Technical Guide

Getting Started with the TQR Series Access Points and Wireless Routers using the Device GUI

Introduction

The TQR Series Access Points and Wireless Routers provide high-speed Wi-Fi connectivity for wireless devices.

Some models also provide a secure Internet connection from the built-in VPN router. This single-unit design enables a simplified yet comprehensive network solution for a small business, or for enterprises with multiple locations, such as retail stores, cafes, and more.

Secure WAN routing ensures reliable connectivity to the Internet, head-office, and other branch locations. Critical data is protected with a zone-based firewall, remote access to cloud-based or head-office based business applications using secure IPsec VPNs.

What information will you find in this document?

The Device GUI provides graphical management and monitoring for devices running the AlliedWare Plus™ operating system.

This guide shows you how to configure a TQR Series device using the Device GUI.

The GUI makes it easy to configure your wireless LAN on TQR Series devices.

For models with an inbuilt VPN router, the Device GUI provides setup of the firewall, enabling the configuration of entities (zones, networks, and hosts) and then creating firewall, NAT, and traffic-control rules for managing traffic between these entities. Features such as the Intrusion Prevention System (IPS) and URL Filtering help protect the network, and manage website access.

The GUI also supports a number of other features such as interface, VLANs, file, log, and wireless network management, as well as a CLI window and a Dashboard for network monitoring. The Dashboard shows interface and firewall traffic, system and environmental

information, and the security monitoring widget lets you view and manage rules and security features.

You can configure the complete AlliedWare Plus feature-set using the GUI's built-in industry standard Command Line Interface (CLI) window.

Contents

Products and software version that apply to this guide

This guide applies to the Allied Telesis TQR Series Access Points and Wireless AP Routers.

Feature support may change in later software versions. For the latest information, see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Related documents

The following document gives you more detailed information about Wireless Management features using TQR Series devices on AlliedWare Plus products:

- The Wireless Management for the TQR Series using the Device GUI

Connecting to the wireless router

This section describes how to connect to your router using the Device GUI. Your router will have a GUI already loaded.

Supported web browsers for connecting to the Device GUI are:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge™
- Apple Safari™

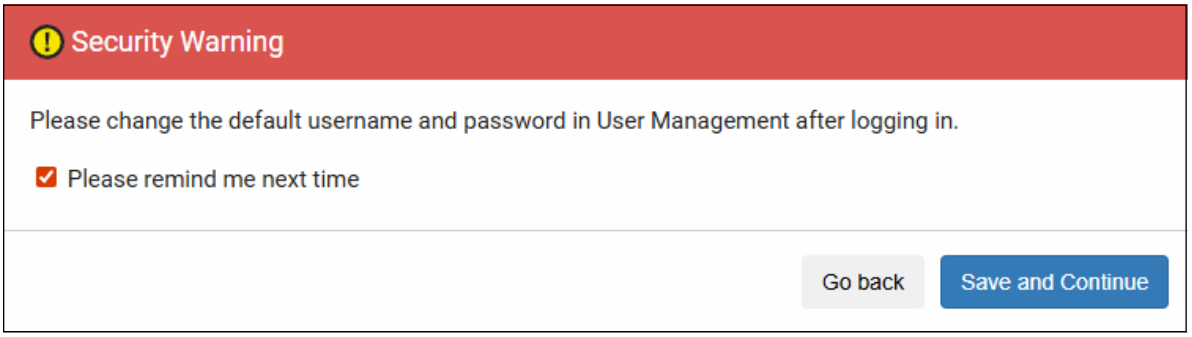
Connecting to the GUI

To connect to the GUI, use the following steps:

Note: You will need to manually assign your device an IP address in the 192.168.1.0/24 network.

1. Connect to LAN1 (in the firmware this port is called eth1).
2. Open a web browser and browse to the default IP address for Eth1.
   - The default IP address is 192.168.1.1
3. Log in with the default username of ***manager*** and the default password of ***friend***.

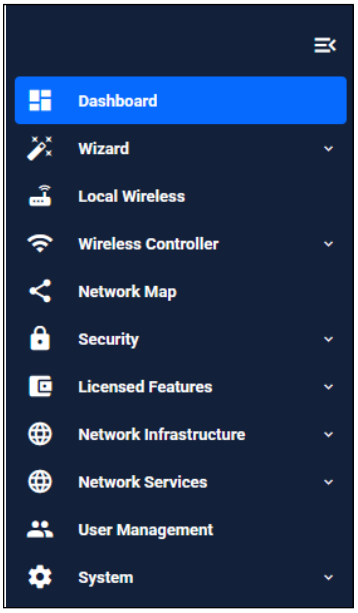
From AlliedWare Plus version 5.5.5-1.1 and Device GUI version 2.21 onwards, when you first login using the default username and password, you will be prompted to change your password:



You can click on the check-box if you want to be reminded next time you login, select Go back, or click Save and Continue to login.

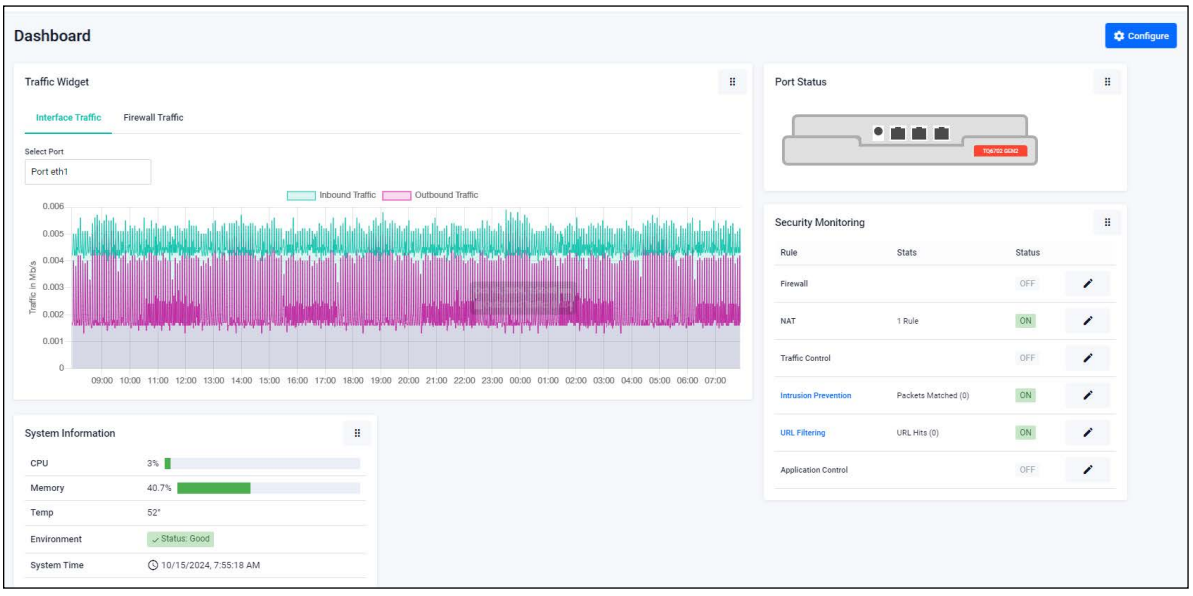
The Menu bar

From here you can access the **Dashboard, Wizard**, **Wireless**, **Security**, **Licensed Features**, **Network Infrastructure**, **Network Services**, **User Management** and **System** menus. More detail is covered later in this document when configuring your router and setting up your network using these menus.



The Dashboard

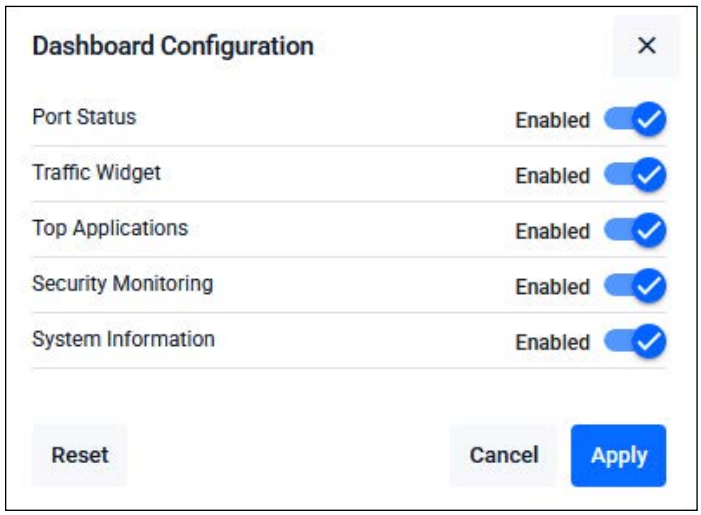
This section describes how to use the dashboard in the device's GUI. This is the first screen that you see after you log in.



The Dashboard has a number of useful widgets for monitoring the state of your router. On the left-hand side of the Dashboard page is the main navigation menu bar.

The **Port Status**, **Traffic Widget**, **System Information** and **Security Monitoring** widgets are switched on by default so that you can monitor router activity from the dashboard.

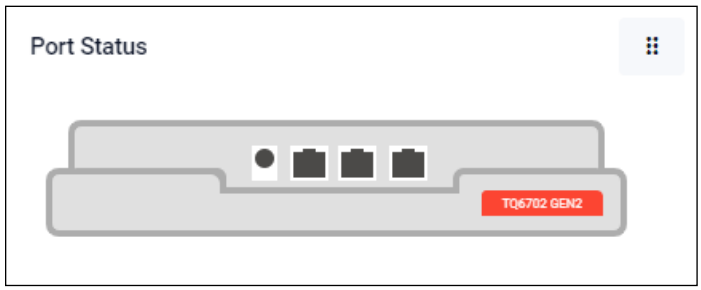
To enable or disable these dashboard features click on the **Configure** button from the Dashboard:



Choose what you want to monitor and turn them on or off, click **Apply**.

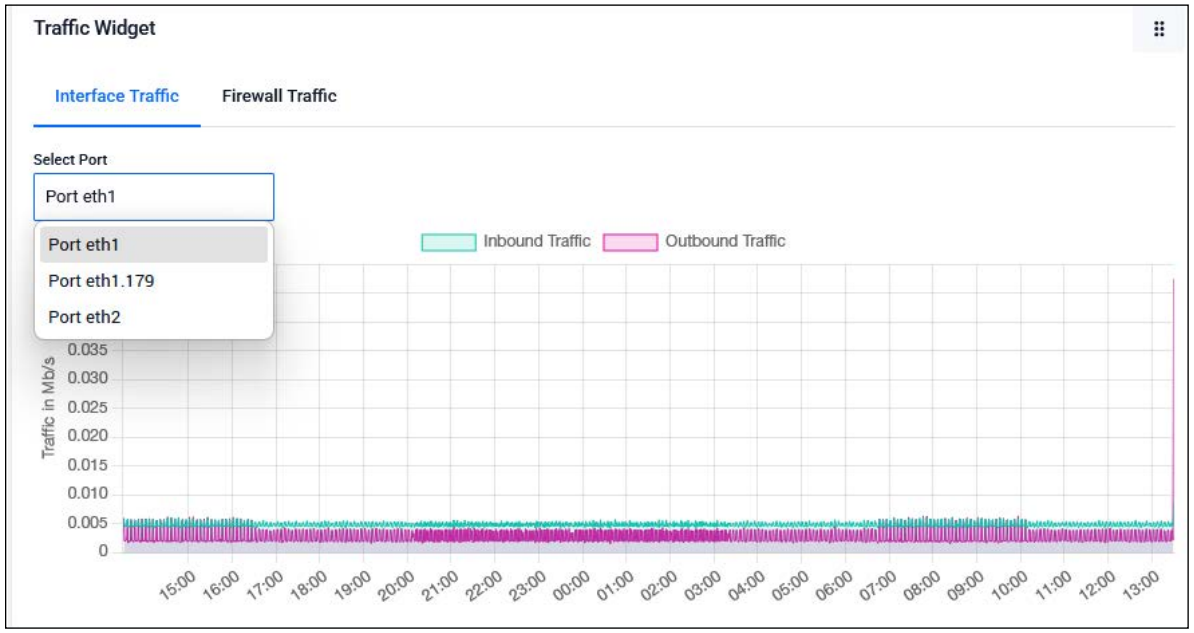
Port Status

The **Port Status** widget shows port information. Click on the port to display the port number, speed, packet TX and RX, utilization, and interface.



Traffic Widget

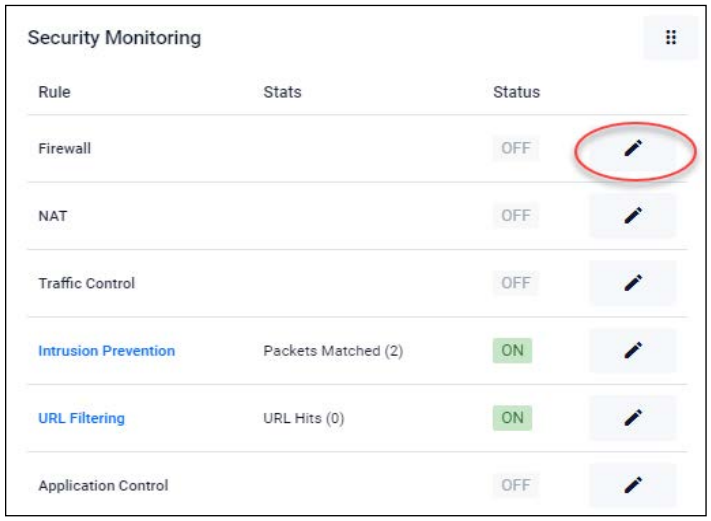
From the **Traffic Widget** you can select an interface from the drop-down list to display inbound and outbound traffic information.



On models that support the firewall, click on the **Firewall Traffic** tab to display inbound and outbound traffic information for the firewall.

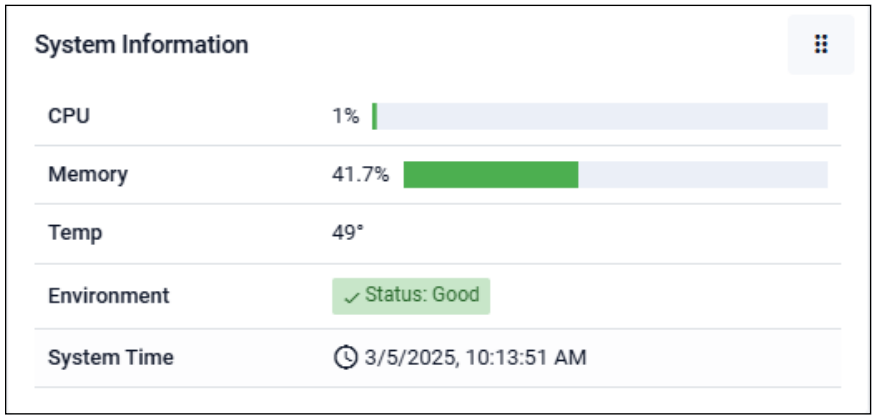
Security Monitoring

On models that support the firewall, you can create or edit rules from **Security Monitoring**, such as Firewall or NAT rules directly from the dashboard. For example, click on the **Edit** button to create or edit a firewall rule:



System Information

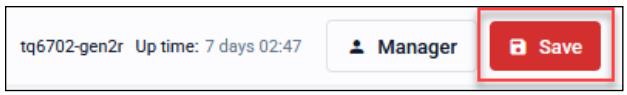
The **System Information** widget shows CPU and memory use, as well as device health and system time.



Save your config

If you have changed your dashboard settings, click the **Save** button at the top right of the GUI screen.

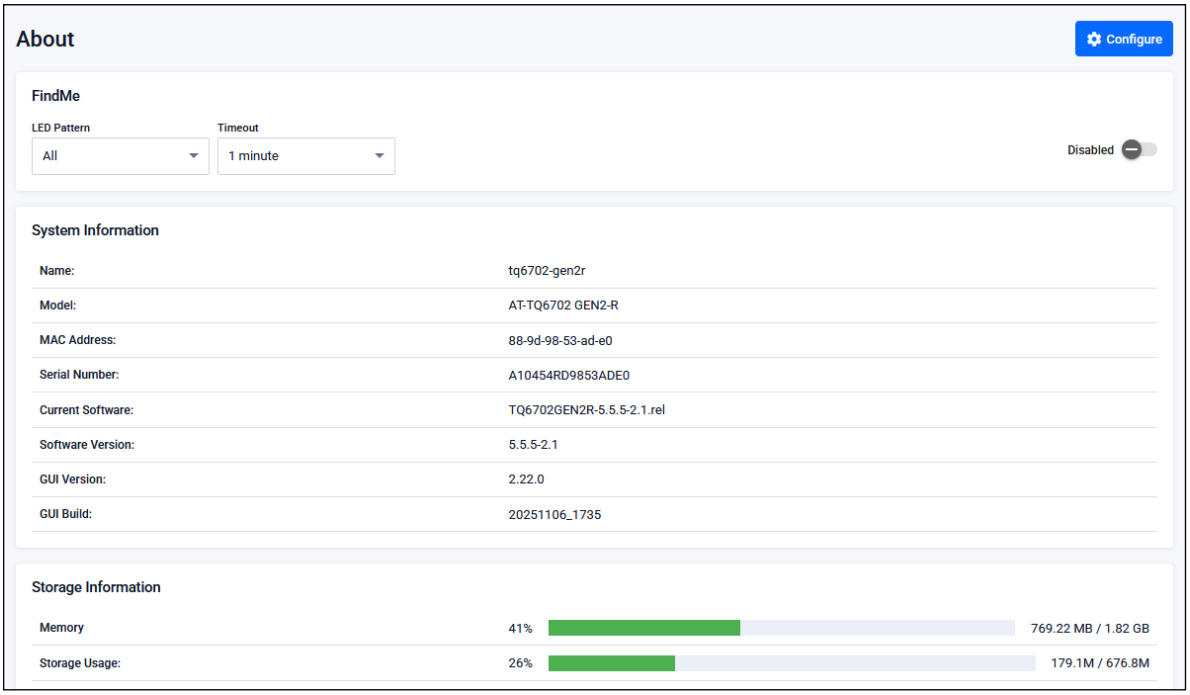
Tip: The **Save** button is red anytime there is unsaved configuration and blue when it is saved.



If you are in another menu and want to return back to the dashboard, click **Dashboard** from the menu bar.

Product and system information

From the menu bar select **System > About** to show more detail about your router, such as the FindMe settings, the host name, model, MAC address, serial number, current software, software version, and also the GUI build and version. It also displays Storage Information about how much space is left in memory and your storage usage.

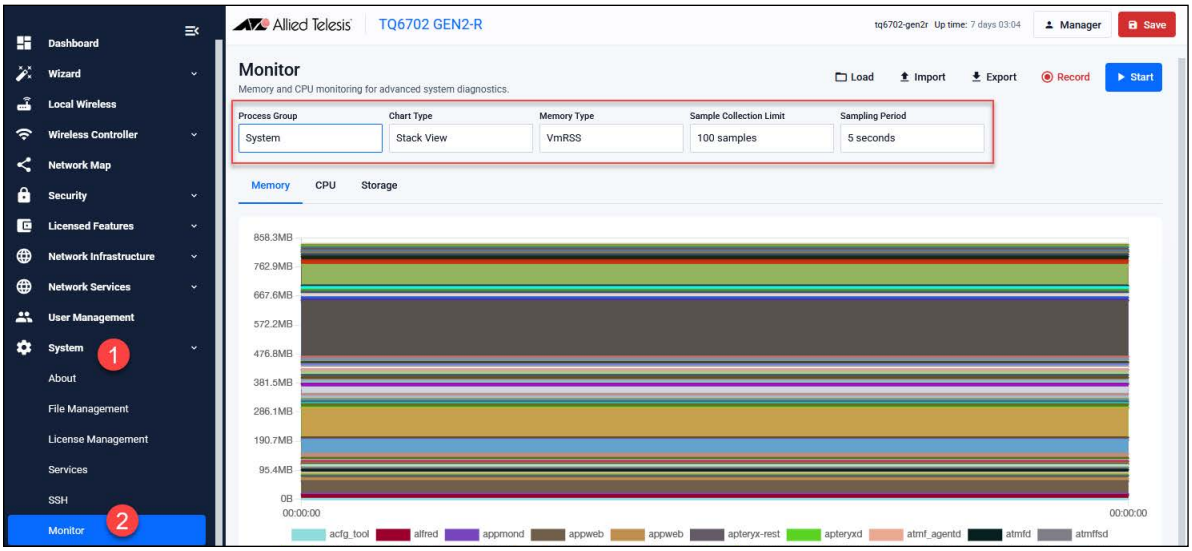


The host name and model are also displayed in the top menu bar:

Process Monitor

From version 2.20.0 onwards, the Device GUI supports a Process Monitor to visualize usage statistics like CPU, memory, and storage I/O. This can help identify processes that are consuming more (or less) resources than expected.

