User Guide

Wi-Fi 6 Gateway – CF40MESH

Doc No. UG01438

Important notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm Wireless Wi-Fi 6 Gateway to transmit or receive such data.

Copyright

NetComm Wireless Limited was acquired by Casa Systems in 2019.

Note – This document is subject to change without notice.

Document history

This document relates to the following product:

NetComm Wi-Fi 6 Gateway – CF40MESH

Ver.	Document description	Date
v1.00	Initial document release	21 December 2022
v1.01	Updated IP/MAC Binding section	27 October 2023
v1.02	Updated Advanced Wi-Fi section to reflect new firmware version	12 January 2024

Table i. – Document revision history

Contents

Overview

Introduction

This document provides you all the information you need to set up, configure and use the NetComm Wireless Wi-Fi 6 Gateway.

Prerequisites

Before continuing with the installation of your Wi-Fi 6 Gateway, please confirm that you have the following:

- An electronic computing device with a working Ethernet network adapter and a web browser such as Google Chrome™ or Safari*.

Notation

The following symbols may be used in this document:

Note – This note contains useful information.

Important – This is important information that may require your attention.

Warning – This is a warning that may require immediate action in order to avoid damage or injury.

* Safari is a trademark of Apple Inc., registered in the U.S. and other countries and regions.

Hardware installation instructions

For instructions on how to connect your Wi-Fi 6 Gateway, refer to the Quick Start Guide available at https://support.netcommwireless.com/products/CF40MESH

Setting up your Internet connection

Note – If you received your gateway from your service provider and they have provided you with their own instructions, refer to those to complete the setup. In some cases, the gateway has been pre-configured for you and is ready to use.
Otherwise, you will need to complete the setup yourself. Refer to the Basic setup section of this User Guide.

Device overview

Interfaces

The Wi-Fi 6 Gateway is designed to be placed on a desktop with the top facing upward.

All of the cables exit from the rear for easy organization along with the power and WPS buttons.

Top view

There are five LED lights on the top of the Wi-Fi 6 Gateway:

Figure 1 – Wi-Fi 6 Gateway top view

LED indicators

The following table contains an explanation of each of the indicator lights on the top of the Wi-Fi 6 Gateway.

Label	Colour/State	Definition
Power	Green	The Wi-Fi 6 Gateway is powered on and operating normally.
	Off	The power is off.
WAN	Green	A device is connected to the Ethernet WAN port.
	Red	Authentication failed.
	Off	No device is connected to the Ethernet WAN port.
LAN	Green	A device is connected to the Ethernet LAN port.
	Off	No device is connected to the Ethernet LAN port.
Wi-Fi	Green	Wi-Fi (either 2.4GHz or 5GHz) is enabled.
	Off	Wi-Fi (both 2.4GHz and 5GHz) is disabled.
WPS	Green	WPS (Wi-Fi Protected Setup) is enabled.
	Green Blinking	WPS pairing is triggered.
	Off	WPS is disabled.

Table 1 - LED icon descriptions

Rear view

The following interfaces are available on the rear panel of the Wi-Fi 6 Gateway:

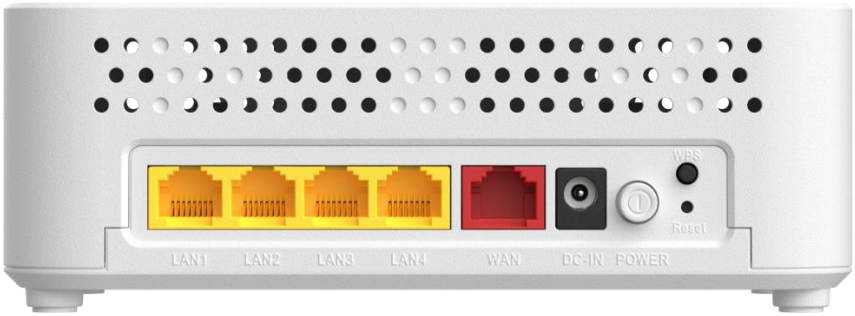


Figure 2 – Wi-Fi 6 Gateway rear view

Interface	Description
LAN 1–4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
WAN	Gigabit capable WAN port for connection to a WAN network. Connect to your Network Termination Device (NTD) for high-speed internet access.
DC IN	Connection point for the included power adapter. Connect the power supply here.
Power button	Turns the Wi-Fi 6 Gateway on or off.

Interface	Description
WPS	When pressed, this triggers the Wi-Fi Protected Setup (WPS) process.
Reset button	Resets the Wi-Fi 6 Gateway to the factory default settings by holding the Reset button down for 10 seconds when it is powered on. To push this button, you may need to use a paperclip or similar object.

Table 2 – Interface descriptions

Advanced configuration of the Wi-Fi 6 Gateway

To perform advanced configuration of the Wi-Fi 6 Gateway, you can access its web interface.

1. Push the power button on the side of the Wi-Fi 6 Gateway to turn it on. Wait a few minutes for it to complete starting up.
2. Open a web browser and type **192.168.20.1** into the address bar, then press **Enter**.
3. At the login screen, type **admin** into the Username field. In the Password field, type the unique password printed on the label on the bottom of the gateway, then click the **Login** button. If you have changed the password, enter your chosen password instead.

