Technical Guide

Allied Telesis™

Getting Started with the TQ6702 GEN2-R Wireless Router using the Device GUI

Introduction

The TQ6702 GEN2-R provides high-speed Wi-Fi 6 connectivity for wireless devices, and a secure Internet connection from the built-in VPN router. The 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, and remote access to cloud-based or head-office based business applications is assured using secure IPsec VPNs.

What information will you find in this document?

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

This guide shows you how to configure a TQ6702 GEN2-R Router using the Device GUI.

The Device GUI provides setup of the router, 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, VLAN, 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.

AlliedWare Plus™
OPERATING SYSTEM

Contents

Products and software version that apply to this guide

This guide applies to all Allied Telesis TQ6702 GEN2-R Routers running AlliedWare Plus™ software version 5.5.3-1.1 or later.

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.

Connecting to the wireless router

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

Supported web browsers for connecting to the Device GUI are:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge or Internet Explorer 11™
- Apple Safari™

Connecting to the GUI

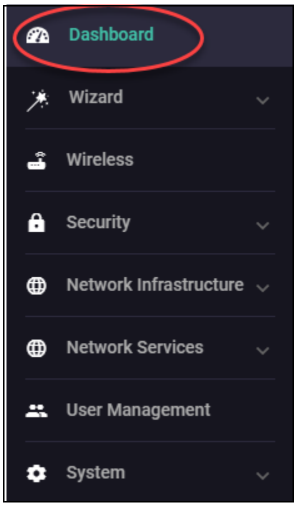
To connect to the GUI, use the following steps:

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

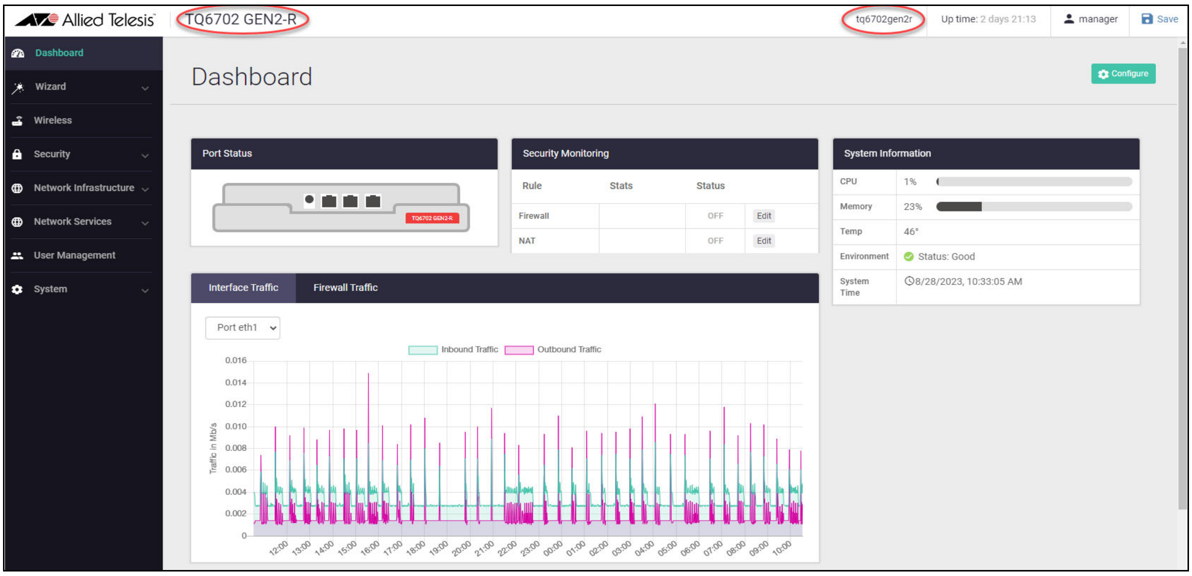
1. Connect to LAN1 (in the firmware this port is called eth1)
2. Open a web browser and browse to the default IP address for Eth1.
   - The default IP address is 192.168.1.1
3. Log in with the default username of ***manager*** and the default password of ***friend***.

The wireless router’s dashboard

This section describes how to use the dashboard in the device’s GUI. This is the first dialog that you see after you log in. If you are in another menu and want to return back to the dashboard, click **Dashboard** from the menu bar:



The **Dashboard** is displayed.



Security Monitoring

Rule	Stats	Status	
Firewall		OFF	Edit
NAT		OFF	Edit

System Information

CPU	1%
Memory	23%
Temp	46°
Environment	Status: Good
System Time	8/28/2023, 10:33:05 AM

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.

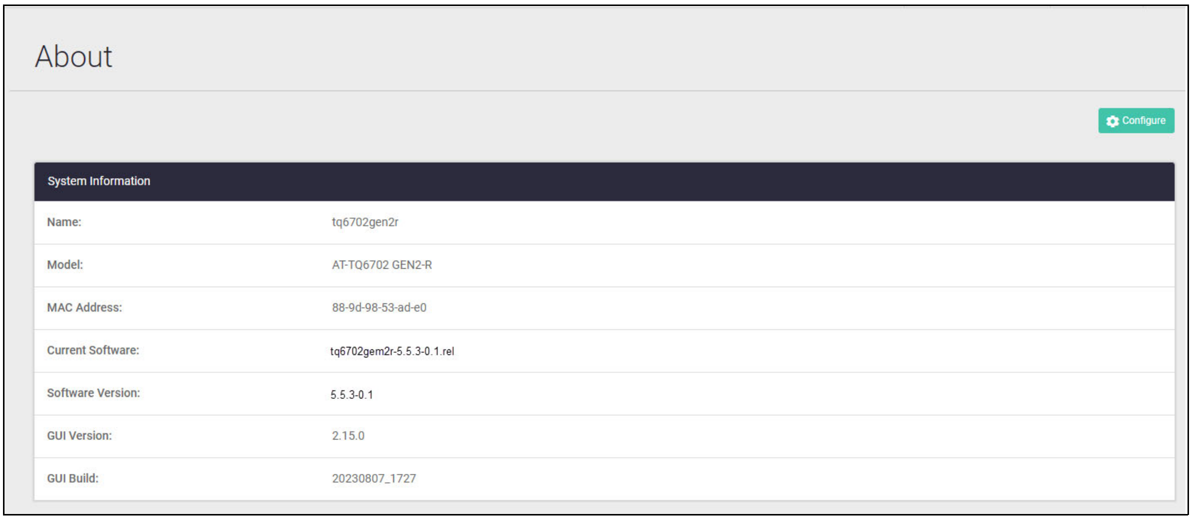
The menu bar

From here you can access the **Wizard**, **Wireless**, **Security**, **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.

Product info

You can identify your product type and host name which are displayed on the top menu bar, in this case it is identifying the TQ6702 GEN2-R router as the product type with the host name tq6702gen2r.

From the menu bar you can also select **System > About** to show more detail about your router, such as the host name, model, MAC address, current software and version, and also GUI build and version:



About

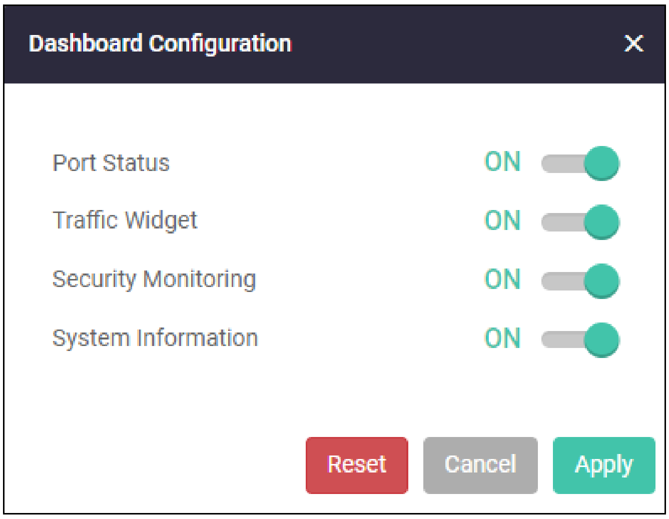
System Information	
Name:	tq6702gen2r
Model:	AT-TQ6702 GEN2-R
MAC Address:	88-9d-98-53-ad-e0
Current Software:	tq6702gem2r-5.5.3-0.1.rel
Software Version:	5.5.3-0.1
GUI Version:	2.15.0
GUI Build:	20230807_1727

The name displayed in this dialog is the host name of your device. In this example the host name has been configured as tq6702gen2r.

Monitoring your router

The **Port Status**, **Traffic Widget**, **Security Monitoring** and **System Information** 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 dialog:

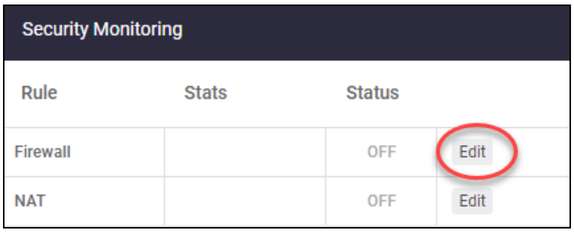


Dashboard Configuration

Port Status	ON
Traffic Widget	ON
Security Monitoring	ON
System Information	ON

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

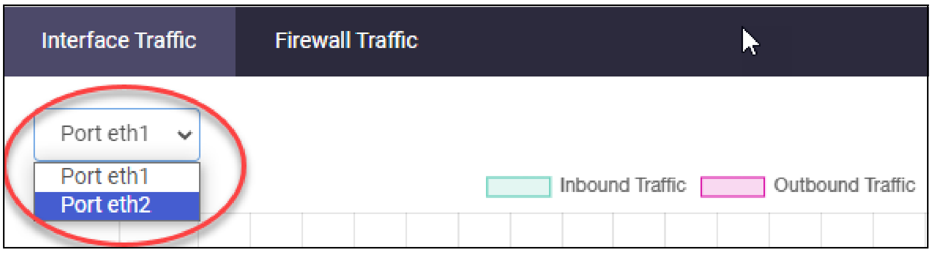
From **Security Monitoring** you can create or edit Firewall or NAT rules directly from the dashboard. For example click on the **Edit** button to create or edit a firewall rule:



Security Monitoring

Rule	Stats	Status	
Firewall		OFF	Edit
NAT		OFF	Edit

On the Interface and Firewall Traffic displays, you can choose which interface (eth1 or eth2) to show information for:



Save your config

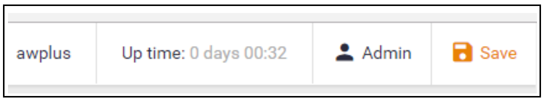
When you configure the wireless router through its GUI, the configuration becomes part of its running-configuration.

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. This enables you to roll back to the previous version if your configuration fails.

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

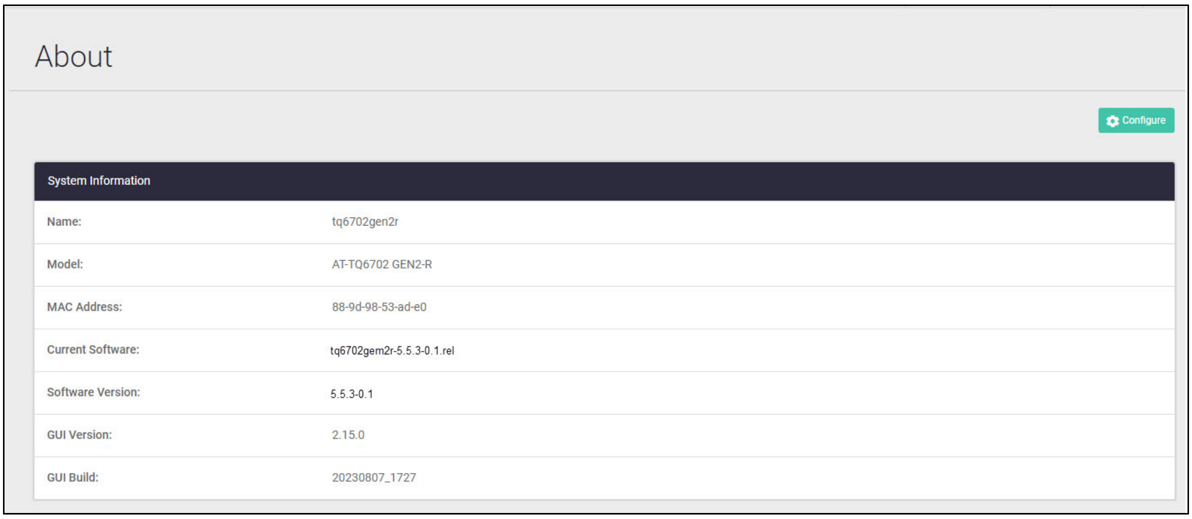
Tip: The **Save** button is orange anytime there is unsaved configuration.



Managing the wireless router firmware and configuration

Check the firmware version

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



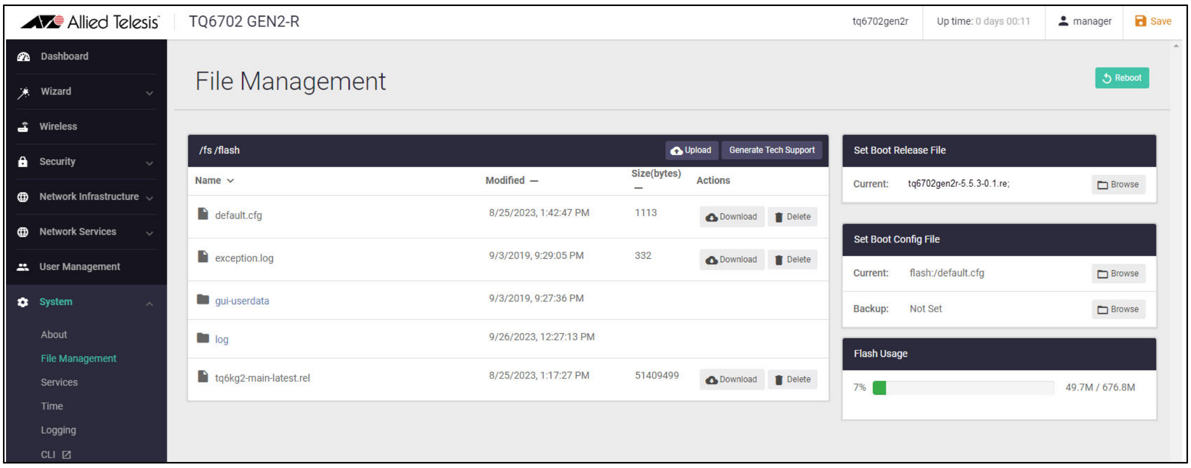
About

System Information	
Name:	tq6702gen2r
Model:	AT-TQ6702 GEN2-R
MAC Address:	88-9d-98-53-ad-e0
Current Software:	tq6702gem2r-5.5.3-0.1.rel
Software Version:	5.5.3-0.1
GUI Version:	2.15.0
GUI Build:	20230807_1727

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 easy firmware upgrade.

The **File Management** page can be found under the **System** menu:



File Management

/fs /flash

Name	Modified	Size(bytes)	Actions
default.cfg	8/25/2023, 1:42:47 PM	1113	Download Delete
exception.log	9/3/2019, 9:29:05 PM	332	Download Delete
gui-userdata	9/3/2019, 9:27:36 PM		
log	9/26/2023, 12:27:13 PM		
tq6kg2-main-latest.rel	8/25/2023, 1:17:27 PM	51409499	Download Delete

Set Boot Release File

Current: tq6702gen2r-5.5.3-0.1.re; Browse

Set Boot Config File

Current: flash:/default.cfg Browse

Backup: Not Set Browse

Flash Usage

7% 49.7M / 676.8M

Upgrade the firmware

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

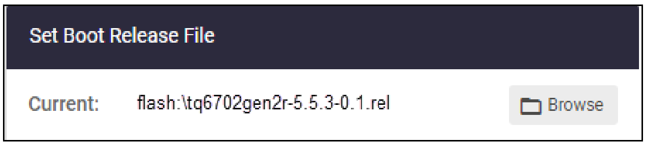
Step 1: **Download the new firmware file**

Download it from the Allied Telesis Download Center 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 dialog.