To use the Process Monitor, go to **System** > **Monitor** in the left-hand menu:



You can select Process Group options, Chart Type options, Memory Types, Sample Collection Limits and Sampling Period options.

Finding a device

From version 5.5.5-1.1 onwards, you can use the Find Me feature to locate a device. When you enable Find Me, all ports on your device will flash based on the pattern that you select.

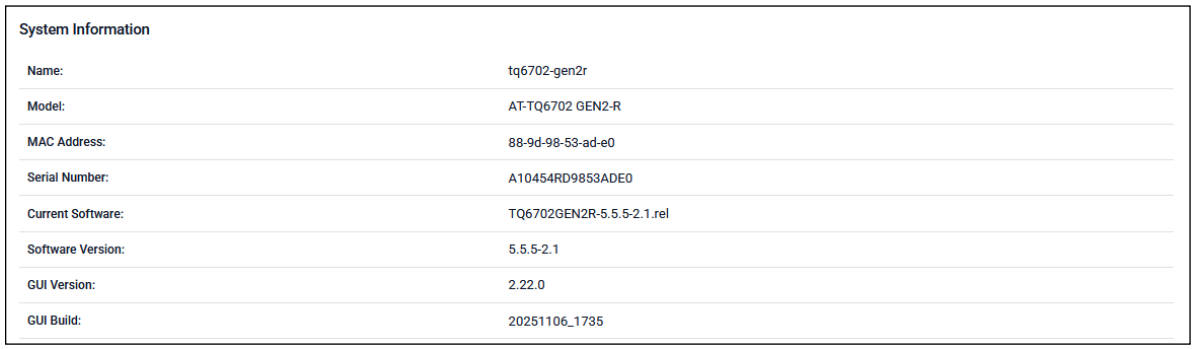
To use the Find Me feature, go to **System > About** in the left-hand menu. On the About page, click the toggle next to the Find Me table to enable Find Me.

You can set the LED pattern and timeout to find what device you are currently using.

Managing firmware and configuration

Check the firmware version

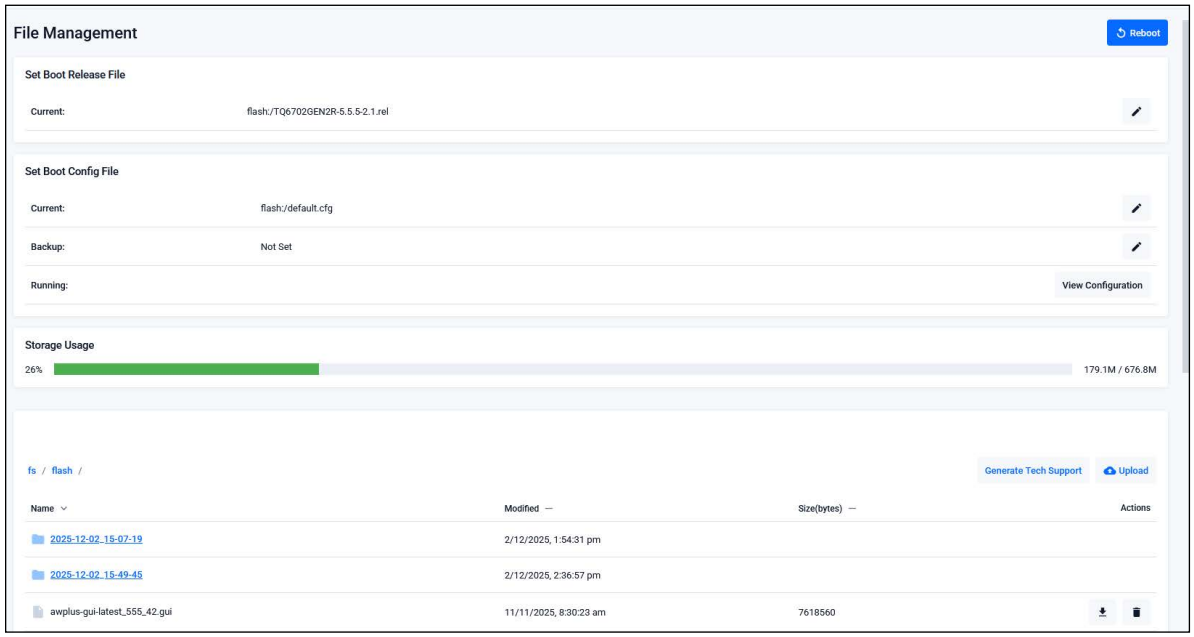
From the menu bar select **System > About** to show the current firmware and versions for both the firmware and GUI:



You can also use the **System > File Management** page to view all files stored on your device, including firmware and GUI files. On the **File Management** page, upload and download functions provide an easy way to add new files such as firmware, configurations, scripts, or URL lists to the device, as well as saving configurations for backup.

You can use this page to check and set the software release and configuration files, and reboot the device for an easy firmware upgrade.

From the menu bar select **System > File Management**:



Upgrade the firmware

If your wireless router is not running the latest firmware, use the following steps to upgrade it.

Step 1: **Download the new firmware file.**

Download it from the Allied Telesis Support Portal and save it on the device that you browse to the wireless router from.

Step 2: **Use the Upload button to add the new firmware file.**

Browse to where you saved the downloaded firmware file and click **Open**. You will see the uploaded file appear in the File Management page.

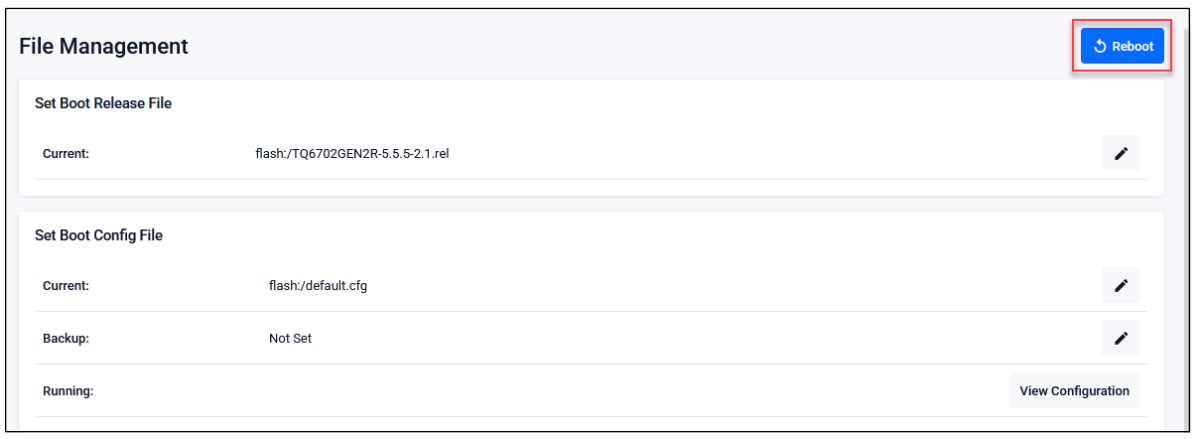
Step 3: **Set the new firmware file to be the boot release.**

Click on the **Edit** button and then select the correct release file you want to use on reboot and click **Apply**.

Step 4: **Backup Boot Config file.**

You cannot set a Backup Boot Config File because the TQR Series do not have an SD card slot or USB port. Currently this is not supported.

Step 5: **Reboot the device.**



Click the **Reboot** button to perform a system reboot so the new release is applied.

Back up the default configuration

Download a copy of the default configuration file so that you can revert back to the original if your configuration changes fail.

Save the configuration

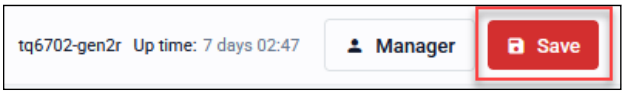
When you configure the wireless router through its GUI, the configuration becomes part of its running-configuration.

Once you are sure your configuration changes work, you need to make them part of the boot configuration, so they can be backed up and will survive a reboot of the wireless router.

Caution: Back up the default configuration before you save the configuration.

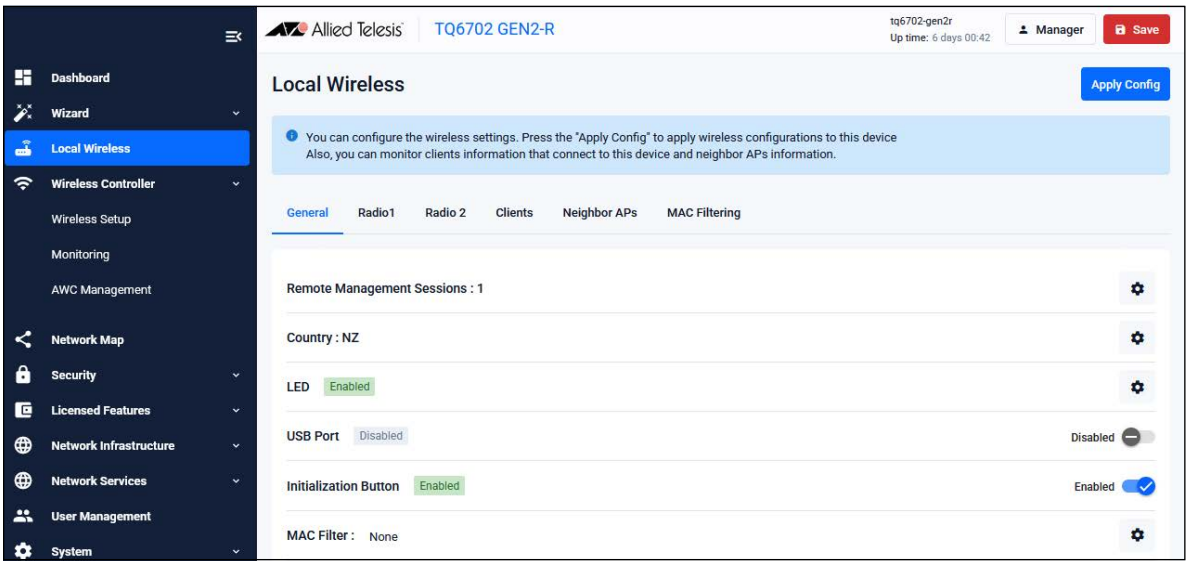
- Click the **Save** button at the top right of the GUI screen.

Tip: The **Save** button is red anytime there is unsaved configuration and blue when it is saved.



Configuring a Wi-Fi network

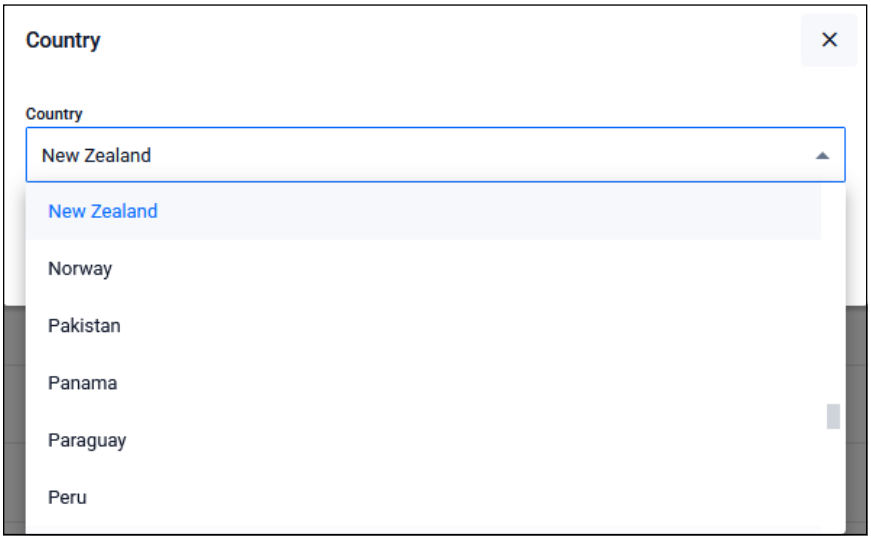
The device GUI includes a Wireless Controller menu, which enables you to set up and monitor your wireless network:



The **Local Wireless** menu displays your wireless settings for General, Radio1, Radio2, or Radio3 (for the TQ7403-R) Clients, Neighbor APs and MAC Filtering. When you click on Local Wireless, the General tab is displayed by default. The following steps show how to set up your Wi-Fi network.

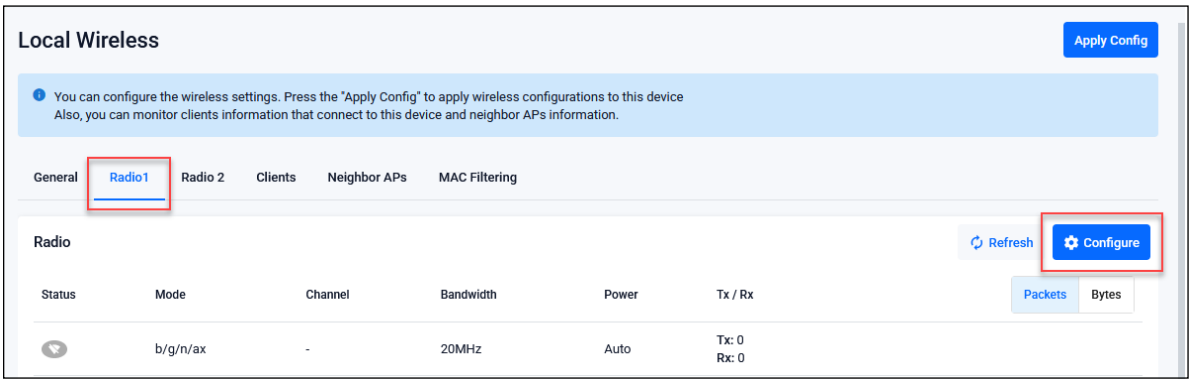
Step 1: **Select your country.**

From the **General** tab, select your country from the drop-down list and click **Apply**.

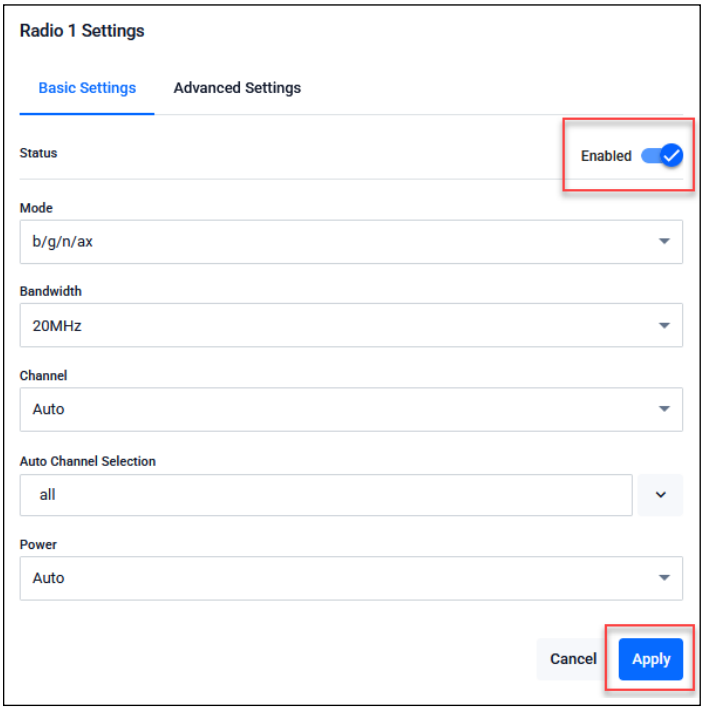


Step 2: **Enable the radio.**

From the **Radio1** tab click the **Configure** button from the Radio settings:



From the **Radio1 Settings** dialog click the **Enabled** button:



Click **Apply**.

Note: The radio channel defaults to automatic. Optionally, you can change the specific channel and reduce the transmit power to limit the range.

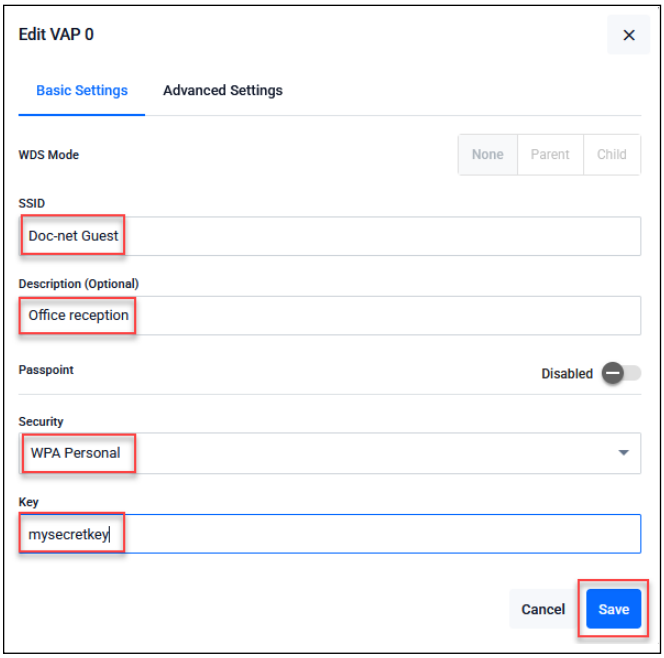
Step 3: **Set up the VAP 0 interface.**

Click on the **Edit** button from the VAP settings:

From the **Edit VAP 0** dialog **Basic Settings** tab enter the following:

- The SSID name.

- Enter a Description (optional).
- From the security drop-down list, select **WPA personal**.
- Set the key to a strong password.

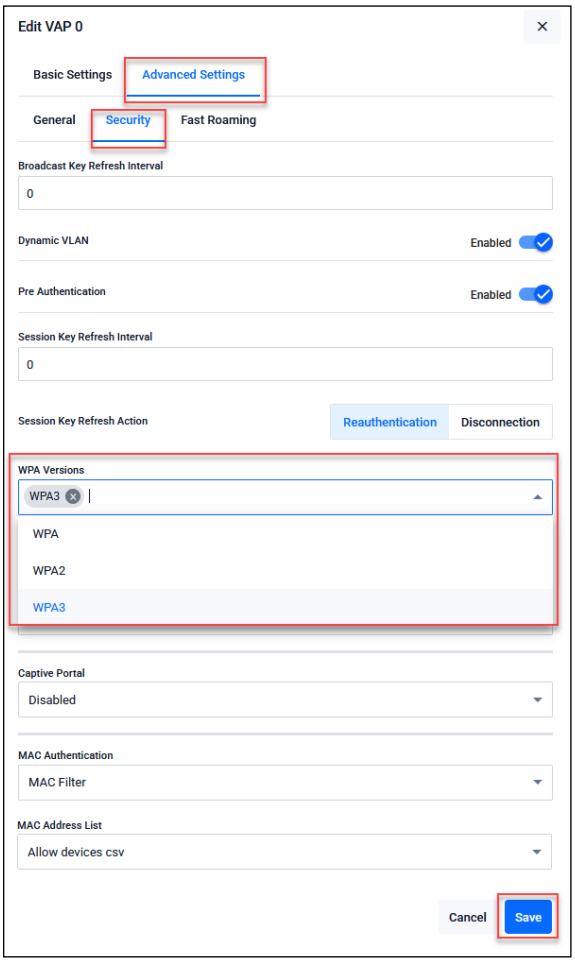


Click **Save**.

Step 4: **Choose a different WPA version.**

If required, you can work with different versions of WPA such as WPA2 or WPA3. To select a different WPA version from the **Edit VAP 0** dialog, click on the **Advanced Settings** tab.

Advanced settings defaults to the General tab, click on the **Security** tab:



From this dialog click on the down arrow to display the WPA versions available to select. Select the WPA version/s you want to work with.

Select the **Encryption Protocol** from the drop down list.