Figure 3 – Login screen

4. The four-section **Summary** screen is displayed.

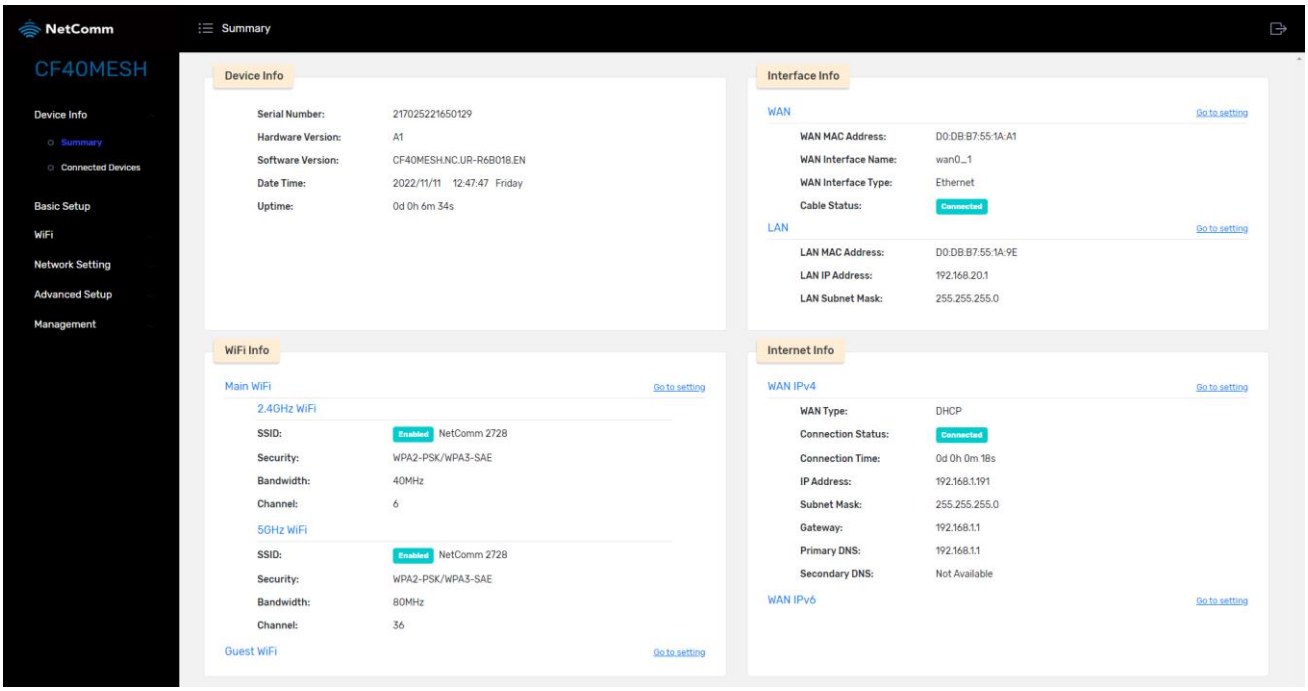


Figure 4 – Device Info > Summary screen

The **Summary** screen displays an overview of some of the critical elements of the gateway.

Navigating the user interface

The user interface of the Wi-Fi 6 Gateway presents a menu on the left side of the screen which provides a means of opening different settings screens.

Some of these menu items expand to show sub-menus below them, as demonstrated below with the Summary page being a sub-page of the Device Info section.

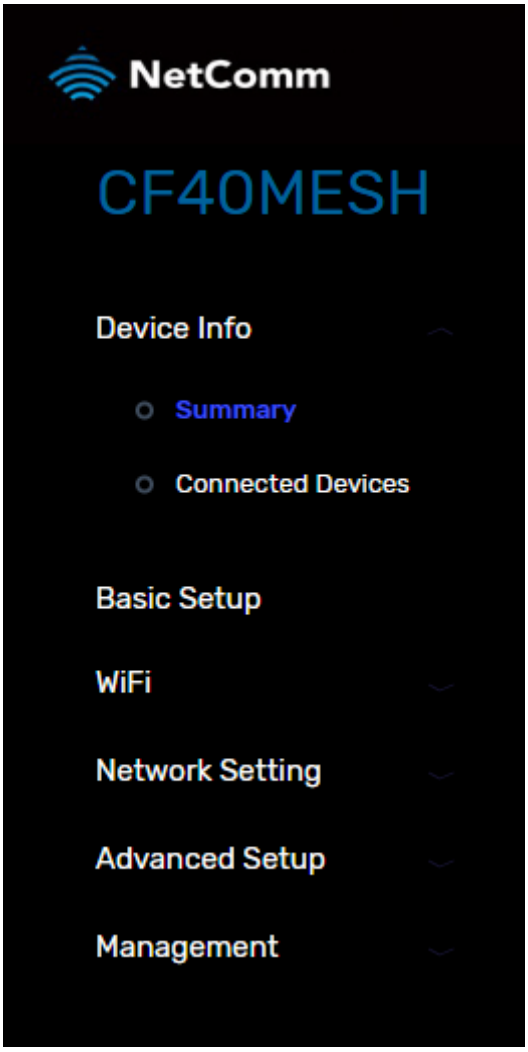


Figure 5 - Navigation menu

To view gateway settings, select a section, for example, Management.

Then select one of the sub-menu items, for example, TR-069.

The TR-069 settings are displayed in the main screen on the right side of the web page.

Basic setup

Normally your CF40MESH Wi-Fi 6 Gateway is shipped pre-configured with connection settings appropriate for your internet and Wi-Fi services. Normally you will not be required to use the tools and settings found in this section.