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

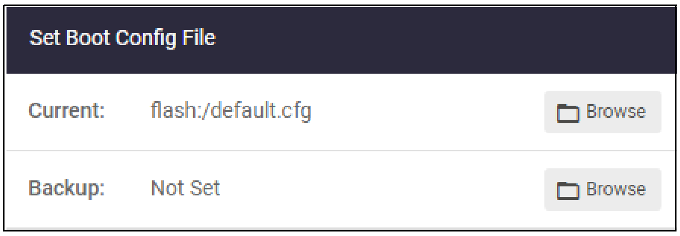


Set Boot Release File

Current: flash:\tq6702gen2r-5.5.3-0.1.rel

Click on the **Browse** button to select the correct release file you want to use on reboot.

Step 4: **Backup Boot Config file**



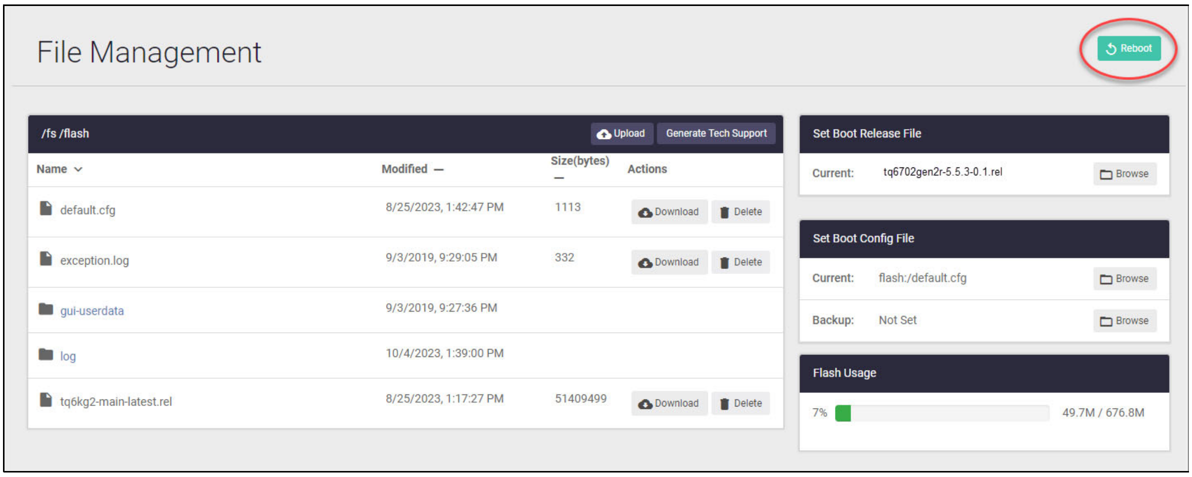
Set Boot Config File

Current: flash:/default.cfg

Backup: Not Set

It is not possible to set a Backup Boot Config File. Currently this is not supported.

Step 5: **Reboot the device.**



File Management

/fs /flash

Name	Modified	Size(bytes)	Actions
default.cfg	8/25/2023, 1:42:47 PM	1113	Download Delete
exception.log	9/3/2019, 9:29:05 PM	332	Download Delete
gui-userdata	9/3/2019, 9:27:36 PM		
log	10/4/2023, 1:39:00 PM		
tq6kg2-main-latest.rel	8/25/2023, 1:17:27 PM	51409499	Download Delete

Set Boot Release File

Current: tq6702gen2r-5.5.3-0.1.rel

Set Boot Config File

Current: flash:/default.cfg

Backup: Not Set

Flash Usage

7% 49.7M / 676.8M

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

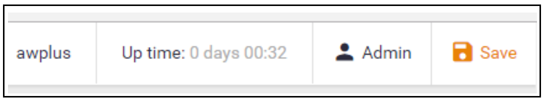
When you configure the wireless router through its GUI, the configuration becomes part of its running-configuration.

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 will be orange anytime there is unsaved configuration.

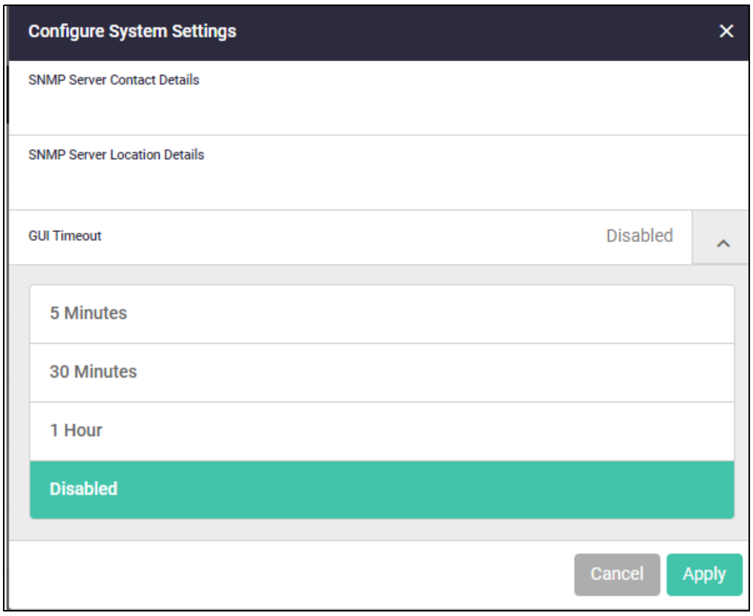


awplus

Up time: 0 days 00:32

Change the GUI timeout

If you want to, you can change the GUI timeout. The default is 5 minutes. To change it click **System > About** from the main menu bar and then select the **Configure** button:



Configure System Settings

SNMP Server Contact Details

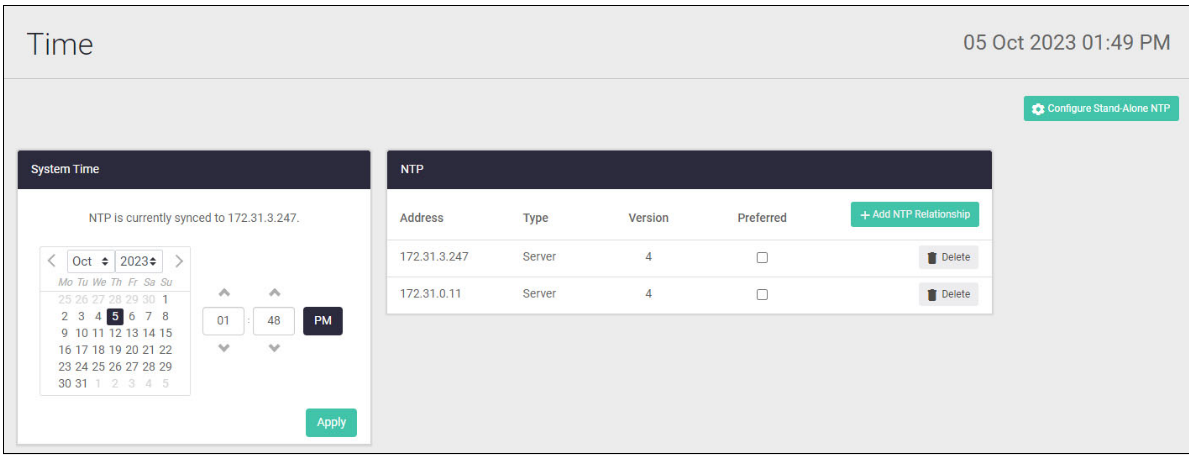
SNMP Server Location Details

GUI Timeout: Disabled

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

Set the time

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



Time — 05 Oct 2023 01:49 PM

Configure Stand-Alone NTP

System Time

NTP is currently synced to 172.31.3.247.

Oct 2023

Mo	Tu	We	Th	Fr	Sa	Su
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

01 : 48 PM

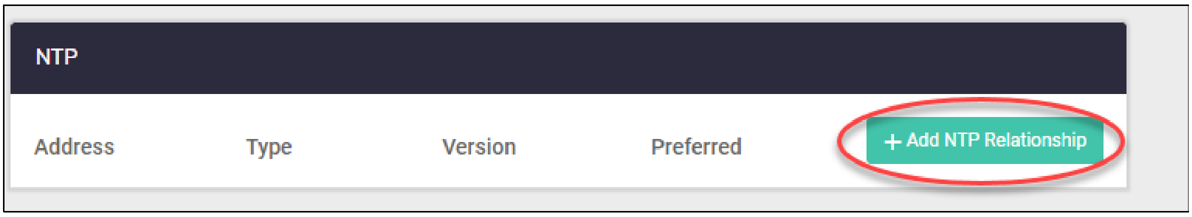
Apply

NTP

Address	Type	Version	Preferred	+ Add NTP Relationship
172.31.3.247	Server	4	□	Delete
172.31.0.11	Server	4	□	Delete

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.

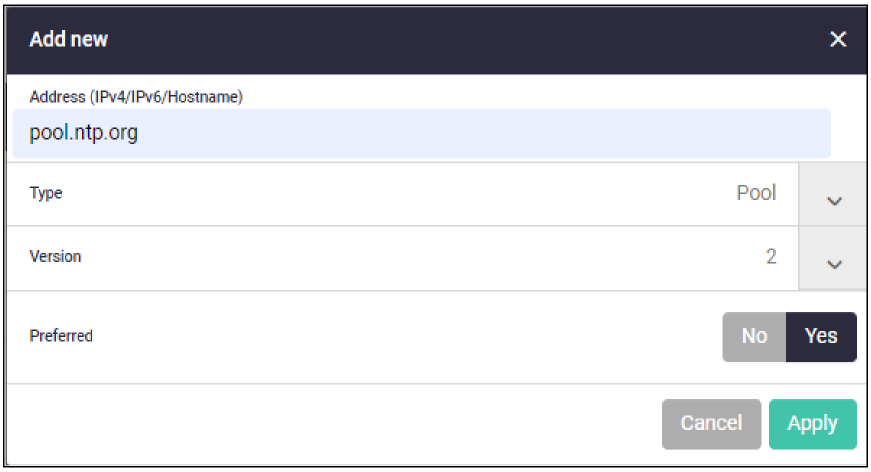
To set an NTP server with a public service, click on the **+Add NTP Relationship button**:



NTP

Address	Type	Version	Preferred	+ Add NTP Relationship

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



Add new ✕

Address (IPv4/IPv6/Hostname): pool.ntp.org

Type: Pool

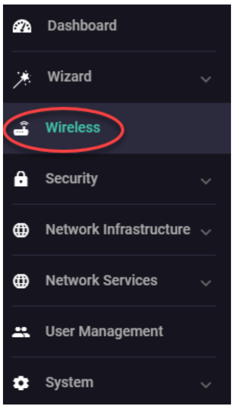
Version: 2

Preferred: No | Yes

Cancel | Apply

Configuring a Wi-Fi network

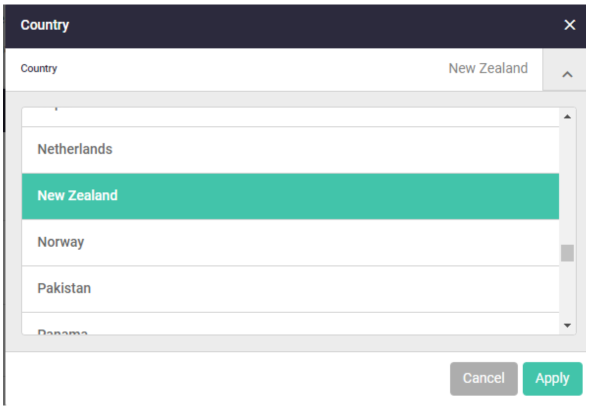
The device GUI includes a Wireless Management menu, which enables you to set up and monitor your wireless network:



The **Wireless** menu displays your wireless settings for General, Radio1, Radio2, Clients and Neighbor APs. The following steps show how to set up your Wi-Fi network.

Step 6: Select your country

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

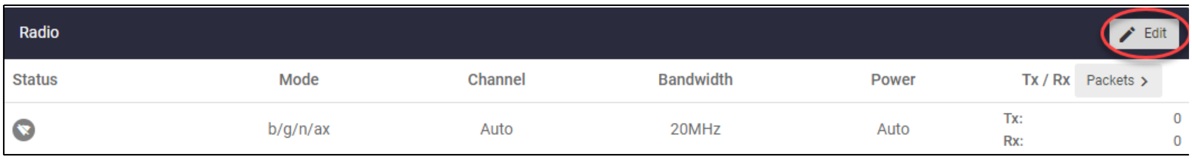


Country

Country New Zealand

Step 7: Enable the radio

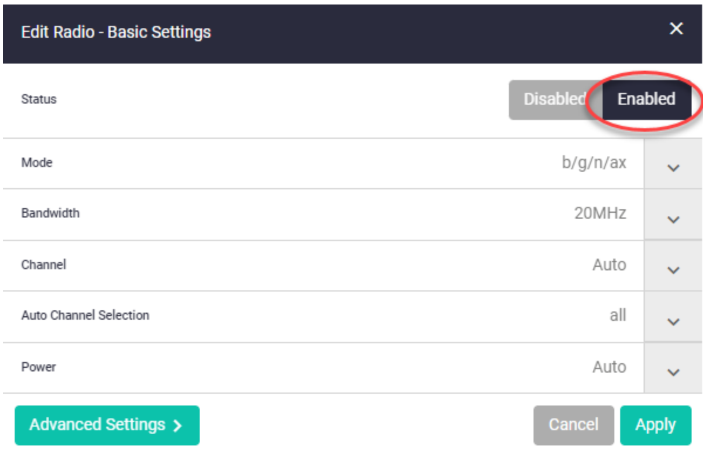
From the **Radio1** tab, click the **Edit** button from the **Radio** dialog:



Radio

Status	Mode	Channel	Bandwidth	Power	Tx / Rx
	b/g/n/ax	Auto	20MHz	Auto	Tx: 0 Rx: 0

The **Edit Radio-Basic Settings** dialog is displayed:



Edit Radio - Basic Settings

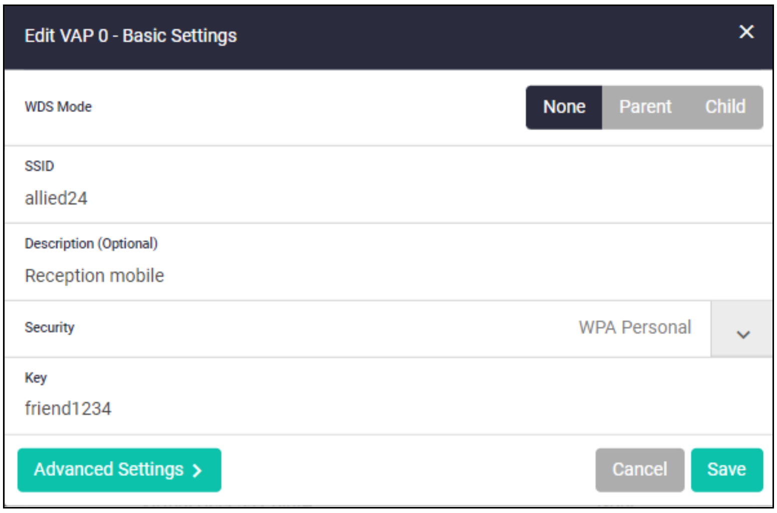
Status	Disabled [✓ Enabled]
Mode	b/g/n/ax
Bandwidth	20MHz
Channel	Auto
Auto Channel Selection	all
Power	Auto

Click the **Enabled** button.

