enhance the multicast performance over wireless.
- **Enable client reject RSSI:** Enables the router to reject wireless clients with signal strengths below a certain threshold.
- **Client reject RSSI threshold (dBm):** Manually sets the minimum signal strength threshold at which a device should connect to a specific radio. We recommend you keep the default setting.

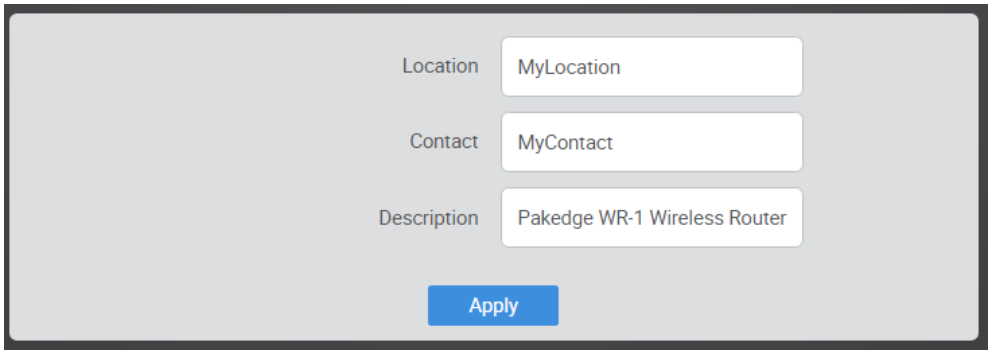
Services menu

SNMP

Simple Network Management Protocol (**SNMP**) is a standard protocol for network management that provides basic information about the device. By default, it is enabled on the wireless router.

To view the SNMP settings:

1. From the dashboard, click **Services**, then click **SNMP**. Click **Apply** after making any changes.



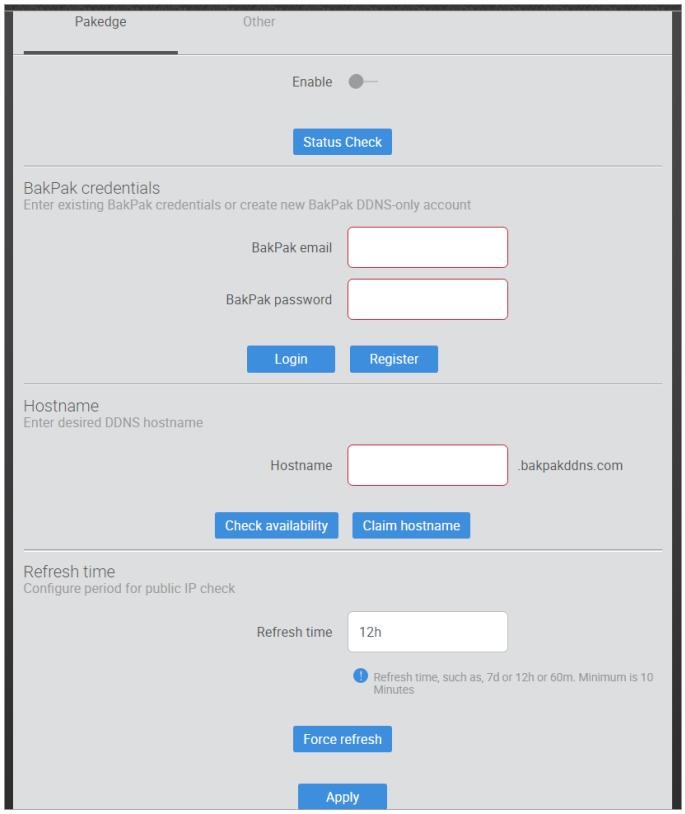
- **Location:** Type the wireless router's location here.
- **Contact:** Type the contact name here.
- **Description:** Type the router's description here.

Dynamic DNS

Dynamic DNS (**DDNS**) allows your wireless router to be reached with a fixed hostname while having a dynamically changing IP address. The wireless router has two options for DDNS. The first is under the **Pakedge** tab. Pakedge offers its own DDNS service.

To create a Pakedge DDNS:

1. From the dashboard, click **Services**, then click **Dynamic DNS**. Click **Apply** after making any changes.



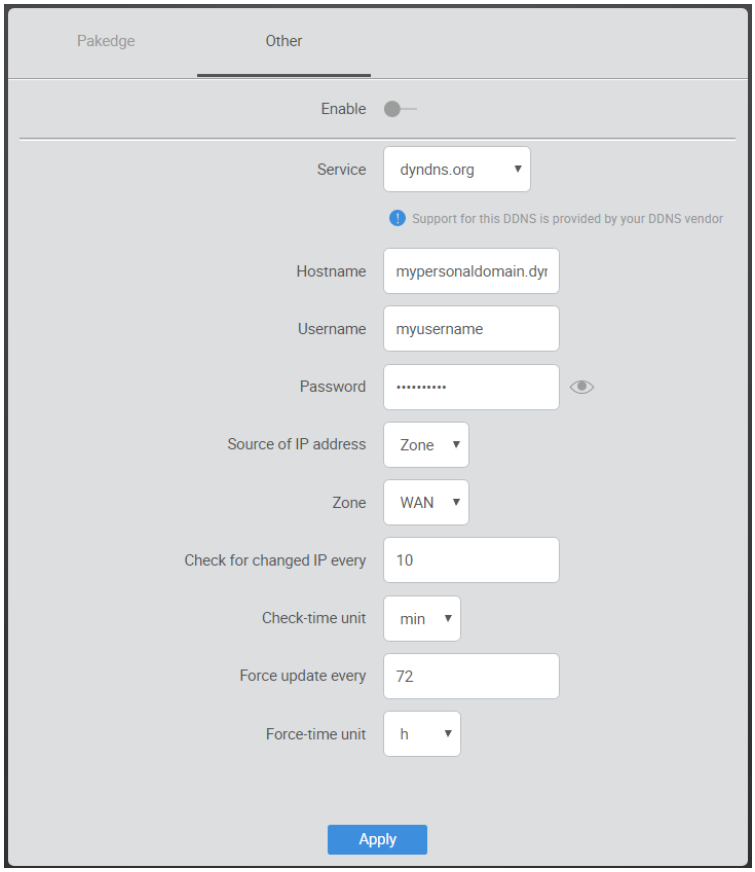
- **Enable:** Use this toggle to enable Pakedge DDNS.
- **Status check:** You can click **Status check** to see the status of your Pakedge DDNS. The wireless router displays the status of the Pakedge DDNS giving you the hostname that the wireless router is currently using.
- **BakPak credentials:** If you have an existing BakPak account, enter your credentials and click **Log in**. Or, if you don't have a BakPak account, you can register for an account to use. Simply enter an email address and password and click **Register**.
  You can change the BakPak user at any given time by simply entering the new credentials and clicking **Change**.

> **Note**: You can register for a new BakPak user only once on this wireless router. After you have registered for a BakPak user once, the Register button will disappear from the screen. Your existing BakPak account will remain active for use of BakPak DDNS.

- **Hostname:** Pakedge DDNS uses the name.BakPakddns.com namespace, where name is a name you choose. Enter a name you would like to use and click Check availability to have the wireless router check if that name is available. In the following example we will check to see if **site1BakPakddns.com** is available. If the name is available, click **Claim hostname**.
  You can change the hostname you are using at any given time by simply entering a new hostname and then clicking **Claim hostname**.
- **Refresh time:** Specify the time between public IP checks, or click **Force refresh** to refresh now.

To configure a non-Pakedge DDNS:

1 In the *Dynamic DNS* screen, click the **Other** tab. Click **Apply** after making any changes.



- **Enable:** Use this toggle to enable DDNS.
- **Service:** Select your non-Pakedge DDNS provider.
- **Hostname:** Enter the full domain name that you signed up for.
- **Username:** Enter the username for your account with your DDNS provider.
- **Password:** Enter the password for your account.
- **Source of IP address:** Select **Zone**.
- **Zone field:** Select **WAN**.
- **Check for changed IP every:** Set how often the wireless router will check to see if the WAN IP address has changed. Unit types are specified in the *Check-time unit*.
- **Check-time unit:** Select the unit of time that is used for the *Check for changed IP every field*.
- **Force update every:** Set how often the wireless router will force an update with the DDNS provider.
- **Force-time unit:** Select the unit of time that is used for the *Force update every field*.

File Sharing

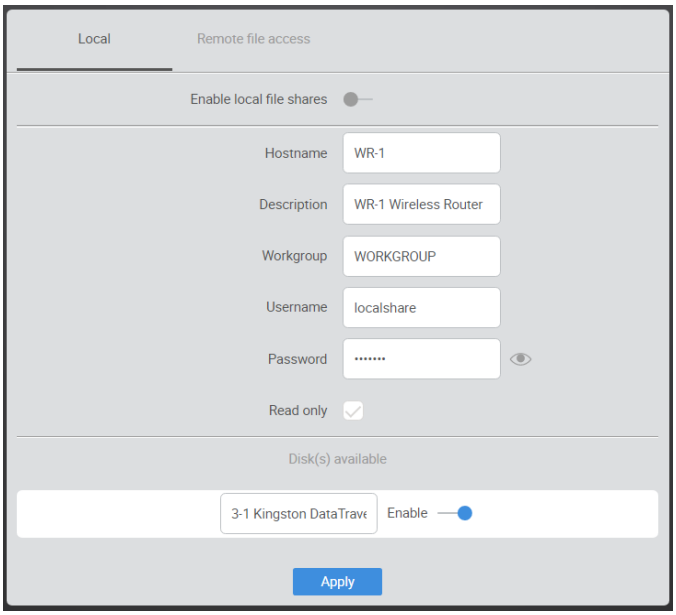
File sharing allows you to connect a USB drive onto the wireless router and share resources. The wireless router offers both local and remote file sharing.

Setting up local file sharing

Local file sharing allows you to share the contents of a connected USB drive on the local network.

To configure local file sharing:

1. From the dashboard, click **Services**, then click **File sharing**. Click **Apply** after making any changes.



- **Enable local file shares:** Use this toggle to enable local file shares, then click **Apply**. You can now access the USB drive over the local network.
- **Description:** Enter how you want to see the local file share described.
- **Workgroup:** Enter the name of your network workgroup.
- **Username:** Enter a new username (default is “pakedge”).
- **Password:** Enter a new password (default is “pakedge”).
- **Read only:** Select this so that computers on the network will be able to only read from the drive and not write to it.

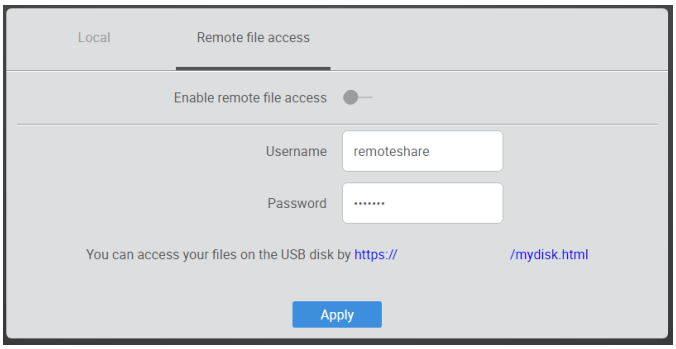
After you have enabled the file sharing and connected a USB drive into the wireless router, you will see your drive listed in the *Disk(s) available* list.

Setting up remote file sharing

Remote File Sharing allows you to access the contents of your USB drive remotely.

To set up remote file sharing:

1. From the dashboard, click **Services**, then **File sharing**, then **Remote file access**. Click **Apply** after making any changes.



- **Enable remote file access:** Use this toggle to enable remote file access, then click Apply.
- **Username:** Enter a new username (default is fileshare).
- **Password:** Enter a new password (default is pakedger).

2. To remotely access the USB drive, use a web browser to go to https://PublicIPaddress:8443/mydisk.html.

> Note: If you configured DDNS on the wireless router, you can use that in place of the public IP address. You will see a login screen similar to when you log into the wireless router.

3. Enter your credentials and click **Log in**. You will see the USB drive listed.
4. Click the USB drive to view the files and folders inside of it, then click a folder to view the contents of it.
5. Select a file and click **Download** to retrieve the file from the USB drive. You can also click **Delete** to remove it.
6. You can also upload a file onto the USB drive remotely. Click the file upload icon, navigate to the file and select it, then click **Upload**.
7. You can also create folders. Enter the folder name in the **Folder to create** field, then click **Create Folder**.
8. Finally, click **Log out** to log out of the file share.

Mapping network drives

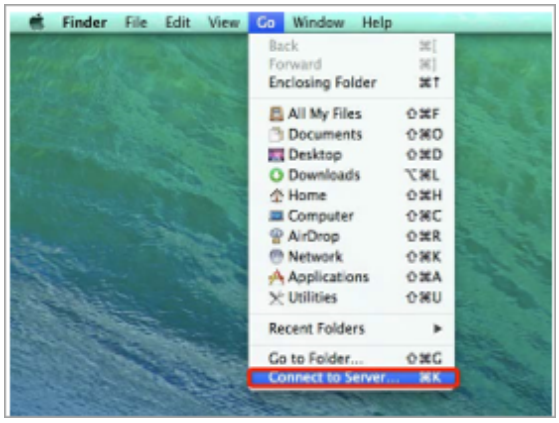
The following section will show you how to map the USB drive on the wireless router on various operating systems.