From version 5.4.4-2.3 onwards, GCMP is an available option from the drop down list:

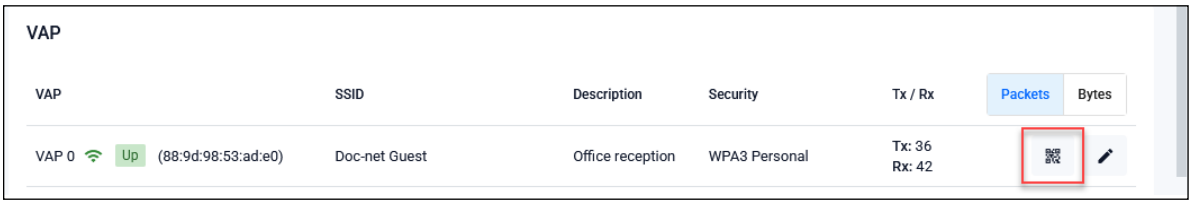
- If the WPA version is 'WPA2 and WPA3' or 'WPA3', the options are 'CCMP or GCMP'.
- If the WPA version is 'WPA2' or lower, 'CCMP' is the default option.
- If 'CCMP and GCMP' are available, these options are shown in the drop down List.

Click **Save**.

Step 5: **Create a QR code for clients to use.**

From the **Wireless** page you can create a QR code that you can use to connect a device to join the wireless network.

To display the QR code, click the **display QR** code button:



From this window you can scan the QR code to your device or download it. Your device automatically connects to the VAP 0 interface.

Step 6: **Save the configuration.**

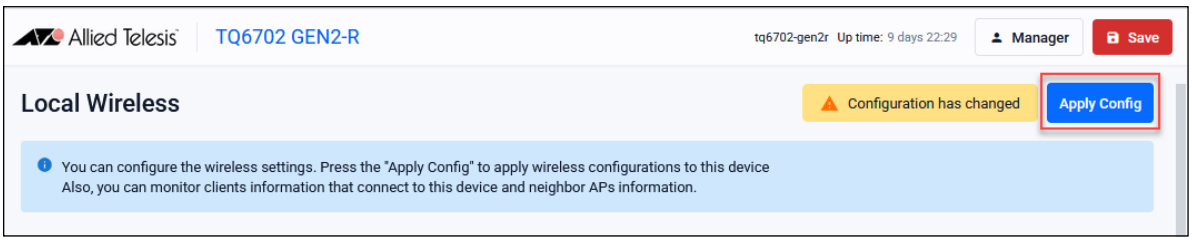
When you configure the wireless router through its GUI, the configuration becomes part of its running-configuration. Once you are sure your configuration changes work, you need to make them part of the boot configuration, so they can be backed up and will survive a reboot of the wireless router.

Caution: Back up the default configuration before you save and apply your configuration.

Once you are happy with the functionality of your configuration, you can then save it.

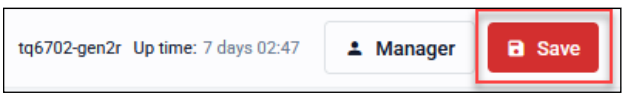
1. Click the **Apply Config** button to apply the settings to your device.

   This step saves the wireless configuration to your device. Notice that the button is orange colored when the configuration requires saving:



2. Click the **Save** button at the top right of the GUI screen (you may need to scroll up to see it).

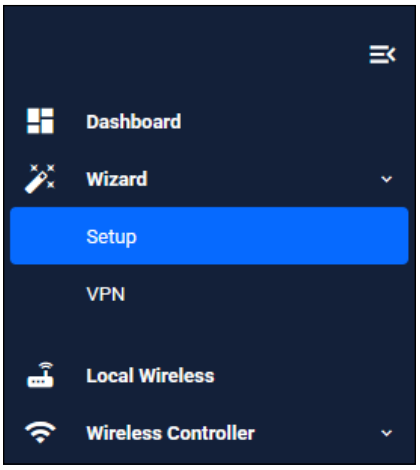
Tip: The **Save** button is red anytime there is unsaved configuration and blue when it is saved.



Using the Wizard to configure Internet and VPN connections

This section only applies to models that support Internet and VPN connections.

Using a wizard makes it easy to set up Internet and VPN connections.



Set up an Internet connection

You can use the wizard to set up a router's WAN interface along with creating a basic configuration for a LAN. There are three IPv4 methods available: DHCP, Fixed IP, and PPPoE, and one IPv6 method available IPoE.

Once the wizard has run, the Setup Wizard summary page displays the current configuration. You can change other things in the GUI after having run the setup wizard, however if you choose to go back and run the wizard again, all your previous configuration will be removed.

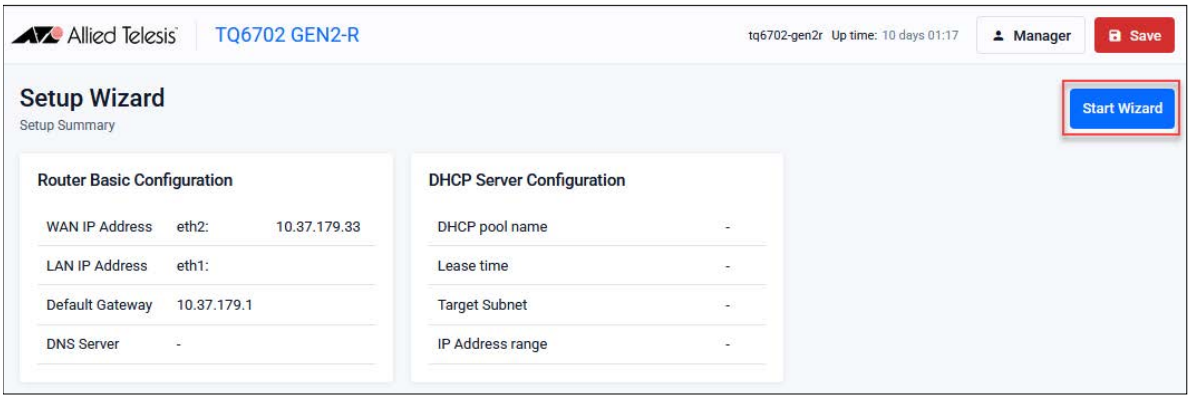
The configuration steps are:

1. Start the Wizard

- Click **Wizard > Setup** from the menu bar.

If you don't have an Internet connection configured, you'll see a blank **Setup Wizard** summary page. If you do have an Internet connection configured, then you'll see those details displayed in the **Setup Wizard** summary page. Click the **Start Wizard** button to reconfigure your current Internet connection settings, or in this example configure new connections:

2. Click the **Start Wizard** button.



3. Choose a connection method.

- Select a method to connect to the Internet.

4. Configure the connection method.

This section describes the configuration settings for each connection method.

Note: If you turn on the DHCP server, it will assign clients addresses that are in the same subnet as the LAN interface's default address. This will not work if you have changed the LAN interface's address. In that case, select OFF for DHCP Server and manually configure the DHCP server from the Network Services menu after the Wizard is complete.

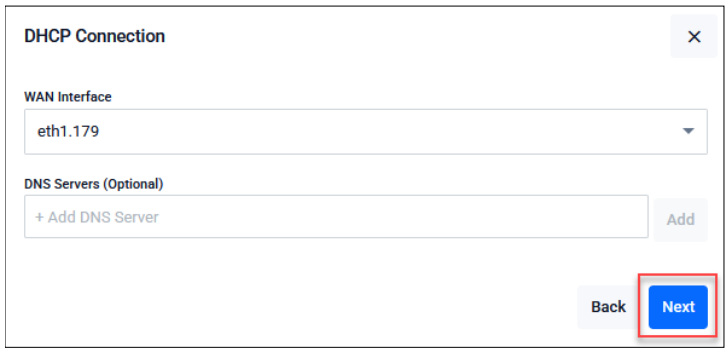
IPv4 - DHCP Connection

To configure the IPv4 DHCP connection, follow these steps:

1. Select **DHCP** from the **Select setup method** drop-down list.

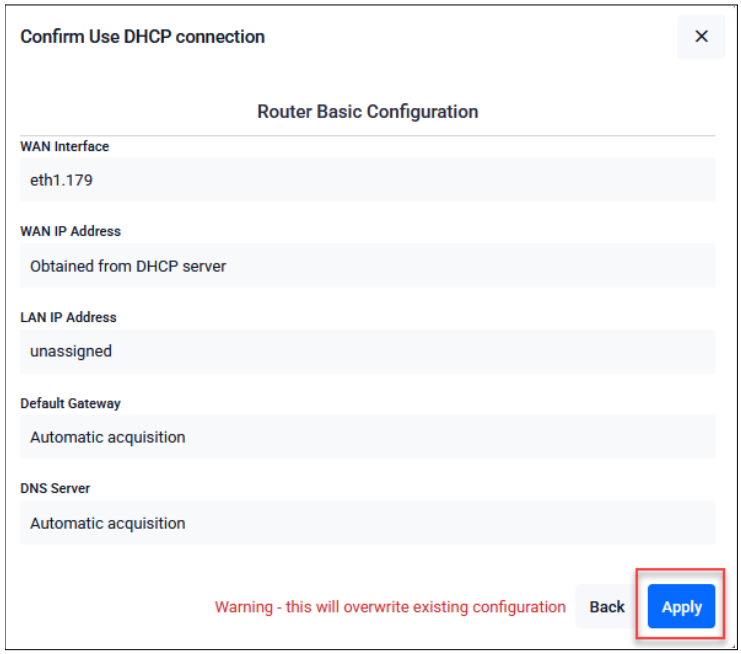
- Enter or select the **WAN Interface**.
- Leave DNS Servers at the default (so that it automatically obtains a DNS server address).

2. Click on the **Next** button to check your settings:



Field	Description
WAN interface	Enter the interface used to connect to the Internet, in this example eth2.
DNS Servers	Specifies the DNS server to use for name resolution. ■ If you want DHCP to automatically obtain a DNS server address, leave it at the default. ■ If fixed settings are required, enter or select the IP address of the DNS server. Click the **Add** button.

3. Click the **Apply** button to confirm your settings.



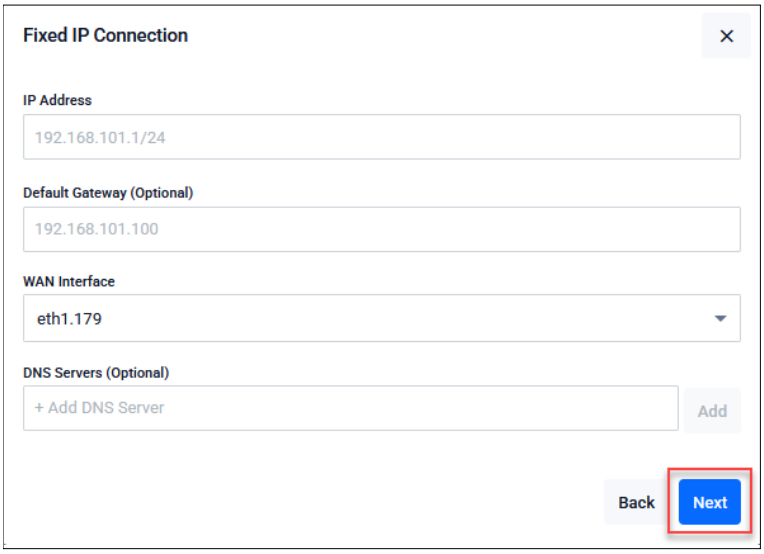
IPv4 - Fixed IP Connection

To configure the IPv4 fixed IP connection, follow these steps:

1. Select **Fixed** from the **Select setup method** drop-down list.

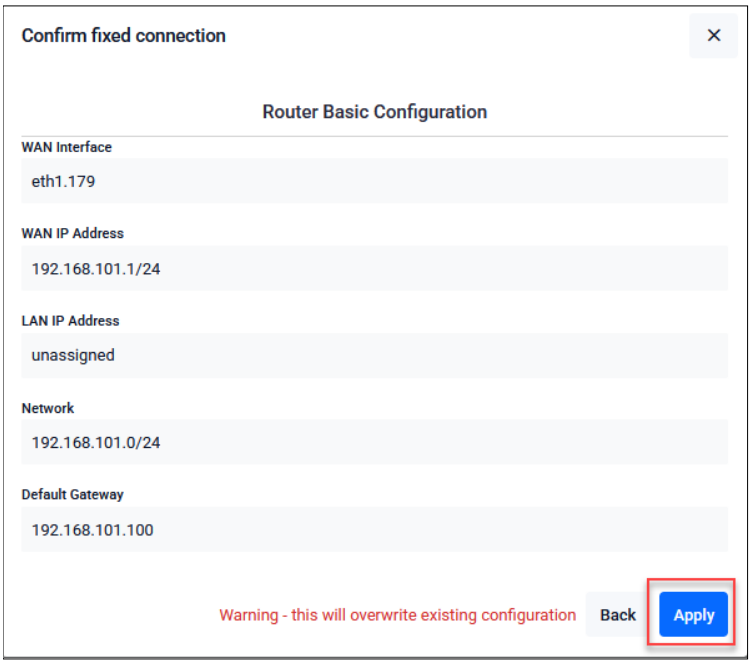
- Enter or select the **IP Address**.
- Enter or select the **Default Gateway** if required.

2. Click on the **Next** button to check your settings:



Field	Description
IP Address	Enter the IP address you want to configure for the WAN-side interface.
Default Gateway (optional)	Enter the IP address of the default gateway that you want to use to connect to the Internet (optional).
WAN interface	Select the interface used to connect to the Internet, in this example eth2.
DNS Servers (optional)	Specifies the DNS server to use for name resolution. Enter or select the IP address of the DNS server. Click the **Add** button.

3. Click the **Apply** button to confirm your settings.



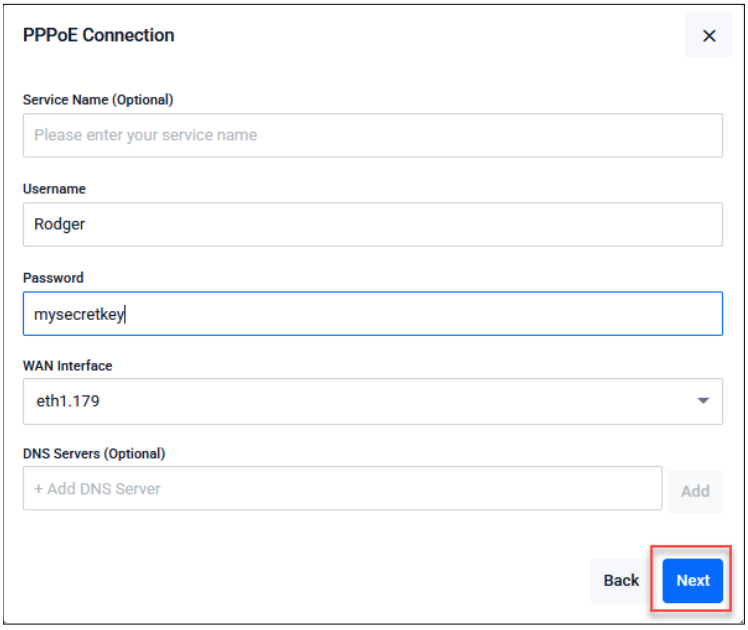
IPv4 - PPPoE Connection

To configure the IPv4 PPPoE connection follow these steps:

1. Select **PPPoE** from the **Select setup method** drop-down list.

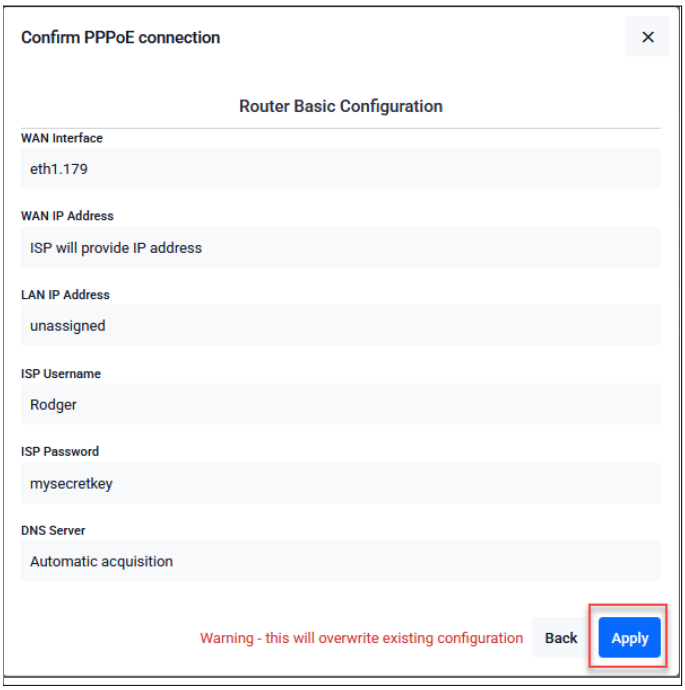
- Enter the **Username**.
- Enter the **Password**.

2. Click on the **Next** button to check your settings:



Field	Description
Service Name (optional)	This is the PPPoE service name. You can usually leave it blank. Enter the PPPoE service name only if your Internet service provider (ISP) has specified it.
Username	PPP user name. Enter the user name for the Internet connection notified by your ISP.
Password	PPP password. Enter the password for the Internet connection provided by your ISP.
WAN interface	This is the interface used to connect to the Internet, in this example eth2.
DNS Servers (optional)	Specifies the DNS server to use for name resolution. ■ If you want IPCP to automatically obtain the DNS server address when connecting to PPPoE, you can leave it as the default. ■ If fixed settings are required, enter or select the IP address of the DNS server and click the **Add** button.

3. Click the **Apply** button to confirm your settings.

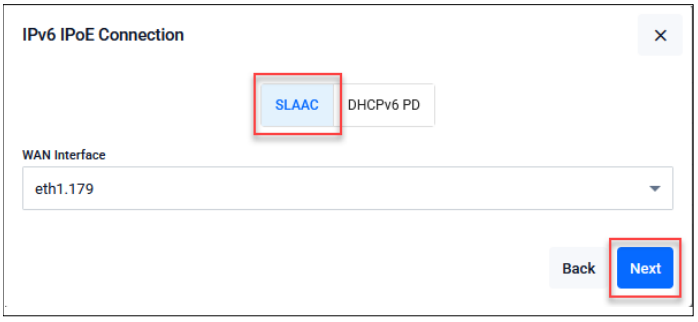


IPv6 - IPoE Connection

Configure the IPv6 IPoE connection. There are two tabs in this window, SLAAC (Stateless Address Auto-Configuration) and DHCPv6 PD (Prefix Delegation).

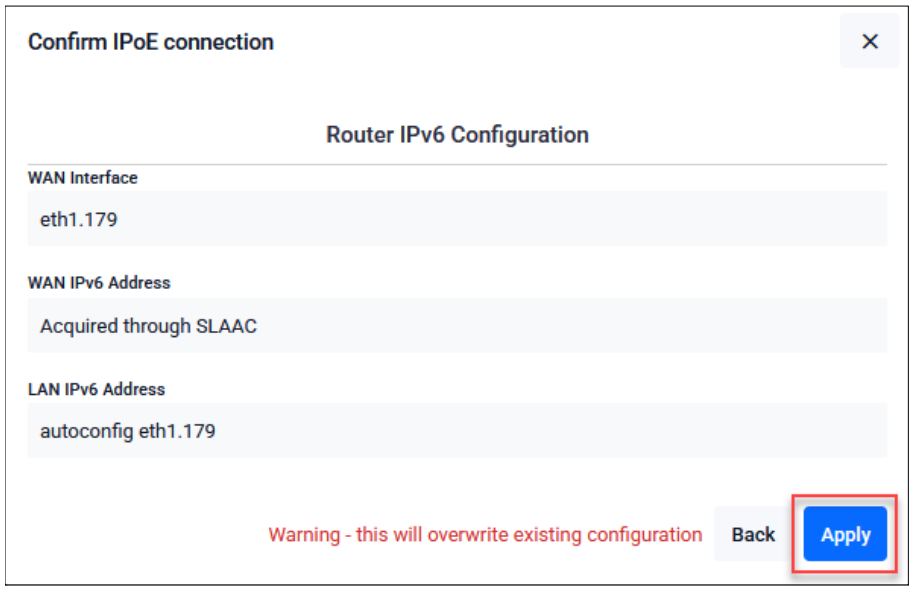
To configure SLAAC follow these steps:

1. Select **IPoE** from the **Select setup method** drop-down list.
2. From the **SLAAC** tab enter or select the **WAN interface**.
3. Click the **Next** button to check your settings:



Field	Description
WAN interface	The interface used to connect to the Internet, in this example eth2.