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

Step 8: Set up the VAP 0 interface

Click on the **Edit** button from the VAP 0 interface:



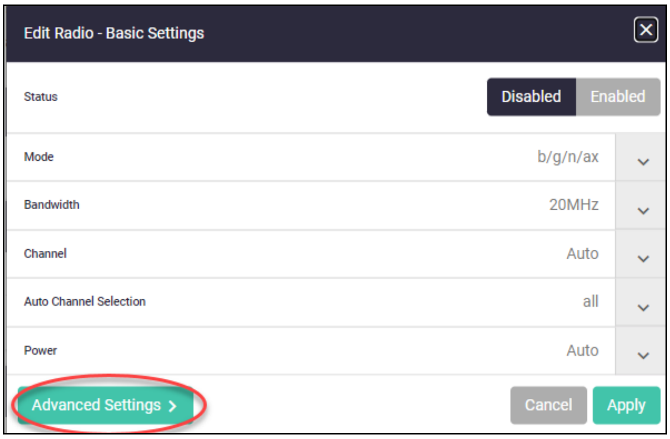
Edit VAP 0 - Basic Settings

WDS Mode	[✓ None] Parent Child
SSID	allied24
Description (Optional)	Reception mobile
Security	WPA Personal
Key	friend1234

- Enter the SSID name.
- From the security drop down list, select WPA personal.
- Set the key to a strong password.

Step 9: 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 click on **Advanced Settings**:



Edit Radio - Basic Settings

Status: Disabled | Enabled

Mode: b/g/n/ax

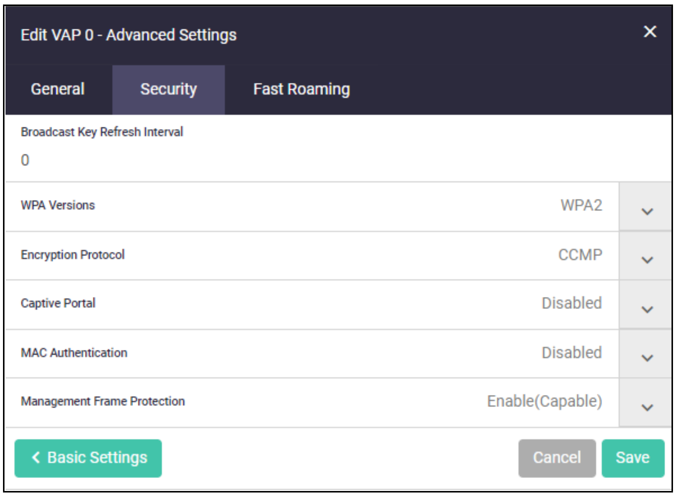
Bandwidth: 20MHz

Channel: Auto

Auto Channel Selection: all

Power: Auto

From the **Edit VAP 0 Advanced Settings** dialog, click on the **Security** tab:



Edit VAP 0 - Advanced Settings

General | Security | Fast Roaming

Broadcast Key Refresh Interval: 0

WPA Versions: WPA2

Encryption Protocol: CCMP

Captive Portal: Disabled

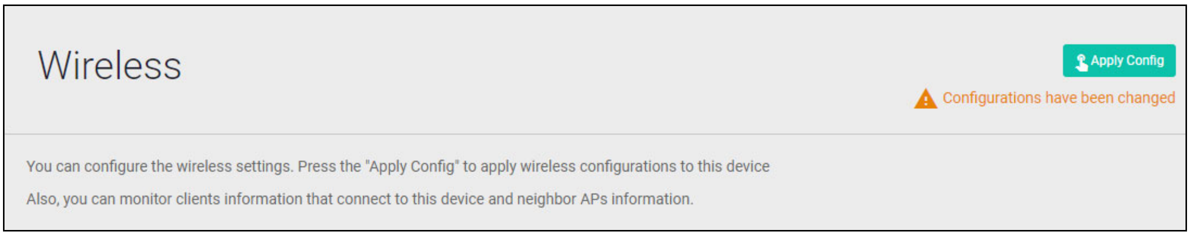
MAC Authentication: Disabled

Management Frame Protection: Enable(Capable)

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

Step 10: **Apply your configuration**

Click the **Apply Config** button to apply the settings to the radio:



Wireless

Configurations have been changed

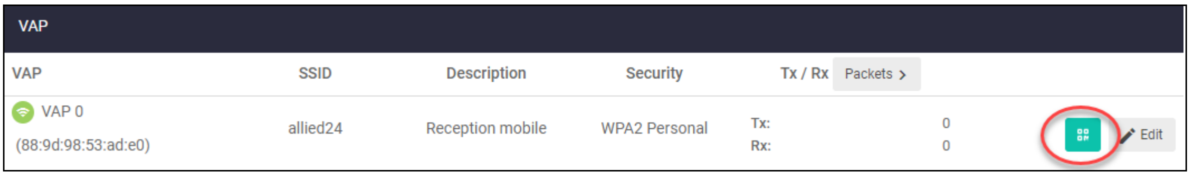
You can configure the wireless settings. Press the "Apply Config" to apply wireless configurations to this device

Also, you can monitor clients information that connect to this device and neighbor APs information.

Step 11: **Create a QR code for clients to use**

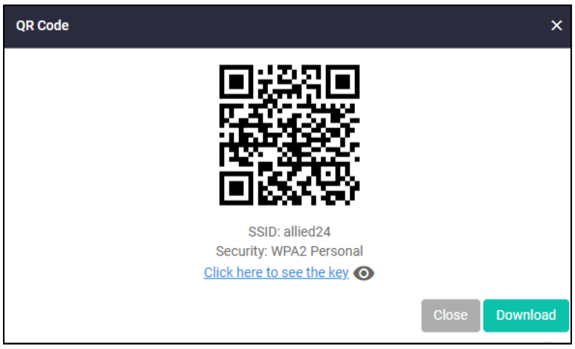
From the **Wireless** page you can create a QR code that you can use to connect a device to join the wireless network.

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



VAP

VAP	SSID	Description	Security	Tx / Rx Packets >	
VAP 0 (88:9d:98:53:ad:e0)	allied24	Reception mobile	WPA2 Personal	Tx: 0 Rx: 0	Edit



QR Code

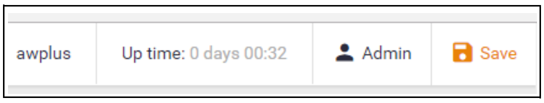
SSID: allied24
Security: WPA2 Personal
Click here to see the key

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

Step 12: Save the configuration

We recommend backing up the default configuration file before you first save the configuration. Make a copy of the file and save it so that you can reinstate it later if your configuration fails.

Once you have confirmed the configuration works, click the **Save** button to save the configuration, so that it persists if the wireless router reboots.

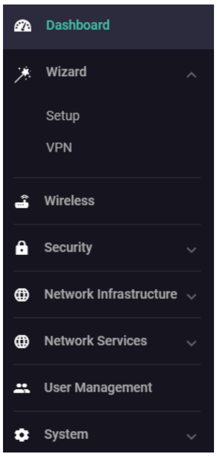


awplus | Up time: 0 days 00:32 | Admin | Save

Note: This saves the device’s whole configuration, not only the wireless configuration.

Using the Wizard to configure Internet connections

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



Setup an Internet connection

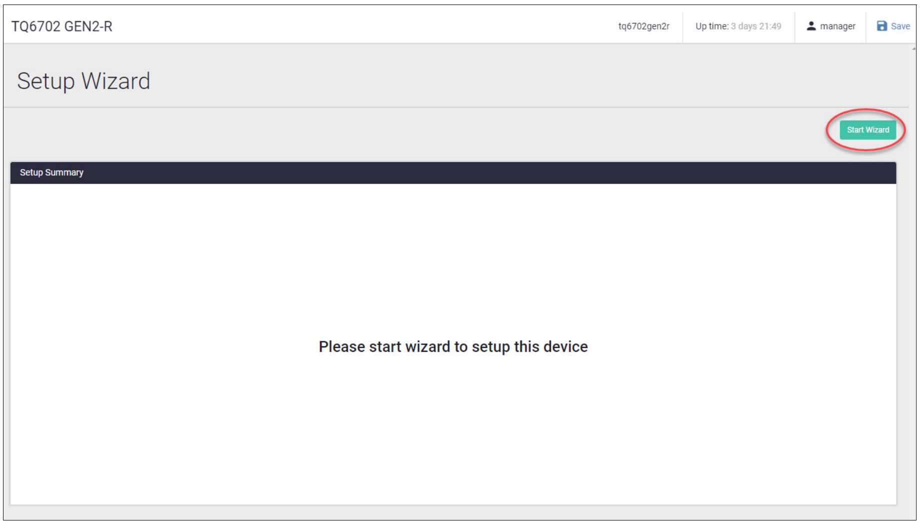
You can use the wizard to set up a router's WAN interface along with creating a basic configuration for a LAN. There are three IPv4 methods available: DHCP, Fixed IP, and PPPoE, and two IPv6 methods available: IPoE and V6 Transition (IPv4 over IPv6).

Once the wizard has run, the Setup 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:

Step 1: **Start the Wizard.**

- Click the **Start Wizard** button.
- If you don't have an Internet connection setup, you'll see a blank **Setup Summary** screen:

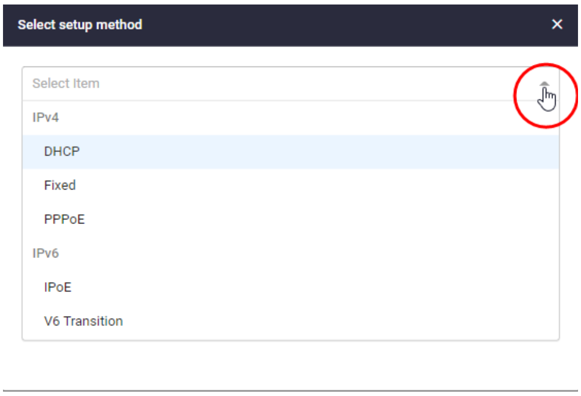


Please start wizard to setup this device

- If you do have an Internet connection setup, then you'll see those details displayed in the **Setup Summary** screen. Click the **Start Wizard** button in that same screen to reconfigure your current Internet connection settings.

Step 2: **Choose a connection method.**

- Select a method to connect to the Internet.



Select setup method

Select Item

IPv4

DHCP

Fixed

PPPoE

IPv6

IPoE

V6 Transition

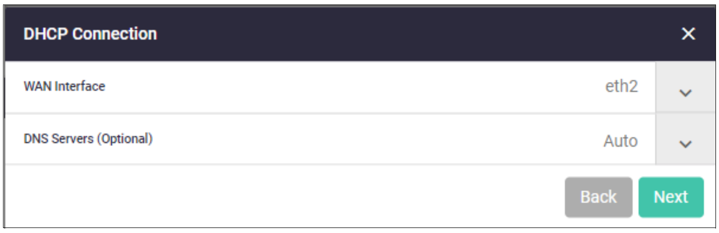
Step 3: **Configure the connection method.**

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

Configure the IPv4 DHCP connection:



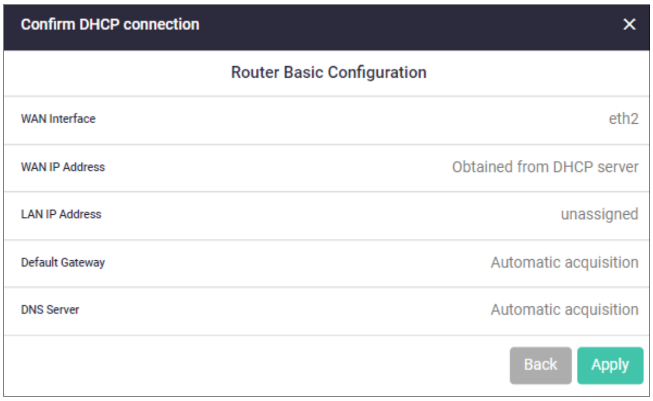
DHCP Connection

WAN Interface: eth2

DNS Servers (Optional): Auto

Field	Description
WAN interface	The interface used to connect to the Internet, eth2.
DNS Servers	Specifies the DNS server to use for name resolution. ■ If you want DHCP to automatically obtain a DNS server address, use the default **Auto**. ■ If fixed settings are required, click the down arrow on the right, click **+ Add DNS Server**, and enter the IP address of the DNS server.

Click on the **Next** button to display the confirm DHCP connection dialog:



Confirm DHCP connection

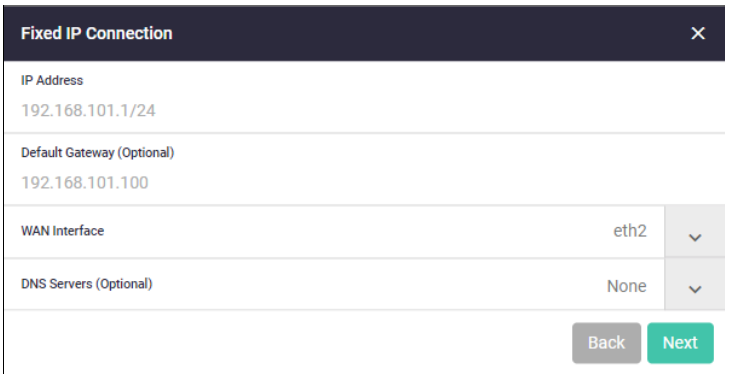
Router Basic Configuration

WAN Interface	eth2
WAN IP Address	Obtained from DHCP server
LAN IP Address	unassigned
Default Gateway	Automatic acquisition
DNS Server	Automatic acquisition

Click the **Apply** button to confirm your DHCP connection configuration.

IPv4 - Fixed IP Connection

Configure the IPv4 fixed IP connection:



Fixed IP Connection

IP Address: 192.168.101.1/24

Default Gateway (Optional): 192.168.101.100

WAN Interface: eth2

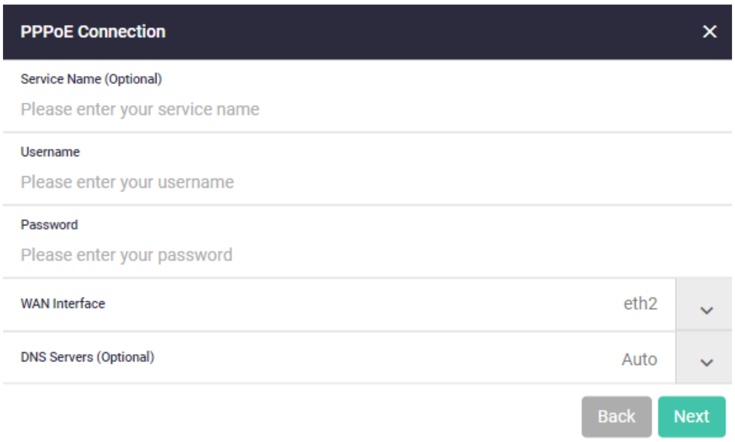
DNS Servers (Optional): None

Field	Description
IP Address	Enter the IP address you want to configure for the WAN-side interface.
Default Gateway	Enter the IP address of the default gateway that you want to use to connect to the Internet.
WAN interface	Select the interface used to connect to the Internet.
DNS Servers	Specifies the DNS server to use for name resolution. Click the down arrow on the right, click **+ Add DNS Server**, and enter the IP address of the DNS server.

Click the **Apply** button to confirm your fixed IP connection.