Mac OS X

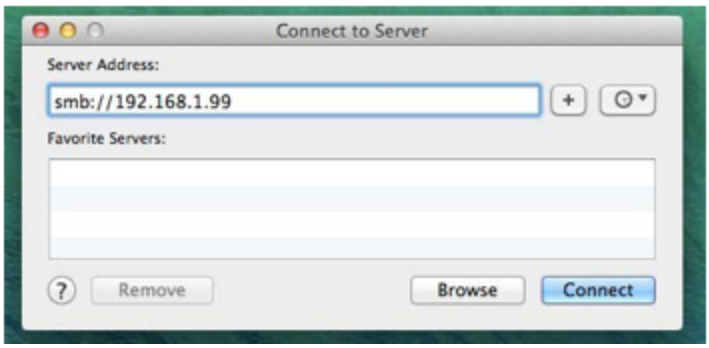
To map the USB drive on Mac OS X:

1. Click **Go** at the upper left.

2. Click **Connect to Server**.

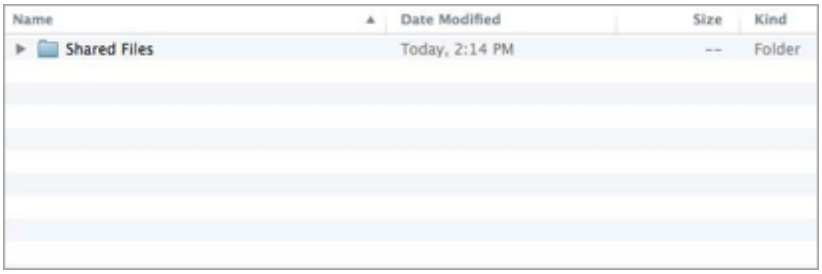


3. In the **Server Address** field, enter **SMB://IP address of your wireless router**. The following image shows an example of this. Click **Connect**.



4. You will be prompted to login as a **guest** or **registered user**. Select **registered user**. In the username and password field enter the credentials you have configured on the wireless router.

5. The USB drive will now be mapped on your computer and you will be able to access files on that drive.

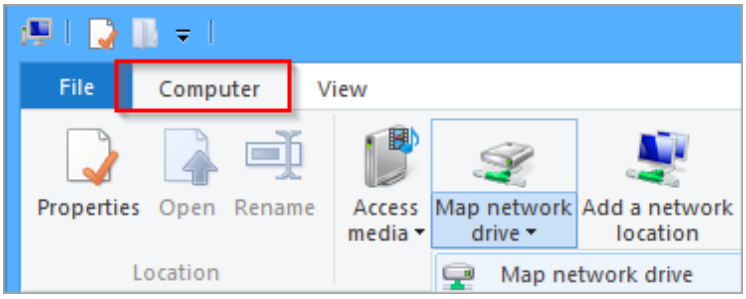


Windows 8/10

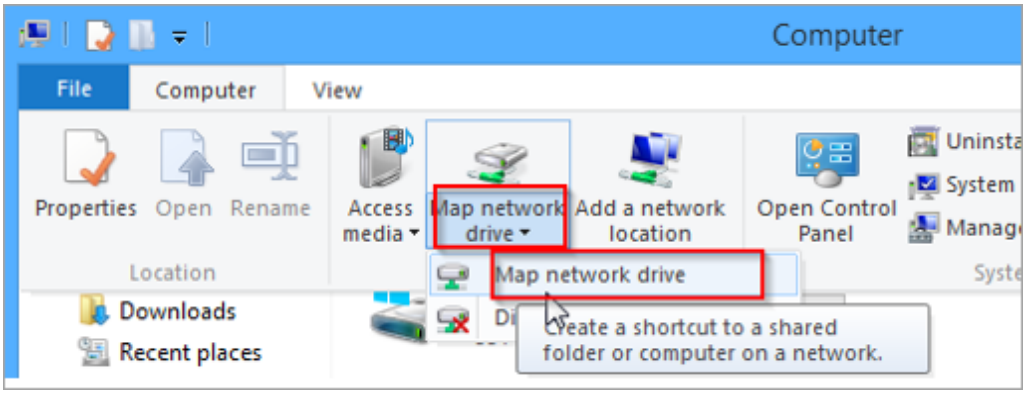
To map the USB drive on the device for Windows 8/10:

1. Press the windows button on your computer. Type "computer" and press **Enter**.

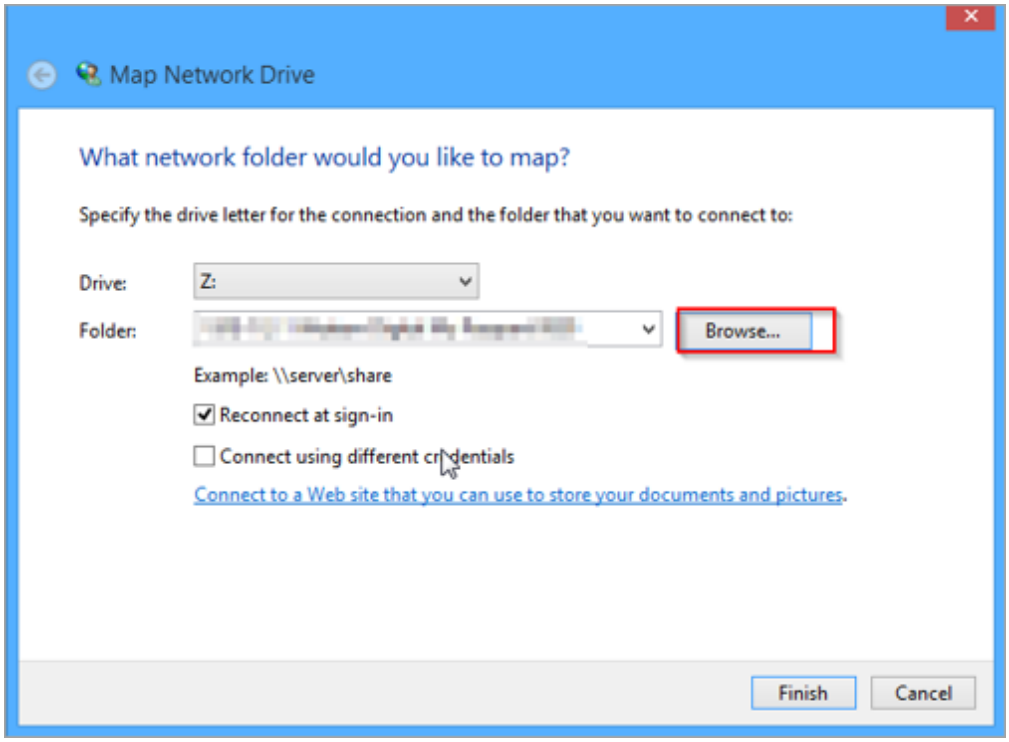
2. Click **Computer** towards the top.



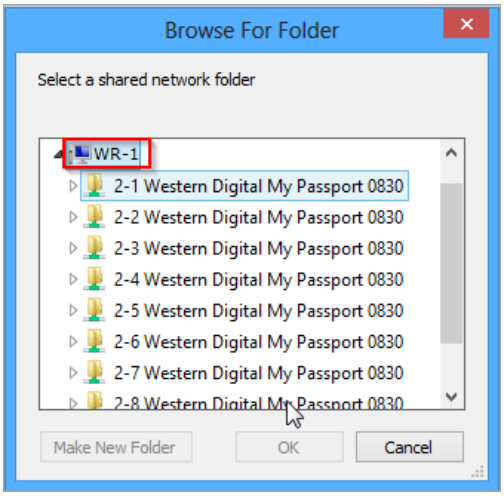
3. Click **Map network drive**.



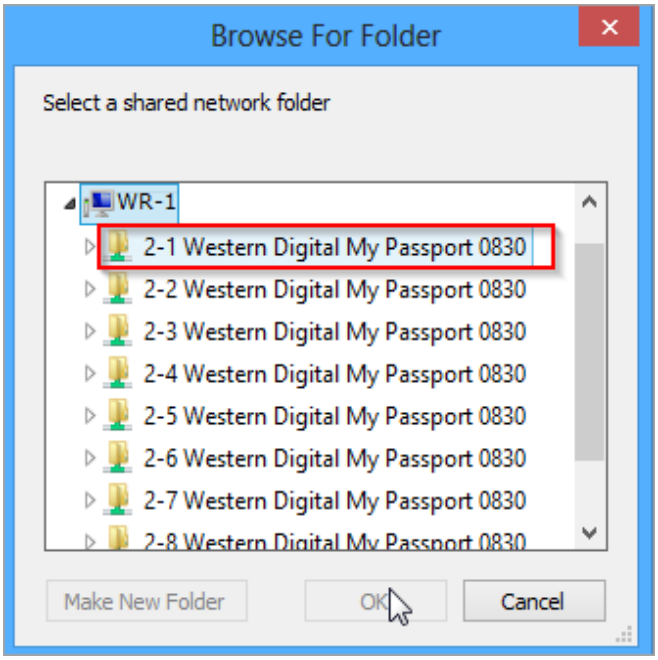
4. Click **Browse**.



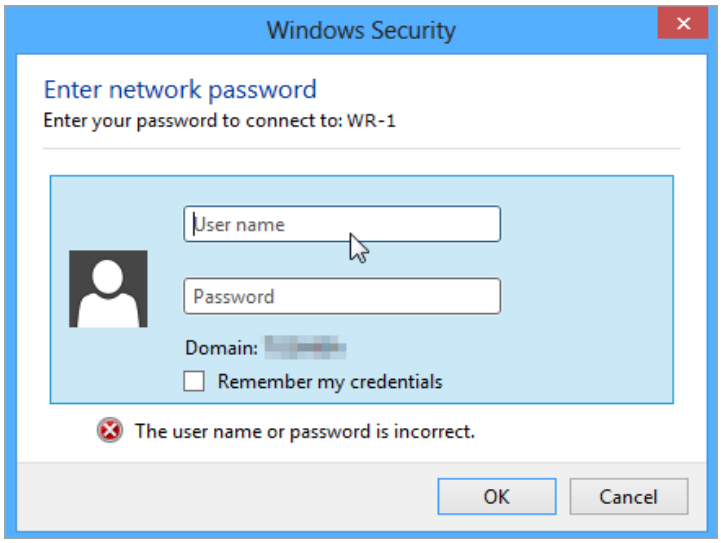
5. You will see the wireless router listed. You will also see all of the folders on the USB drive connected to the wireless router.



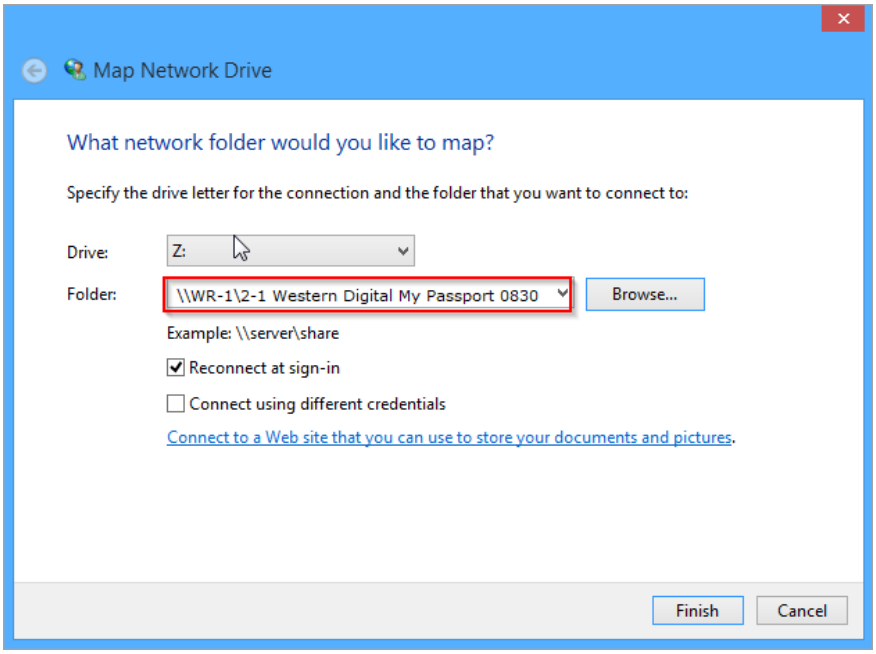
6. Select the folder you want to map and click **OK**.



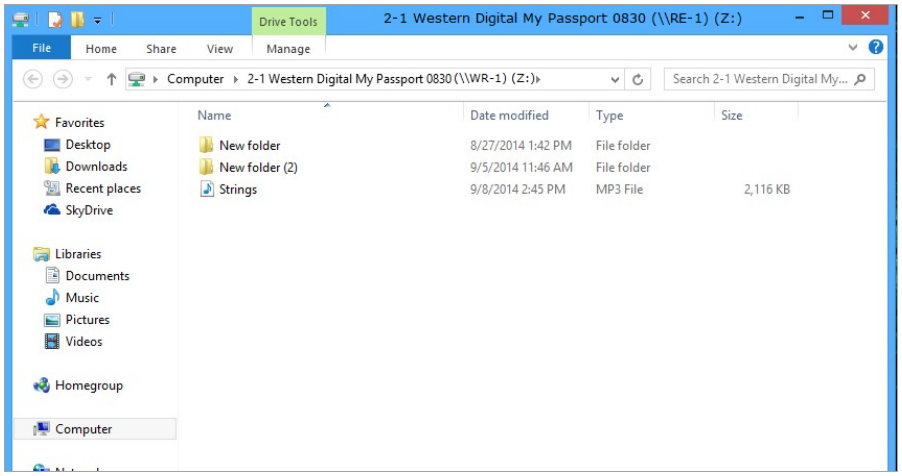
7. Enter the credentials to access the folder.



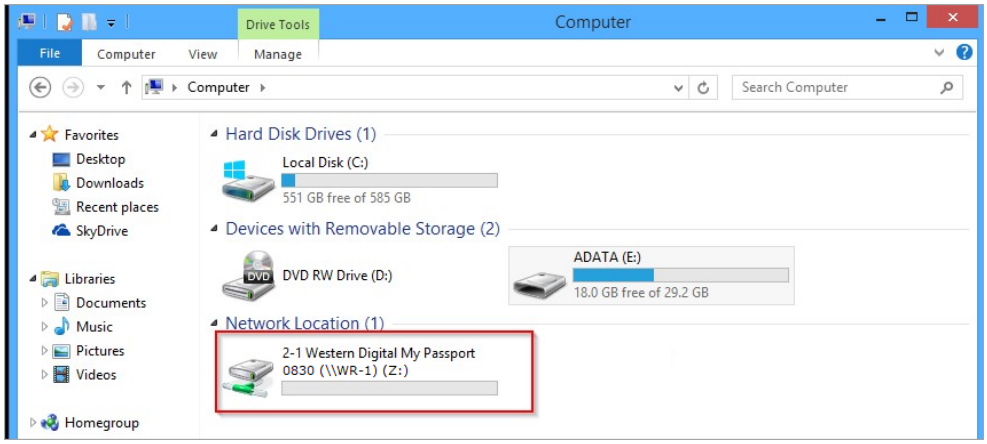
8. Your folder field will have auto populated with the name of the folder. Click **Finish**.