However, if the pre-configured default profile does not connect, you should run through the Basic Setup wizard described in this section.

This wizard prompts you for the details necessary to set up your internet connection and helps you to configure the Wi-Fi on the gateway. If you are unsure of the settings to enter, please contact your Internet Service Provider.

To access the Basic setup wizard, select Basic Setup from the menu on the left.

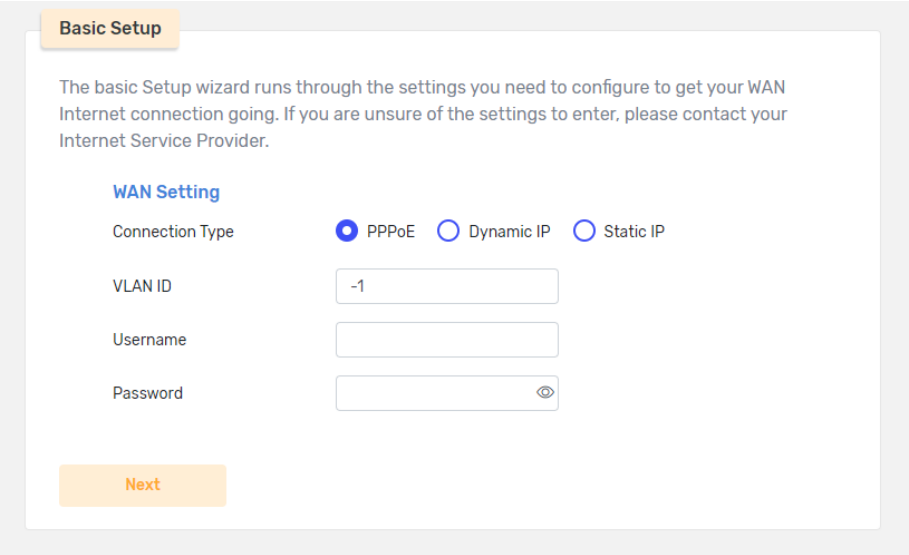


Figure 6 - Basic Setup

To complete the wizard, you will need to know a few settings about your internet connection, such as Connection Type, VLAN ID and username and password. If you don't know what these are, you should contact your internet service provider.

1. Select the connection type and enter the required details depending on the connection type selected. When you have entered the details for your connection, select the Next button.

2. Enter an SSID (network name) and password for your wireless network. These are required whenever you want to connect a wireless device to your network.

Note – If you are replacing an existing wireless network, you can set the same username and password on the Wi-Fi 6 Gateway and all your devices will connect automatically to the new one.

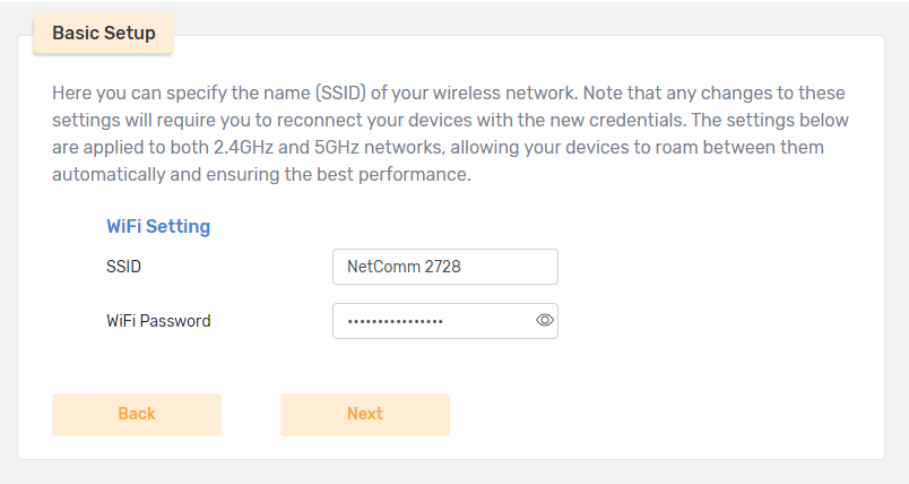


Figure 7 – Basic Setup - Wi-Fi Settings

When you have entered the Wi-Fi details, select the **Next** button.

3 Select a time zone offset. This is mainly used for maintaining accurate log data.

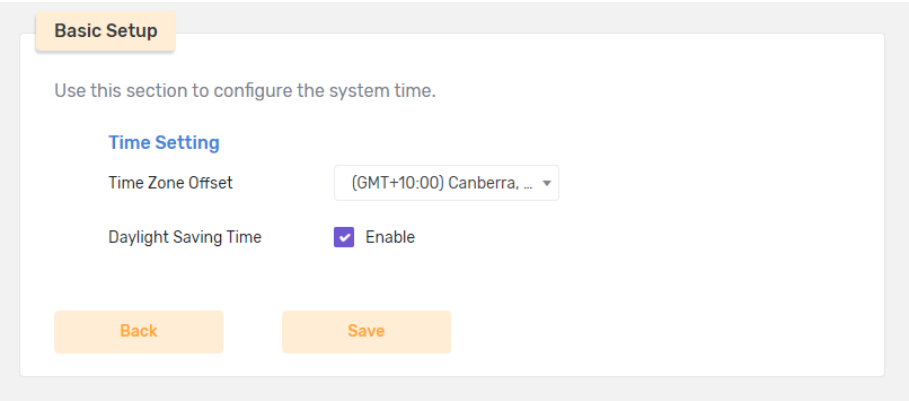


Figure 8 – Basic Setup - Time zone setting

When you have chosen the correct time zone and daylight saving setting, select the **Save** button.