IPv4 - PPPoE Connection

Configure the IPv4 PPPoE connection:



PPPoE Connection

Service Name (Optional)
Please enter your service name

Username
Please enter your username

Password
Please enter your password

WAN Interface eth2

DNS Servers (Optional) Auto

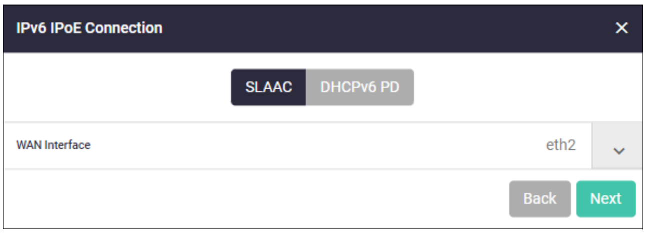
Field	Description
Service Name	This is the PPPoE service name. You can usually leave it blank. Enter the PPPoE service name only if your Internet service provider (ISP) has specified it.
Username	PPP user name. Enter the user name for the Internet connection notified by your ISP.
Password	PPP password. Enter the password for the Internet connection provided by your ISP.
WAN interface	This is the interface used to connect to the Internet.
DNS Servers	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, click the down arrow on the right, click **+ Add DNS Server**, and enter the IP address of the DNS server.

Click the **Apply** button to confirm your IPv4 PPPoE connection.

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).

Step 1: **SLAAC number (RA method)**

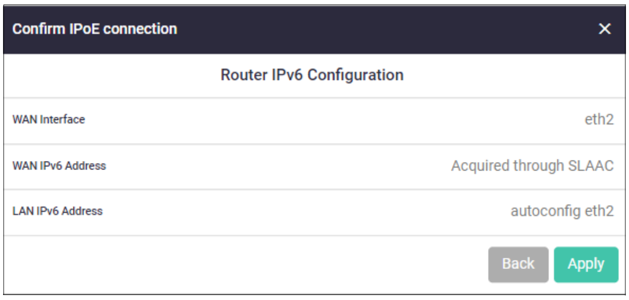


IPv6 IPoE Connection

WAN Interface eth2

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

- Click the drop down arrow to select the WAN interface.
- Click **Next.** The following confirmation window appears:



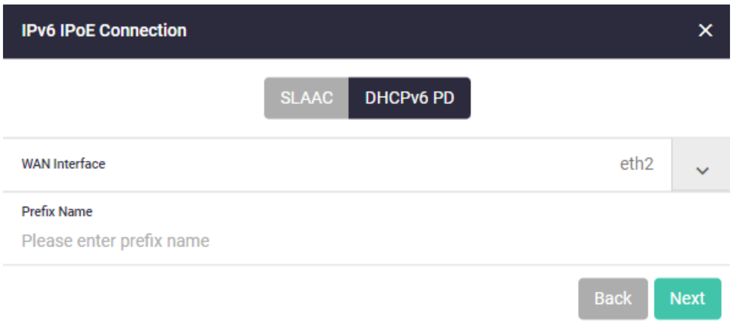
Confirm IPoE connection

Router IPv6 Configuration

WAN Interface	eth2
WAN IPv6 Address	Acquired through SLAAC
LAN IPv6 Address	autoconfig eth2

- Click the **Apply** button to confirm your IPoE connection.

Step 2: **DHCPv6 PD (Prefix Delegation)**



IPv6 IPoE Connection

SLAAC | DHCPv6 PD

WAN Interface: eth2

Prefix Name: Please enter prefix name

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.

- Click the drop down arrow to select the WAN interface.
- Enter a **Prefix Name**.
- Click **Next**

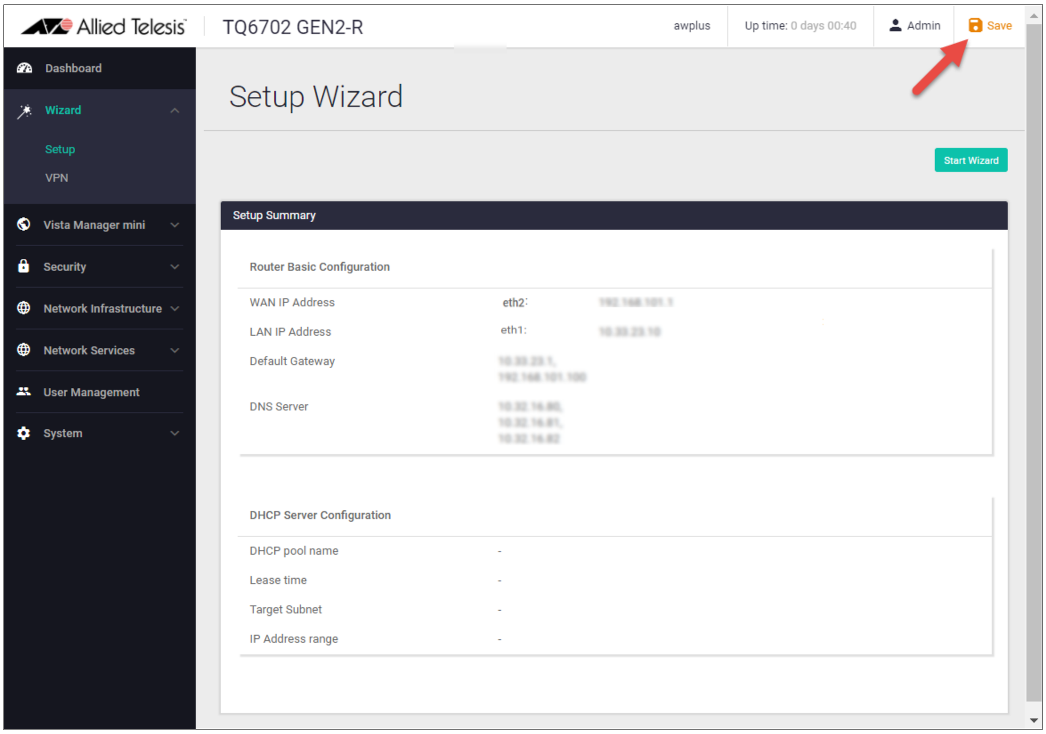
Step 3: **Check and Save the settings.**

- Check your configuration is correct and click **Save** to continue.

Step 4: **Save the settings to the startup configuration.**

When the configuration save is complete, a summary of the connection status is displayed.

- The contents set in the simple setting 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.
- You can run the Wizard again to make changes to your connection method settings.



Setup Summary

Router Basic Configuration

WAN IP Address	eth2:	[redacted]
LAN IP Address	eth1:	[redacted]
Default Gateway	[redacted]	
DNS Server	[redacted]	

DHCP Server Configuration

DHCP pool name	-
Lease time	-
Target Subnet	-
IP Address range	-

Configuring firewall and NAT

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

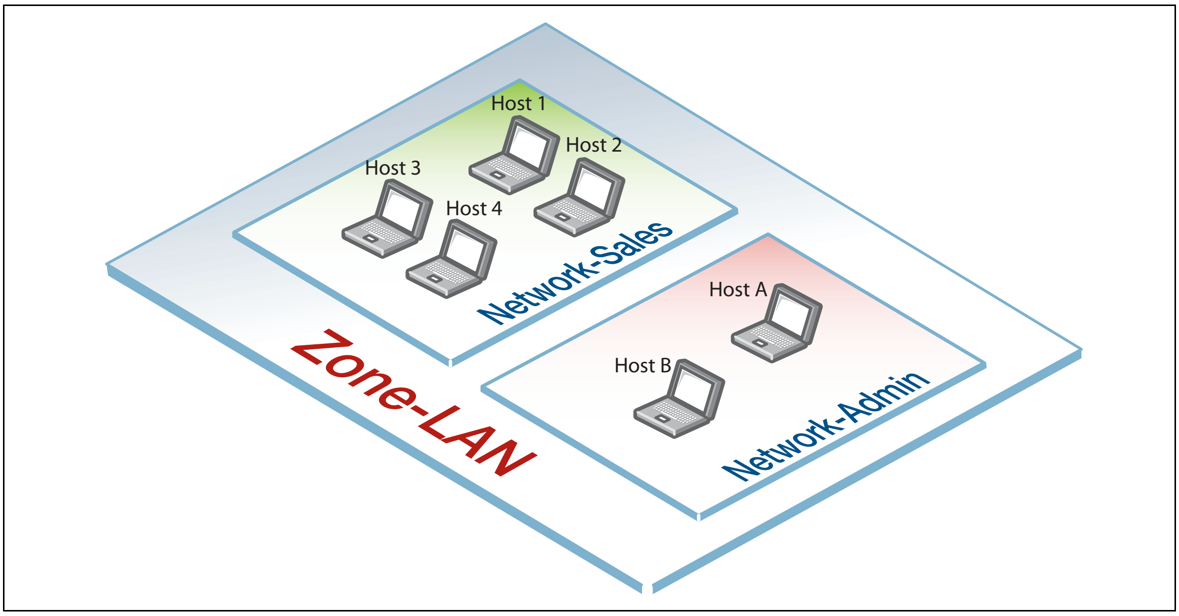
Applications can be created using a combination of protocol and port numbers, and then be used by firewall, NAT, and traffic control rules to manage traffic.

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 below shows PC Wilma 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.

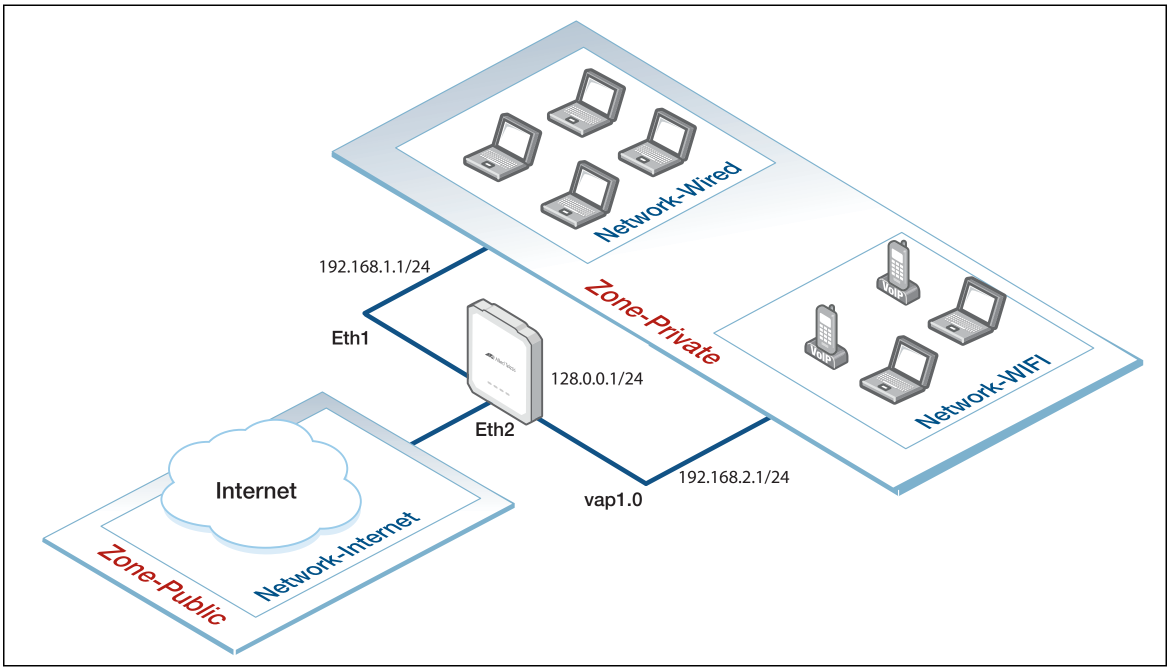
Network Address Translation (NAT) rules: hide private network addresses for traffic bound for the Internet. All company traffic leaving the corporate office can share a public network address for routing through the Internet to its destination.

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 **Configuring a Wi-Fi network** and
- the radio interface, see **Using the Wizard to configure Internet connections**

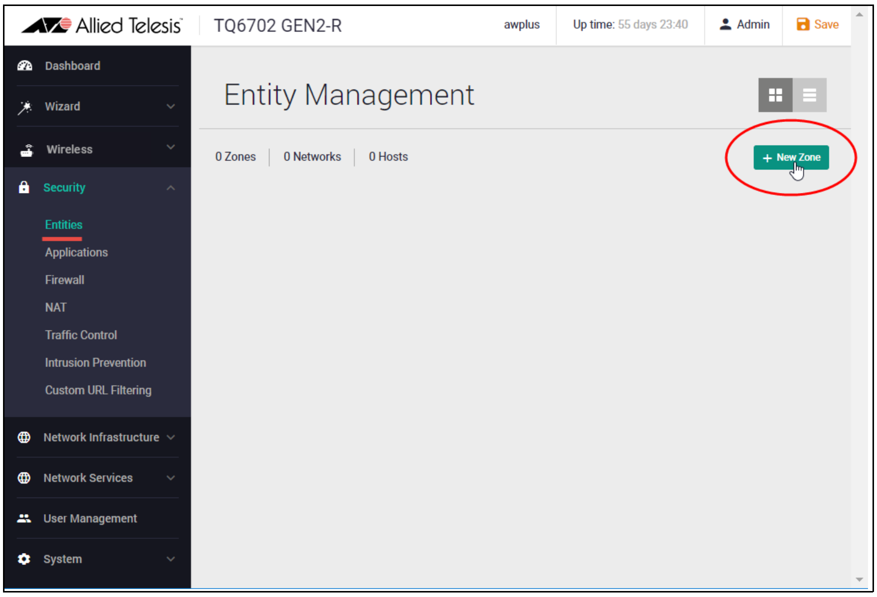
It uses the following IP addresses

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

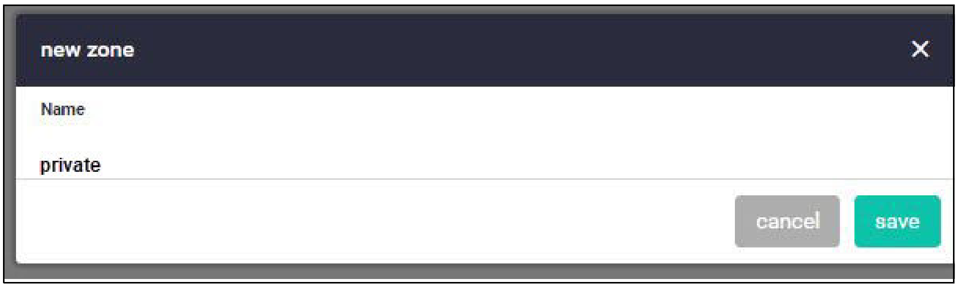
Step 1: **Configure Entities.**

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

- Select **Entities** from the **Security** menu.

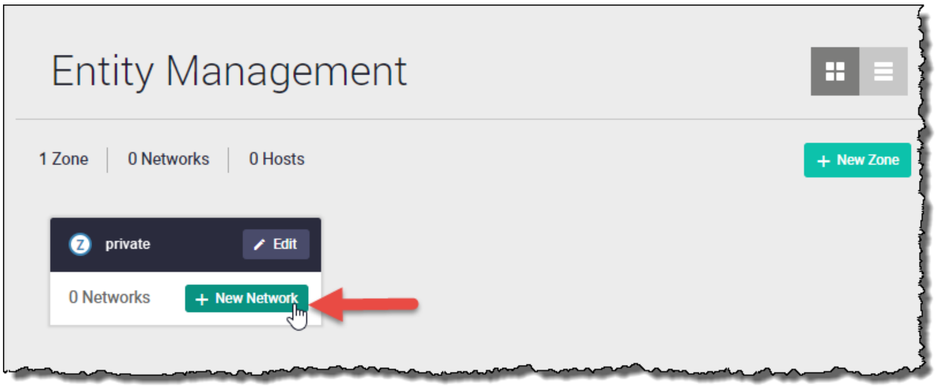


- As no entities have yet been created, click the green **+ New Zone** button to add a zone.
- The first zone we will add is the **private** zone to be used for wired clients that we want to be accessible from the Internet.