You will now have access to the files on the USB drive.



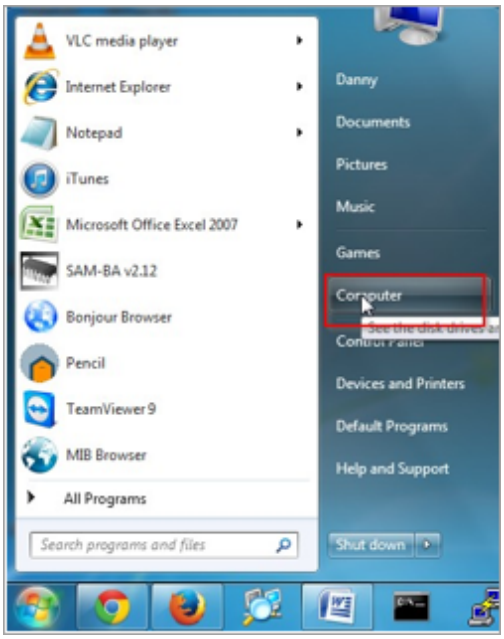
Your folder will now show up as a mapped drive.



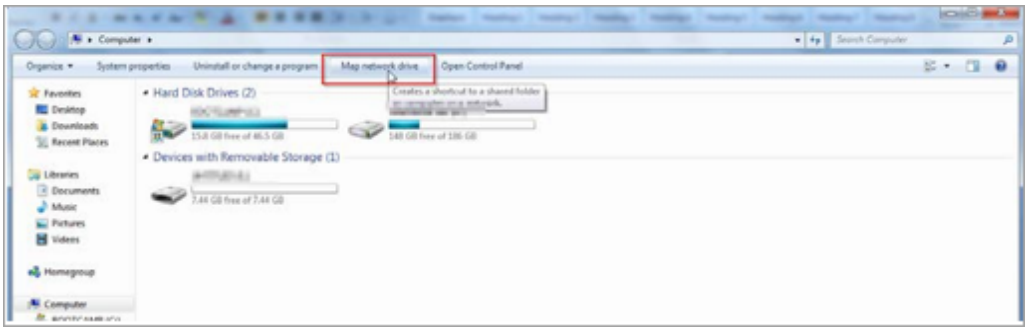
Windows 7

To map the USB drive on the device in Windows 7:

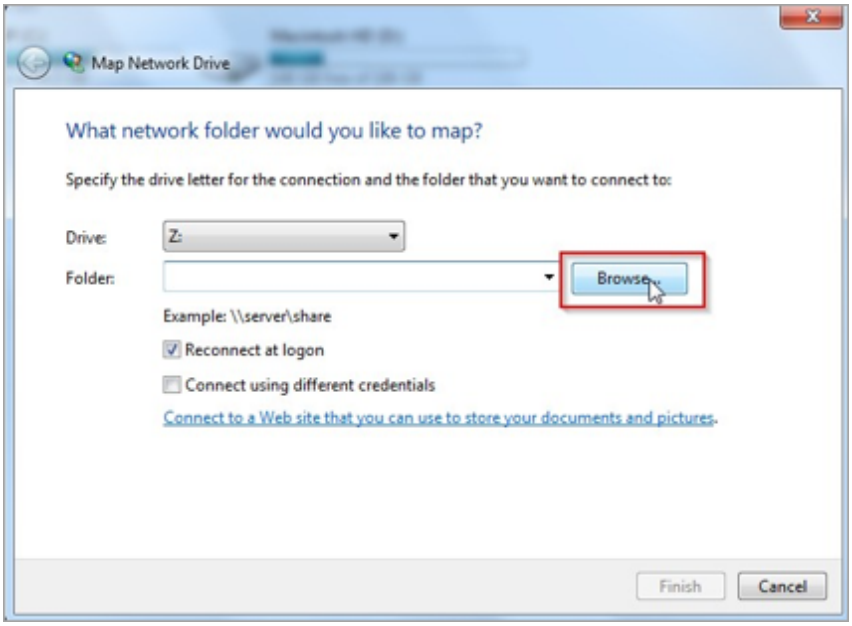
1. Click the start button at the bottom left hand side. Click **Computer**.



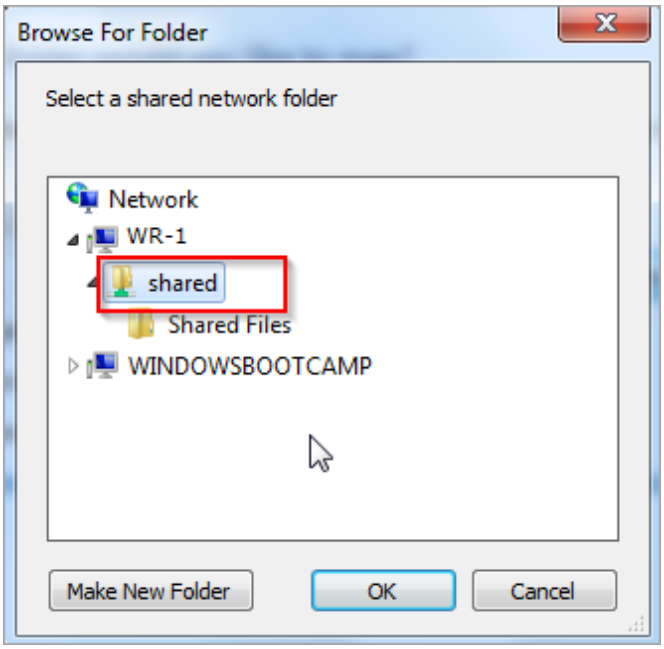
2. Click **Map Network Drive**.



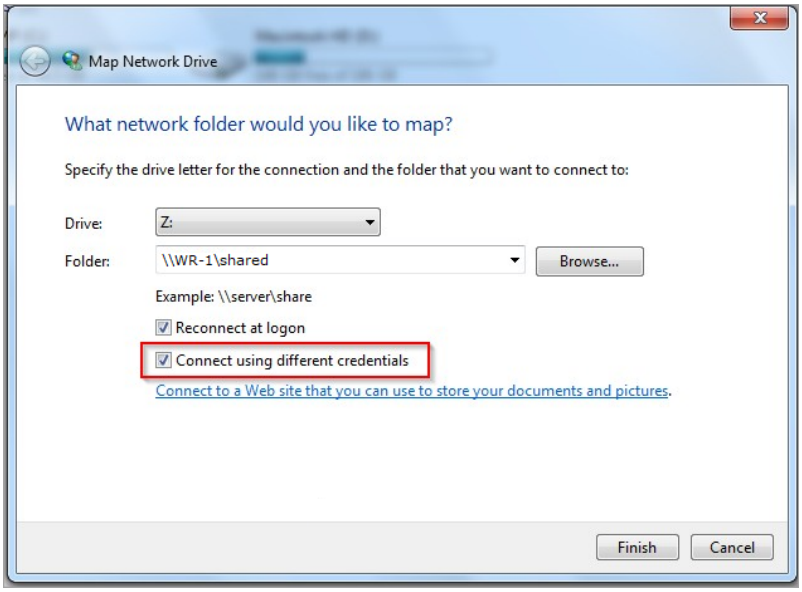
3. Click **Browse**.



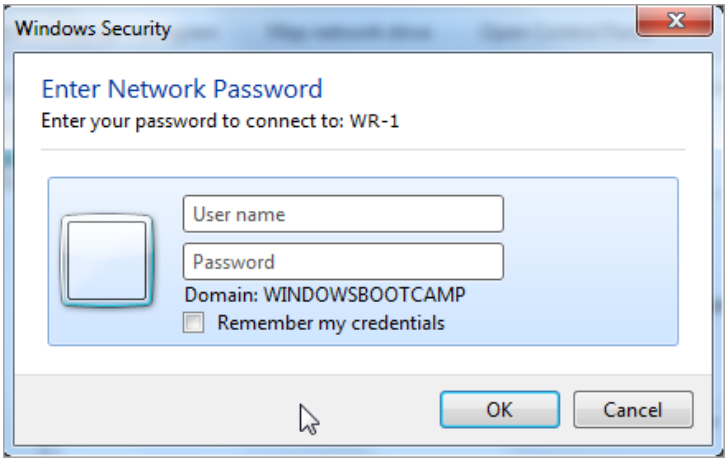
4. Click **WR-1**to expand it. Click the folder you want to map underneath it to select it. Click **OK**.



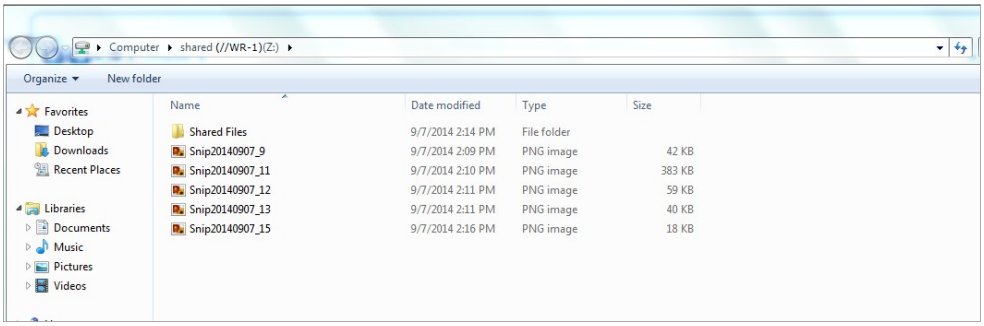
5. Check the box titled **Connect using different credentials**, then click **Finish**.



6. Enter the username and password to access the folder. Click **OK**.



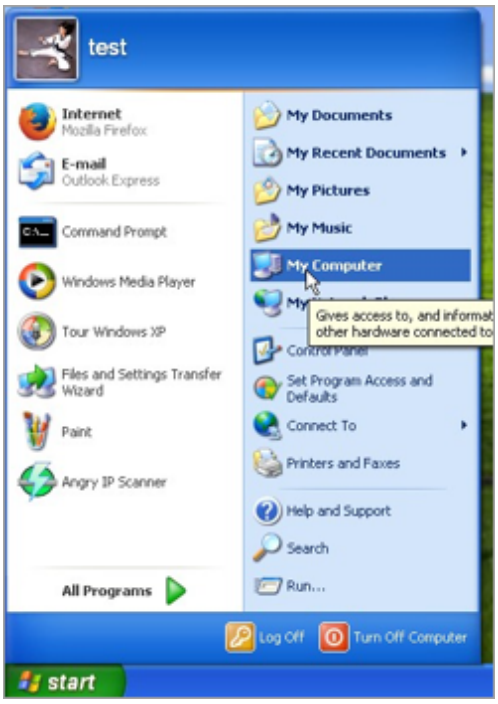
7. You will now have access to the files on the USB drive.



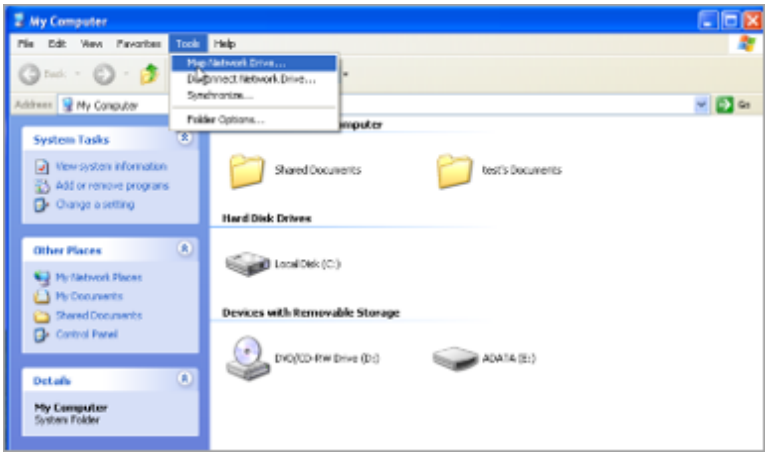
Windows XP

To map a USB drive in Windows XP:

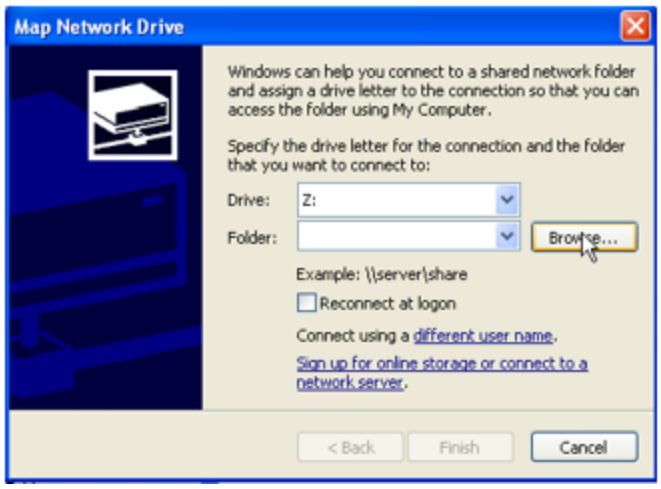
1. Click **My Computer**.