4. Click the **Apply** button to confirm your settings.

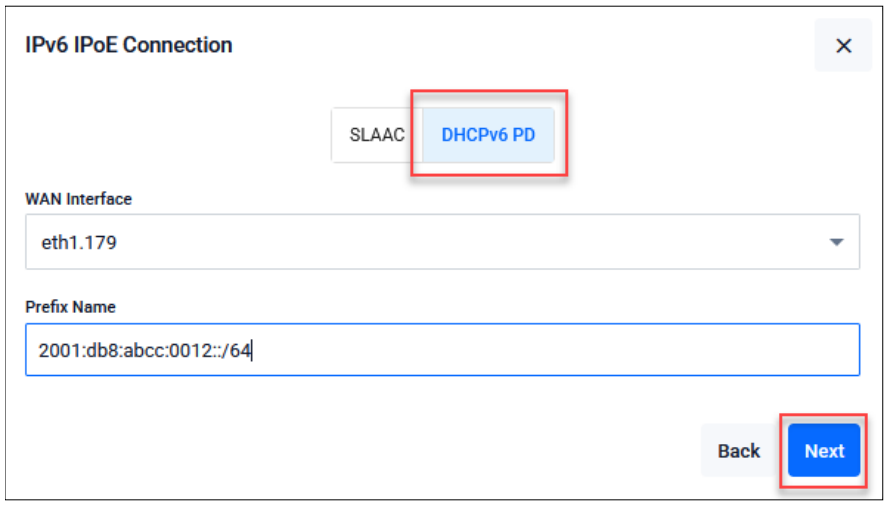


To configure DHCPv6 PD follow these steps:

1. Click on the **DHCPv6 PD** tab.

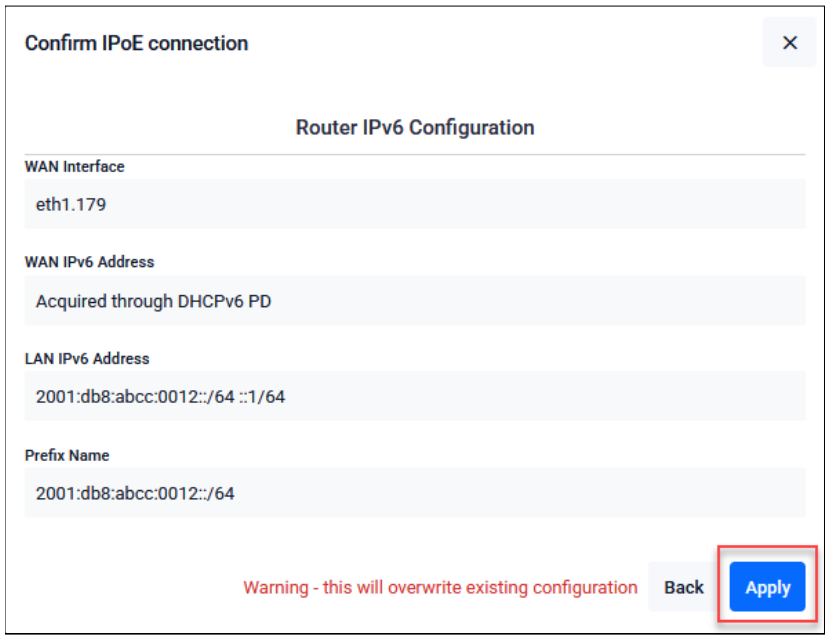
- Enter or select the **WAN interface**.
- Enter a **Prefix Name**.

2. Click the **Next** button to check your settings:



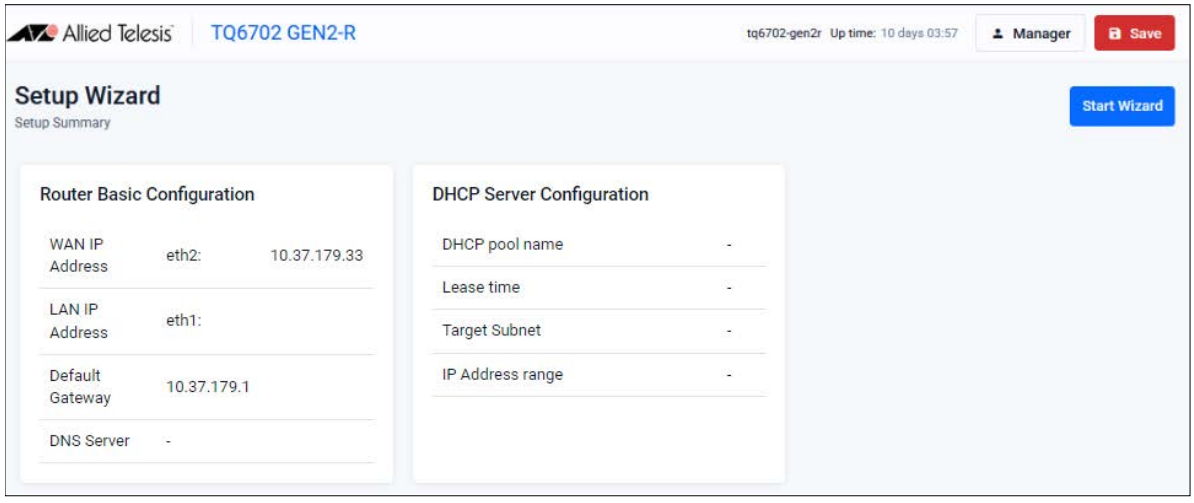
Field	Description
WAN interface	The interface used to connect to the Internet, eth2.
Prefix Name	Enter a name to refer to the retrieved prefix. This is the IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.

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



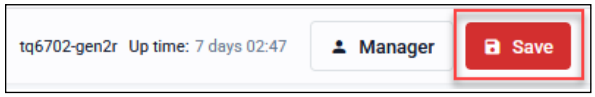
4. Review your configuration.

Check that your configuration works because applying your configuration will overwrite existing configuration. The Setup Wizard displays a summary of the connection status that you can use to check that it is correct.



5. Save your configuration.

- The settings in the wizard are stored in the **running**-configuration and reflected in the operation, but are not automatically saved in the **startup**-configuration.
- After confirming that there are no problems with the settings, manually save the settings to the **startup**-configuration using the **Save** button in the navigation bar. This keeps your settings if the wireless router reboots.



- You can run the Wizard again to make changes to your connection method settings.

Configure a VPN connection

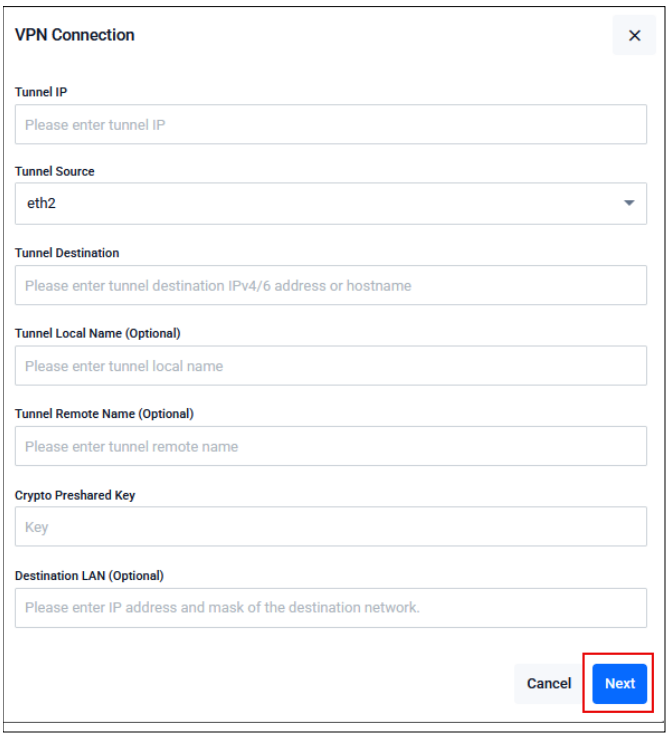
To configure a secure VPN connection, first make sure you have an Internet connection (as described on page 19), and then use the following steps:

1. Select **Wizard > VPN** from the menu bar.

- If you don't have an existing VPN connection, you'll see a blank **VPN Wizard** summary page.
- If you do have an existing VPN connection, then you'll see those details displayed in the **VPN Wizard** summary page.

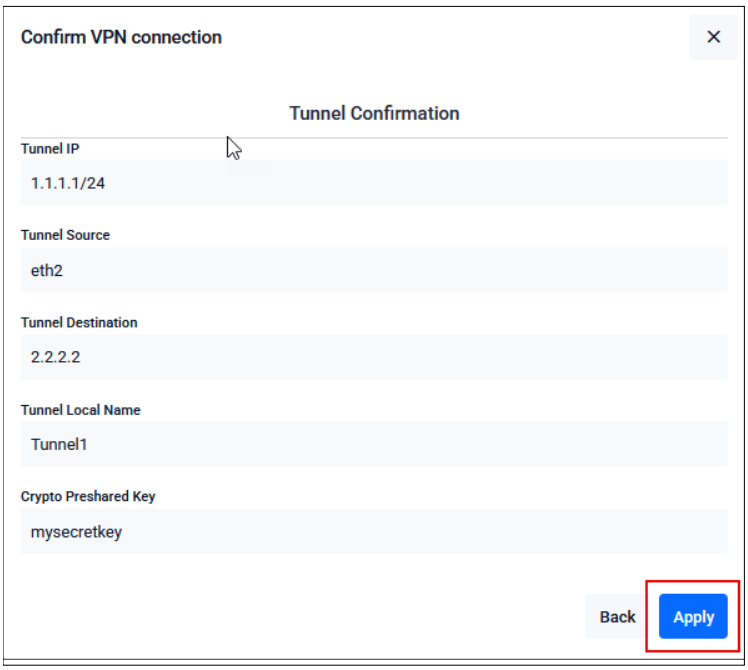
2. Click the **Start Wizard** button.

3. Enter the **VPN Connection** information as described in the table below.



Field	Description
Tunnel IP	Enter the IPv4 address of the tunnel interface.
Tunnel Source	Select or enter the interface for the VPN connection.
Tunnel Destination	Enter the end IP address or host name of the VPN destination.
Tunnel Local Name	Enter the ISAKMP IP (local ID) for the local router.
Tunnel Remote Name	Enter the ISAKMP IP (remote ID) for the remote router.
Crypto Preshared Key	Enter the password (ISAKMP pre-shared key) for the VPN connection.
Destination LAN	Enter the LAN-side IPv4 address of the destination network.

4. Click the **Next** button to check the settings you have entered.

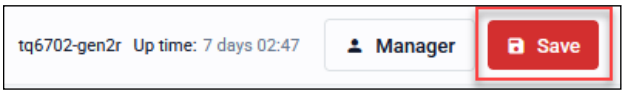


5. Click the **Apply** button to confirm your settings.
6. Review your configuration.

Check that your configuration works because applying your configuration will overwrite existing configuration. The VPN Wizard displays a summary of the connection status that you can use to check that it is correct.

7. Save your configuration.

- The settings in the wizard are stored in the **running**-configuration and reflected in the operation, but are not automatically saved in the **startup**-configuration.
- After confirming that there are no problems with the settings, manually save the settings to the **startup**-configuration using the **Save** button in the navigation bar. This keeps your settings if the wireless router reboots.



- You can run the Wizard again to make changes to your connection method settings.

Configuring firewall and NAT

The next sections describe the AlliedWare Plus firewall and how to configure it.

These sections only apply to models that support the AlliedWare Plus firewall.

The router's firewall, at its simplest level, controls traffic flow between a trusted network (such as a corporate LAN) and an untrusted or public network (such as the Internet). Firewalls determine whether traffic is allowed or disallowed based on characteristics of the packets, including their destination and source IP addresses and TCP/ UDP port numbers.

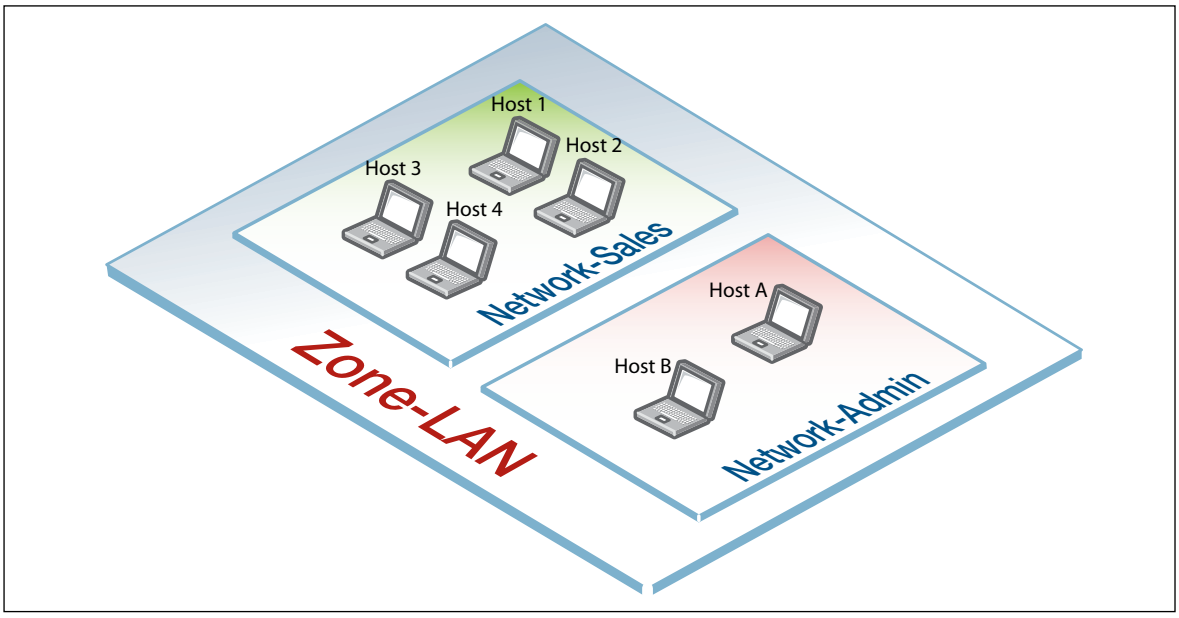
Applications can be created using a combination of protocol and port numbers, and then be used by firewall, NAT, and traffic control rules to manage traffic.

Entities: zones, networks and hosts

Before we begin configuring, let's take a look at the building blocks that allow this advanced control of online network activity.

When the device is deciding how it should treat a traffic stream, among the questions it needs to ask are "***where is the stream coming from?***" and "***where is it going to?***".

To help answer those questions, the device needs to have a logical map of the network environment, so that it can categorize the sources and destinations of the flows that it is managing. Allied Telesis firewalls and routers map out the network environment into regions, using three levels: **zones**, **networks**, and **hosts**:



Allied Telesis refers to these divisions as **entities**. This hierarchy of entities empowers organizations to accurately apply security policies at company, department, or individual level.

A **zone** is the highest level of division within the network. It defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. A typical network environment might contain a public (WAN) zone representing the Internet, a private (LAN) zone behind the firewall, and a Demilitarized zone (DMZ) containing publicly accessible web servers. Zones are divided up into networks, which in turn contain hosts.

A **network** is a logical grouping of hosts within a zone, for example, the sales network within the LAN zone. Networks consist of the IP subnets and interfaces over which they are reachable. The allocating of networks to zones is the core activity in dividing the network up into logical regions to which different security policies apply. A zone has no real meaning in itself until it has one or more networks allocated to it. Once networks have been allocated to a zone, the zone is then the entity that collectively represents that set of networks. Then rules can be applied to the zone as a whole, or to individual networks within the zone.

A **host** is a single node in a network, for example, the PC of a specific employee. The diagram above shows Host 1 is a host within the sales network within the LAN zone. Host entities are defined so that specific rules can be applied to those particular hosts - e.g. a server to which certain types of sessions may be initiated.

Using rules

Rules allow the advanced control of users, and the applications they use on the network.

Firewall rules: filter traffic, allowing or denying, between any two entities. This allows for granular control, as rules can be based on traffic sources that might be zones, networks, or hosts, and traffic destinations that might be zones, networks, or hosts.

For example, an organization may choose to block Skype™ company-wide (i.e. from ANY zone to ANY zone), or allow it only for the marketing department (i.e. allow Skype from the Marketing network to ANY zone, but block it from any other network, zone, or host).

Traffic control rules: control the bandwidth that applications use. For example, Spotify™ music streaming may be allowed, but limited in bandwidth due to an acceptable use policy ensuring company Internet connectivity is prioritized for business traffic.

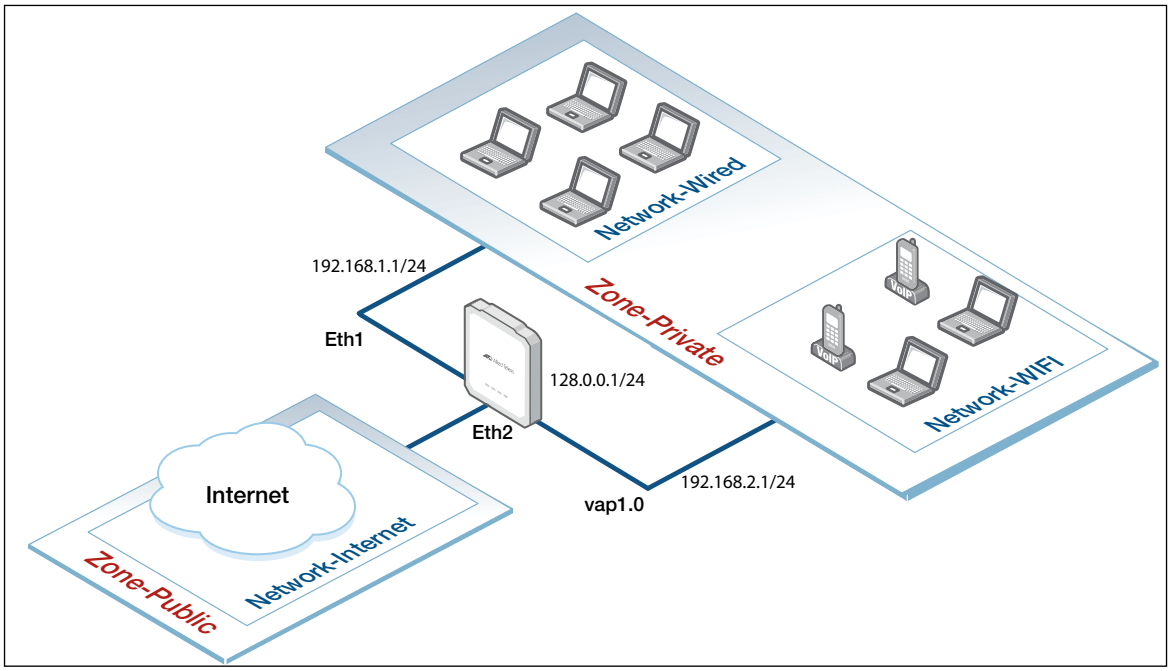
Network Address Translation (NAT) rules: hide private network addresses for traffic bound for the Internet. All company traffic leaving the corporate office can share a public network address for routing through the Internet to its destination.

The firewall supports:

- NAT with IP masquerade, where private source addresses are mapped to a public source address with source port translation to identify the association. The single public IP address masquerades as the source IP on traffic from the private addresses as it goes out to the Internet.
- Port forwarding, to provide public access to internal servers. Port forwarding redirects traffic to a specific host, e.g. forwarding HTTP traffic to a web server in the DMZ.

Example: configure a standard 2-zone network

This section comprises two parts, and describes how to configure a standard 2-zone network:



If your router is new and unused, it will already have the Device GUI installed from the factory, with the IP address 192.168.1.1 on Eth1, and the HTTP service enabled.

This example assumes that you have already configured:

- the WAN interfaces, see "Using the Wizard to configure Internet and VPN connections" on page 19 and
- the radio interface, see "Configuring a Wi-Fi network" on page 14

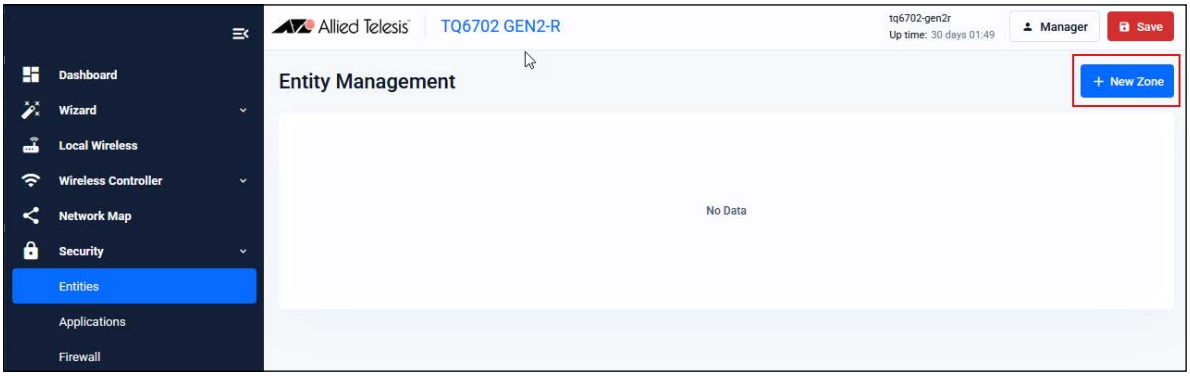
It uses the following IP addresses:

- eth1: 192.168.1.1/24
- eth2: 128.0.0.1/24
- vap1.0: 192.168.2.1/24

Step 1: **Configure Entities**

To configure the firewall and NAT, we will first create entities to which rules can be applied.