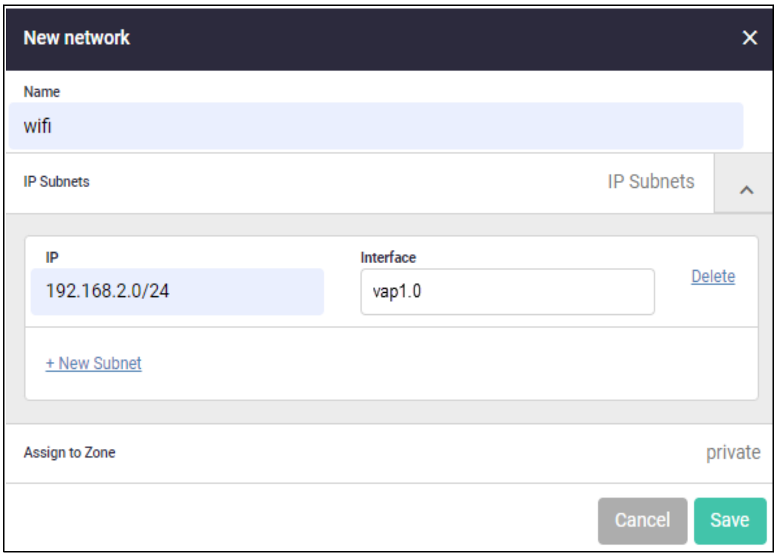


private

- Next click the green **+ New Network** button in the private zone to add the wired network.



- Name the new network wifi.
- Add the IP subnet 192.168.2.0/24 and **vap1.0** as the interface over which this network will be reachable.
- Click **Save**.



New network

Name: wifi

IP Subnets

IP: 192.168.2.0/24
Interface: vap1.0

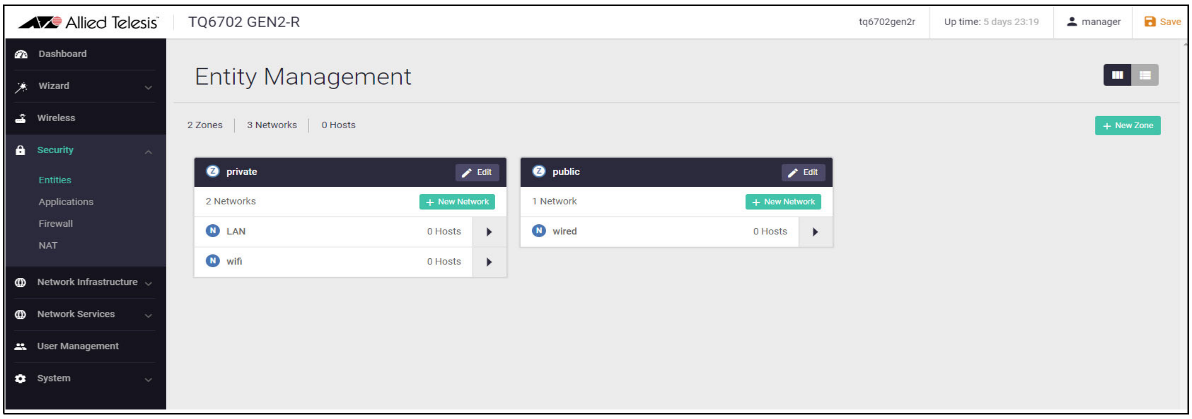
Assign to Zone: private

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.



Entity Management

2 Zones | 3 Networks | 0 Hosts

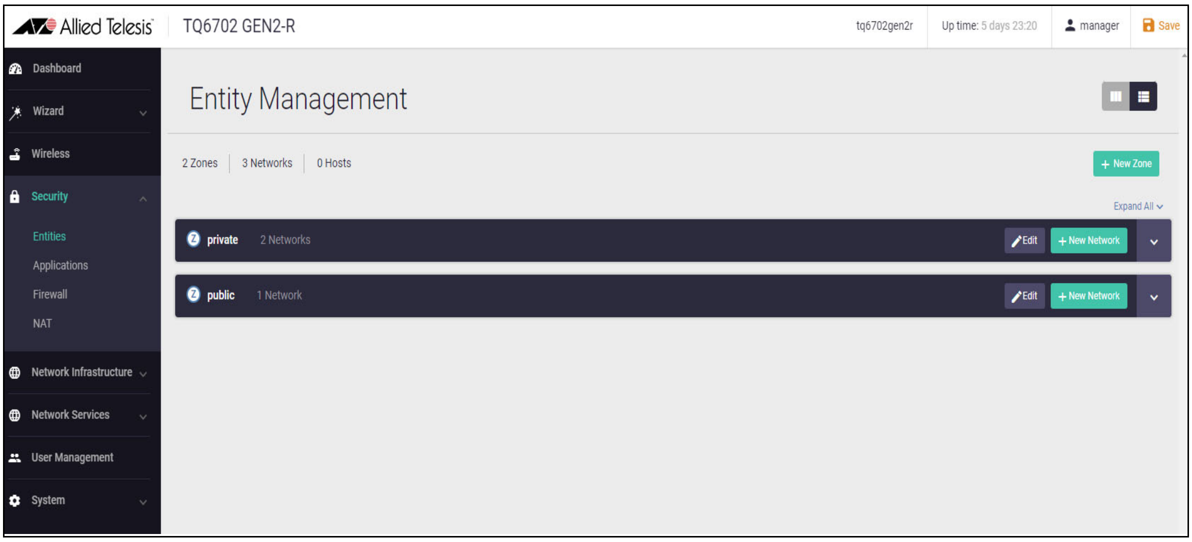
private: 2 Networks
- LAN 0 Hosts
- wifi 0 Hosts

public: 1 Network
- wired 0 Hosts

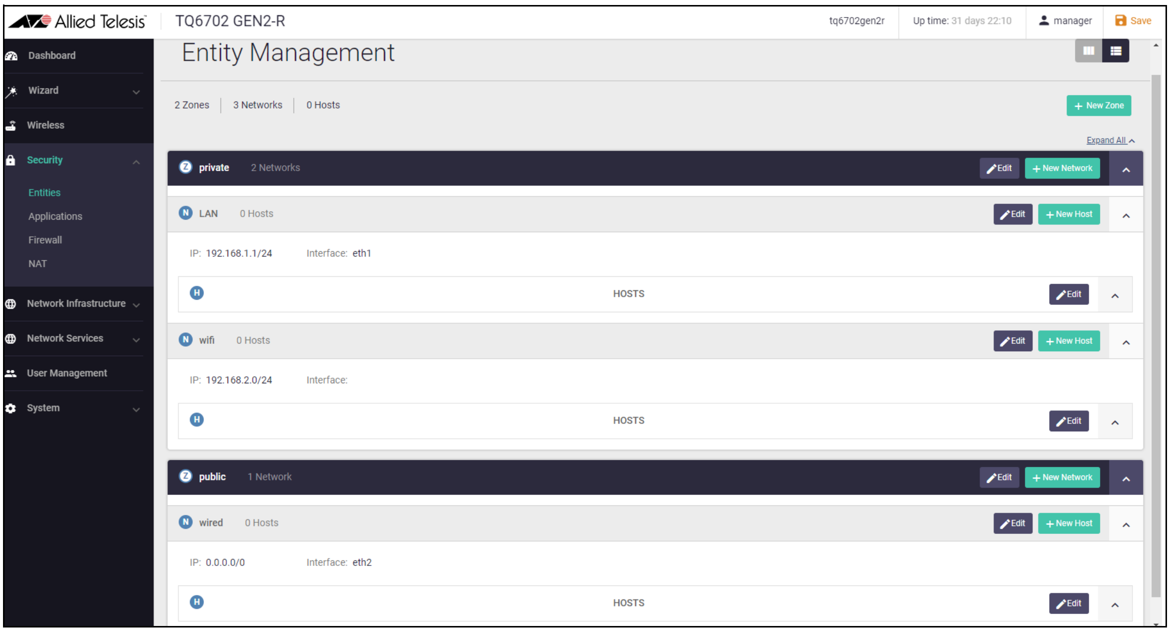
- Click the **Save** button at the top right of the window to continue.

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.



IP: 192.168.1.1/24 Interface: eth1

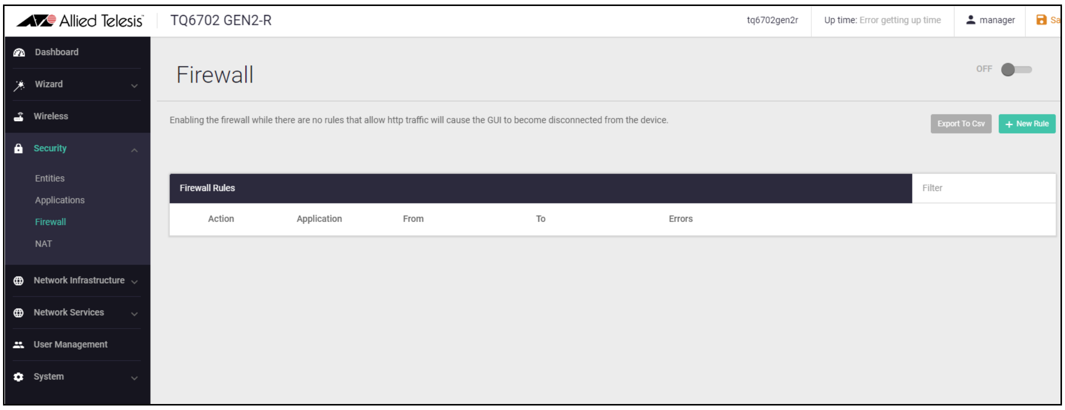
IP: 192.168.2.0/24 Interface:

IP: 0.0.0.0/0 Interface: eth2

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.

- Navigate to **Firewall** under the **Security** menu.



Enabling the firewall while there are no rules that allow http traffic will cause the GUI to become disconnected from the device.

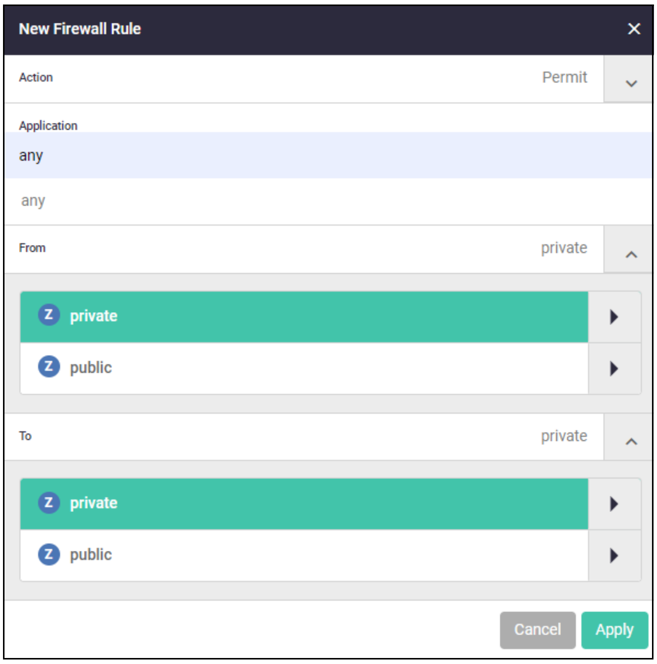
Action	Application	From	To	Errors

WARNING: Enabling the firewall with the **ON/OFF** 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:

- Click the **+New Rule** Button:



Action: Permit

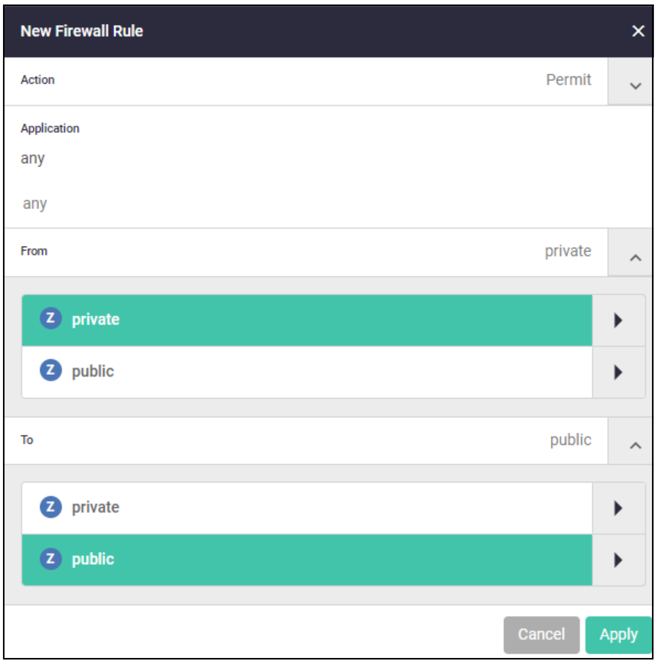
Application: any

From: private

To: private

Next, create a new rule to permit 'any' from private to public:

- Click the **+New Rule** Button:



New Firewall Rule

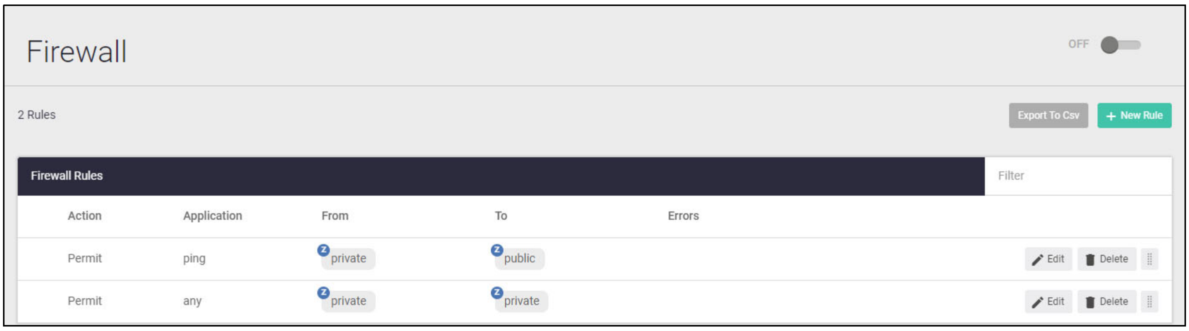
Action: Permit

Application: any

From: private

To: public

We can now see all these firewall rules displayed:

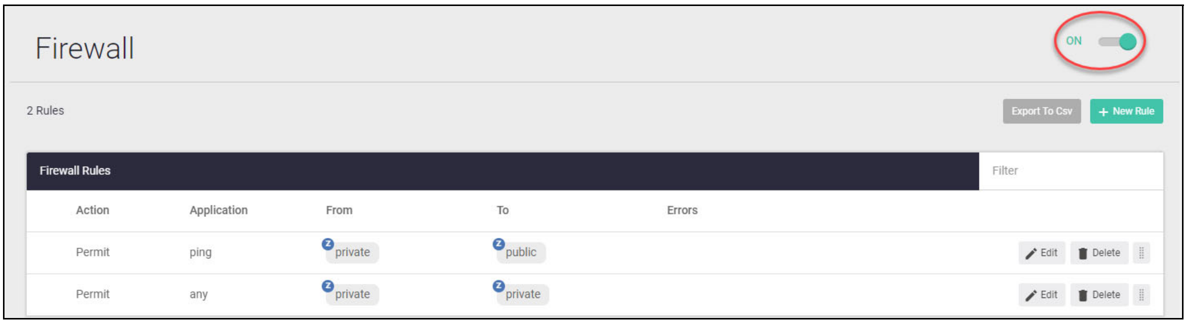


Firewall

2 Rules

Action	Application	From	To	Errors
Permit	ping	private	public	
Permit	any	private	private	

- Now that the firewall rules are created, you can turn the firewall **on** using the **ON/OFF** button at the top right of the Dashboard page.