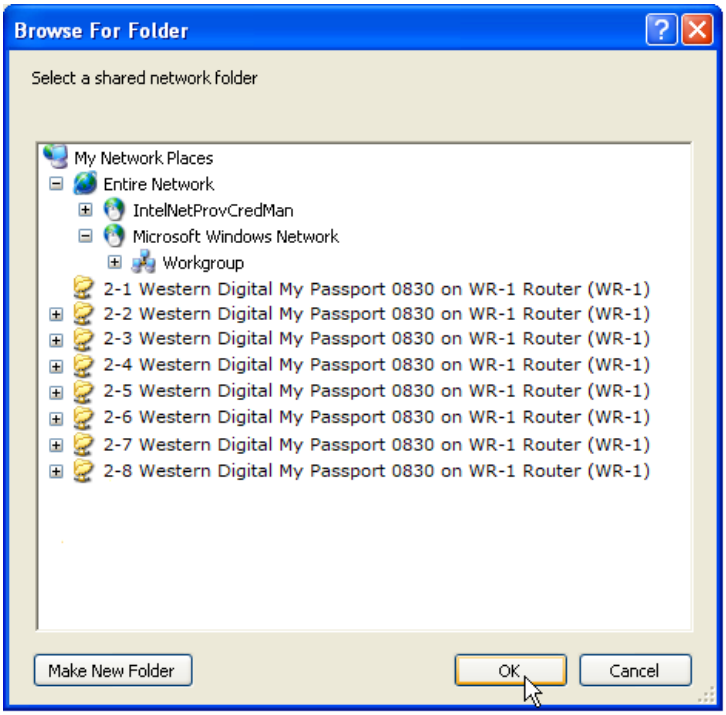
2. Click **Tools > Map Network Drive**.



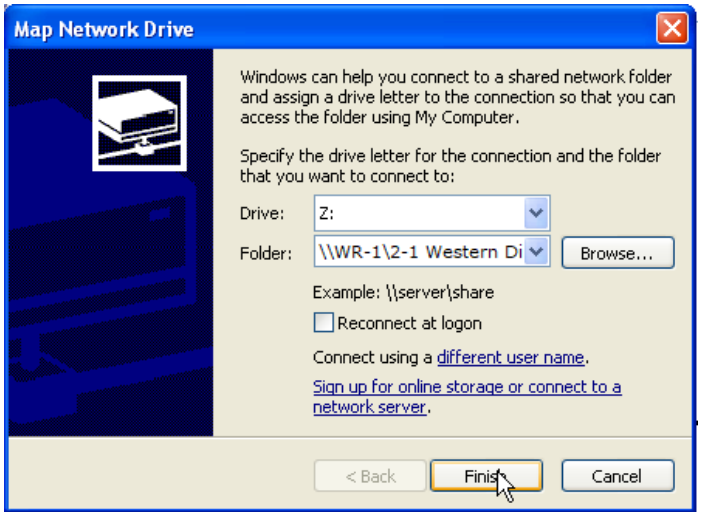
3. Click **Browse**.



4. Select the folder you want to map. Click **OK**.

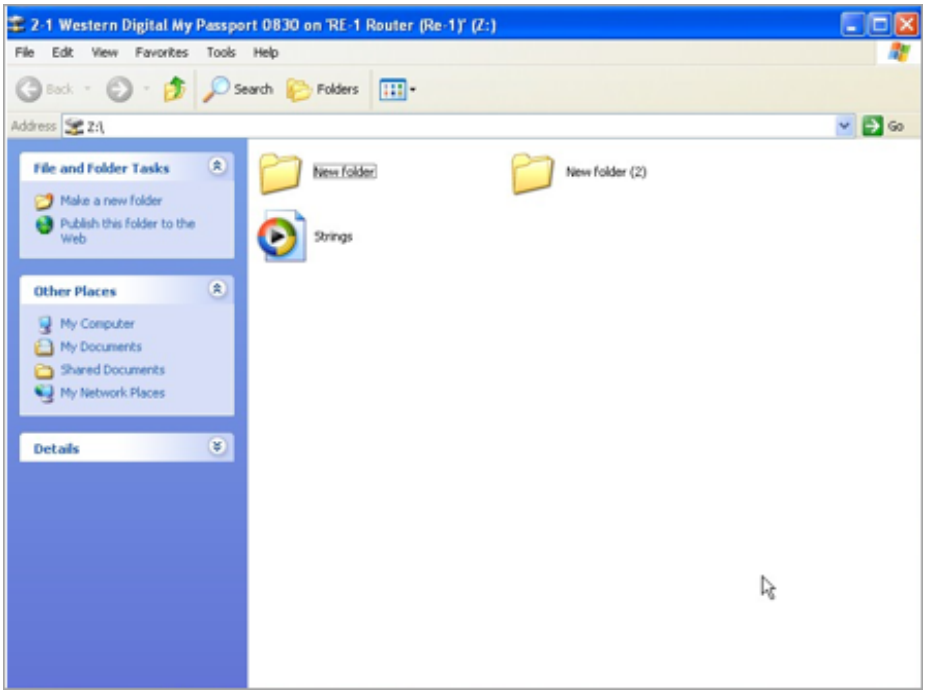


5. Click **Finish**.

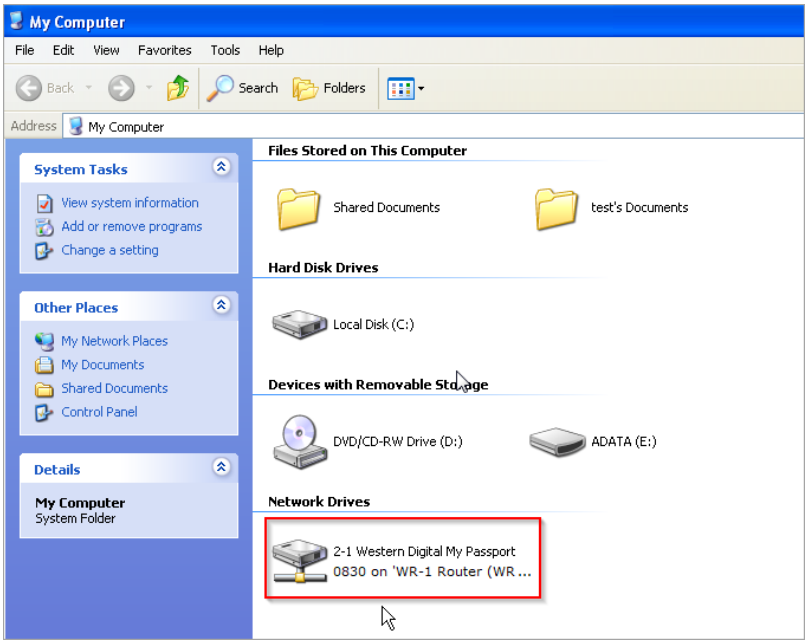


6. Enter the credentials to access the folder.

You will now have access to the folder.



Your folder will now be mapped on your computer.

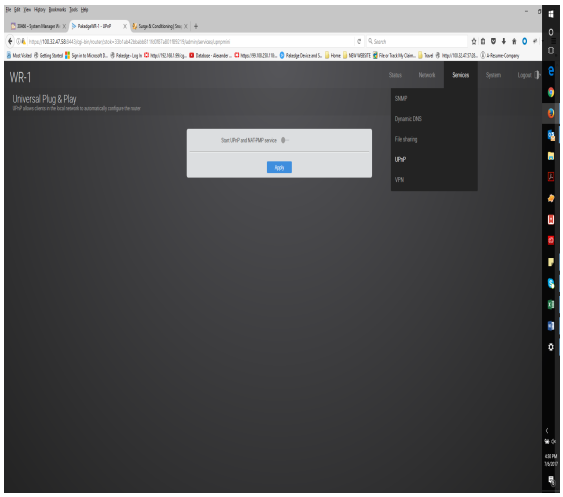


UPnP

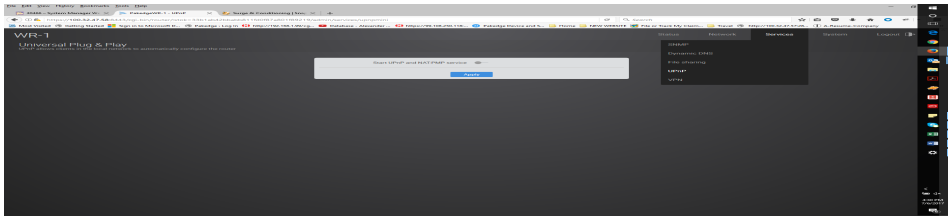
UPnP allows for automatic configuration of the wireless router for your devices. This can be essential for certain audio/video systems and devices such as game consoles.

To enable UPnP:

1 From the dashboard, click **Services**, then **UPnP**.



2. Select the toggle for **Start UPnP** and **NAT-PMP** service, then click **Apply**.



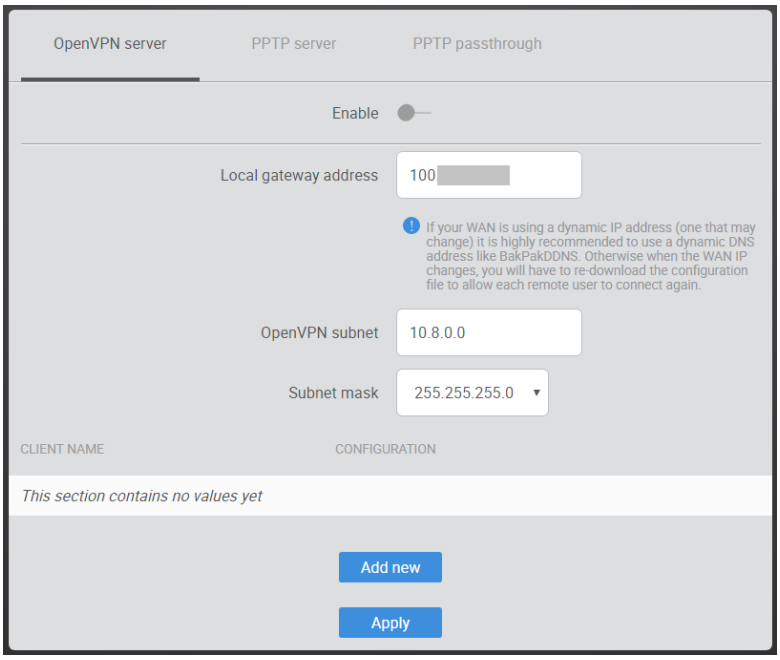
VPN

The wireless router supports OpenVPN. You can connect to the wireless router remotely and have access to all network resources.

Configuring OpenVPN

To configure OpenVPN:

1. From the dashboard, click **Services**, then **VPN**.



2. Select the **Enable** toggle, then configure the following fields:
   - **Local gateway address:** The Public IP address or DDNS name of the WAN interface. We recommend that you use DDNS or BakPakDDNS because if the WAN IP changes, all remote clients will require new configurations made for them.
   - **OpenVPN subnet:** The IP Subnet used by the OpenVPN connected clients. The OpenVPN clients will connect using their own dedicated IP subnet. This IP subnet cannot overlap with any of the local LAN or VLAN networks on the wireless router. This is why the default is set to 10.8.0.0. This should be in IP Subnet notation (with 0 at the end of the address).
   - **Subnet mask:** The subnet mask size to use for the OpenVPN network.

> Note: the default username is **pakedge** and the default password is **pakedgev**. To add users to the VPN, click **Add new** and specify a name. Each remote client connecting to the wireless router's OpenVPN server will need to have a profile created for them. The profile only requires a name given to it. Then the profile is downloaded as a configuration file and sent to the device that will be connecting.

When you connect to the VPN you will have full access to all of your devices on the network.

> Note: When you connect to the VPN, you will receive an IP address from the same IP scheme as your LAN zone. For example, if your LAN zone is setup for 192.168.1.X you will receive an IP address from the IP range of 192.168.1.20 thru 192.168.1.30. If your network LAN zone is setup as 192.168.10.X you will receive an IP address from the IP range of 192.168.10.20 thru 192.168.10.30.

OpenVPN client setup

After creating a client profile and downloading the configuration file, you need to load the configuration file into the OpenVPN program you are using.

- Each operating system has its own version of an OpenVPN client. The connecting device will need to download an OpenVPN client (which we have recommendations on below).
- If the configuration file was downloaded to a PC which is not the device that will be connecting, email the configuration file to an account that the device can access. This will allow mobile devices to open the configuration file directly to their OpenVPN app.

> Important: Each configuration created for the OpenVPN server will only allow one connection at a time. Multiple users must have individual configurations created for them. If a second user attempts to connect to a configuration with a user already connected, the first user will be dropped from the connection.

Windows

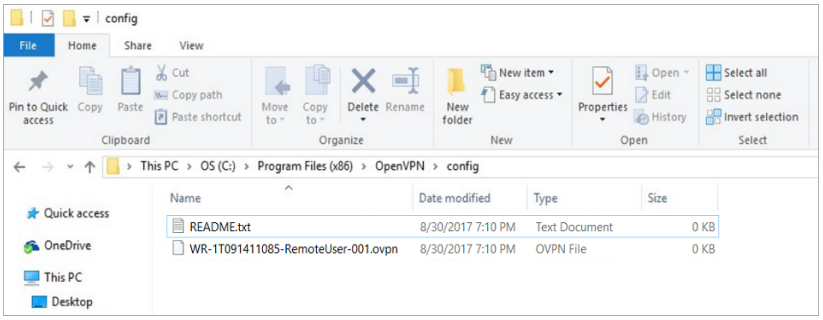
The official OpenVPN release for Windows ships with a GUI frontend called simply "OpenVPN-GUI" and can be found in the .\bin\ subdirectory of the installation path, with shortcuts placed on the desktop and start menu unless unselected during program installation. This wiki page describes how to use this GUI frontend.

The GUI lives in the system tray, so controlling one or more VPN processes is always done through the context menu of the GUI icon. When the GUI is launched, nothing will happen beyond placing the icon in the tray. To do something useful with the GUI, you need to interact with it by right-clicking to bring up the context menu.

Note the GUI will start the VPN process in the context of the running user. When this user does not have administrative rights (or has rights limited through UAC) it will most likely fail to correctly start the VPN as routes and addressing cannot be changed by unprivileged users.

When starting the OpenVPN GUI, the standard Windows practice of right-clicking on the shortcut and selecting "Run As Administrator" will allow a UAC user to run it in administrative context. If the user lacks admin rights, it will be necessary to "Run As..." and enter credentials for an administrative user. Once started in this fashion, further interaction via the tray icon will be run in the context of the elevated user.