The gateway saves your settings and returns to the **Summary** page. The basic setup is complete.

Device info

Summary

The **Summary** page is the main page displayed when you first log in to the gateway.

It summarizes the important functions of the gateway so that you can see at a glance whether everything is functioning correctly.

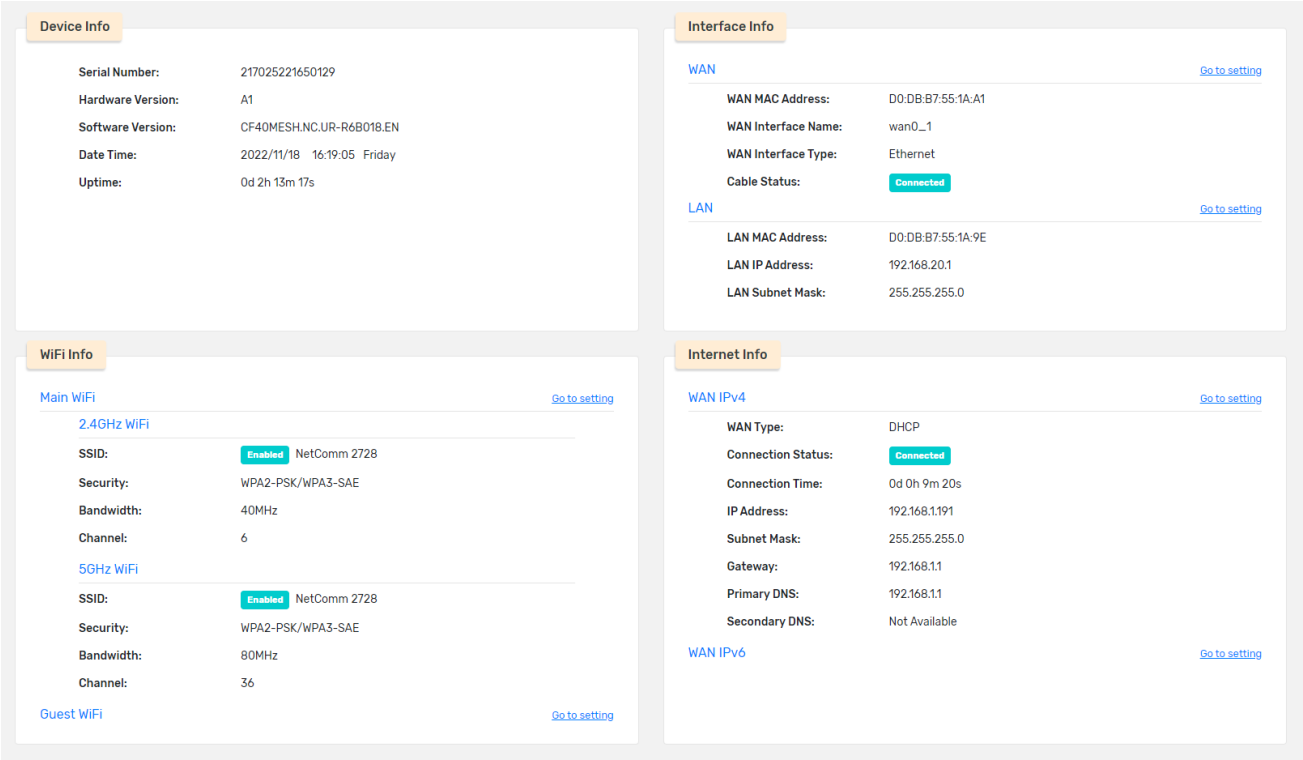


Figure 9 - Device info – Summary

Device Info

The **Device Info** section provides details about the individual gateway unit and information in real time about its current connection status.