Firewall

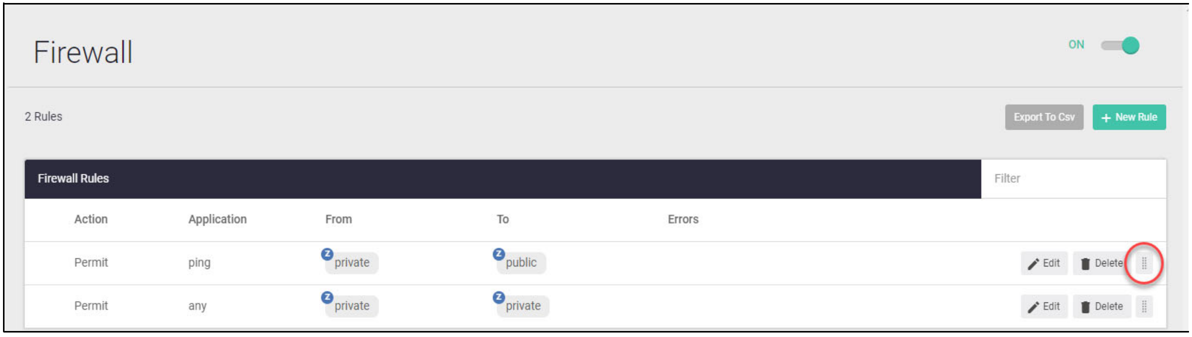
2 Rules

Action	Application	From	To	Errors
Permit	ping	private	public	
Permit	any	private	private	

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:



2 Rules

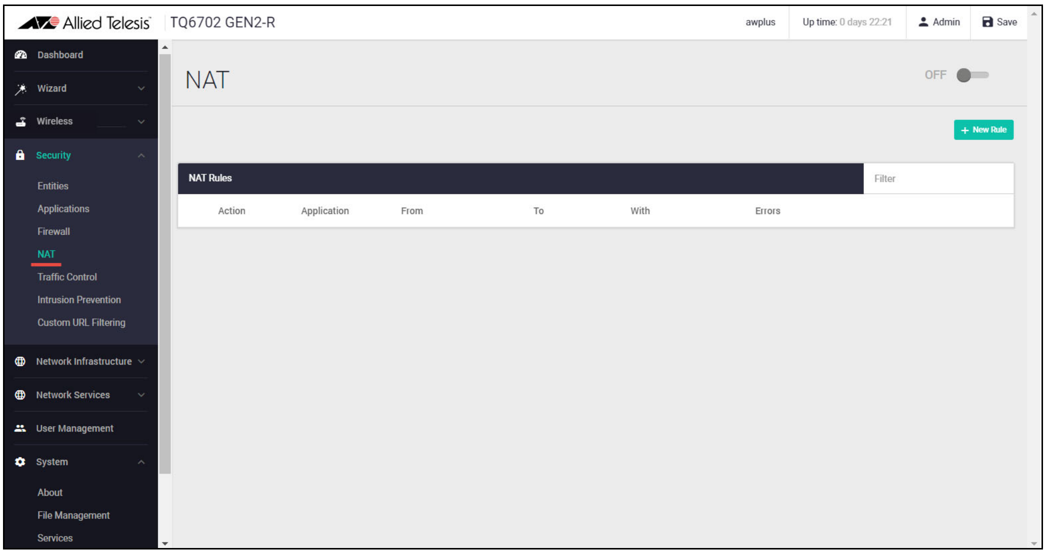
Firewall Rules

Action	Application	From	To	Errors
Permit	ping	private	public	
Permit	any	private	private	

Step 3: Configure NAT rules.

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

Navigate to **NAT** under the **Security** menu.



NAT Rules

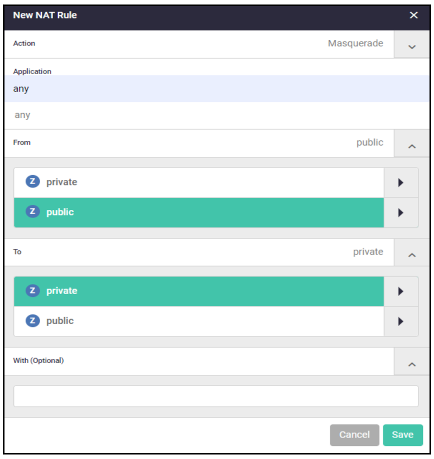
Action	Application	From	To	With	Errors

We need a NAT masquerade rule for private to public address translation, which are:

1. 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

Click **+ new rule** to create the first rule for Private to Public traffic:

- Action = Masquerade, Application = any, From = Private, To = Public



New NAT Rule

Action: Masquerade

Application: any

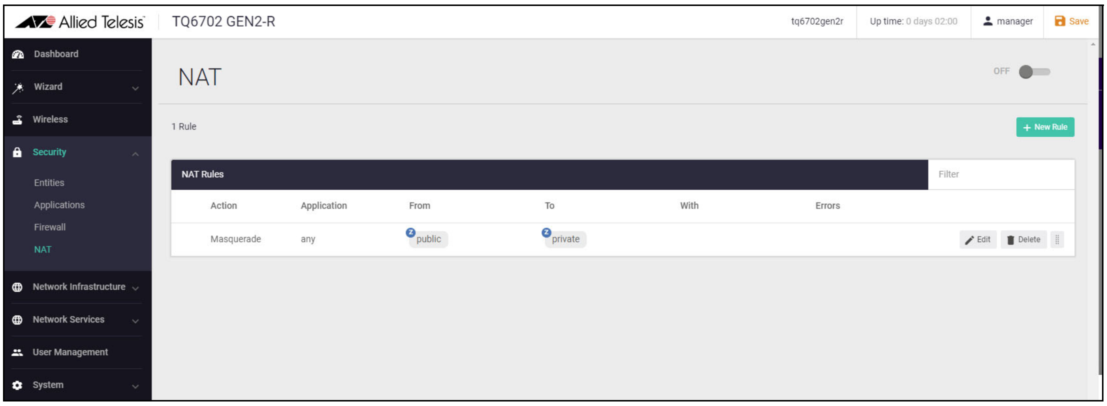
From: public

To: private

With (Optional)

Now click the **ON/OFF** button at the top right of the Dashboard page to activate NAT.

You can see the new NAT rule:



NAT

1 Rule

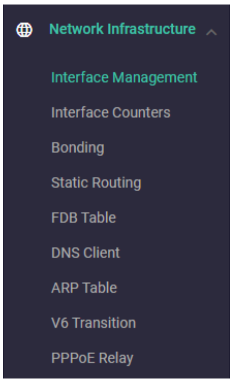
NAT Rules

Action	Application	From	To	With	Errors
Masquerade	any	public	private		

Step 4: **Save configuration changes.**

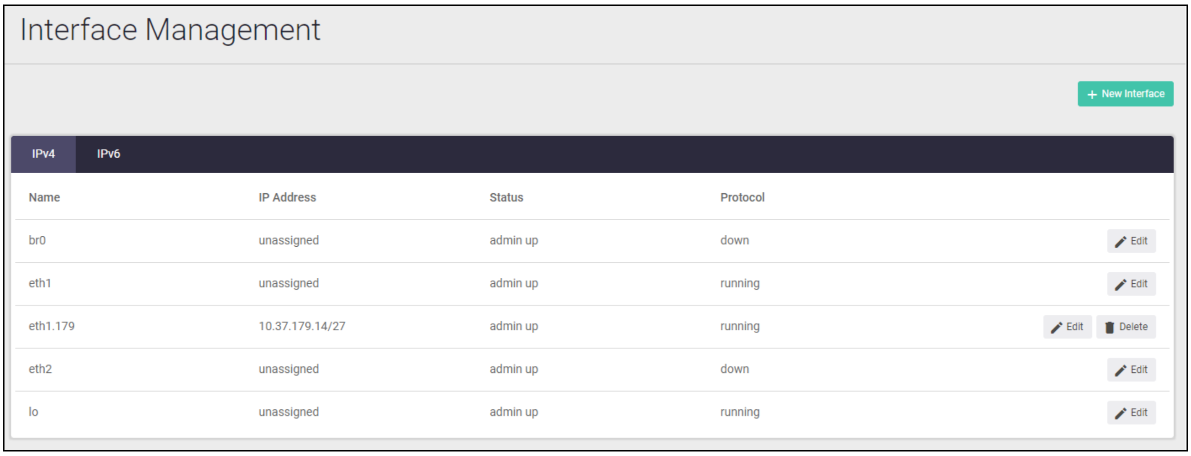
Network Infrastructure

From the Network Infrastructure menu you can access information about the network interfaces, interface counters, bonding, static routing, FDB table, DNS client, ARP table, IPv4 to IPv6 transition, and PPPoE relay:



Interface Management

From Interface Management you can display IPv4 and IPv6 Names, addresses, status and protocol. You can also edit the DHCP or fixed IP address or secondary IP address by clicking on the **Edit** button.

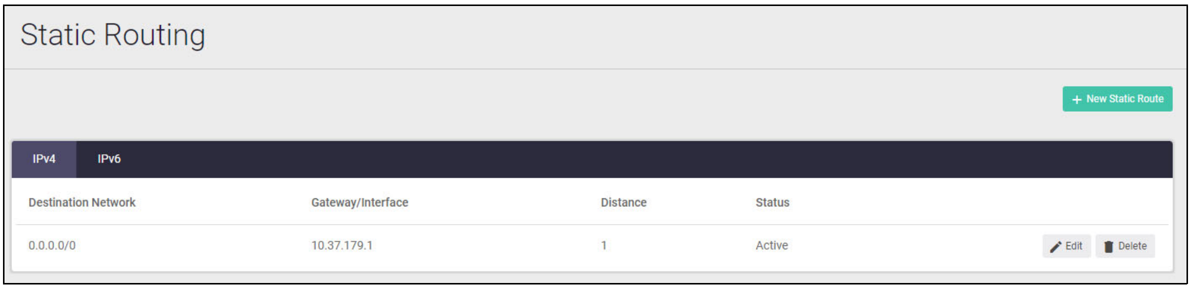


Name	IP Address	Status	Protocol	
br0	unassigned	admin up	down	Edit
eth1	unassigned	admin up	running	Edit
eth1.179	10.37.179.14/27	admin up	running	Edit Delete
eth2	unassigned	admin up	down	Edit
lo	unassigned	admin up	running	Edit

Click on **Interface Counters** to display information if ports are available to show the counters.

Static Routing

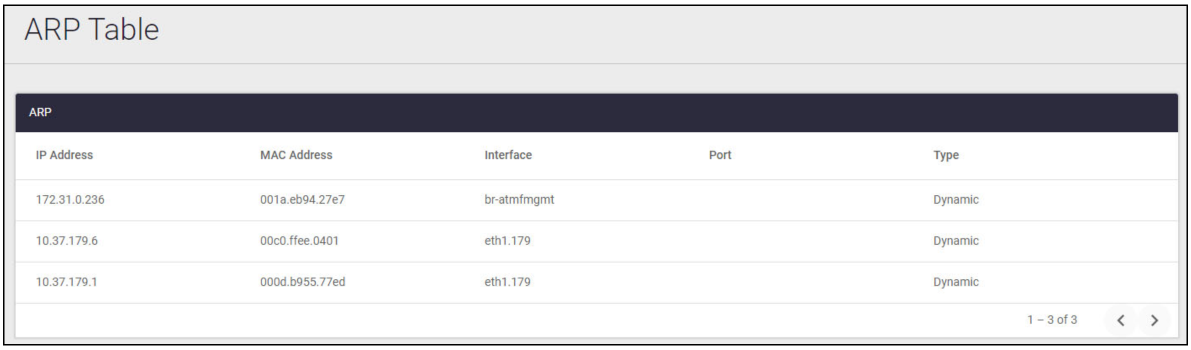
Static routing displays information about IPv4 and IPv4 destination and gateway interfaces, the distance and status. Click on the **Edit Static Route** button to change the destination network, gateway/interface or distance.



Destination Network	Gateway/Interface	Distance	Status	
0.0.0.0/0	10.37.179.1	1	Active	Edit Delete

ARP table

The ARP table shows address resolution records:



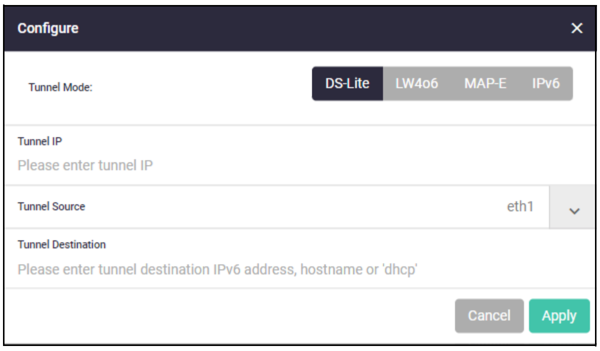
ARP Table

ARP

IP Address	MAC Address	Interface	Port	Type
172.31.0.236	001a.eb94.27e7	br-atmfmgmt		Dynamic
10.37.179.6	00c0.ffee.0401	eth1.179		Dynamic
10.37.179.1	000d.b955.77ed	eth1.179		Dynamic

v6 Transition

You can configure IPv4 to IPv6 transition using tunnel modes DS-Lite, LW4o6 (Lightweight 4over6), MAP-E or IPv6:



Configure

Tunnel Mode: DS-Lite

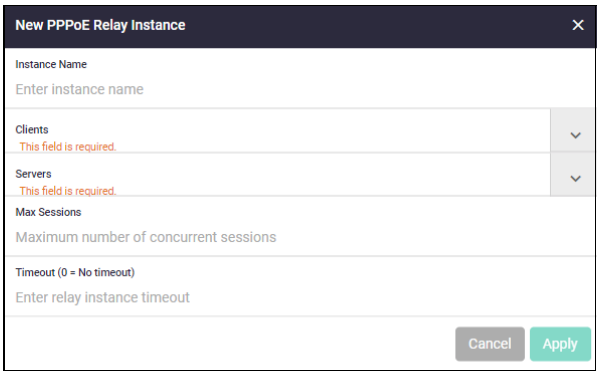
Tunnel IP: Please enter tunnel IP

Tunnel Source: eth1

Tunnel Destination: Please enter tunnel destination IPv6 address, hostname or 'dhcp'

PPPoE Relay

You can configure a new PPPoE relay instance:



New PPPoE Relay Instance

Instance Name: Enter instance name

Clients: This field is required.

Servers: This field is required.

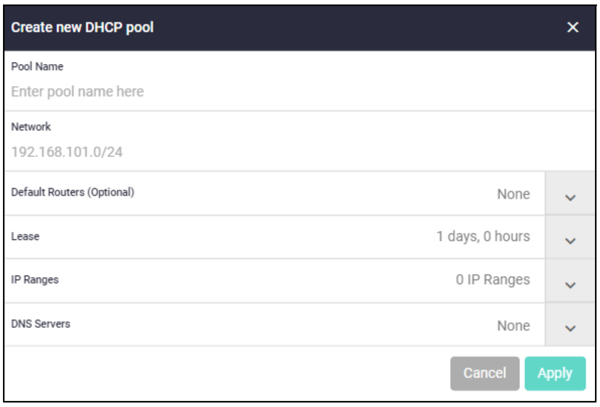
Max Sessions: Maximum number of concurrent sessions

Timeout (0 = No timeout): Enter relay instance timeout

Network Services

From the **Network Services** menu you can configure a DHCP server pool, SMTP server, use the traceroute or ping tools, configure RADIUS, AAA or SNMP. The following dialog shows configuration for a server pool.