1. Select **Security > Entities** from the menu bar.
2. As no entities have yet been created, click the **+ New Zone** button to add a zone.

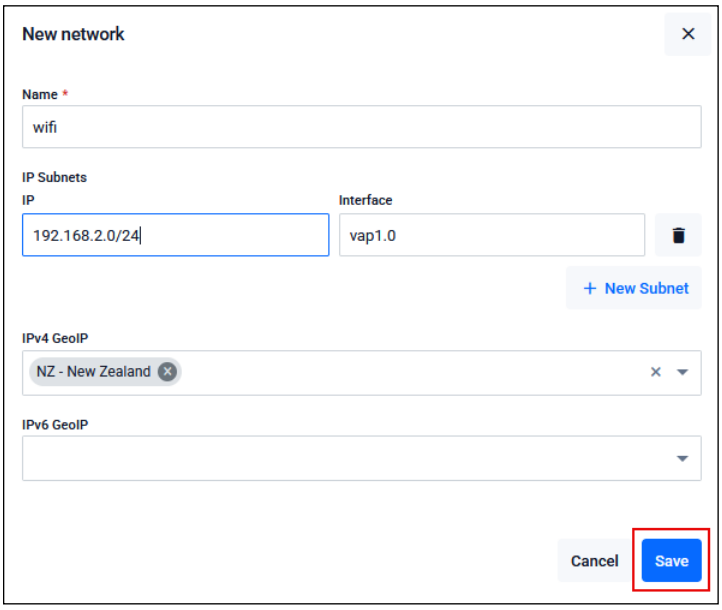


The first zone we will add is the **private** zone to be used for wired clients that we want to be accessible from the Internet

3. Enter the new zone **private**.
4. Click **Apply**:

5. Click the **+ New Network** button from the private zone to add the wired network.

6. Enter the network **wifi**.
7. Add the IP subnet **192.168.2.0/24** and **vap1.0** as the interface over which this network will be reachable.
8. Click **Save**.

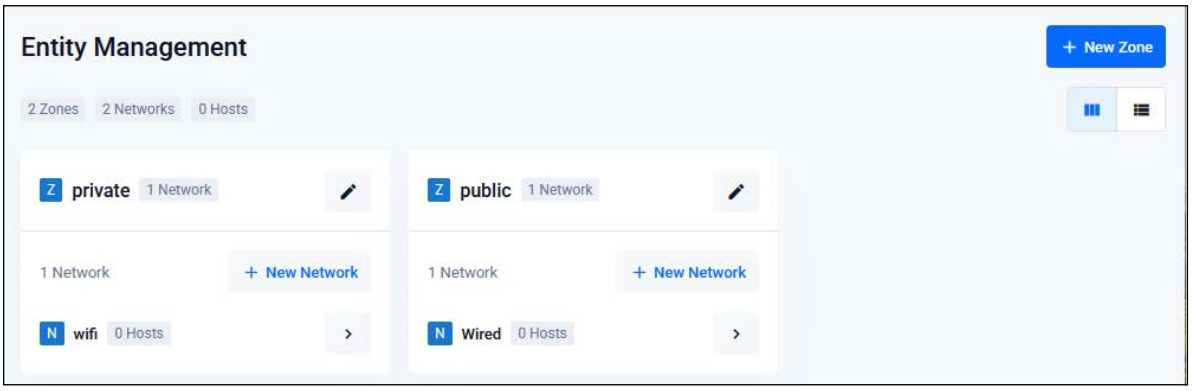


Repeat the same steps to create the public zone network for the LAN with the following details:

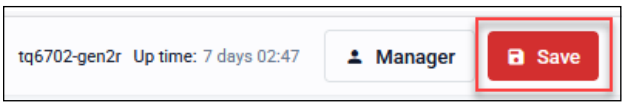
Public zone:

- Zone name = public
- Network name = Wired
- Network subnet and interface = 0.0.0.0/0, eth2

The Entities Management page now contains our 2-zone network:



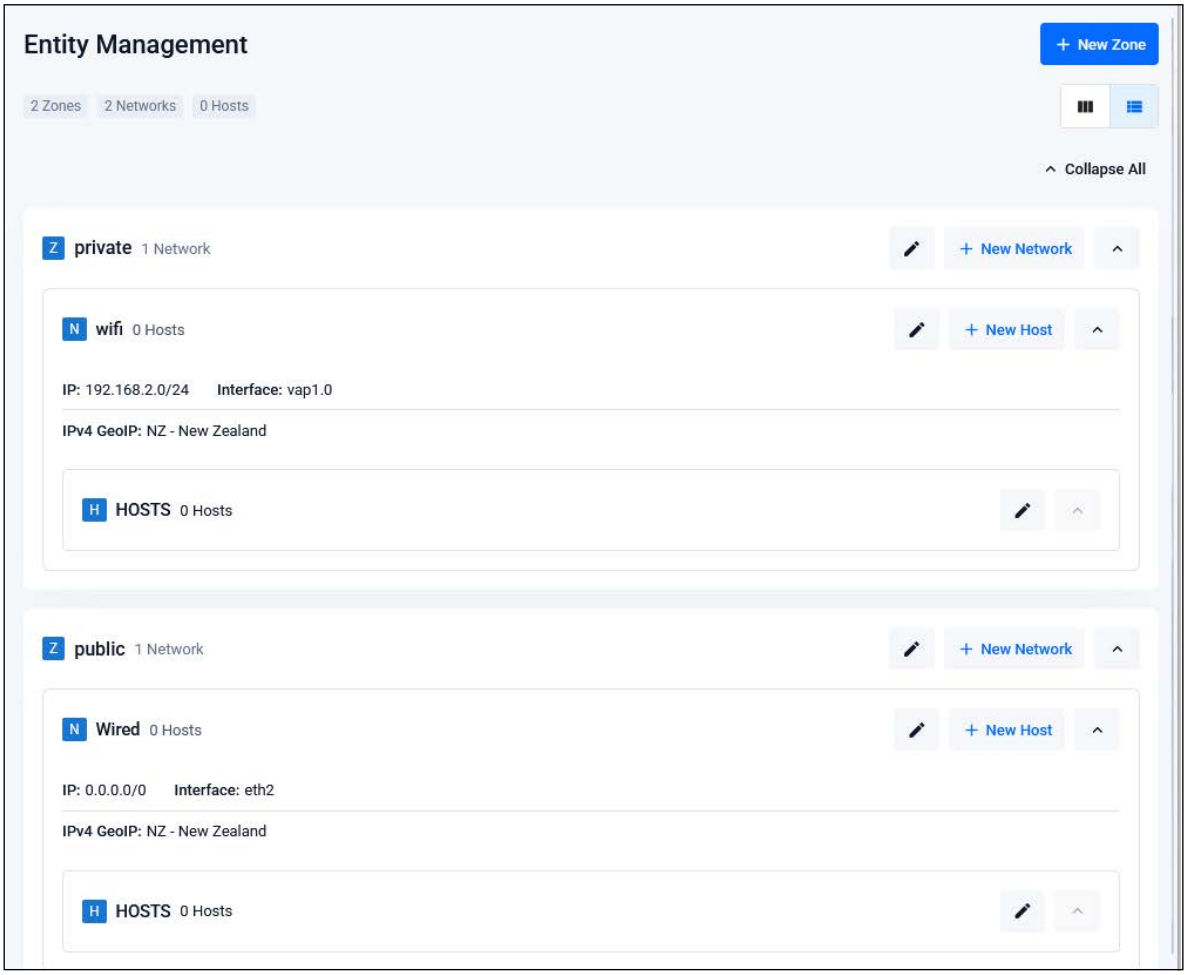
9. Click the **Save** button to save your configuration to the device and startup configuration:



Entity list view

An alternative view from the tiled view shown above, is the list view. To view and manage entities in a list view, click on the list icon on the right side of the page.

Clicking **Expand All** (on the right side of the page) displays all entities and their interfaces, IP addresses, and so on. The list view is a good option for an overall entity view:



Step 2: **Configure firewall rules**

We now have a 2-zone network (Public and Private), so we can now configure the firewall rules to manage the traffic between these entities.

1. Select **Security > Firewall** from the menu bar:

Caution: Enabling the firewall with the **Enable** switch will block all applications between all entities by default. No traffic will flow. It is therefore important to create firewall rules to allow application usage as desired **before** enabling the firewall.

Tip: To select an application such as ‘any’, simply start typing ‘any’ in the application field. If you don’t see any applications, turn on the built-in list of applications, or create your own custom applications from the **Applications** page, under the **Security** menu.

Allow private side firewall zones to initiate traffic flows with each other and out to the Internet. First create a new rule to permit ‘any’ from private to private.

2. Click the **+New Rule** Button.

- Select **Permit** as the Action.
- Enter or select **any** for the Application.
- Select **private** for the From network.
- Select **public** for the To network.

3. Click **Apply**.

Next, create a new rule to permit ‘ping’ from private to public:

4. Click the **+New Rule** Button.

- Select **Permit** as the Action.
- Enter or select **ping** for the Application.
- Select **private** for the From network.
- Select **public** for the To network.

5. Click **Apply**.

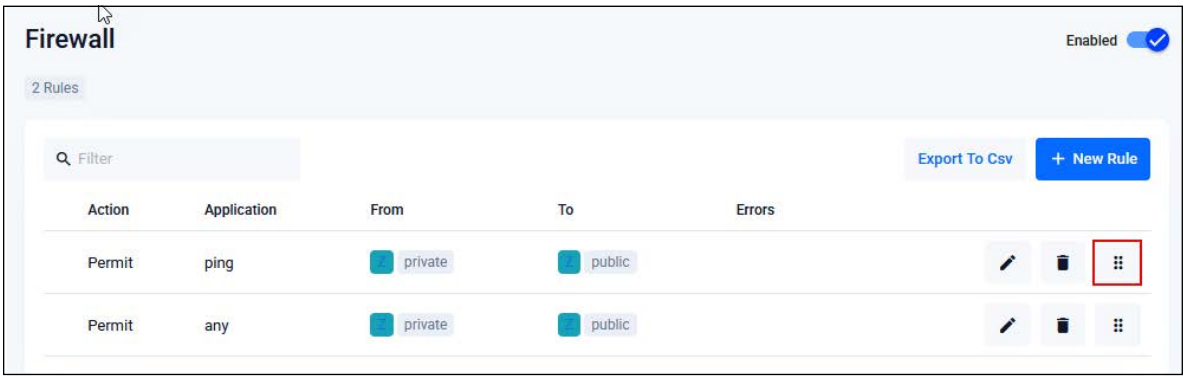
We can now see the firewall rules displayed:

Now that the firewall rules are created, you can turn the firewall **on** using the **Enabled/Disabled** button at the top right of the Firewall page.

Firewall rule placement

The firewall rules are displayed in the order they were created, which is also the order in which they will be **actioned** by the router. If you need to change the order of any specific rule, it can be dragged to a different location in the list. Click on the move icon on the right to click and drag your rules to a new order.

By default a new rule is added to the bottom of the list, and can then be dragged to a new location using the move icon:



Step 3: **Configure NAT rules**

Now let's configure NAT rules to manage IP address translation between the Internet and our internal networks.

1. Select **Security > NAT** from the menu bar:

We need a NAT masquerade rule for private to public address translation. Any traffic going from the Private zone out to the Public zone will have NAT applied, so that it appears to have come from the IP address of the eth1 interface.

2. Click **+ new rule**.

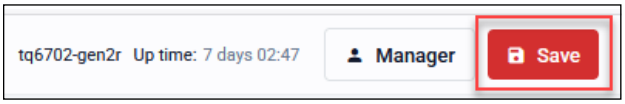
- Select **Masquerade** as the Action.
- Select **any** for the Application.
- Select **private** for the From network.
- Select **public** for the To network.

3. Click **Save**.

You can see the new NAT rule.

4. To activate NAT click the **Enabled** switch to turn it on.

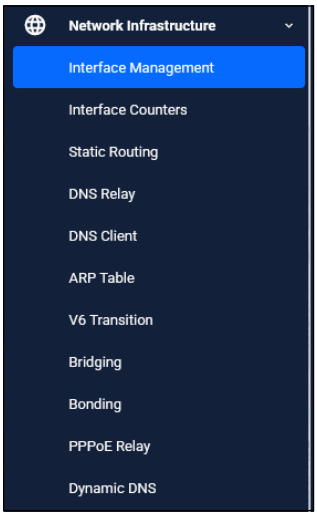
5. Click the **Save** button to save your configuration to the device and startup configuration:



Network Infrastructure

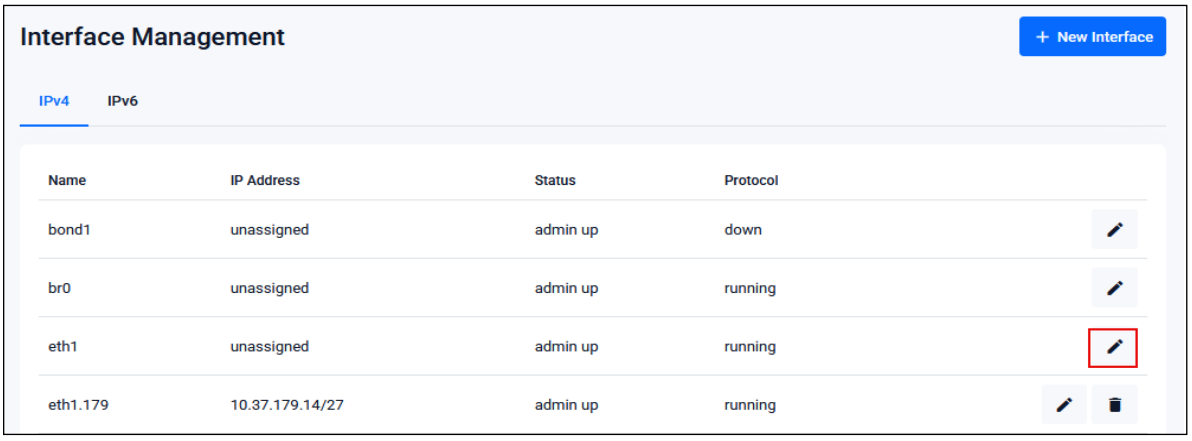
Some of the features in this section only apply to models that support Internet connections.

From the Network Infrastructure menu you can access and configure information such as network interfaces, interface counters, static routing, DNS, ARP, Bridging, Bonding and PPPoE relay. Here are some examples:



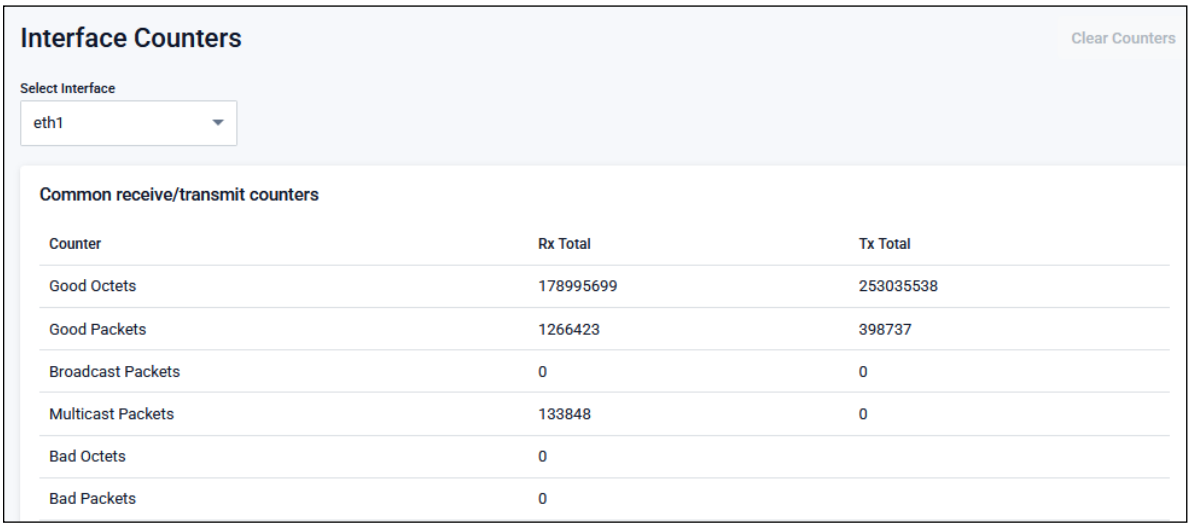
Interface Management

From Interface Management you can display IPv4 and IPv6 interface names, addresses, status and protocol. You can edit the DHCP or fixed IP address information by clicking on the **Edit** button or add new interfaces with the **+ New Interface** button:



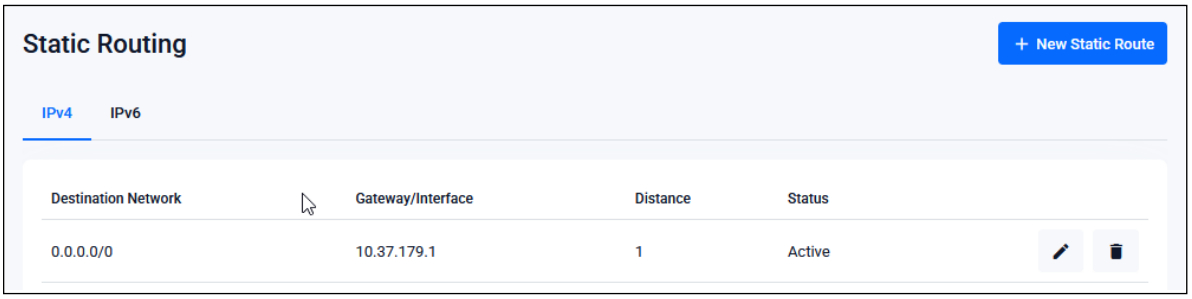
Interface Counters

From **Interface Counters** you can display receive/transmit information for common counters when the ports are available:



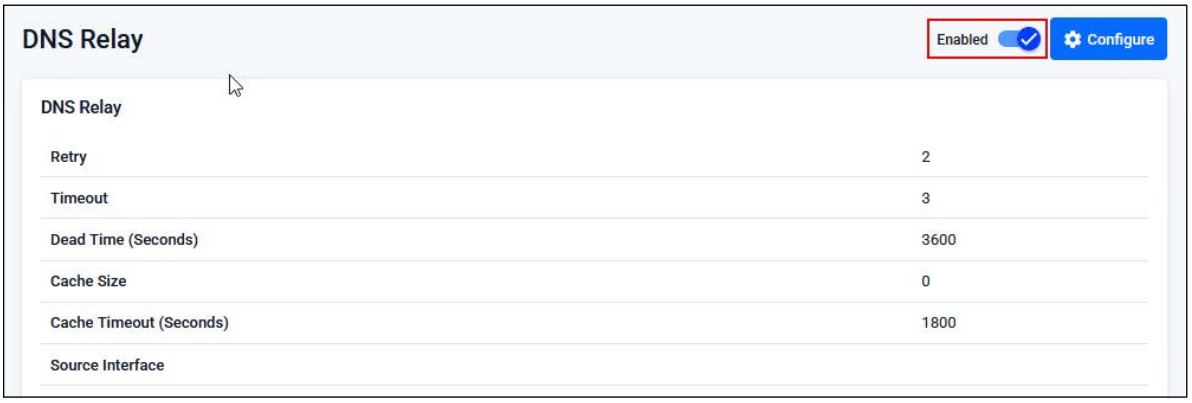
Static Routing

Static routing displays information about IPv4 and IPv6 destination and gateway interfaces, the distance and status. Click on the **Edit Static Route** button to change the destination network, gateway/interface or distance. To add a new static route click on the **+New Static Route** button:

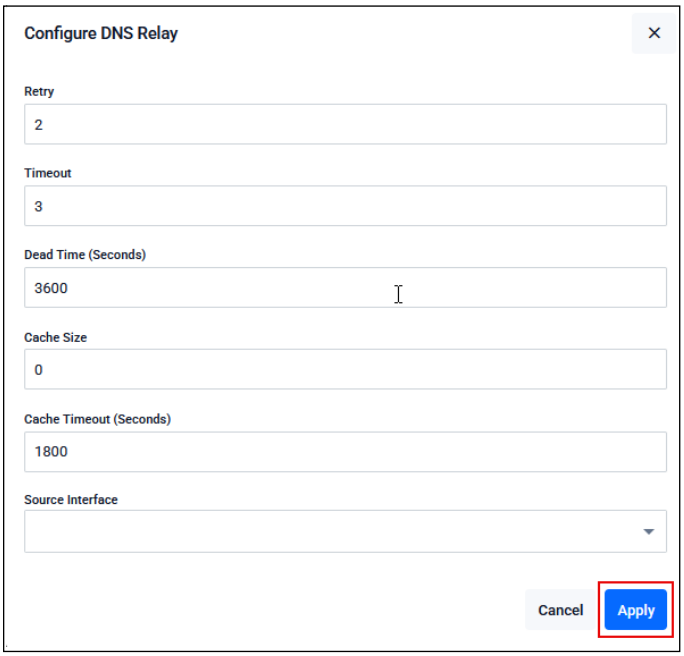


DNS Relay

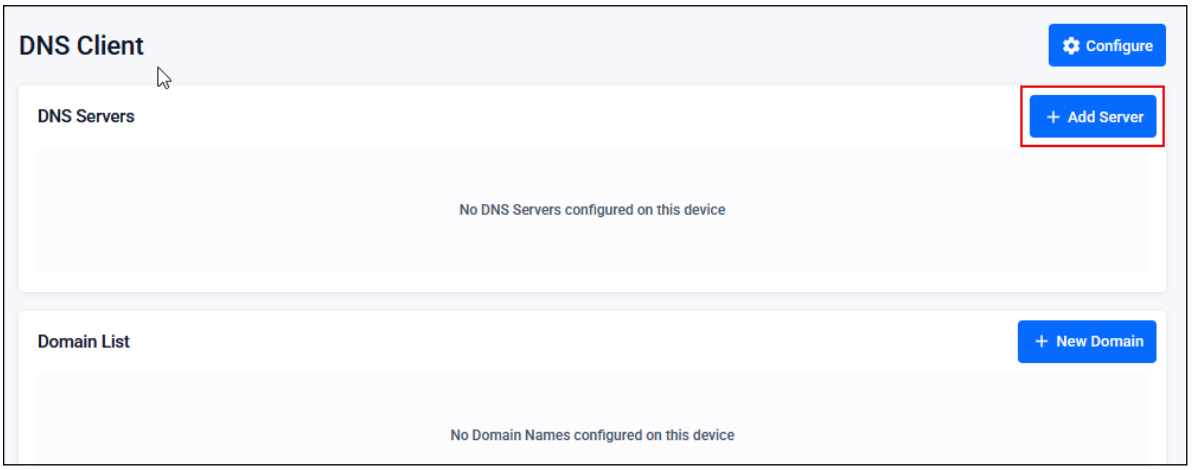
Click on **DNS Relay** from the menu. Enable DNS Relay with the toggle button. To add or change a new DNS Relay entry, click on the **Configure** button:



From the **Configure DNS Relay** dialog Enter the Retry period, the Timeout period, the Dead Time, Cache Size, Cache Timeout and Source Interface. Click the **Apply** button:

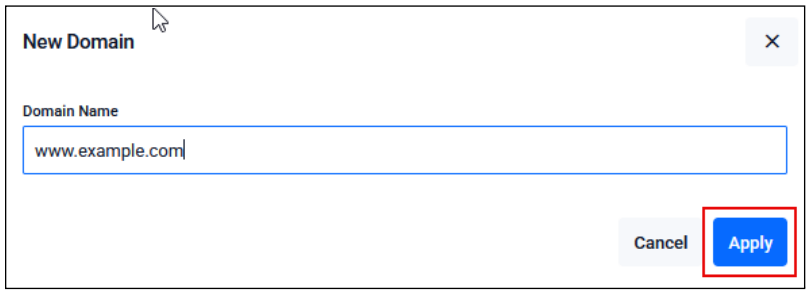


DNS Client Click on **DNS Client** from the menu. To add a DNS Server, click on the **+Add Server** button:



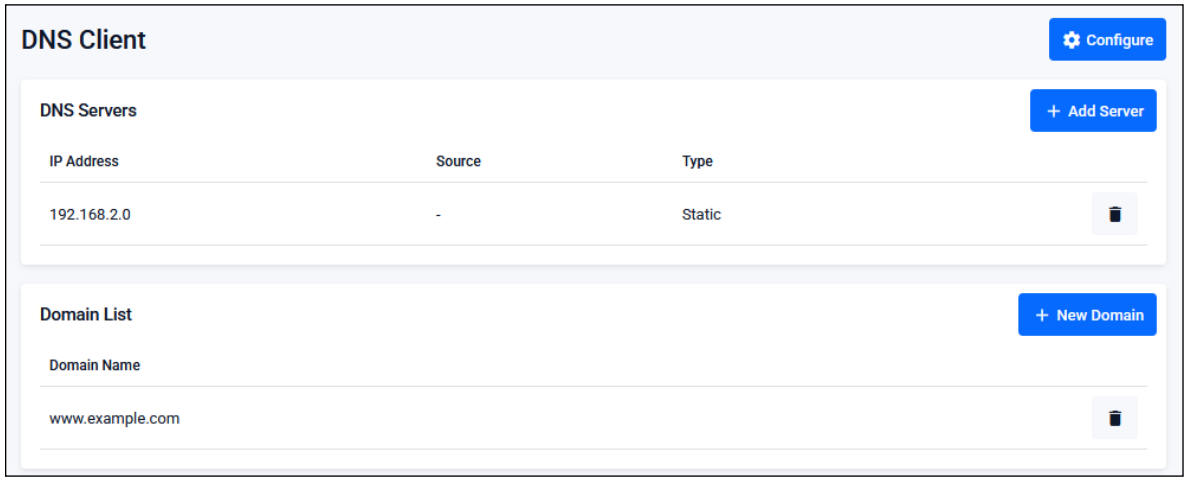
Add the new server IP Address. Then click on the **Apply** button:

To add a new Domain, click on the **+Add Domain** button. Enter the Domain Name and click on the **Apply** button.

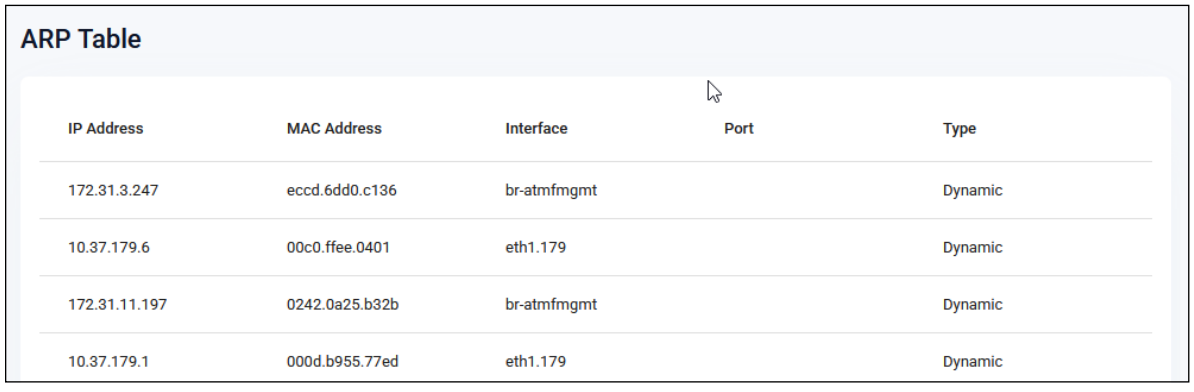


Click on the **Configure** button to set up a Domain Lookup option, select the DNS Servers Preferred Order, and enter the Default Domain Name.

You can see the DNS Server and Domain that you have created from the DNS Client window:

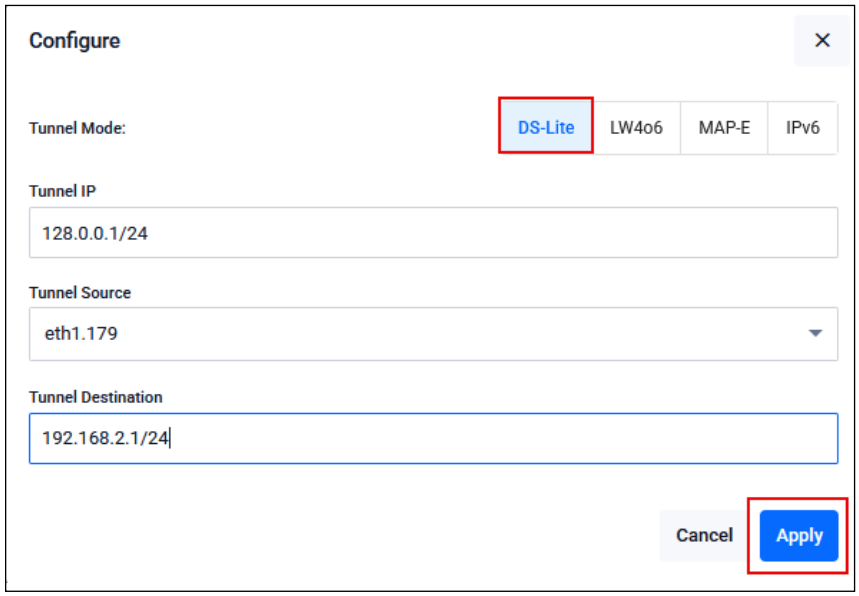


ARP table The ARP table shows address resolution records:



V6 Transition

Clcik on **V6 Transition** from the menu. To configure V6 Transition, click the **Configure** button. Select the **Tunnel Mode** from the available tabs DS-Lite, LW406, MAP-E or IPV6. Enter the required fields and then click on **Apply**:



Bridging

Click on **Bridging** from the menu. To add a bridge, To add a new bridge, click on the **+New Bridge** button. Give the bridge and ID, and select or add the Ports, click on **Apply**:

Bonding

Ethernet Bonding is a way to either improve the throughput or add redundancy to Ethernet links by using a set of interfaces that work together to send the traffic and appear as a single interface to higher layers. There are 2 types of Ethernet bonding, static (fixed) configuration and LACP (peer-negotiated) configuration.

Click the **New Bond** button to create a bond, give it a number and choose a bond type of either static or LACP and click on **Apply**.

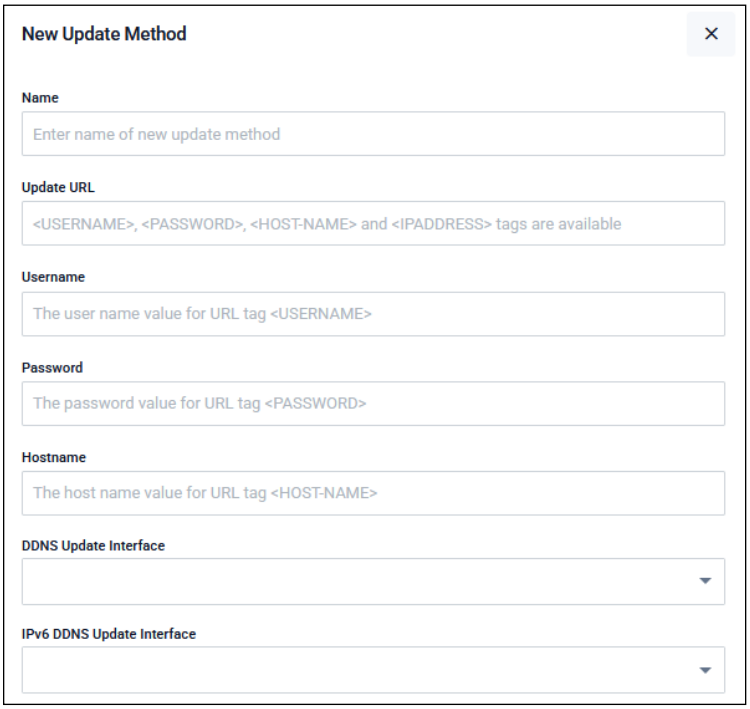
PPPoE Relay

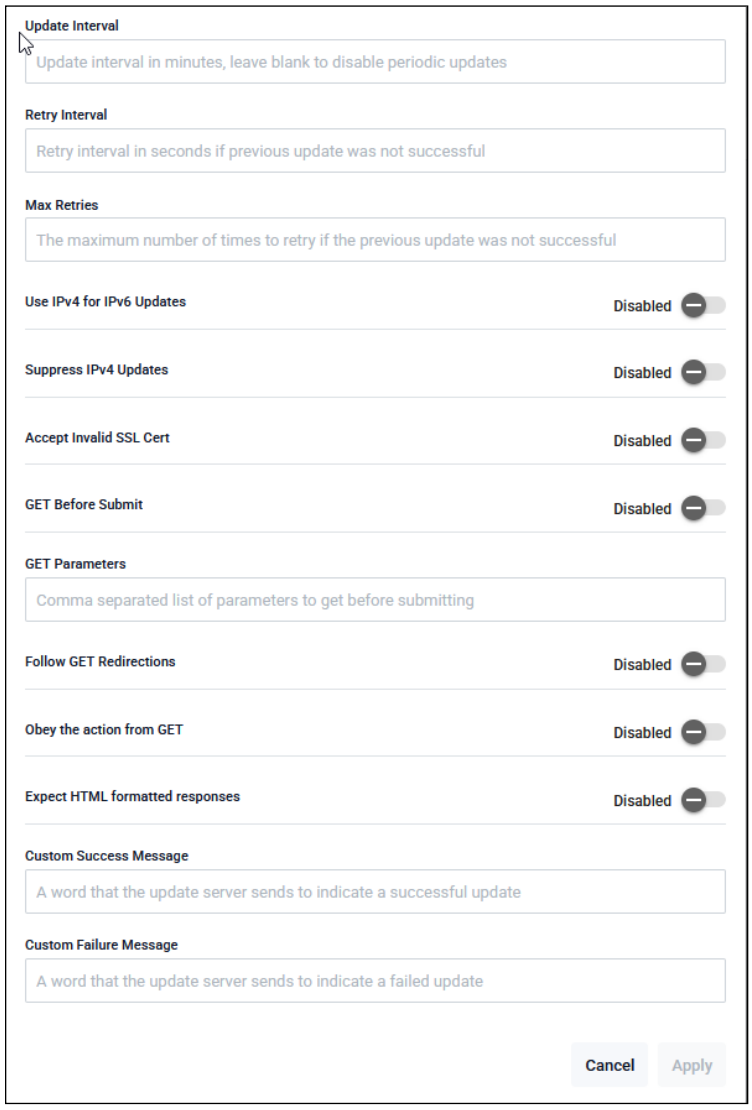
To configure a new PPPoE relay instance click on the **+Add Relay Instance**. Fill in the required fields and click **Apply**:

Dynamic DNS

To configure Dynamic DNS, click on **Dynamic DNS** from the menu. Enable Dynamic DNS with the **Toggle** button.

To add a new update method, click on the **+New Update Method** button:

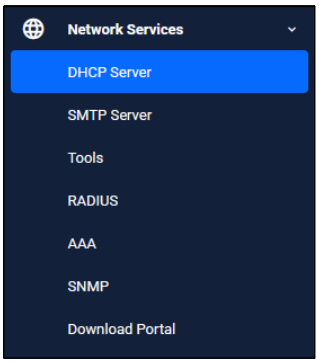




Select and add all of the information required. Click the **Apply** button to apply your entries.

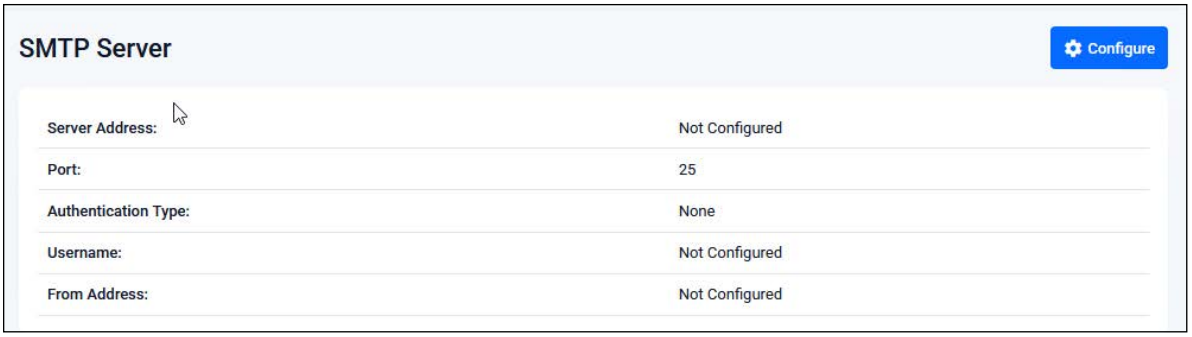
Network Services

From the **Network Services** menu you can configure features such as DHCP server pool, SMTP server, use traceroute or ping tools and configure RADIUS, AAA or SNMP.

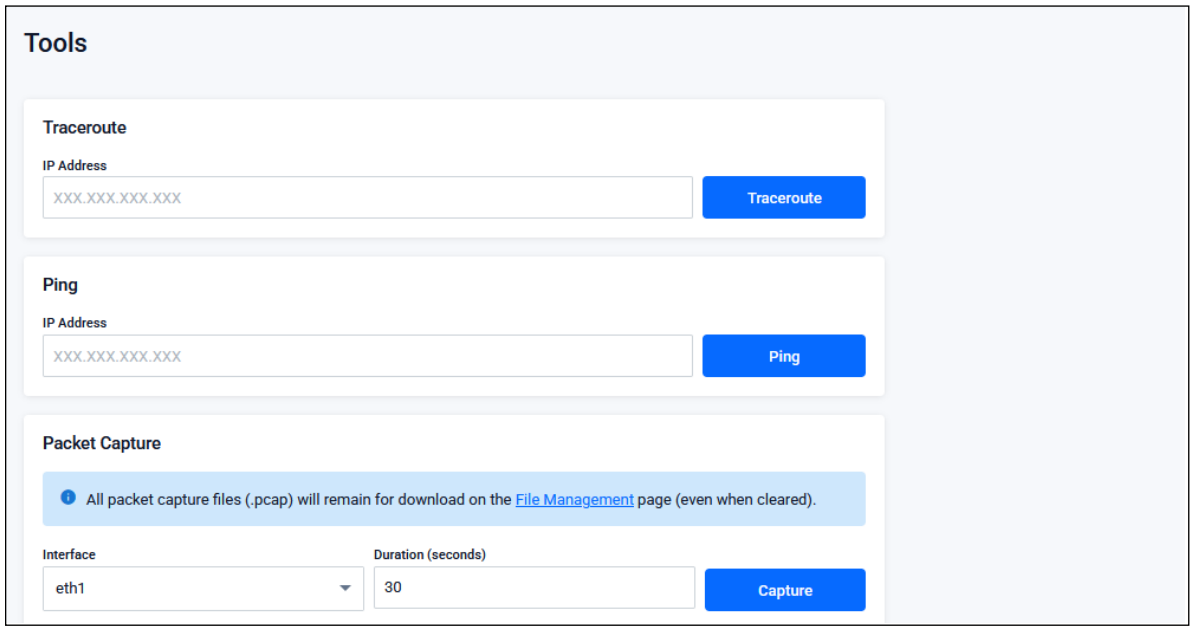


From the **DHCP Server** menu, you can display or configure a new DHCP pool:

From the **SMTP Server** menu, you can display or configure the following information about sending and receiving email on the wireless router:



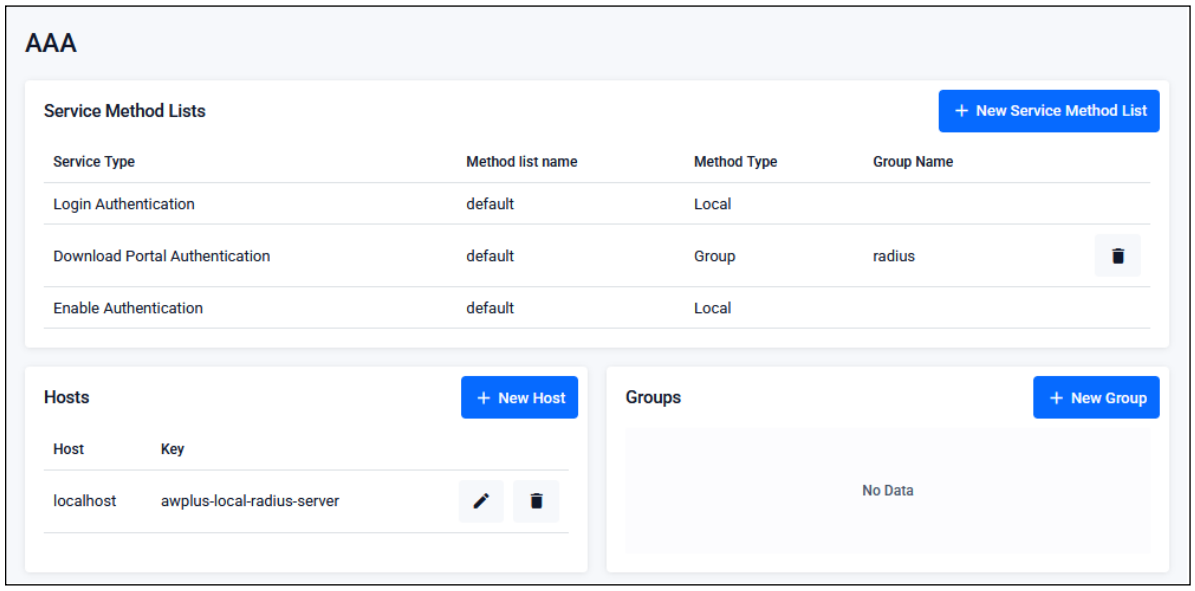
From the **Tools** menu you can use traceroute to trace the path to a device, ping an IP address or capture packets:



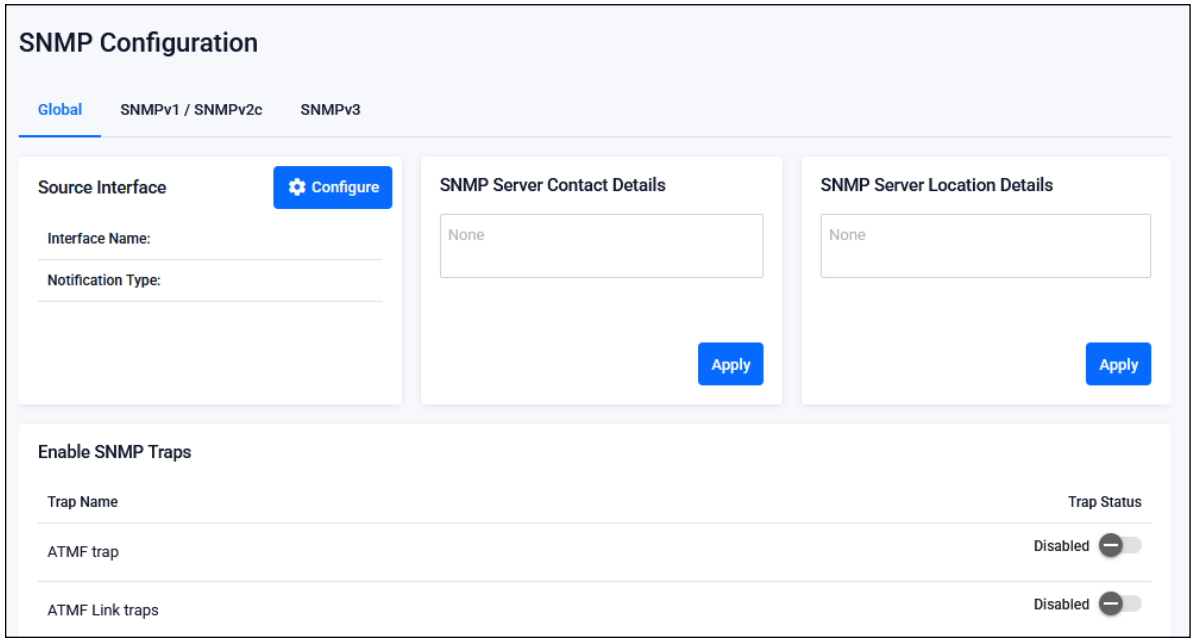
From the **RADIUS** menu you can display the following information about the wireless router's inbuilt local RADIUS server:

From this page you can add new users, groups and NAS information and you can import or export CSV files about users, groups and NAS. You can also export local CA certificates.

From the **AAA** menu you can display and configure the following information about hosts and groups:



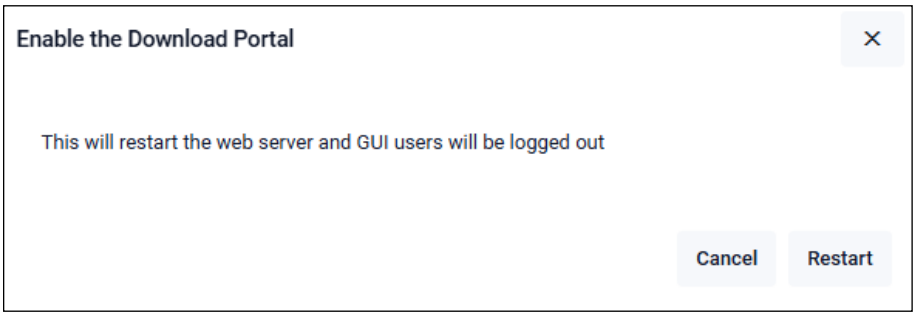
From the **SNMP** menu, the following information is displayed in the SNMP Configuration dialog:



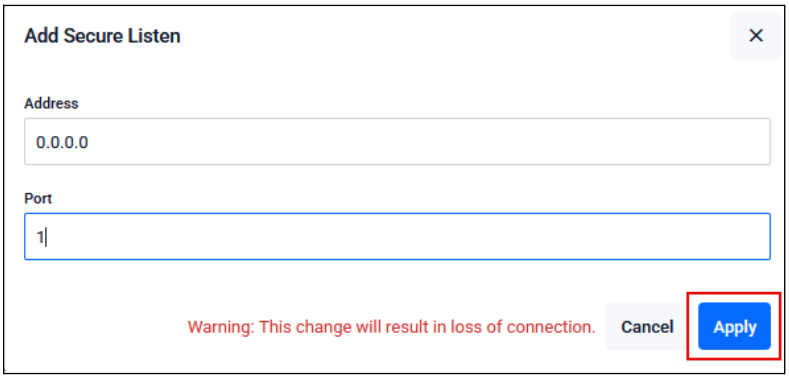
From this page you can configure the Source Interface, enter and apply SNMP Server Contact Details, and enter SNMP Server Location Details. You can also enable or disable SNMP traps and display OIDs for the traps.

From the **Download Portal** menu you can display and configure the following information about HTTP Listening Addresses, and Resources you can utilize:

Click on the **Configure** button to enable the Download Portal. Note that this will restart the web server and GUI users will be logged out.



Click on the **Configure** button to enable the Download Portal. Note that this will restart the web server and GUI users will be logged out. Enter the Address and Port. Click **Apply**.



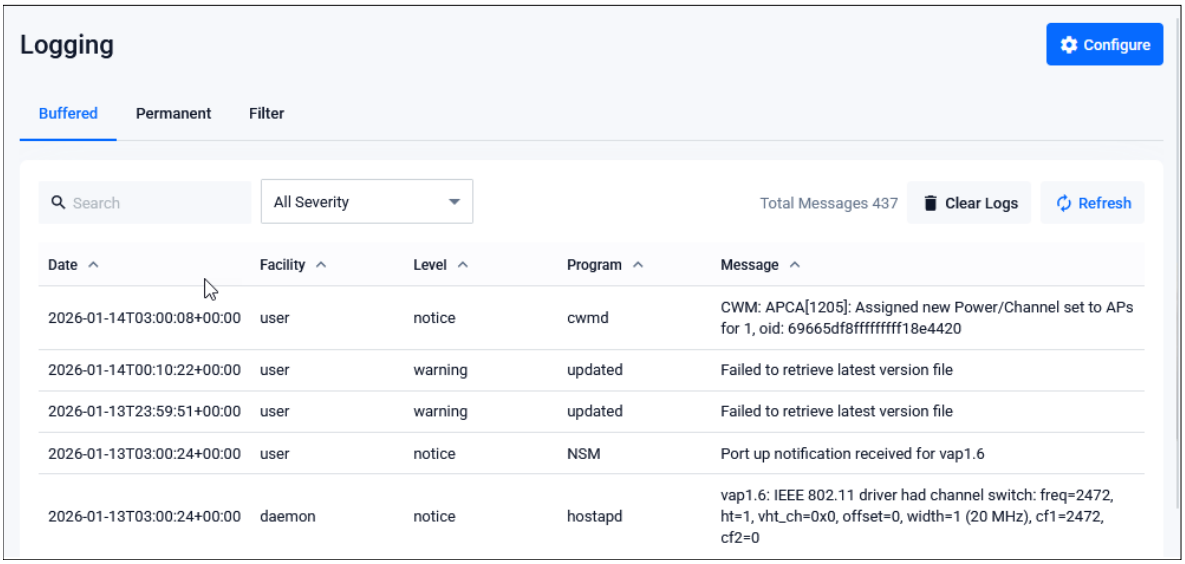
Note: Enabling the Download Portal and Applying Add Secure Listen both will result in loss of connection.

Logging

The **Logging** page shows buffered and permanent log messages stored on the device.

Select **System > Logging** from the menu bar.

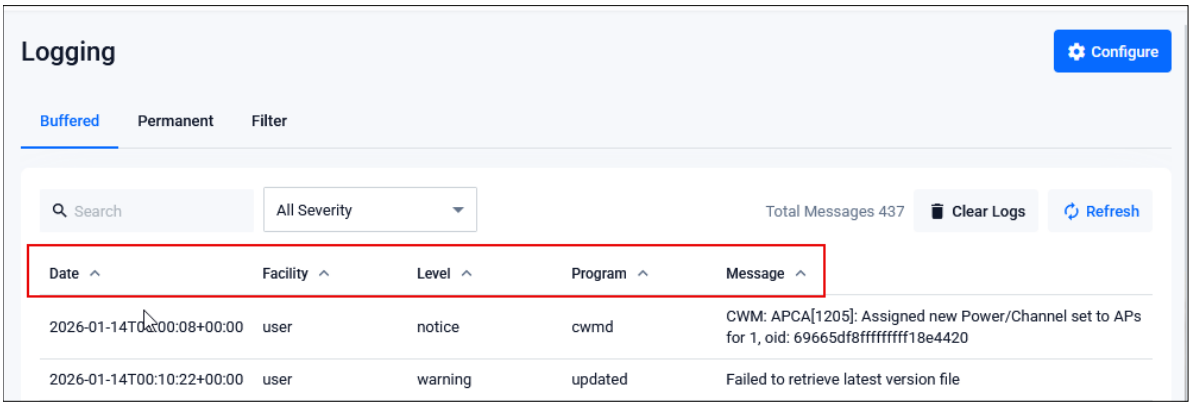
- There are three tabs to choose from, **Buffered**, **Permanent** or **Filter**.
- By default the **buffered** logs are displayed:



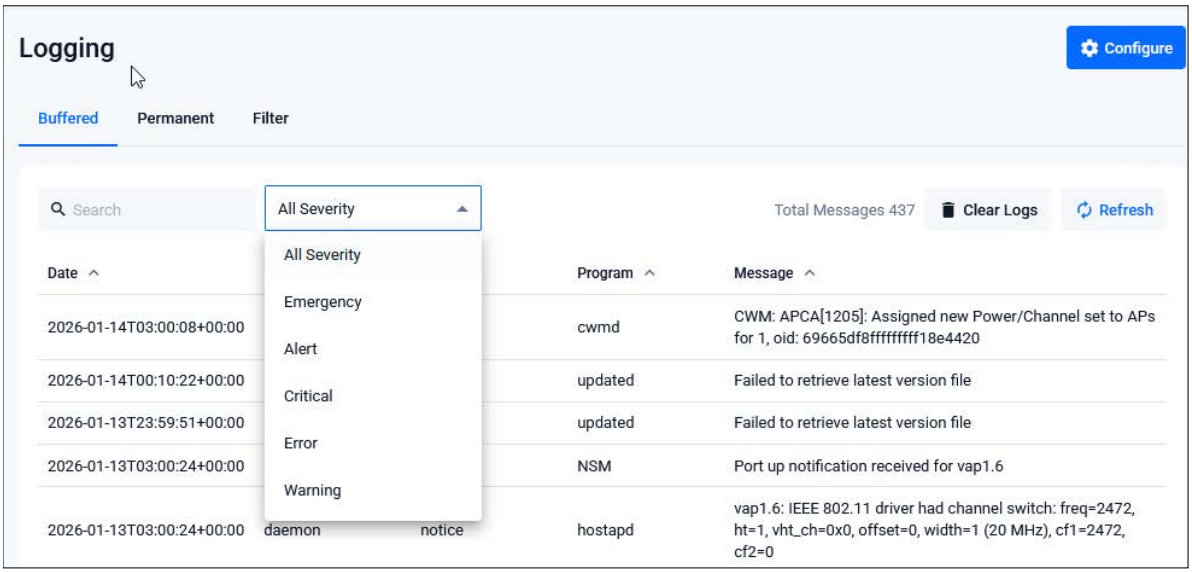
Sort and format options

You can sort Buffered or Permanent logs from their tabs to focus your view and support easy analysis. You can sort in the following ways:

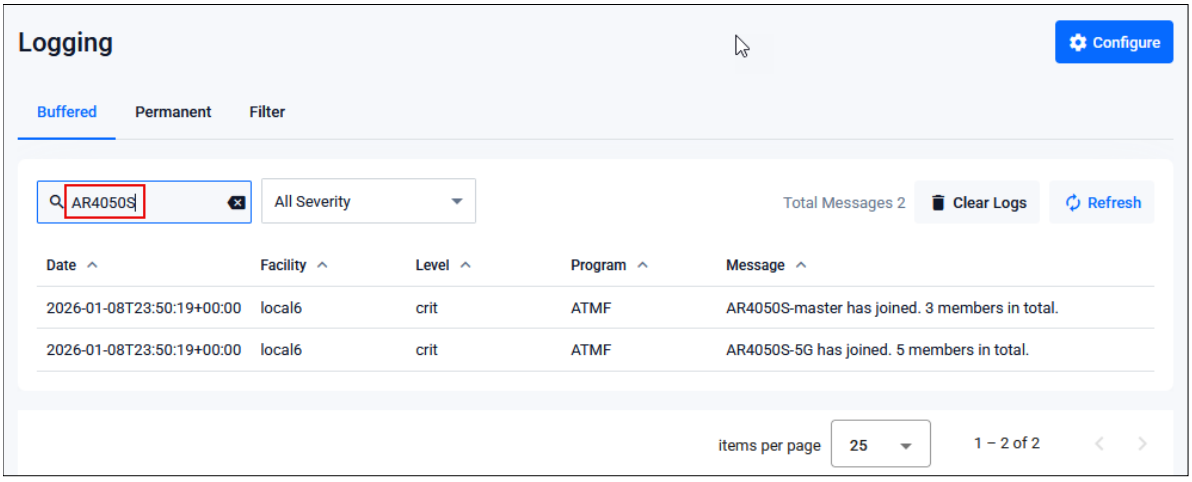
By **column title** in ascending or descending order:



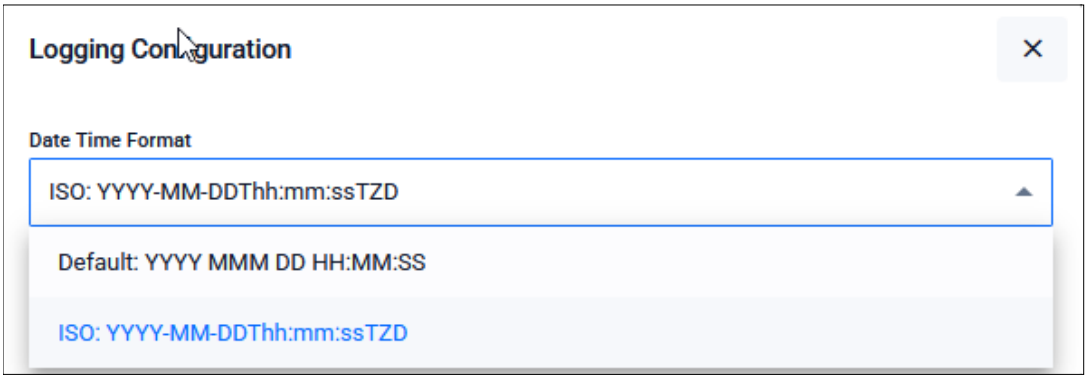
By **Severity** such as All Severity, Emergency, Alert etc:



By **Search** where you can enter any text string found in the logs:



Click the **Configure** button to access the **Date Time Format** options:

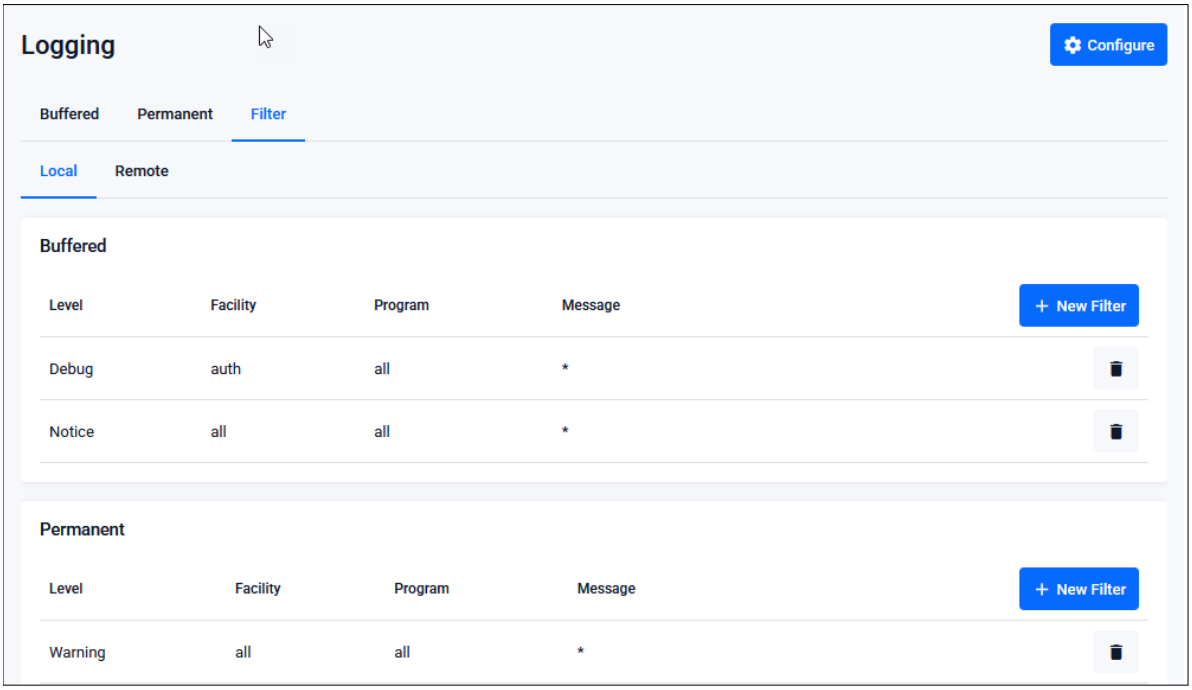


You can delete the buffered or permanent logs using the **Clear Logs** button. Use the **Refresh** button see the latest updated log activity.