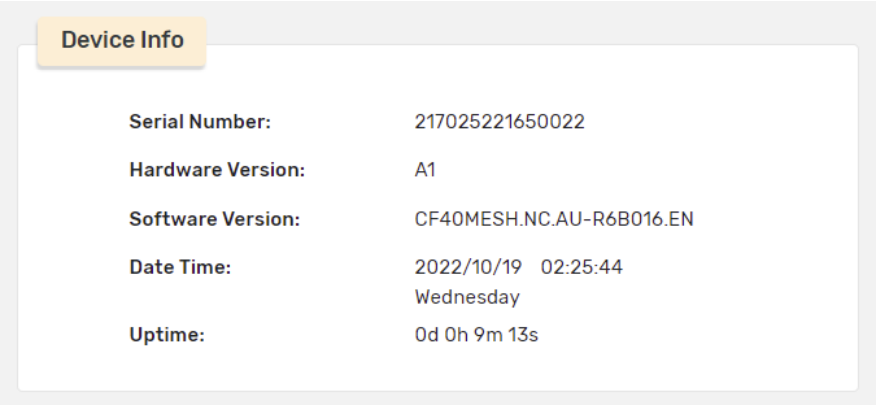


Figure 10 - Device Info section

WiFi Info

The **WiFi Info** section provides real time information

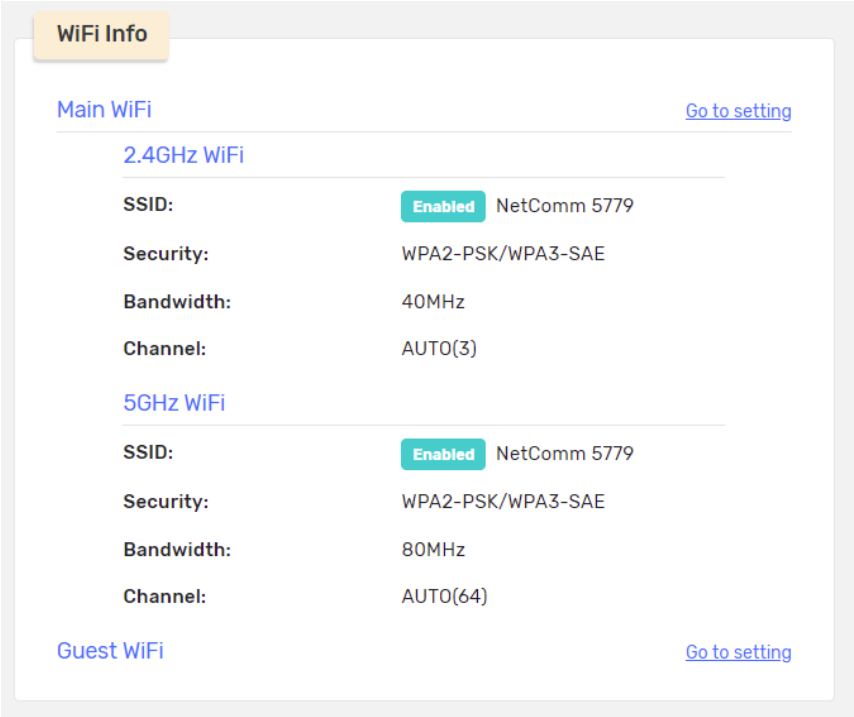


Figure 11 - Device info section

Click either Go to setting link to access the **WiFi** > **Main WiFi** page where you can enable or disable the service and see important details regarding either the 2.4GHz or 5GHz WiFi connection.

For more information, go to the **WiFi** section at page 17 in this User Guide.

Interface Info

The Interface Info section provides real time information

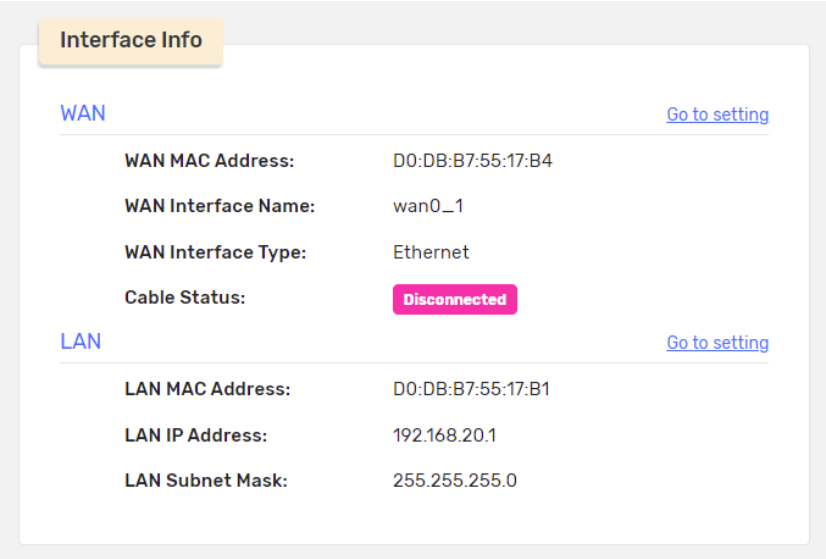


Figure 12 – Interface info section

Click either Go to setting ink to access the Network Setting > WAN or LAN pages where you can you configure the local network settings of the router.

For more information, go to the Network Setting section at page 23 in this User Guide.