Creating and placing config files



By default, the GUI will present context entries to connect to any *.ovpn file under the .\config\ dir of the installation path (including subfolders.) If you do not place any config files here, the context menu in the GUI will not allow you to connect anywhere (since it has nowhere to connect to.)

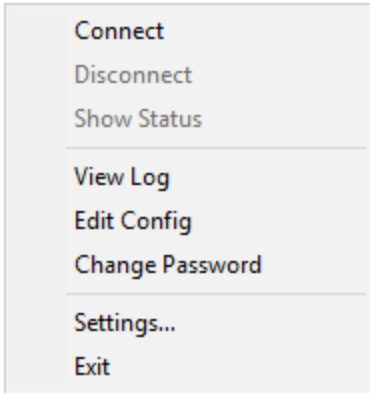
The screenshots below demonstrate use of the OpenVPN-GUI, step-by-step.

After Startup

After initially launching the OpenVPN-GUI program, the GUI icon will be show in the tray, as shown in the image below. Note that this icon can be hidden when marked "inactive" by the OS, so check the expanding arrows to the side of the system tray if it's started but not shown.

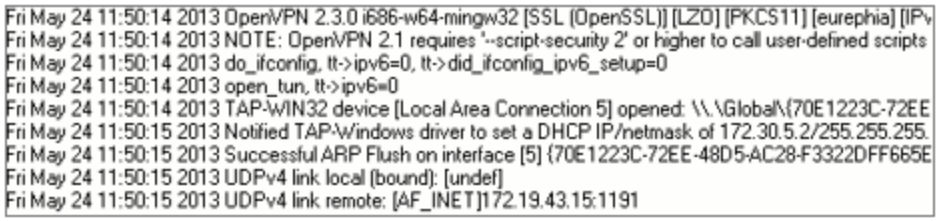
Context Menu

Right-clicking on the icon will pull up the context menu. This menu will allow you to connect any of the config files placed as explained above. Note that you must name these files with the .ovpn file extension. Windows has a bad habit of hiding "known" file extensions, so be careful not to name a config file something like “Sample.ovpn.txt” by mistake.



Connecting and disconnecting

After you have created a config file, going into the context menu and selecting the "Connect" entry will start openvpn on that config file. A status window will open up showing the log output while the connection attempt is in progress (see screenshot below). After successful connection, the status window will be hidden, but can be viewed from the context menu if desired.



After connecting, the context menu will allow that VPN to be disconnected; select that option to terminate the active connection.

When one or more VPN instances are running from the GUI, the tray icon will change color.

OS X

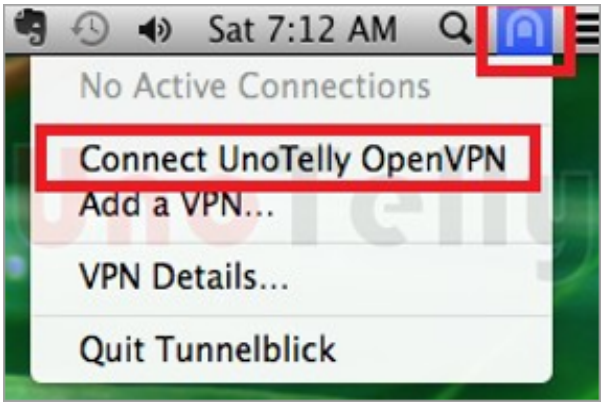
Tunnelblick is a popular, free, open source OpenVPN client for OS X.

To install Tunnelblick:

1. Download Tunnelblick here, and save it to a safe location.
2. Download the Tunnelblick OpenVPN configuration files here and save them to a safe location.
3. Double-click the **.ovpn** file you downloaded earlier. A dialog opens asking you for your configuration preference. You can choose to install the OpenVPN configuration for all users or just your account.

4. Enter your Computer username and password, then click **OK**.

5. Click the Tunnelblick icon in your menu bar, then click **Connect OpenVPN**.



6. If the connection is successful, you will see the following window appear briefly:

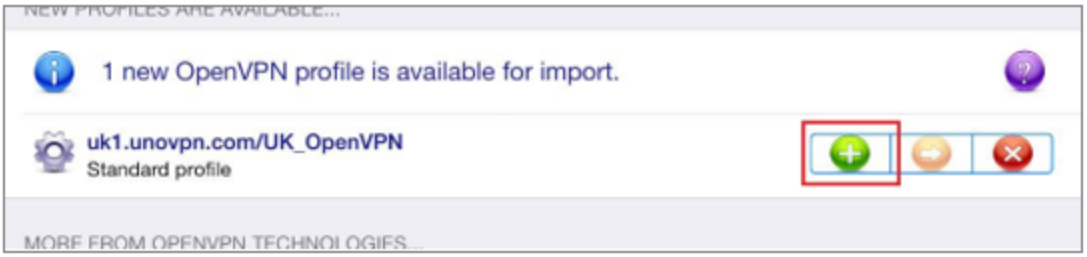
iOS

OpenVPN Connect is a free OpenVPN client for iOS devices.

To install OpenVPN Connect:

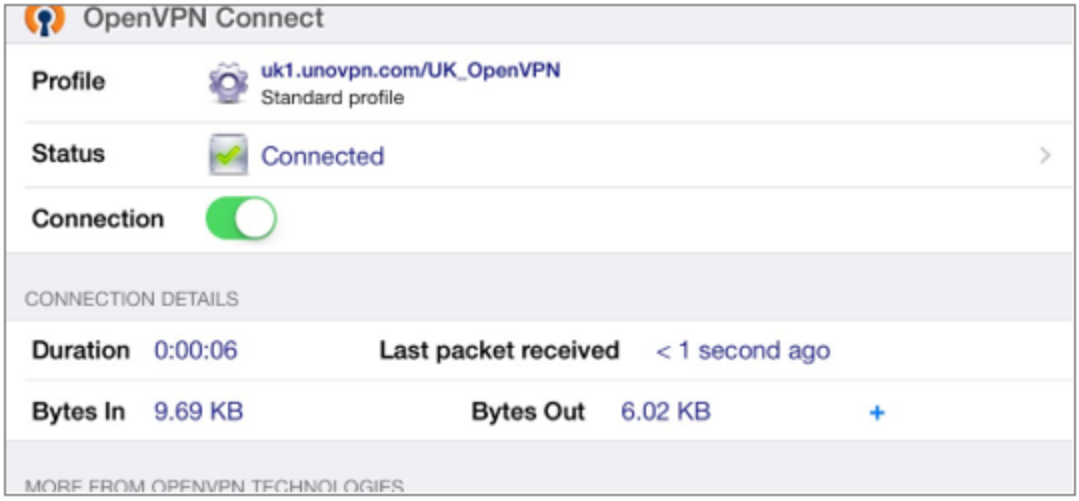
1. Download and install OpenVPN Connect from the App Store.
2. Open the email you sent yourself with the config file on your iOS device and tap the attached file.
3. Tap **Open in OpenVPN** and the OpenVPN Connect app should open automatically.

4. Tap “+” to import the profile.



5. Type the User ID and Password for your UnoVPN account.
6. Tap **Connection** to connect to the VPN.

7. If connected successfully, you will see something like the following screen:

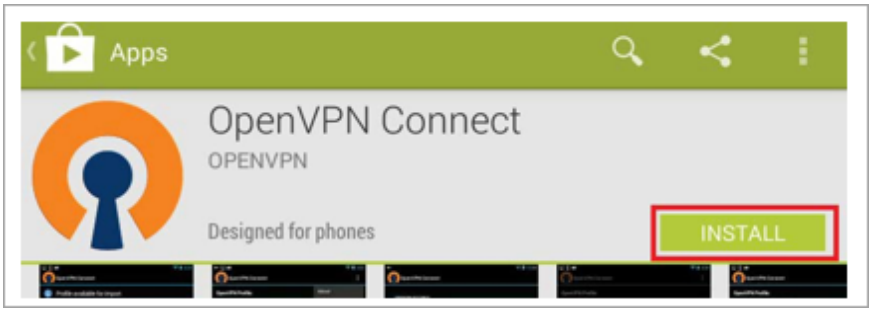


Android

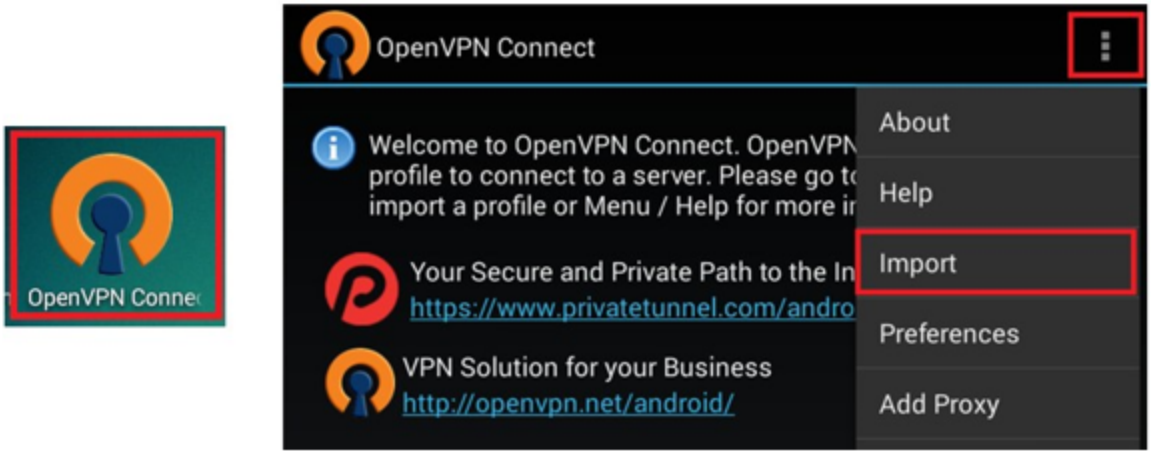
OpenVPN Connect is a free OpenVPN client for Android devices.

To install OpenVPN Connect:

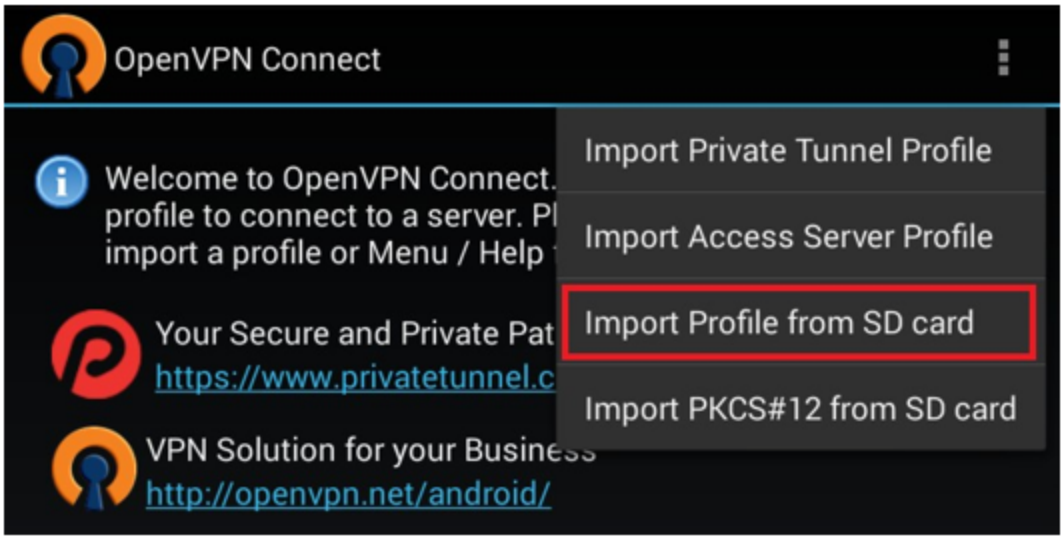
1 Download and install the OpenVPN Connect app from Google Play.



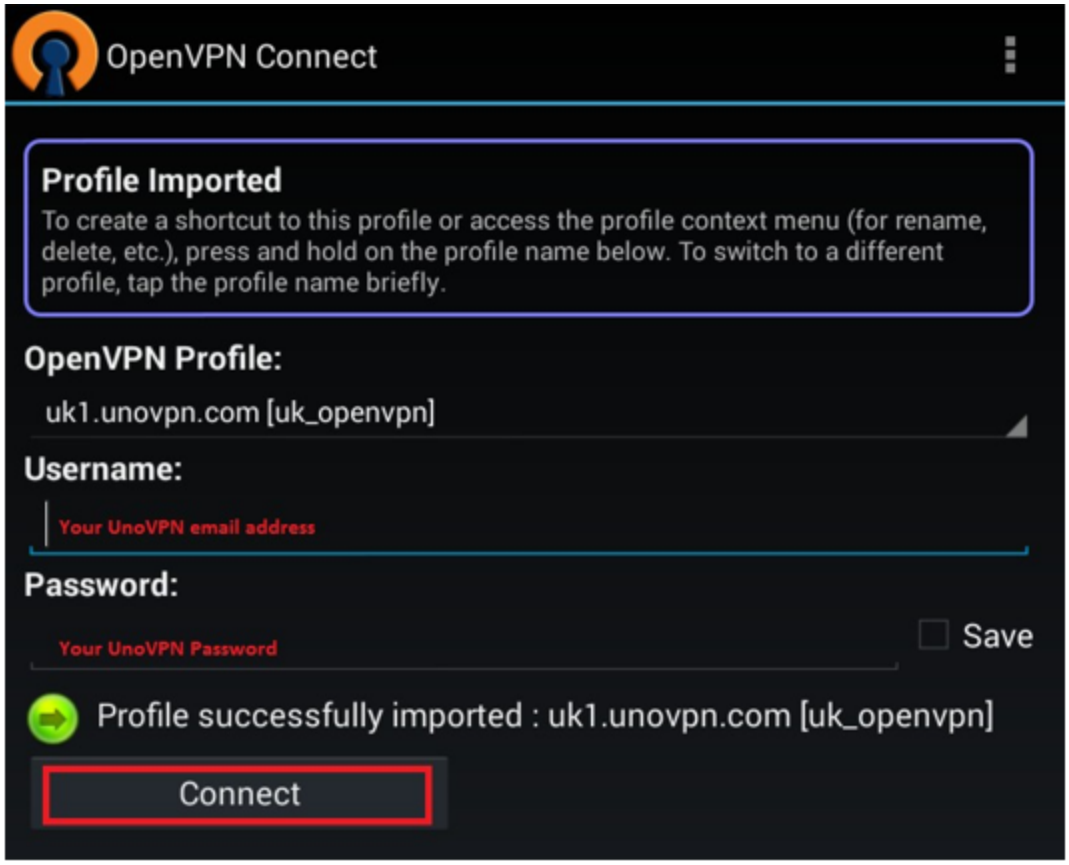
2. Download the OpenVPN Config file here and save it on your Android device.
3. Open the OpenVPN Connect app, tap its **Menu** icon, then tap **Import**.