Filter options

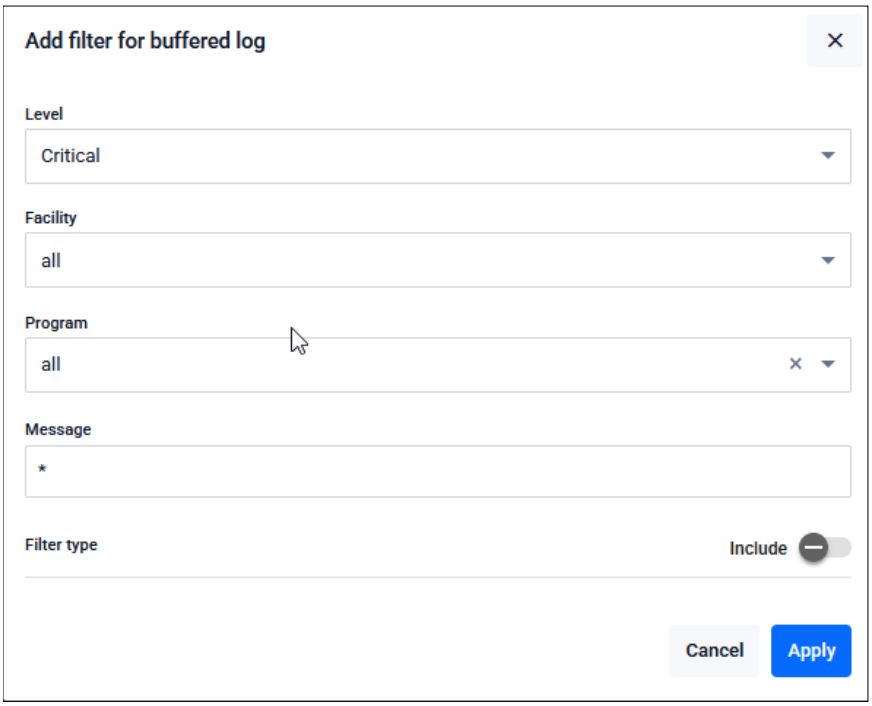
Click on the **Filter** tab to create filters to manage which logs are stored on the device and also set up a Syslog server(s) for remote log storage.

The **Filter** view has tabs for **local** and **remote** (syslog server) settings:



Use the **Local** tab (default) to create filters to manage the level of logs that are stored in the buffered and permanent logs on the device.

When you create a new logging filter you can specify any/all of level, facility, program, and message to be included or excluded in the log storage. This means you can configure log storage exactly as you want it.



Use the **Remote** tab and the **+New Host** button to set up a syslog server to send log messages for storage and analysis. Use the **+New Filter** button to configure filters that specify the type of logs to (include or exclude) to be sent to the syslog server.

Optional features

The following optional features are supported from release 5.5.3-0.1 onwards for the TQR Series:

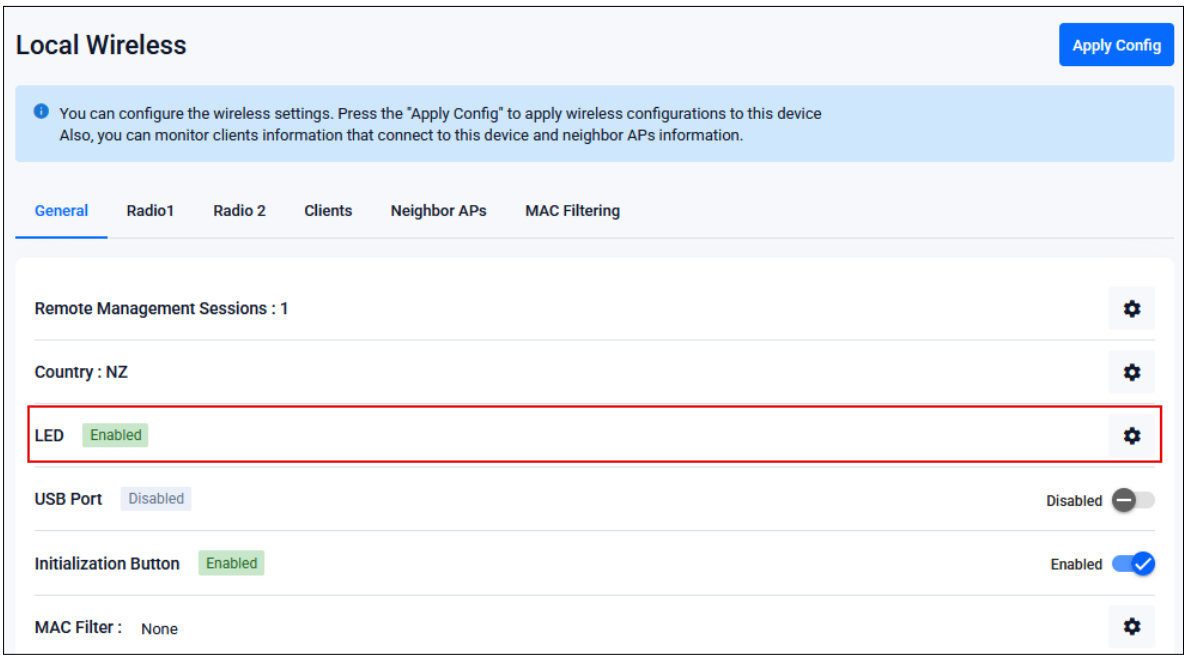
- **ECO LED**
- **Reset button**
- **Change the GUI timeout**
- **Set the time**
- **User Management**

ECO LED

This feature can be enabled or disabled. The LEDs are located on the top front of the device.

- The default is Disabled, so the LEDs are ON by default.
- Enable to stop LED activity.
- Disable to start LED activity.

Step 1: To set up ECO LED on your device, click on **Wireless** from the menu bar. The Wireless page is displayed defaulting to the **General** tab:



Notice that the ECO mode defaults to Disabled. This means that the lights are on.

Step 2: If you want to turn the LEDs off, From the LED options click on the **Settings** button.

Step 3: Click the ECO Mode **Enabled/Disabled** to toggle to Enabled.

From this LED dialog you can also choose the color of the PoE LED to be either Green or Amber when ECO Mode is Disabled (LEDs On). The default is Amber.

Step 4: Click **Apply**.

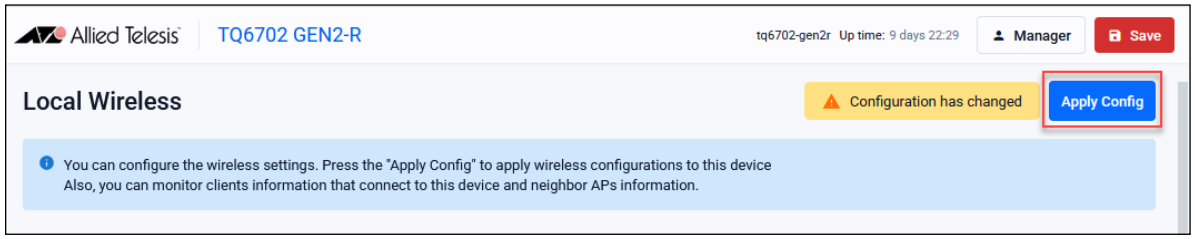
When you configure the wireless router through its GUI, the configuration becomes part of its running-configuration. Once you are sure your configuration changes work, you need to make them part of the boot configuration, so they can be backed up and will survive a reboot of the wireless router.

Caution: Back up the default configuration before you save and apply your configuration.

Once you are happy with the functionality of your configuration, you can then save it.

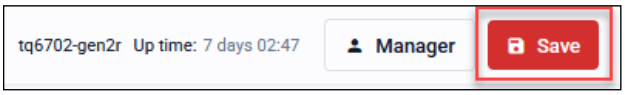
1. Click the **Apply Config** button to apply the settings to your device.

   This step saves the wireless configuration to your device. Notice that the button is orange colored when the configuration requires saving:



2. Click the **Save** button at the top right of the GUI screen (you may need to scroll up to see it).

Tip: The **Save** button is red anytime there is unsaved configuration and blue when it is saved.

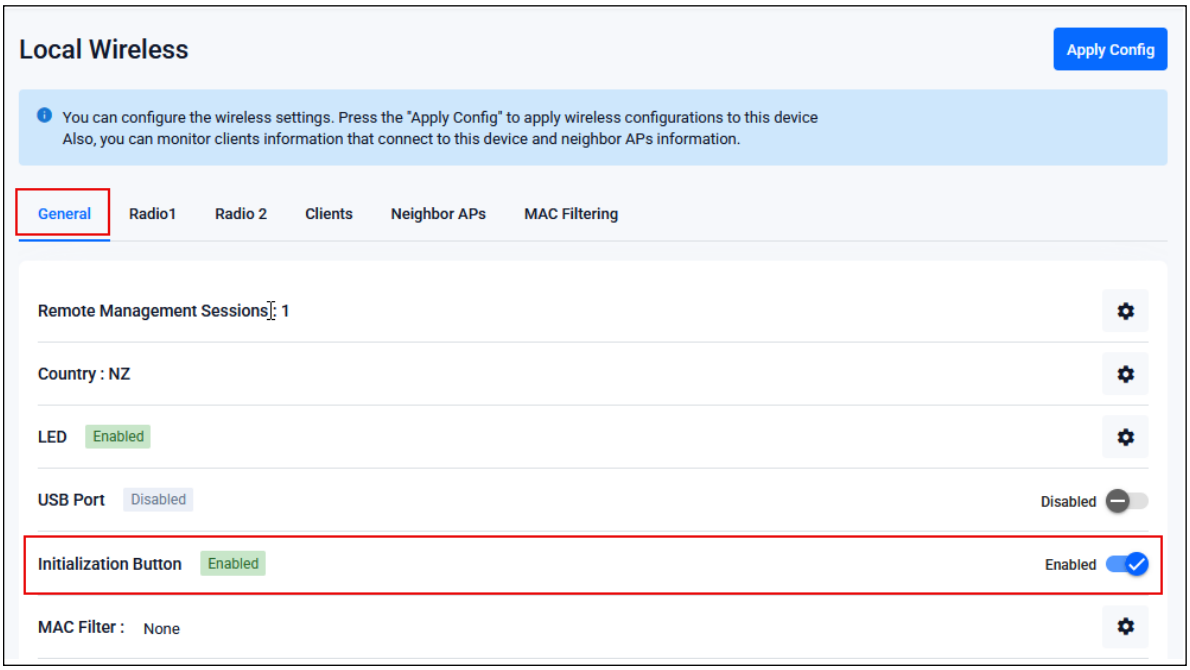


Reset button

The Reset button is recessed and located to the left of the Power button. To press it, use a small pointed tool, such as a metal pin. Pressing it for:

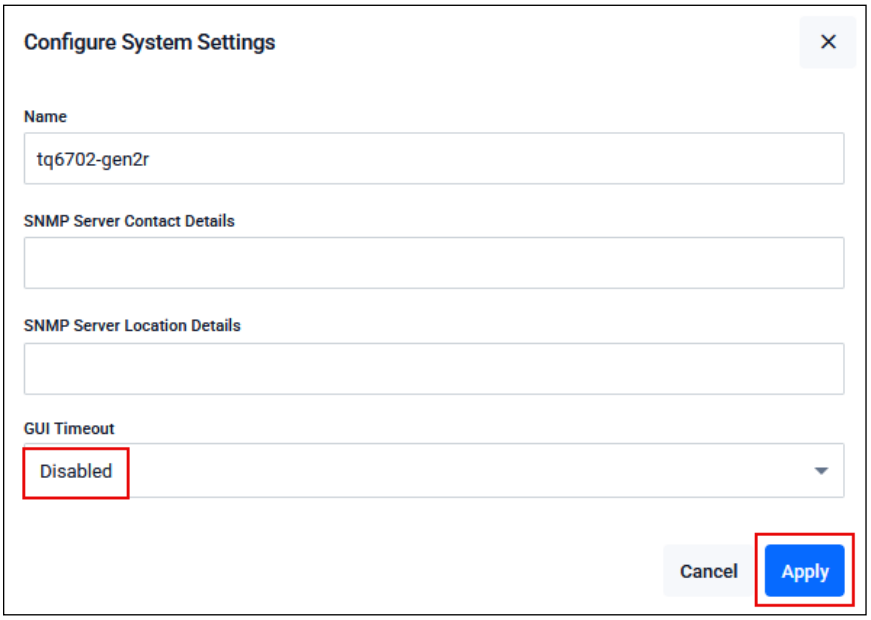
- **over five seconds**, results in a reboot that will restore the configuration back to the equivalent of a factory reset (ready for an AMF Plus recovery). **This means you will lose your configuration and any files stored on your device.**
- **less than five seconds** reboots your device.

The **Initialization Button** displayed in the Device GUI **Wireless** page performs the same function as the Reset button, (factory reset). By default it is enabled.



Change the GUI timeout

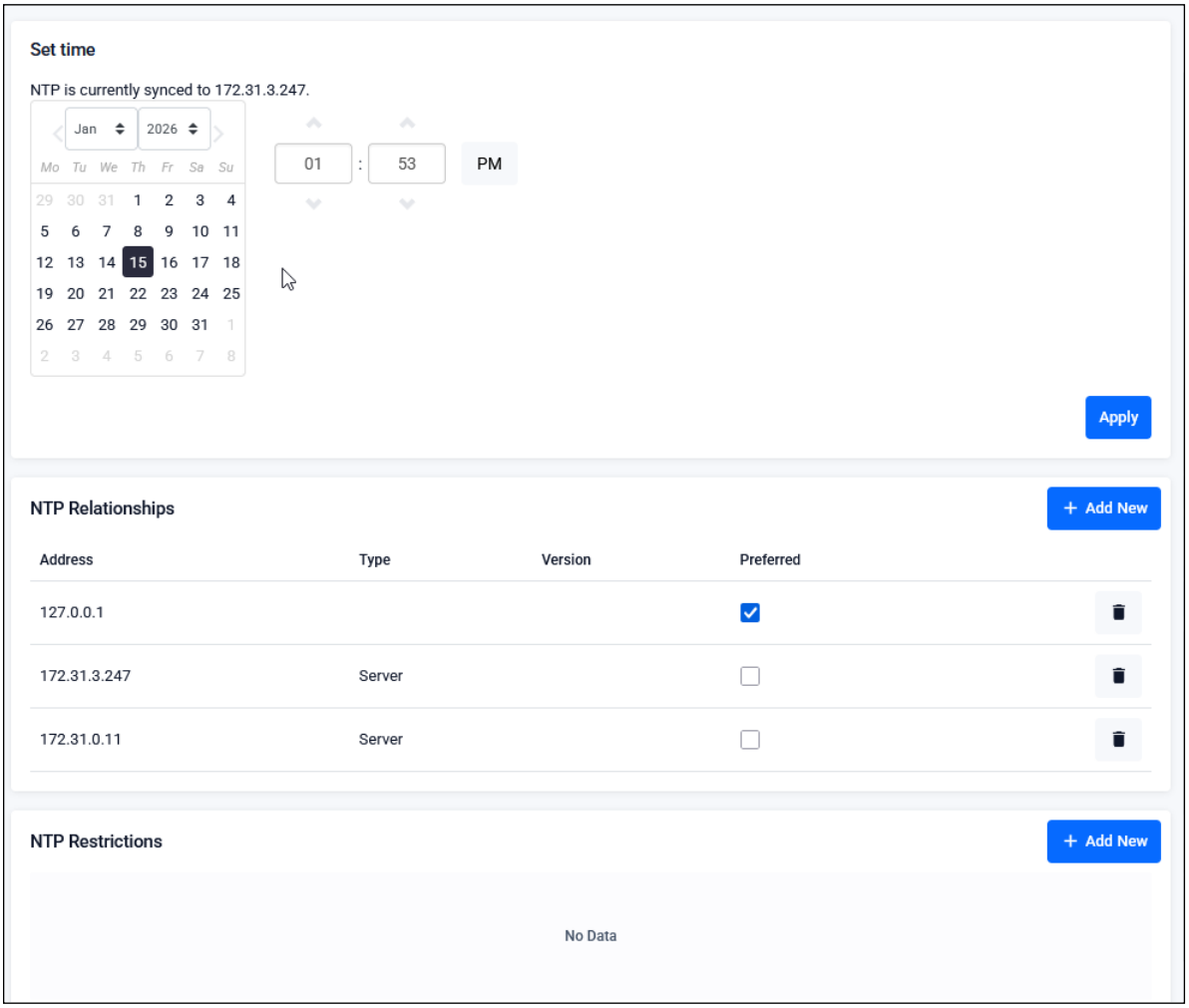
To set the GUI timeout click **System > About** from the menu bar and then select the **Configure** button:



You can select 5 minutes, 30 minutes, 1 hour, or disable the timeout completely. The default is 5 minutes.

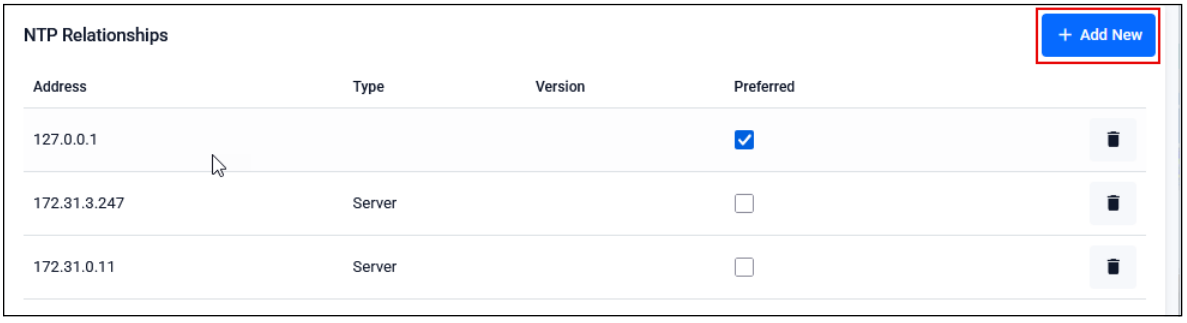
Set the time

To set the time click **System > Time** from the menu bar:

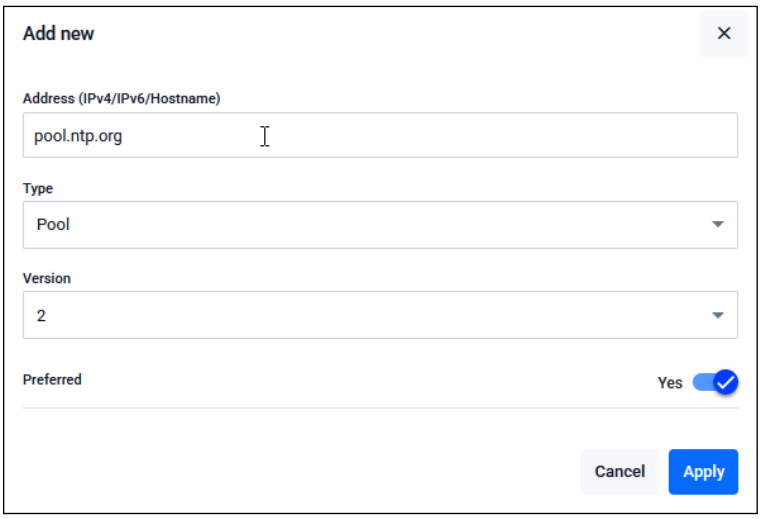


You can set the time manually with this dialog, or you can specify an NTP server to automatically get the time from. If you do not have an NTP server, you can use a public NTP service such as pool.ntp.org.

To set an NTP server with a public service, click on the **+Add New** button:



Enter the host name for the server and click **Apply**.

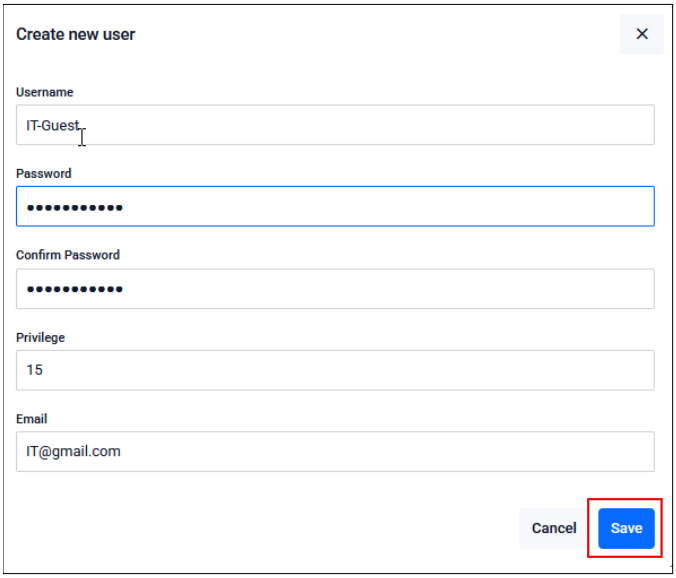


User Management

This section shows you how to add, edit and delete users that can access the Device GUI.

1. From **User Management** click **+New User**.

2. Enter the **Username**, **Password**, **Privilege** number and optional **Email** address.



The privilege level is 15 for users to access the device GUI.

3. Click **Save**.
4. To edit saved users use the **+Edit Password, +Edit Privilege** and **+Edit Email** buttons. To delete saved users click on the **Delete** button.
5. Click the **Save** button at the top right of the GUI screen (you may need to scroll up to see it).

Tip: The **Save** button is red anytime there is unsaved configuration and blue when it is saved.