Internet Info

The Internet Info section provides real time information

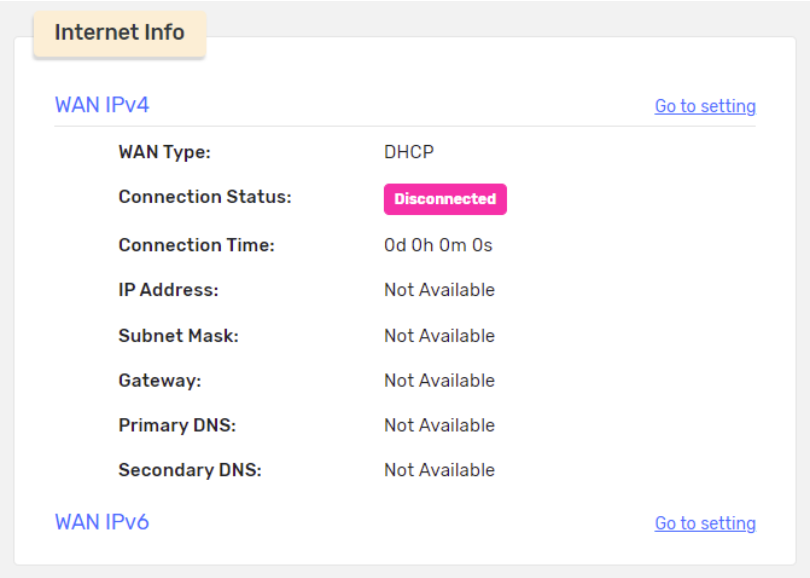


Figure 13 – Internet info section

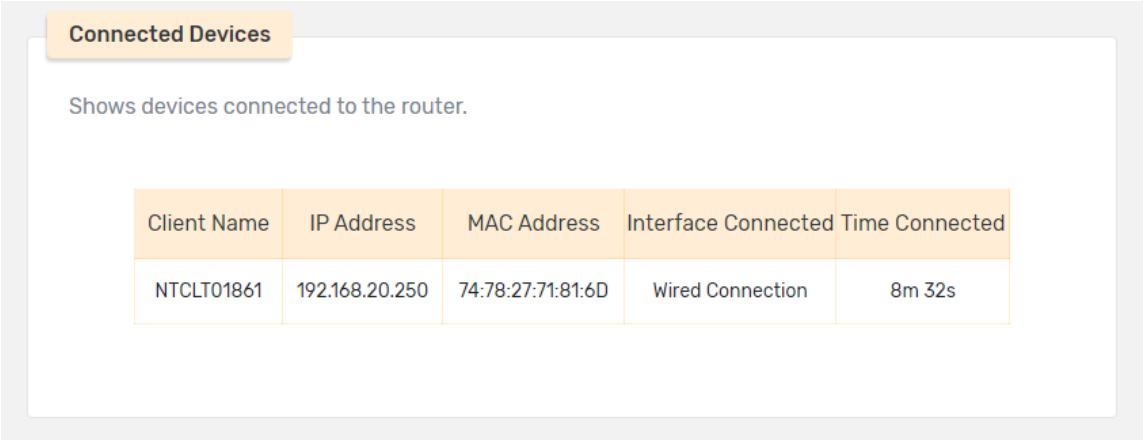
Click the Go to setting link to access the Network Setting > WAN page.

For more information, go to the WAN section at page 23 in this User Guide.

Connected devices

To access this page, from the menu on the left, select **Device info**, then **Connected devices.**

The **Connected devices** page displays a list of all devices connected via the Wi-Fi 6 Gateway, both on the wireless network and the wired local network, along with their IP address, MAC address and the time they have been connected.



Client Name	IP Address	MAC Address	Interface Connected	Time Connected
NTCLT01861	192.168.20.250	74:78:27:71:81:6D	Wired Connection	8m 32s

Figure 14 - Device info - Connected devices list

WiFi

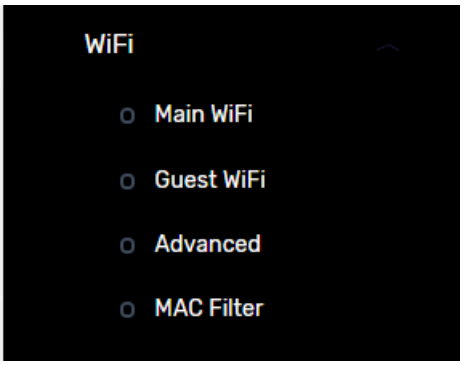


Figure 15 – WiFi menu

The **WiFi** section of the user interface contains various settings related to the configuration of your local wireless network.

This section also includes links to pages to set up Guest WiFi accounts and other WiFi security tools, filters and settings.

Main WiFi

To access this page, select **WiFi** from the menu on the left, then choose **Main WiFi** from the submenu.