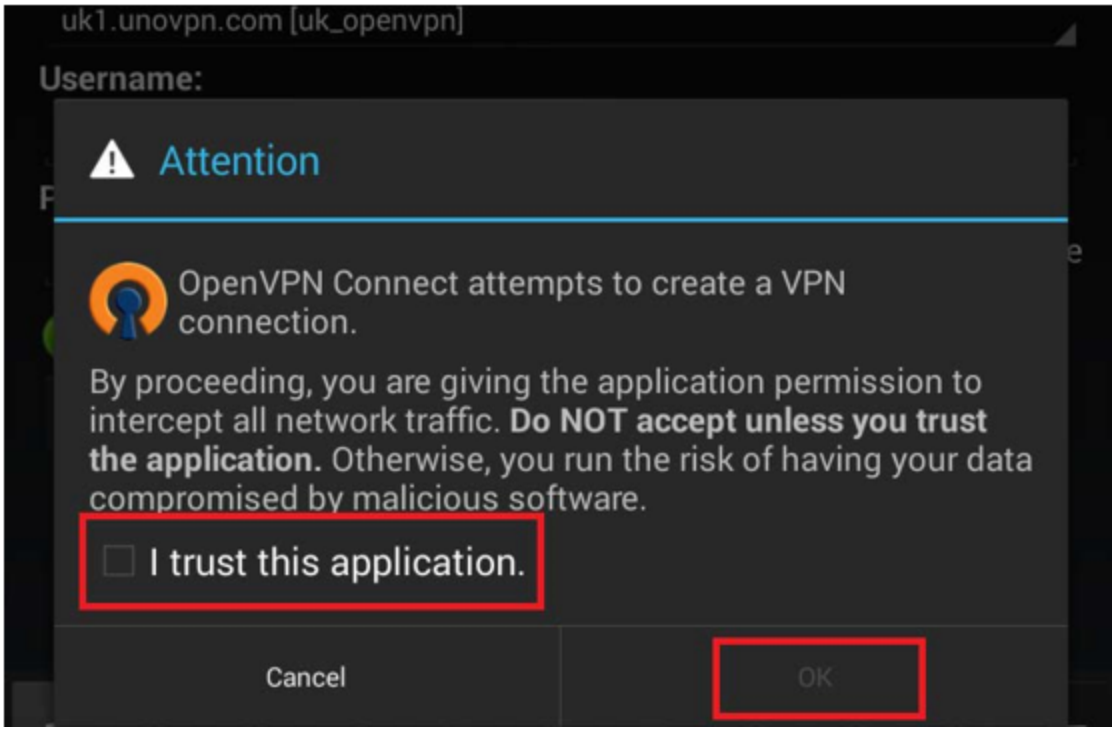
4. Tap **Import Profile from SD card**, locate your downloaded OpenVPN Config file, then tap Select to import the file.



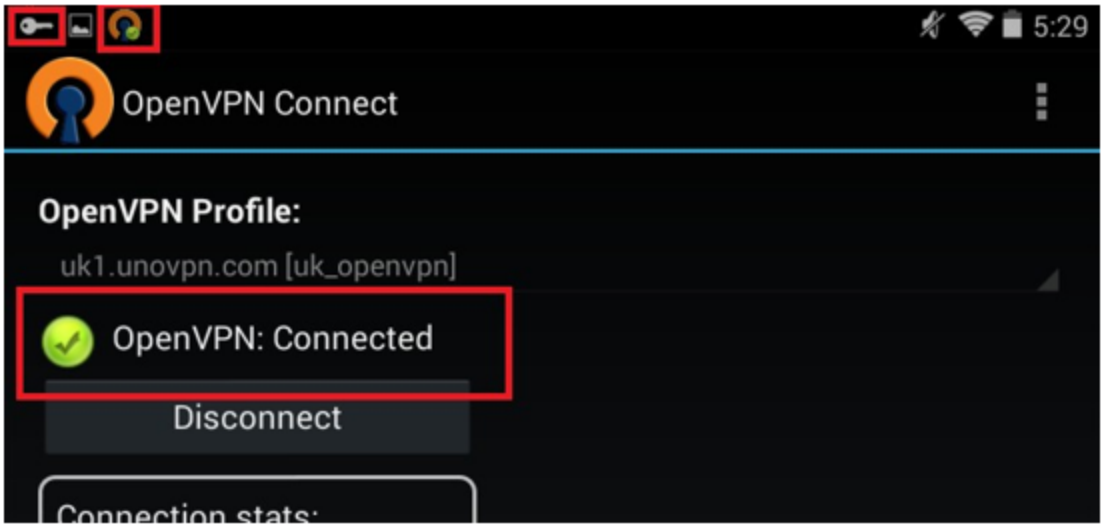
5. Enter your UnoVPN Username and Password, then tap **Connect**.



6. Allow permission to run OpenVPN by selecting **I trust this application**, then tap **OK**.

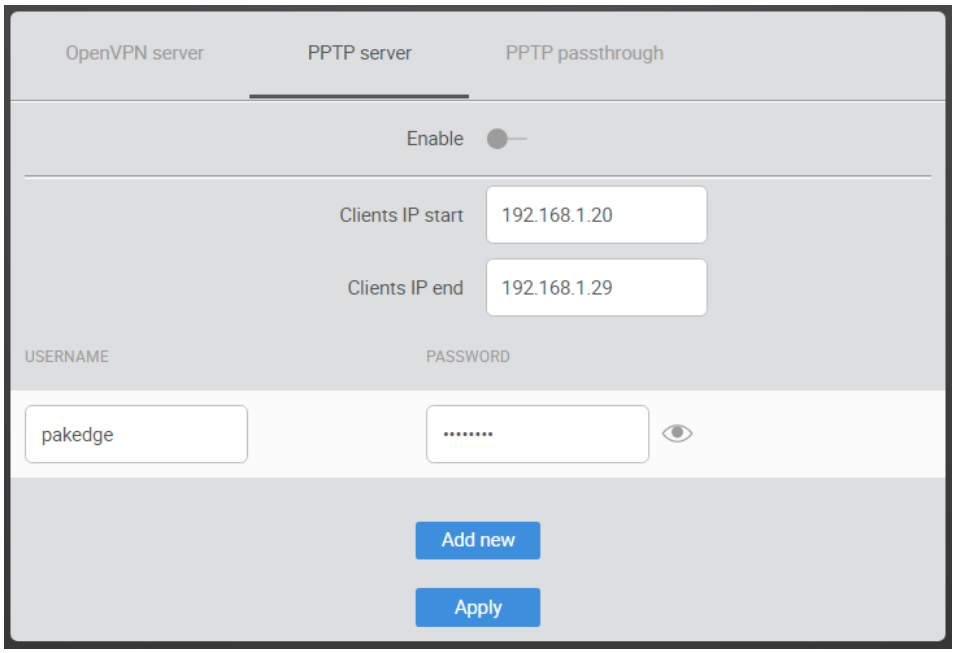


You are connected to OpenVPN.



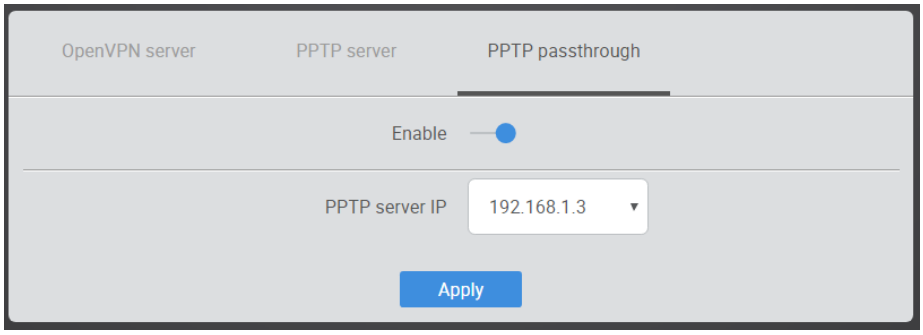
Configuring PPTP server

A less secure VPN option compared to OpenVPN, PPTP is faster and uses fewer CPU resources.



1. Select the **Enable** toggle, then configure the following fields:
   - **Client IP start:** Set the lowest number of the range of IP addresses to allow.
   - **Client IP end:** Set the highest number of the range of IP addresses to allow. This limits the number of clients that can be connected to this network simultaneously.
   - **Username:** Enter a username for PPTP access (default is **pakedge**).
   - **Password:** Enter a password for PPTP access (default is **pakedgev**).
2. You can add new users to this list. Just click **Add new**, type a new username and password, then click **Apply**.

Configuring PPTP passthrough



1 Select the **Enable toggle**, then configure the following field:

- **PPTP server IP:** Enter the PPTP server's IP address.

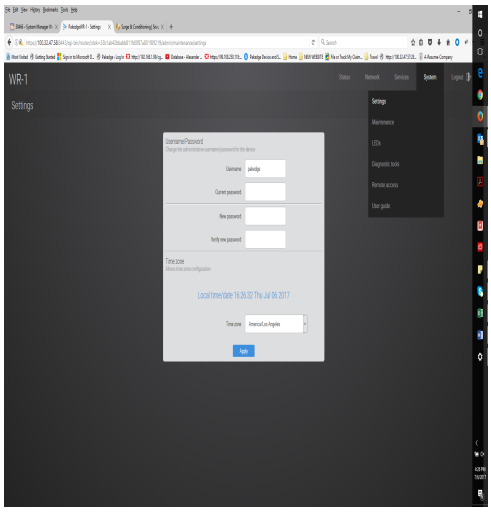
System menu

Settings

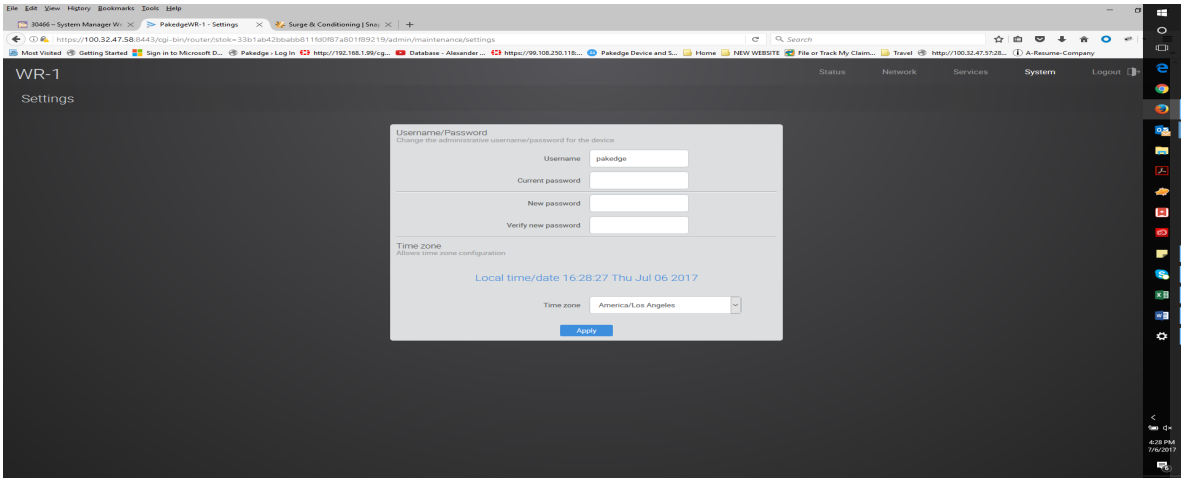
Username/ Password

To change the password:

1. After you're logged into the wireless router, navigate to **System > Settings**.



2. Enter the password you would like to use for the wireless router. There are no specified requirements for the password. You will need to enter the password a second time to confirm it.



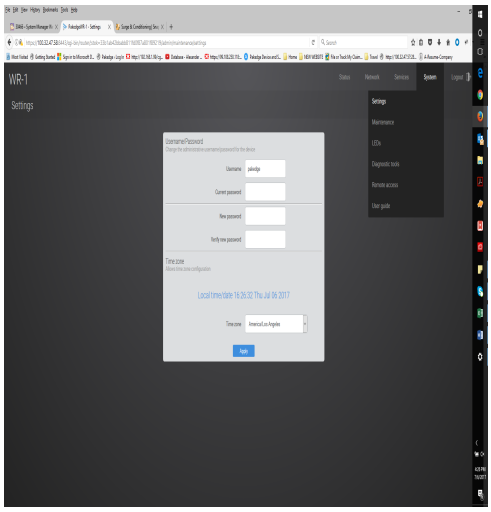
3. You can also change the default username. Simply type in the username you would like to use. Click **Apply** to finalize the settings.
4. You will then be prompted to log into the wireless router with the new password.