Click on the **DHCP Server** menu. From this dialog you can create a new DHCP pool:



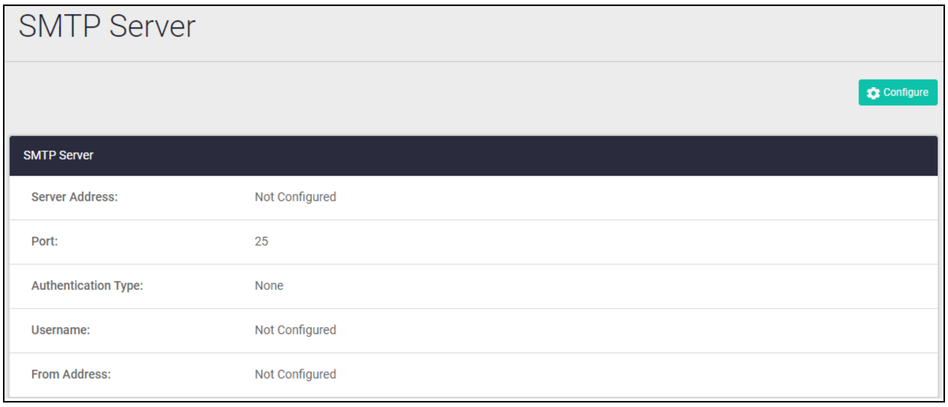
Create new DHCP pool

Pool Name
Enter pool name here

Network
192.168.101.0/24

Default Routers (Optional)	None
Lease	1 days, 0 hours
IP Ranges	0 IP Ranges
DNS Servers	None

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

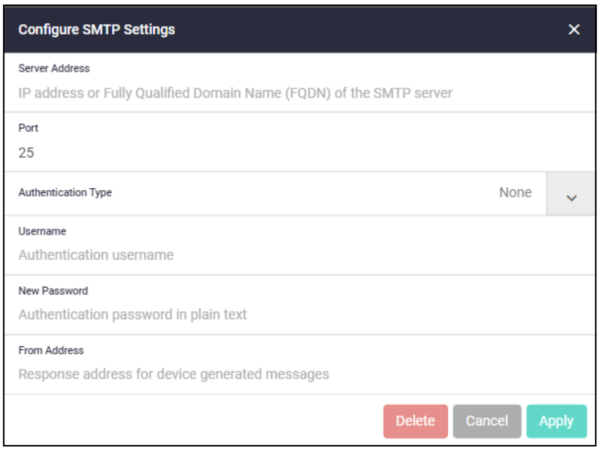


SMTP Server

SMTP Server

Server Address:	Not Configured
Port:	25
Authentication Type:	None
Username:	Not Configured
From Address:	Not Configured

Click the **Configure** button to set up or modify the SMTP server:



Configure SMTP Settings

Server Address
IP address or Fully Qualified Domain Name (FQDN) of the SMTP server

Port
25

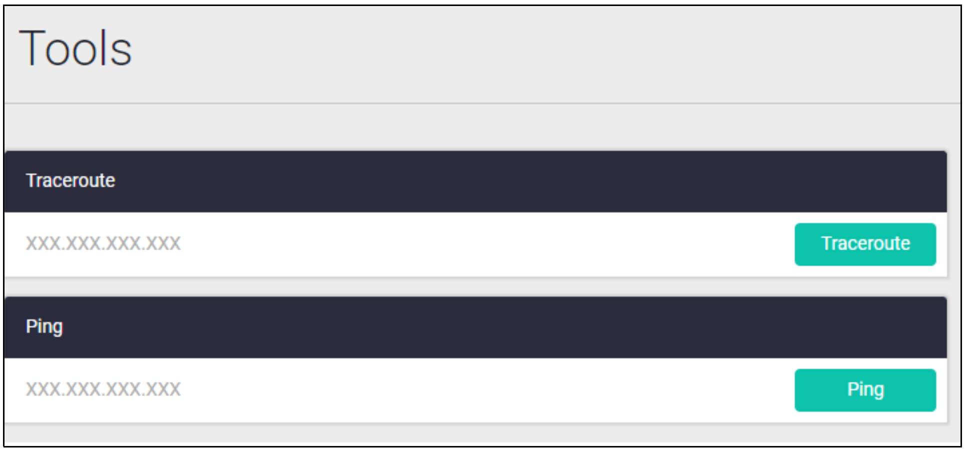
Authentication Type None

Username
Authentication username

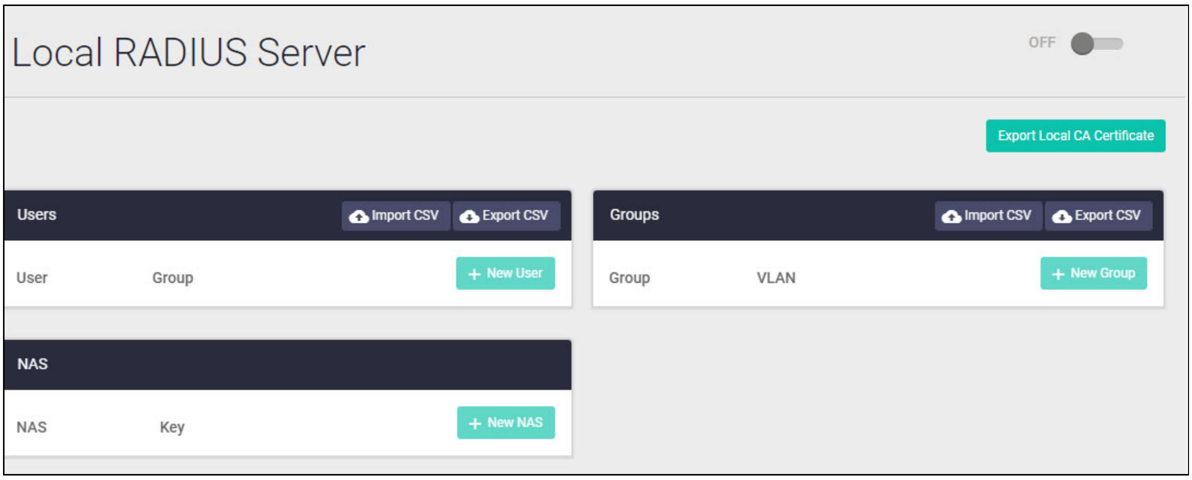
New Password
Authentication password in plain text

From Address
Response address for device generated messages

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

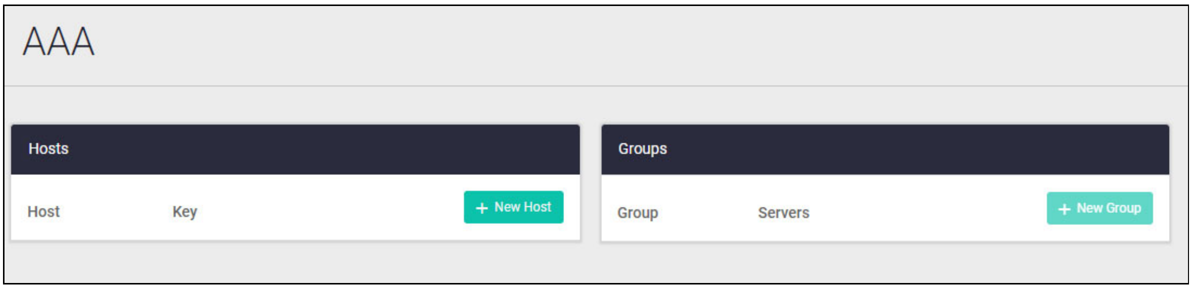


From the RADIUS menu you can display the following information about the wireless router's inbuilt local RADIUS server:

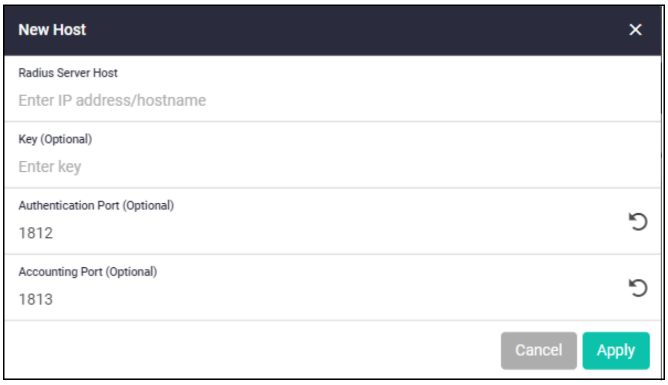


From this dialog you can add new users, groups and NAS information and you can import or export CSV files about users, groups and NAS. You can also export local CA certificates.

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



Click on the **New Host** button to add new hosts or the **New Group** button to add new groups:



New Host ✕

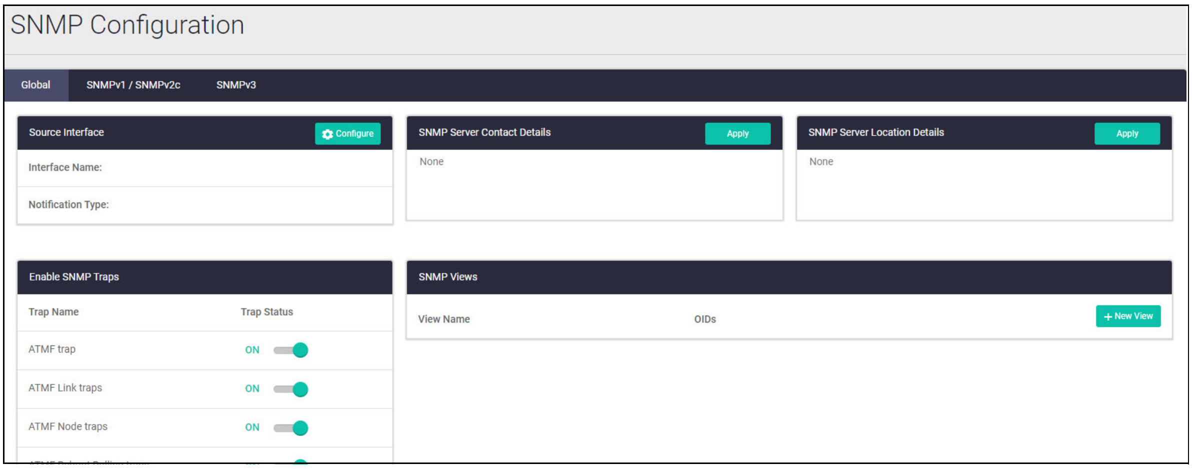
Radius Server Host
Enter IP address/hostname

Key (Optional)
Enter key

Authentication Port (Optional)
1812

Accounting Port (Optional)
1813

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



SNMP Configuration

Source Interface
Interface Name:
Notification Type:

SNMP Server Contact Details
None

SNMP Server Location Details
None

Enable SNMP Traps

Trap Name	Trap Status
ATMF trap	ON
ATMF Link traps	ON
ATMF Node traps	ON

SNMP Views

View Name	OIDs

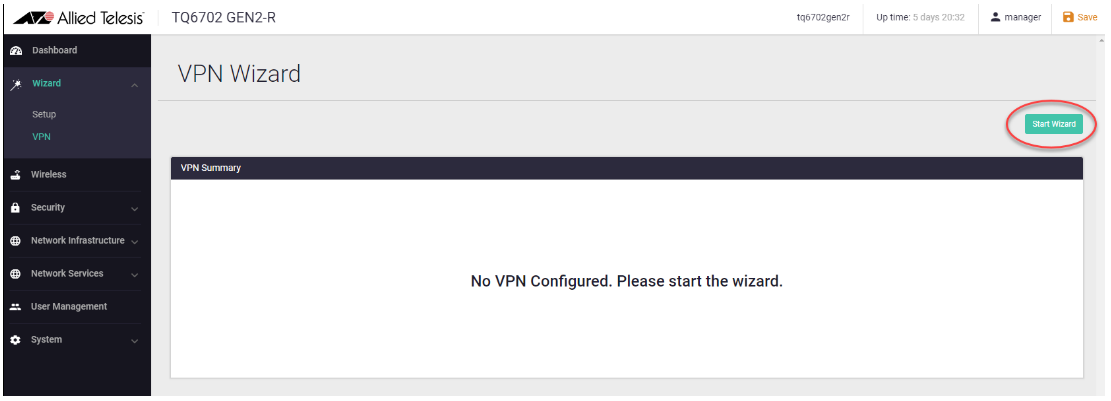
From this dialog you can configure the Source Interface, enter and apply SNMP Server Contact Details, and enter SNMP Server Location Details. You can also enable or disable SNMP traps and display OIDs for the traps.

Configuring a VPN connection

To configure a secure VPN connection, first make sure you have an Internet connection, and then use the following steps:

Step 1: **Start the Wizard.**

- Click the **Start Wizard** button.
- If you don't have an existing VPN connection, you'll see a blank **VPN Summary** screen:



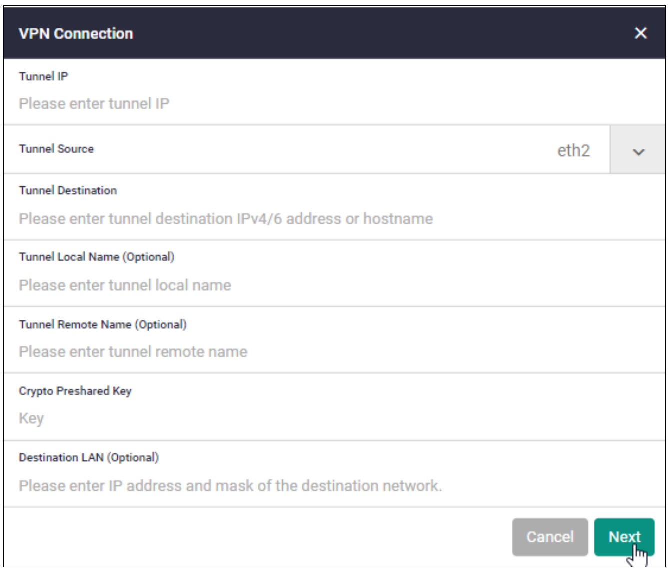
VPN Wizard

VPN Summary

No VPN Configured. Please start the wizard.

- If you do have an existing VPN connection, then you’ll see those details displayed in the **VPN Summary** screen. Click the **Start Wizard** button on that same screen to reconfigure your current VPN connection settings.

Step 2: **Enter the VPN connection information.**



VPN Connection

Tunnel IP
Please enter tunnel IP

Tunnel Source: eth2

Tunnel Destination
Please enter tunnel destination IPv4/6 address or hostname

Tunnel Local Name (Optional)
Please enter tunnel local name

Tunnel Remote Name (Optional)
Please enter tunnel remote name

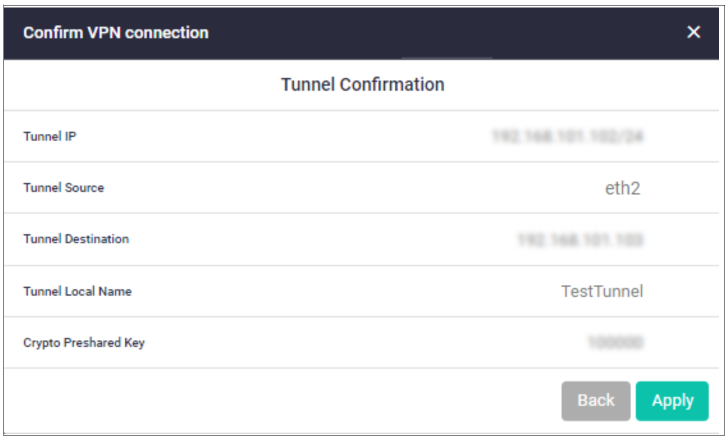
Crypto Preshared Key
Key

Destination LAN (Optional)
Please enter IP address and mask of the destination network.

Field	Description
Tunnel IP	Enter the IPv4 address of the tunnel interface.
Tunnel Source	Select 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.

Field	Description
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.