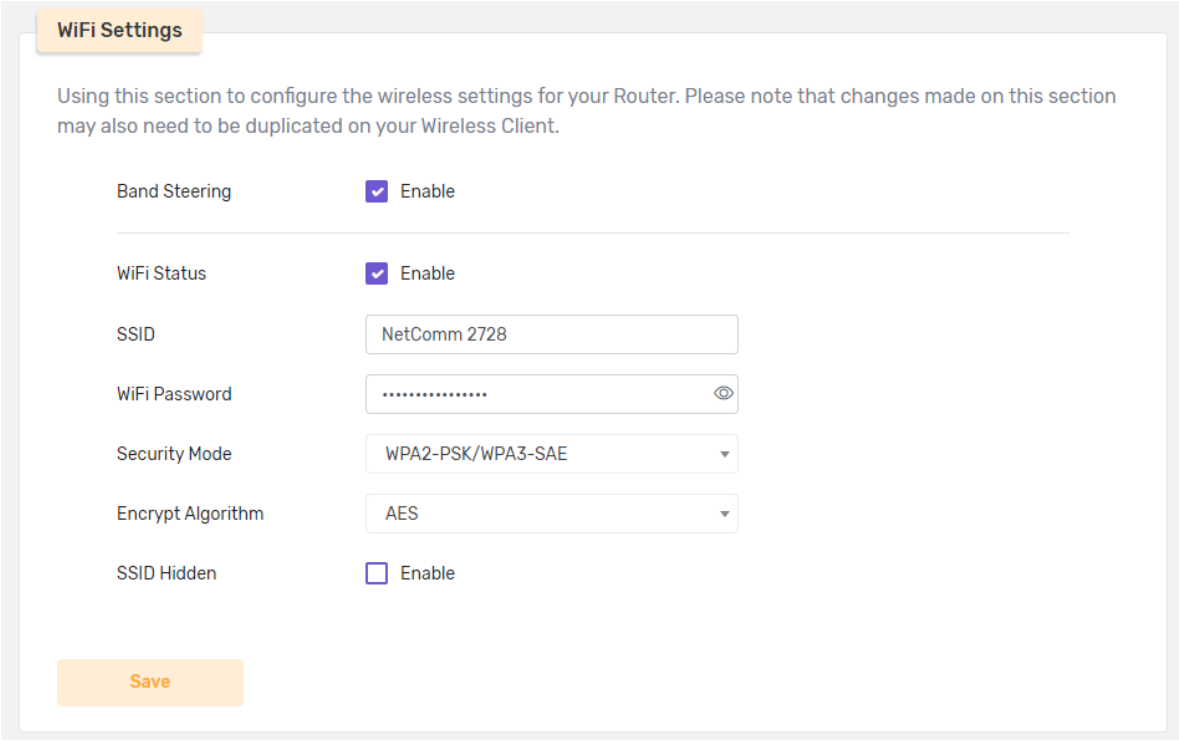


Figure 16 - WiFi - Main WiFi

The Main WiFi page provides basic configuration options for the main wireless network of the Wi-Fi 6 Gateway.

The table below describes the meaning of each setting.

Field	Description
Band Steering	Band steering is a technique that aims to optimise the band (2.4GHz or 5GHz) that clients connect to based on their signal strength, with a focus on encouraging wireless devices to prioritise the less congested 5GHz network where possible. If you have some older devices and experience connection problems, you may consider disabling this option, but in most cases, band steering improves the performance of your wireless network.
WiFi Status	Enables or disables the Main Wi-Fi network of your Wi-Fi 6 Gateway.
SSID	The SSID is also known as the wireless network name that appears when you scan for nearby wireless networks.
WiFi Password	The password for the wireless network. This is the password that must be entered when attempting to connect to the Wi-Fi 6 Gateway's Wi-Fi network.
Security Mode	This is the security protocol used to secure your wireless network. The default setting is WPA2-PSK/WPA3-SAE. This is a combination of WPA2 and WPA3. If the wireless device supports WPA3, it will use that as it is the newer and more secure protocol. If you have any problems with connecting to Wi-Fi, try to select "WPA2" or "WPA2-PSK" as the security mode as it is possible that some devices could have trouble connecting with the WPA3 protocol.
Encrypt Algorithm	The Advanced Encryption Standard (AES) is the most secure wireless encryption standard and is the default setting on the Wi-Fi 6 Gateway. As it is the most secure option, no other options are provided.
SSID Hidden	When this option is enabled, your wireless network will not appear when a device does a scan for nearby wireless networks. This means that a wireless device must use the manual connection method and enter the SSID and password together in order to connect.

Table 3 - Main WiFi - Descriptions

Guest WiFi

Use a Guest network to allow others to use your internet connection while preserving the security of your own local network.

To access this page, select **WiFi** from the menu on the left, then choose **Guest WiFi** from the submenu.