Time zone

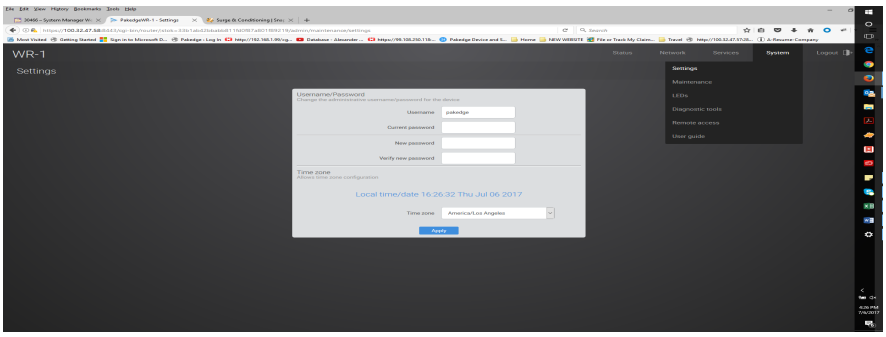
The Time zone page allows you to set the appropriate time on the wireless router.

To set the time zone:

1. Click **System > Settings**.



2. Select your time zone from the drop-down menu.



3. Click **Apply** to finalize your settings.

Maintenance

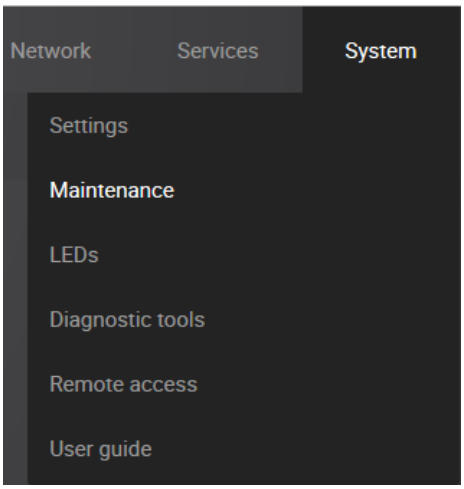
The *Maintenance* page allows you to back up and restore a configuration file, return the router to factory default settings, remotely reboot the router, and update the router firmware.

Backup

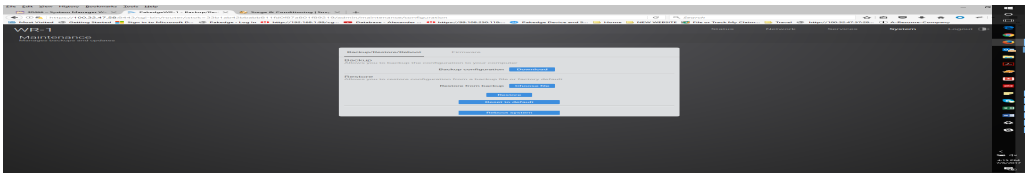
You can download a backup configuration file to your computer, so that later you can restore the same settings.

To make a backup of your configuration:

1. Click **System**, then **Maintenance**.



2. Click **Download**.

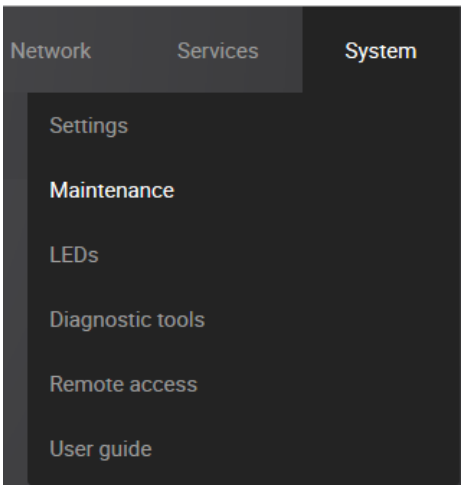


The configuration file will be downloaded to your computer.

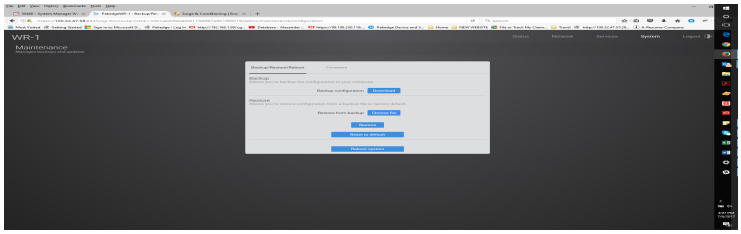
Restore

To restore a configuration from a previous backup:

1. Click **System**, then **Maintenance**.



2. Click **Choose file**.



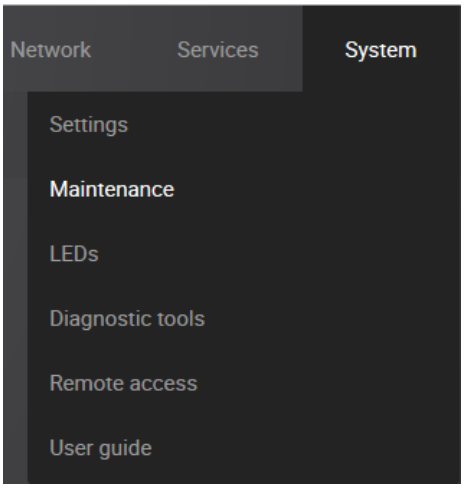
3. After you have selected your backup file, click **Restore**.
4. The wireless router will then upload your configuration file and reboot itself.

Reset to default

You can restore your router to its factory default settings.

To reset the wireless router to factory default settings:

1. Click **System**, then **Maintenance**.



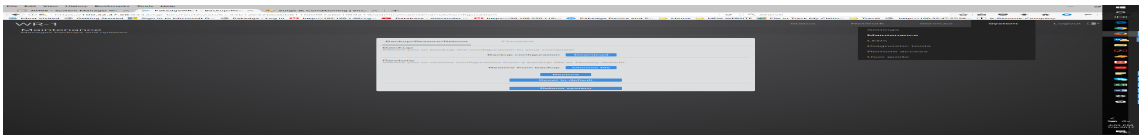
2. Click **Reset to default**. The wireless router returns to factory default settings.

You can also return the router to factory defaults by pressing the pinhole reset button on the back. Simply hold down this button for 10 seconds while the wireless router is powered on, and then release it. The wireless router will then return to factory default settings.

Reboot system

To reboot the router:

1. Click **System**, then **Maintenance**.
2. Click **Reboot system** located at the bottom of the *Backup/ Restore/ Reboot* tab



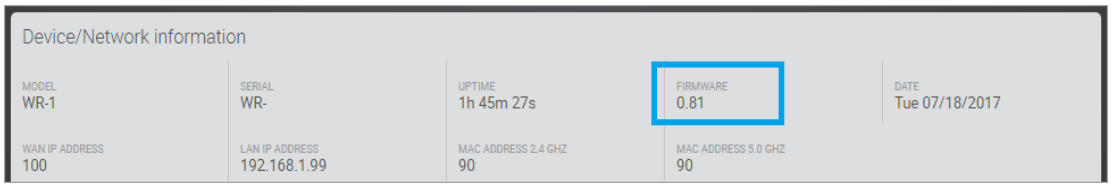
3. The wireless router reboots.

Firmware

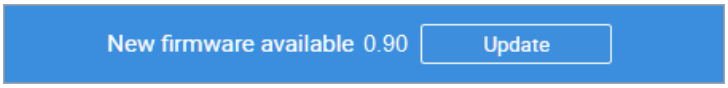
The Firmware page will allow you to update the firmware on your wireless router.

To update the firmware:

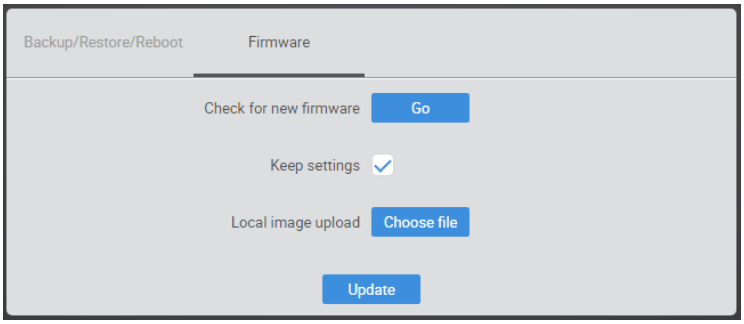
1. The current firmware version of the wireless router is displayed near the top of the dashboard.



2. If there is new firmware available for your wireless router, you will see a message on the dashboard informing you. You can click Update to have the wireless router update its firmware.



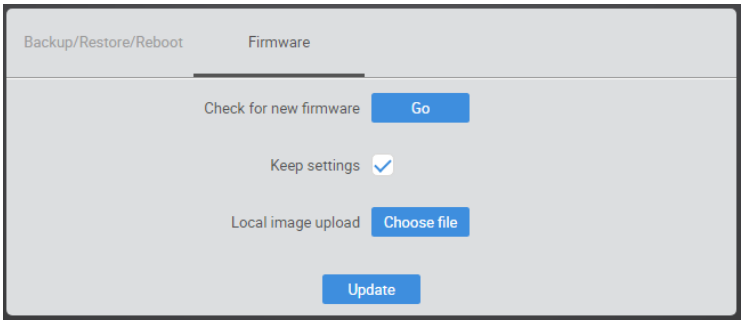
3. You can also click **System, Maintenance,** the **Firmware** tab, then **Update**.



The **Keep settings** option indicates that the wireless router will keep its configuration after the firmware update. If you uncheck this box before clicking **Update**, the wireless router will factory default itself and come back up with the new firmware and the wireless router's default configuration, including the default username and password.

The firmware update will take a few minutes to complete.

4. The **Go** option will force the wireless router to pull the latest firmware available and update itself.

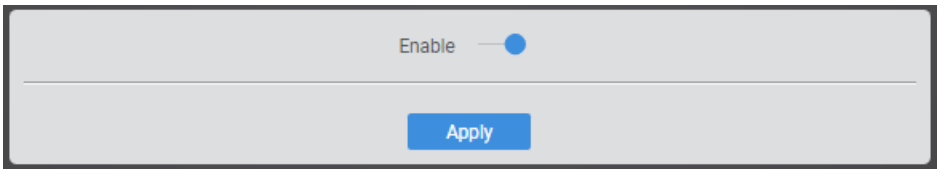


LEDs

For aesthetics, you can turn off the router's LEDs if you like.

To turn off the router LEDs:

1. Click **System**, then LEDs.



2. Click the **Enable** toggle, then click **Apply**.

Diagnostic tools

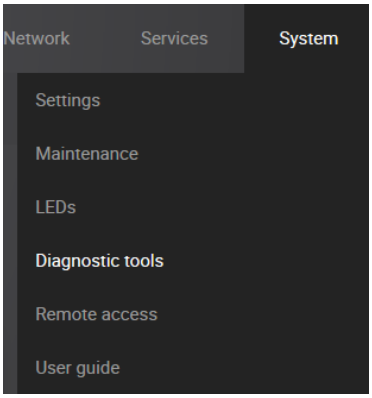
The Diagnostics page allows you to easily troubleshoot your network.

Ping

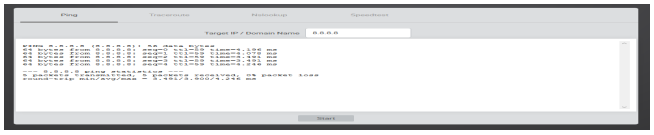
Ping allows you to test communication between two devices on the network.

To ping from the wireless router:

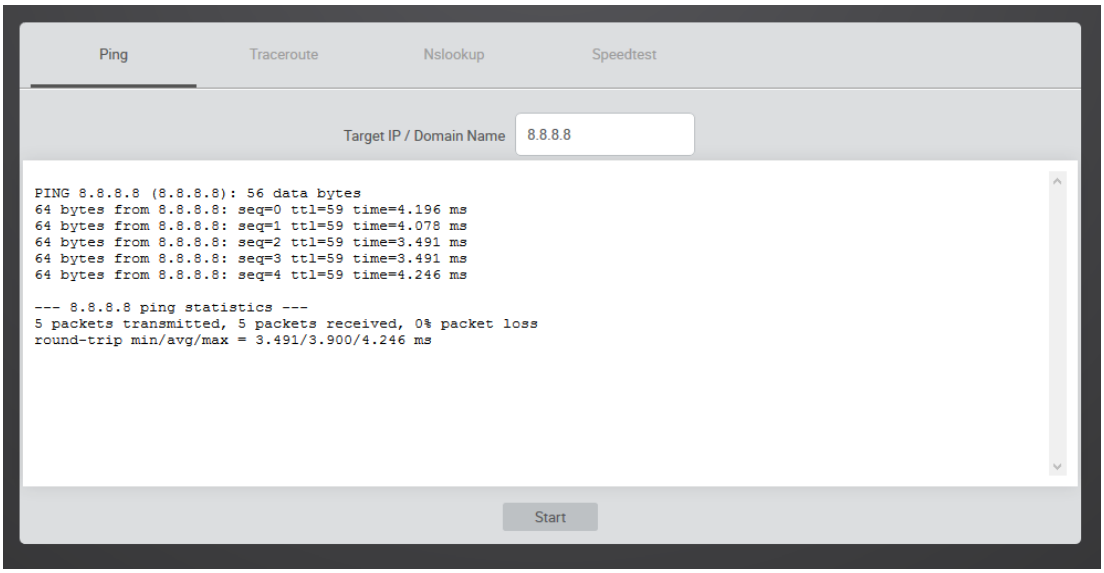
1. From the **System** menu, click **Diagnostic tools**.



2. Click **Start**. If you want to ping a different IP address or hostname, you may type it in instead.



After a few moments, your ping results will be displayed.

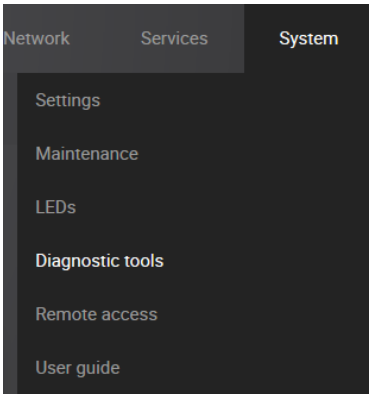


Traceroute

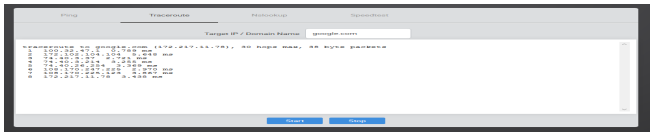
A traceroute allows you to see how many wireless routers, or hops, there are between the wireless router and a certain destination.