Step 3: **Confirm VPN tunnel connection.**



Tunnel Confirmation

Tunnel IP	[redacted]
Tunnel Source	eth2
Tunnel Destination	[redacted]
Tunnel Local Name	TestTunnel
Crypto Preshared Key	[redacted]

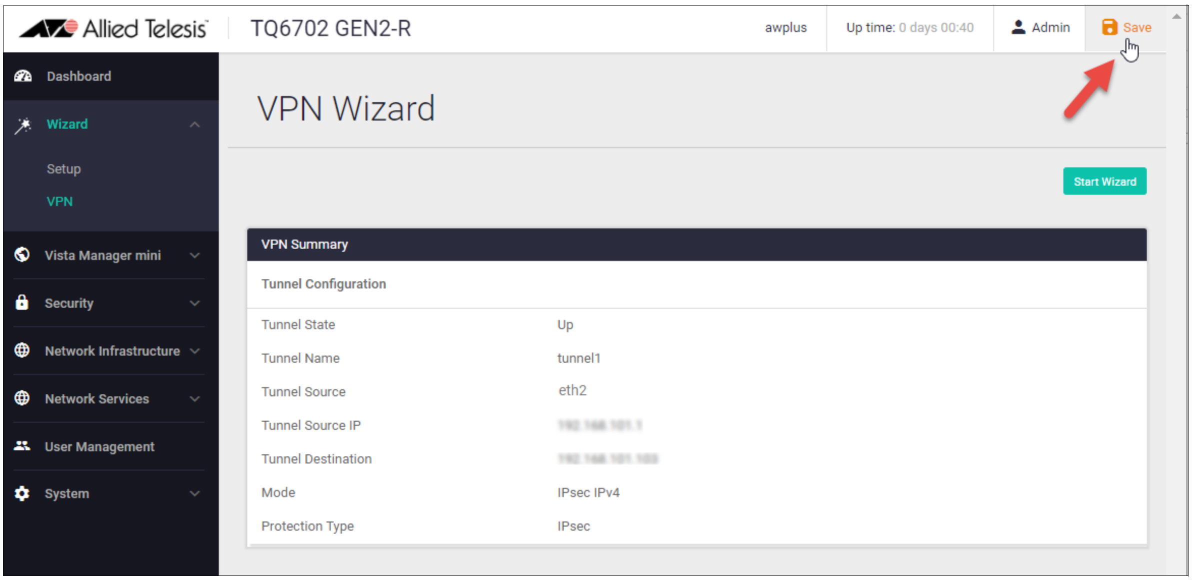
Step 4: **Review and Save your settings.**

- Check your configuration is correct and click **Apply** to continue.
- If you click **Save** with a VPN connection already set up, the existing settings on the running configuration will be erased and replaced with the newly configured content.

Step 5: **Save the settings to the startup configuration.**

When the configuration save is complete, a summary of the VPN connection status is displayed.

- The contents set in the simple setting 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.
- You can always run the Wizard again to make changes to your VPN connection settings.



VPN Wizard

VPN Summary

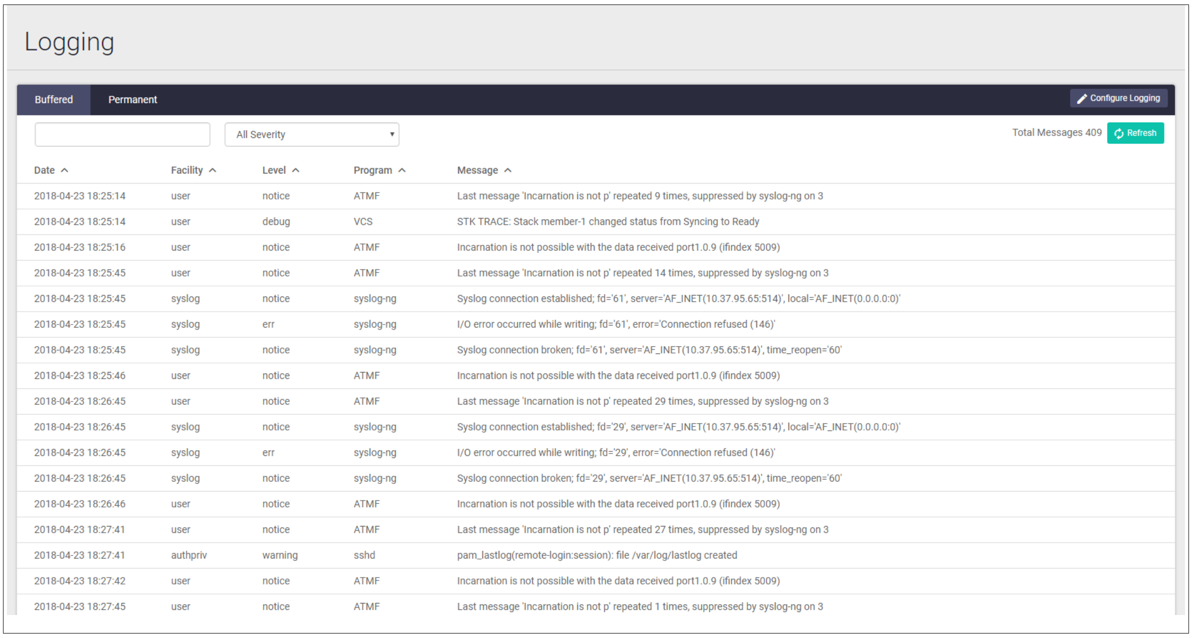
Tunnel Configuration

Tunnel State	Up
Tunnel Name	tunnel1
Tunnel Source	eth2
Tunnel Source IP	[redacted]
Tunnel Destination	[redacted]
Mode	IPsec IPv4
Protection Type	IPsec

Logging

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

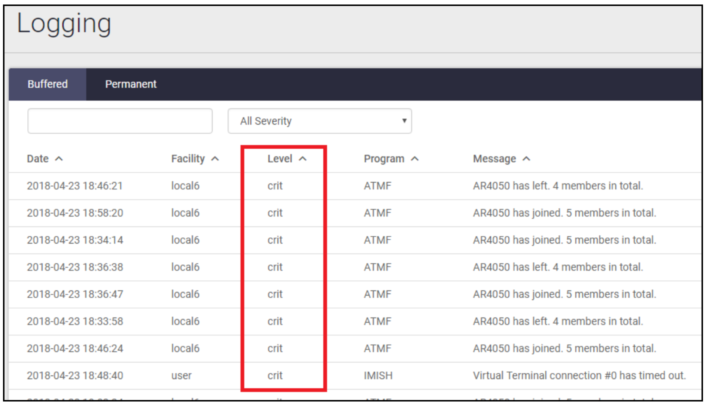
- By default the buffered logs tab is displayed.



Date	Facility	Level	Program	Message
2018-04-23 18:25:14	user	notice	ATMF	Last message 'Incarnation is not p' repeated 9 times, suppressed by syslog-ng on 3
2018-04-23 18:25:14	user	debug	VCS	STK TRACE: Stack member-1 changed status from Syncing to Ready
2018-04-23 18:25:16	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifindex 5009)
2018-04-23 18:25:45	user	notice	ATMF	Last message 'Incarnation is not p' repeated 14 times, suppressed by syslog-ng on 3
2018-04-23 18:25:45	syslog	notice	syslog-ng	Syslog connection established; fd='61', server='AF_INET(10.37.95.65:514)', local='AF_INET(0.0.0.0:0)'
2018-04-23 18:25:45	syslog	err	syslog-ng	I/O error occurred while writing; fd='61', error='Connection refused (146)'
2018-04-23 18:25:45	syslog	notice	syslog-ng	Syslog connection broken; fd='61', server='AF_INET(10.37.95.65:514)', time_reopen='60'
2018-04-23 18:25:46	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifindex 5009)
2018-04-23 18:26:45	user	notice	ATMF	Last message 'Incarnation is not p' repeated 29 times, suppressed by syslog-ng on 3
2018-04-23 18:26:45	syslog	notice	syslog-ng	Syslog connection established; fd='29', server='AF_INET(10.37.95.65:514)', local='AF_INET(0.0.0.0:0)'
2018-04-23 18:26:45	syslog	err	syslog-ng	I/O error occurred while writing; fd='29', error='Connection refused (146)'
2018-04-23 18:26:45	syslog	notice	syslog-ng	Syslog connection broken; fd='29', server='AF_INET(10.37.95.65:514)', time_reopen='60'
2018-04-23 18:26:46	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifindex 5009)
2018-04-23 18:27:41	user	notice	ATMF	Last message 'Incarnation is not p' repeated 27 times, suppressed by syslog-ng on 3
2018-04-23 18:27:41	authpriv	warning	sshd	pam_lastlog(remote-login:session): file /var/log/lastlog created
2018-04-23 18:27:42	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifindex 5009)
2018-04-23 18:27:45	user	notice	ATMF	Last message 'Incarnation is not p' repeated 1 times, suppressed by syslog-ng on 3

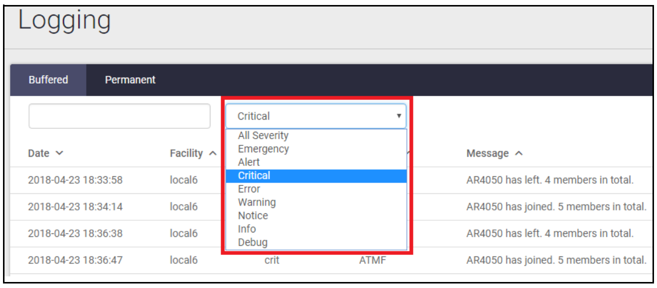
You can filter the logs in three ways to focus your view and support easy analysis:

1. any information column in ascending or descending order



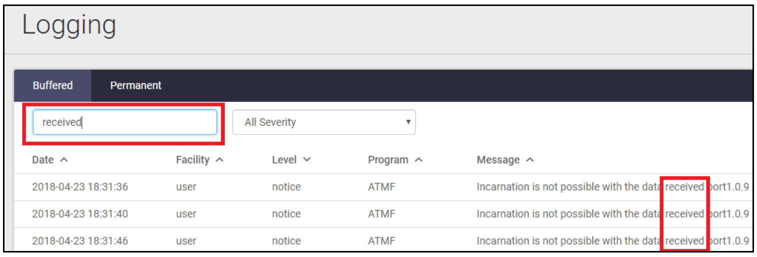
Date	Facility	Level	Program	Message
2018-04-23 18:46:21	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:58:20	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:34:14	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:36:38	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:33:58	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:46:24	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:48:40	user	crit	IMISH	Virtual Terminal connection #0 has timed out.

2. selecting the level of logs to display: Critical, Warning, Error etc.



Date	Facility			Message
2018-04-23 18:33:58	local6			AR4050 has left. 4 members in total.
2018-04-23 18:34:14	local6			AR4050 has joined. 5 members in total.
2018-04-23 18:36:38	local6			AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in total.

3. searching for any text string found in the logs.

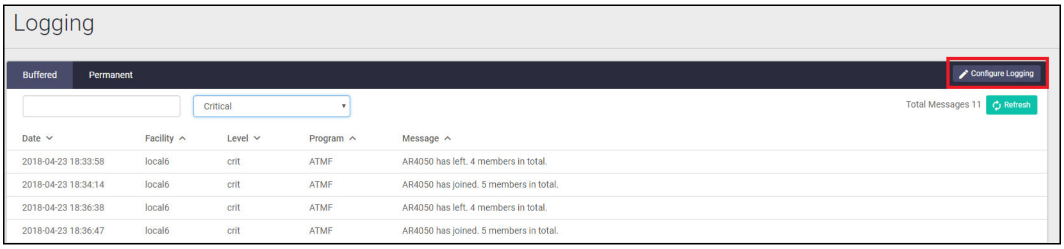


received

All Severity

Date	Facility	Level	Program	Message
2018-04-23 18:31:36	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9
2018-04-23 18:31:40	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9
2018-04-23 18:31:46	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9

Click the **Configure Logging** button to access the Logging Configuration page. This page allows you to create filters to manage which logs are stored on the device and also set up a Syslog server(s) for remote log storage.

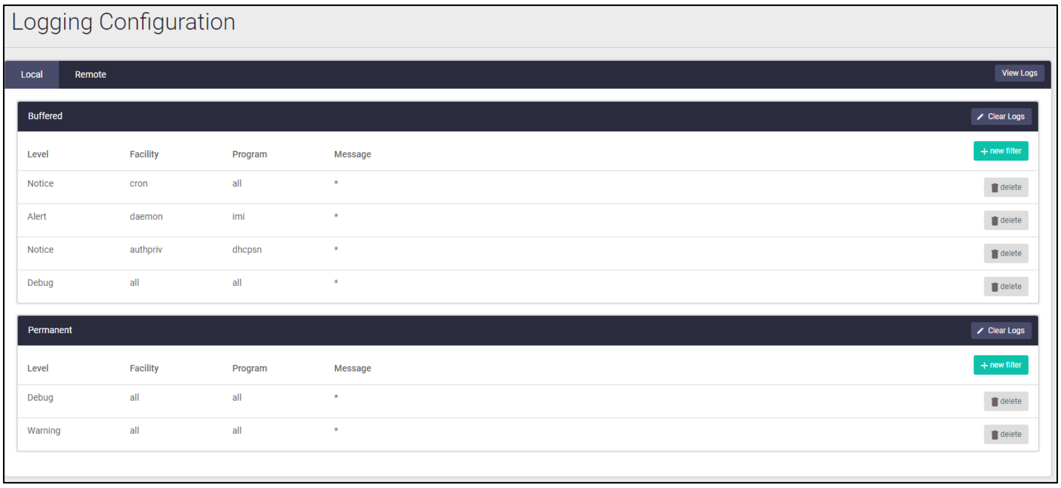


Critical

Total Messages 11

Date	Facility	Level	Program	Message
2018-04-23 18:33:58	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:34:14	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:36:38	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in total.

The **Logging Configuration** page has tabs for local and remote (syslog server) settings.



Buffered

Level	Facility	Program	Message
Notice	cron	all	*
Alert	daemon	imi	*
Notice	authpriv	dhcpsn	*
Debug	all	all	*

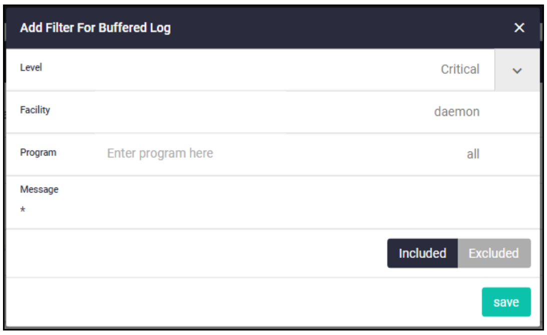
Permanent

Level	Facility	Program	Message
Debug	all	all	*
Warning	all	all	*

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. You can also delete the buffered or permanent logs using the **Clear Logs** button.

Use the **View Logs** button to return to the Logging page.

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.



Add Filter For Buffered Log

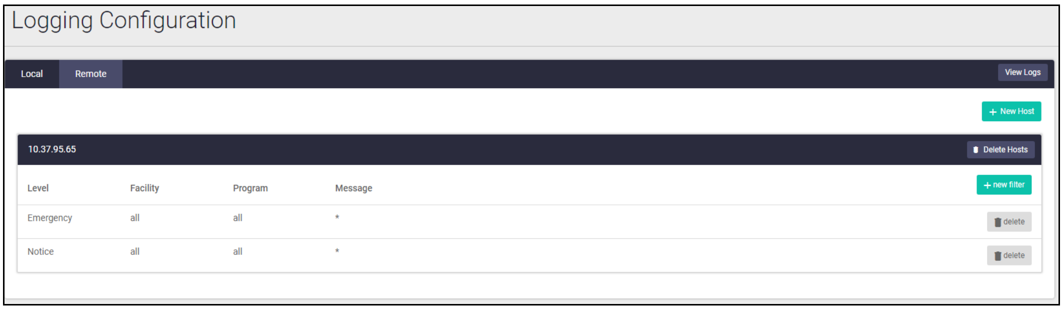
Level: Critical

Facility: daemon

Program: Enter program here — all

Message: *

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



Logging Configuration

10.37.95.65

Level	Facility	Program	Message
Emergency	all	all	*
Notice	all	all	*

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com