To perform a traceroute:

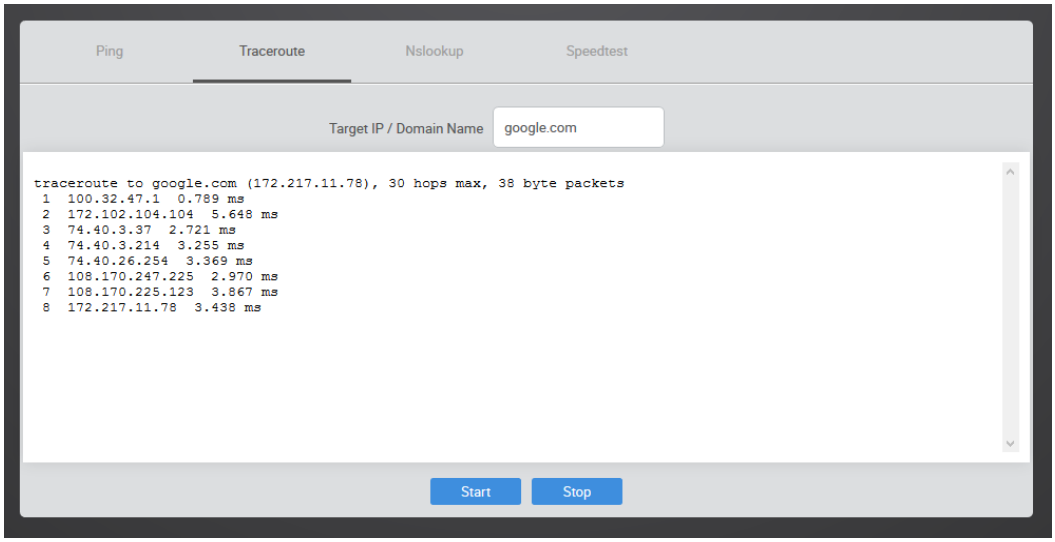
1. From the **System** menu, click **Diagnostic tools**.



2. Click **traceroute**. If you wish to perform a traceroute to a different website or IP address you may enter it instead.



3. After a few moments, your traceroute results will be displayed.

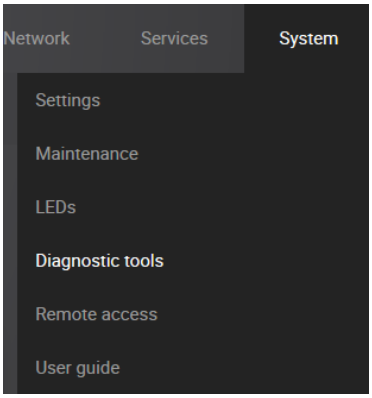


NSlookup

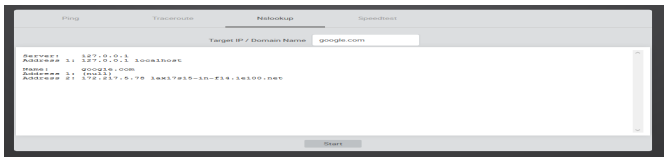
NSlookup allows you to find name server information for domains.

To perform an NSlookup:

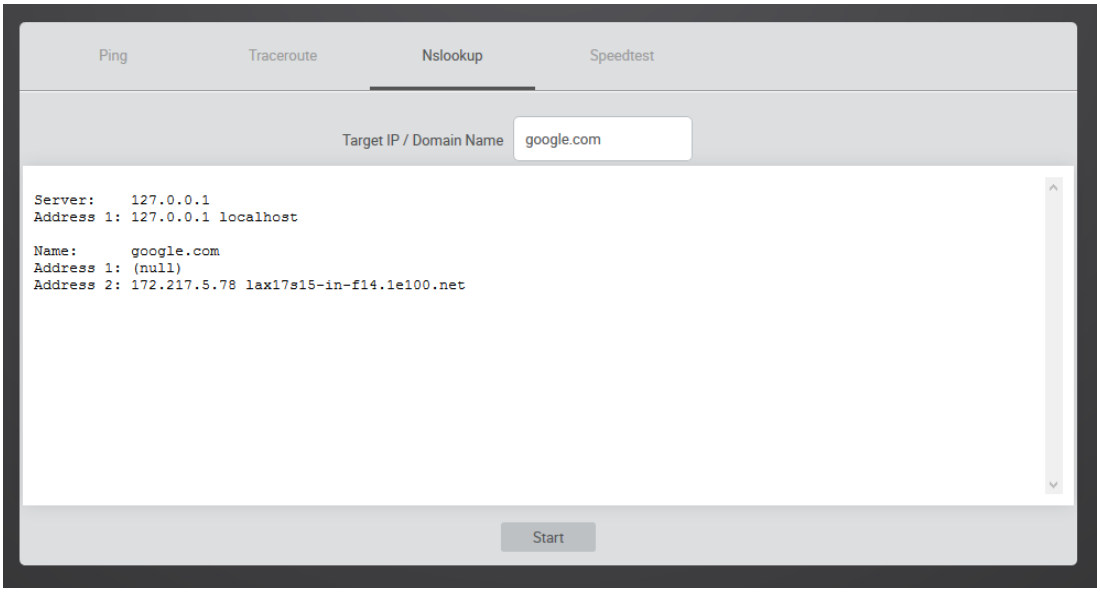
1 Click **Diagnostic tools**.



2. Click **NSlookup**. If you wish to do an NSlookup for a different website you can type it in instead.



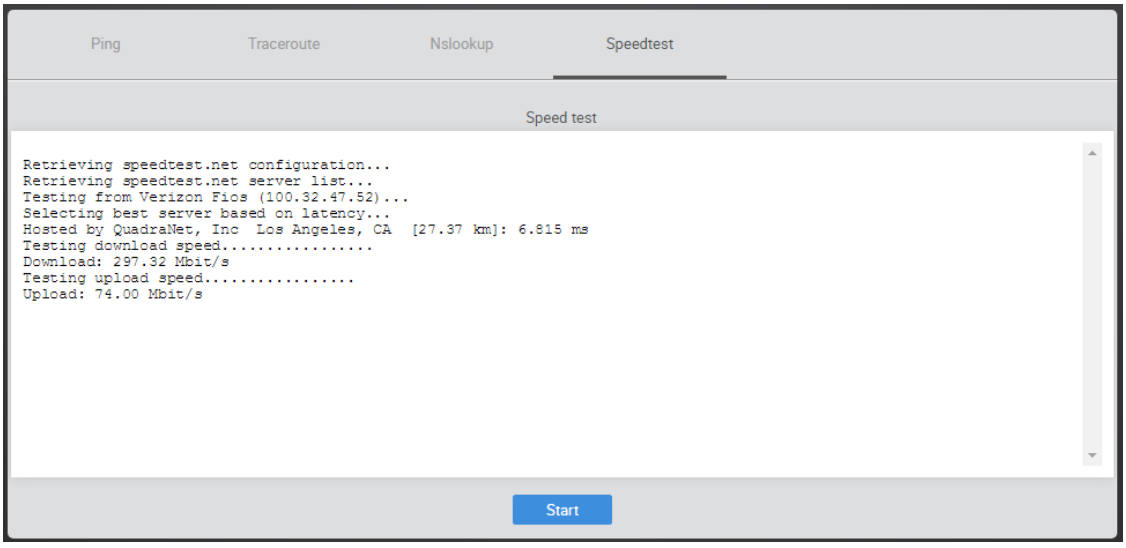
3. After a few moments, your NSlookup results will be displayed.



Speed test

To test the current Internet download and upload speeds of your router:

1. Click **System, Diagnostic tools,** then the **Speed test** tab.
2. Click **Start**. The test is performed, and the results appear on the screen.

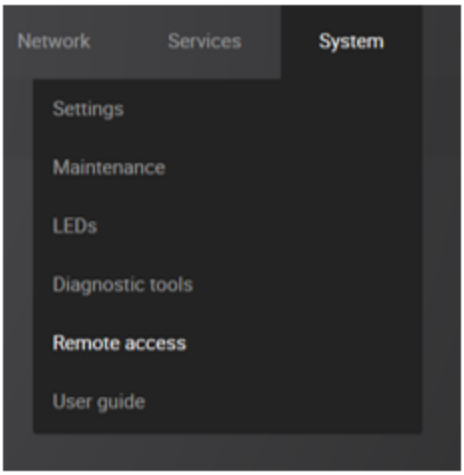


Remote access

The *Remote access* page allows you to change the default port used to access the wireless router remotely.

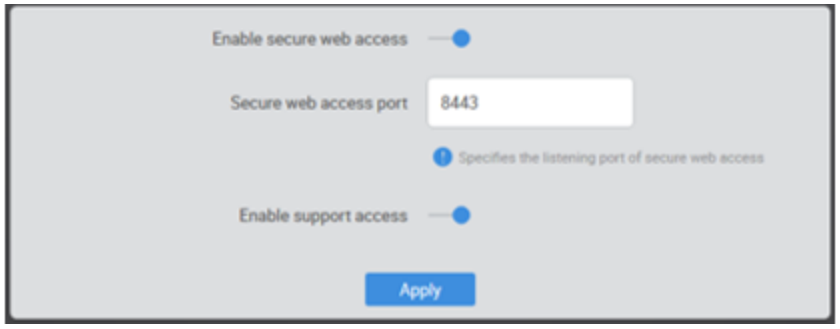
To change the secure web port:

1. Click **Remote access**.



2. You can type a new port number into the **Secure web access port** field if you want to change it from its default. (By default, *Enable secure web access* is disabled). You can also disable remote access altogether if you uncheck the **Enable secure web access** option.

3. By default, **Enable support access** is enabled. This allows the support team at Pakedge to perform advanced diagnostics on your wireless router. It is recommended that you keep this option enabled.



4. If you have made any changes on this page click **Apply** to finalize the settings.

User guide

To see the WR-1User Guide:

1. Click **System**, then **User Guide**. The user guide opens.

-OR-

Use any web browser to go to pkdge.co/wr1-ug.

Appendix A - Limited Warranty

Congratulations on your purchase of a Pakedge Device & Software product! We believe Pakedge designs and manufacture the finest home networking products on the market. With proper installation, setup, and care, you should enjoy many years of unparalleled performance. Please read this consumer protection plan carefully and retain it with your other important documents.

This is a LIMITED WARRANTY as defined by the U.S. Consumer Product Warranty and Federal Trade Commission Improvement Act.

What Is Covered Under the Terms of This Warranty

SERVICE LABOR: Pakedge will pay for service labor by an approved Pakedge service center when needed as a result of a manufacturing defect for a period of three (3) years from the effective date of delivery to the end user.

PARTS: Pakedge will provide new or rebuilt replacement parts for the parts that fail due to defects in materials or workmanship for a period of three (3) years from the effective date of delivery to the end user. Such replacement parts are then subsequently warranted for the remaining portion (if any) of the original warranty period.

What Is Not Covered Under the Terms of This Warranty

This warranty only covers failure due to defects in materials and workmanship that occur during normal use and does not cover normal system. This warranty does not cover any appearance item; any damage to living structure; failure resulting from accident (for example: flood, electrical shorts, insulation); misuse, abuse, neglect, mishandling, misapplication, faulty or improper installation or setup adjustments; improper system, alteration, improper use of any input signal and/or power, damage due to lightning or power line surges, spikes and brownouts; damage that occurs during shipping or transit; or damage that is attributed to acts of God.

The foregoing limited warranty is Pakedge's sole warranty and is applicable only to products sold as new by Authorized Dealers. The remedies provided herein are in lieu of a) any and all other remedies and warranties, whether expressed, implied or statutory, including but not limited to) any implied warranty of merchantability, fitness for a particular purpose or non-infringement, and b) any and all obligations and liabilities of Pakedge for damages including but not limited to: incidental, consequential or special damages, or any financial loss, lost profits or expense, or loss of network connection arising out of or in connection with the purchase, use or performance of the product, even if Pakedge has been advised of the possibility of such damages.

> CAUTION: DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM IMPROPER INSTALLATION OR SETUP IS SPECIFICALLY EXCLUDED FROM COVERAGE UNDER THIS WARRRANTY. IT IS IMPERATIVE THAT INSTALLATION AND SETUP WORK BE PERFORMED ONLY BY AN AUTHORIZED PAKEDGE DEALER TO PROTECT YOUR RIGHTS UNDER THIS WARRANTY. THIS WILL ALSO ENSURE THAT YOU ENJOY THE FINE PERFORMANCE YOUR PAKEDGE PRODUCT IS CAPABLE OF PROVIDING.

Rights, Limits, and Exclusions

Pakedge limits its obligation under any implied warranties under state laws to a period not to exceed the warranty period. There are no express warranties. Pakedge also excludes any obligation on its part for incidental or consequential damages related to the failure of this product to function properly. Some states do not allow limitations on how long an implied warranty lasts, and some states do not allow the exclusion or limitation of incidental or consequential damages. In this case, the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

Effective Warranty Date

This warranty begins on the effective date of delivery to the end user. For your convenience, keep the original bill of sale as evidence of the purchase date from your authorized dealer.

Important: Warranty Registration

Please register your product at www.pakedge.com. It is imperative that Pakedge knows how to reach you promptly if we should discover a safety problem or product update for which you must be notified. In addition, you may be eligible for discounts on future upgrades as new networking standards come about.

To Obtain Service, Contact Your Pakedge Dealer.

Repairs made under the terms of the Limited Warranty covering your Pakedge product will be performed by an Authorized Pakedge Service Center. These arrangements must be made through the selling Pakedge Dealer. If this is not possible, contact Pakedge directly for further instructions. Prior to returning a defective product directly to Pakedge, you must obtain a Return Material Authorization number and shipping instructions. Return shipping costs will be the responsibility of the owner.

For additional information about this warranty, visit our website at www.pakedge.com.

Email: support@pakedge.com

Phone: (650) 385-8703

11734 S Election Road
Draper, UT 84020

www.pakedge.com

200-00590-D