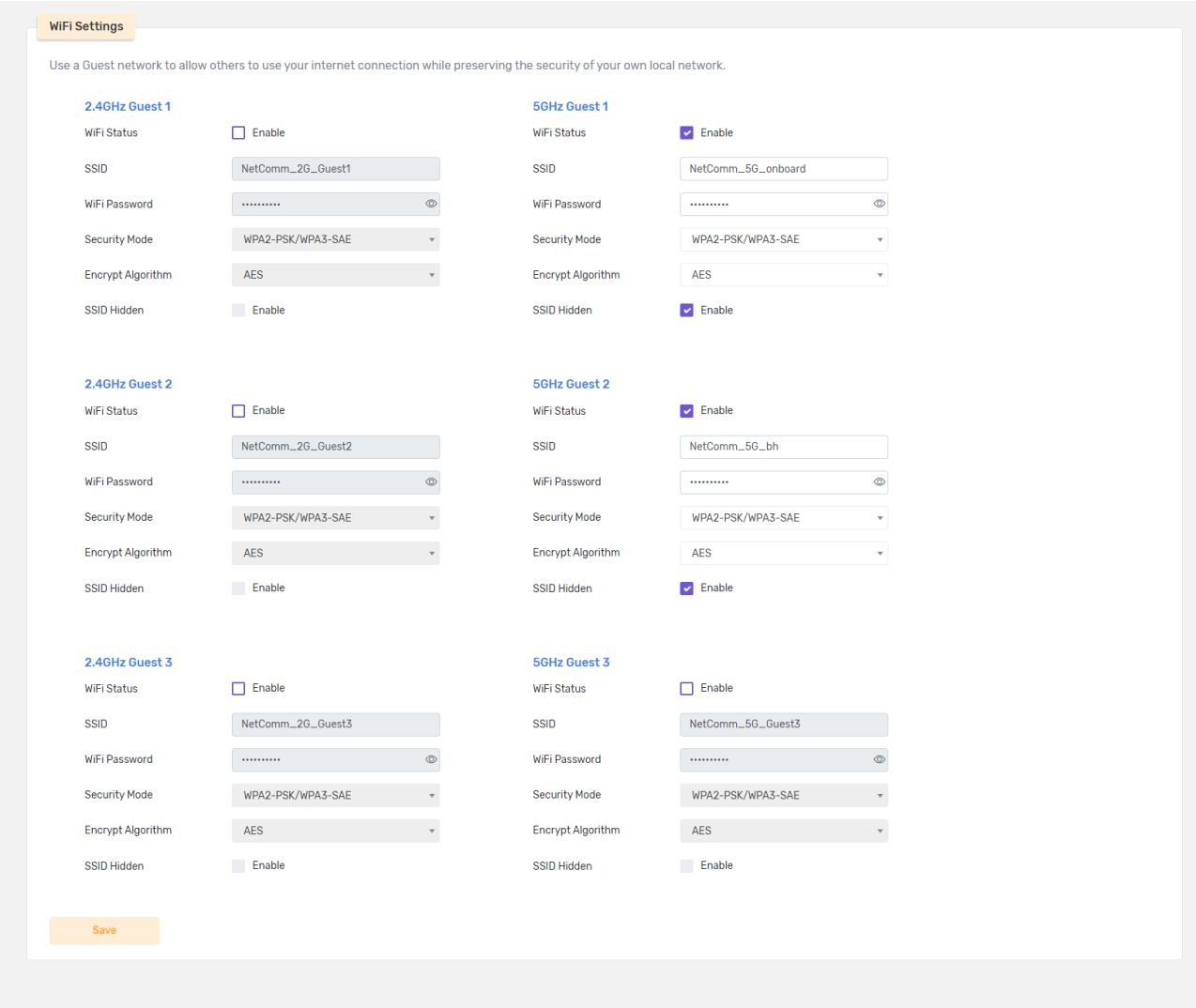


Figure 17 - Guest WiFi settings page

The Guest WiFi page provides you with the option of configuring up to six guest networks in total; three on the 2.4GHz band and three on the 5GHz band. Refer to *Table 3 – Main WiFi – Descriptions* for a description of each field.

Each wireless network should run a unique SSID (network name) so that it is easily identifiable when a scan for nearby networks is performed.

Advanced

To access this page, select **WiFi** from the menu on the left, then choose **Advanced** from the submenu.

The **Advanced** page has two separate subsections: **WiFi Settings** and **WPS Settings**

WiFi Settings

These Wi-Fi configuration options can be used to adjust advanced settings to suit your environment.

The default settings are the ideal settings.

Important – Only make changes in this section if you understand the impact of those changes. Any changes could result in lower performance.

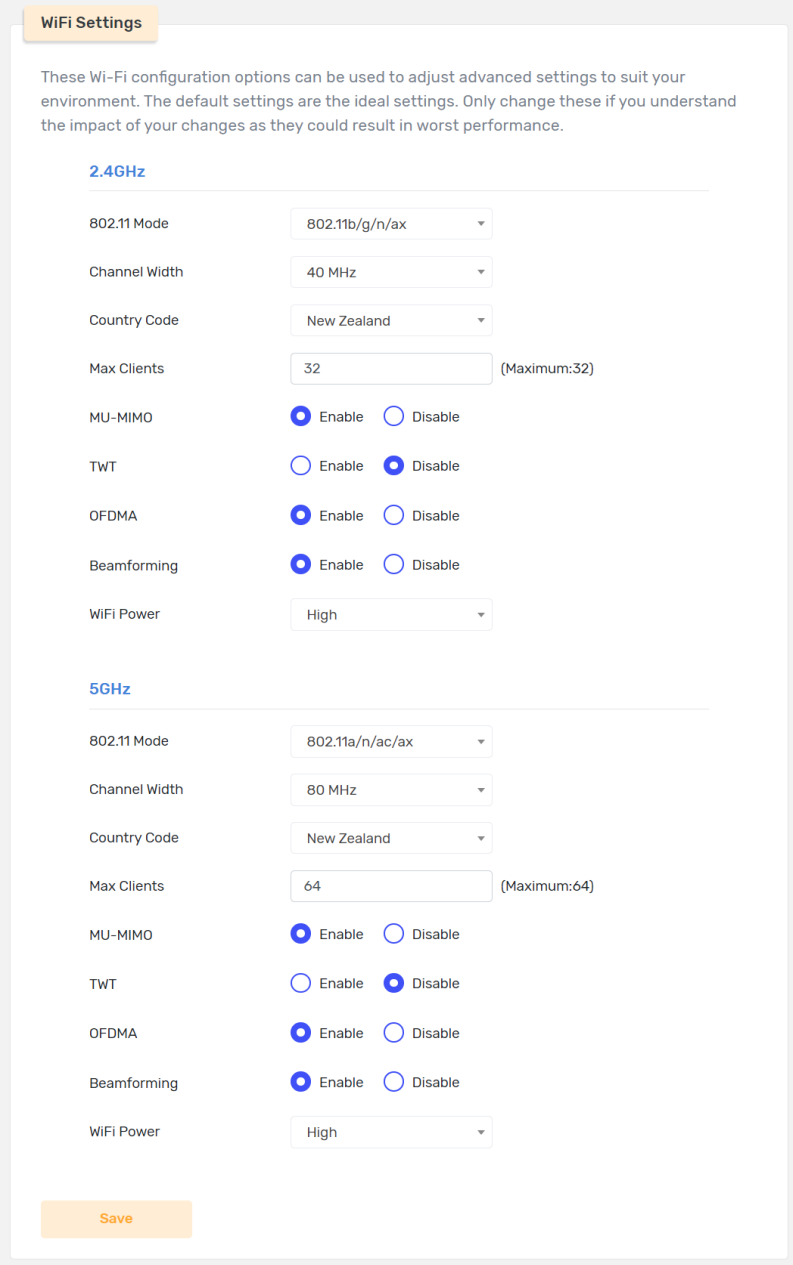


Figure 18 - WiFi – Advanced Settings

WPS Settings

Use the WPS function to easily connect a wireless device to your gateway using WiFi.

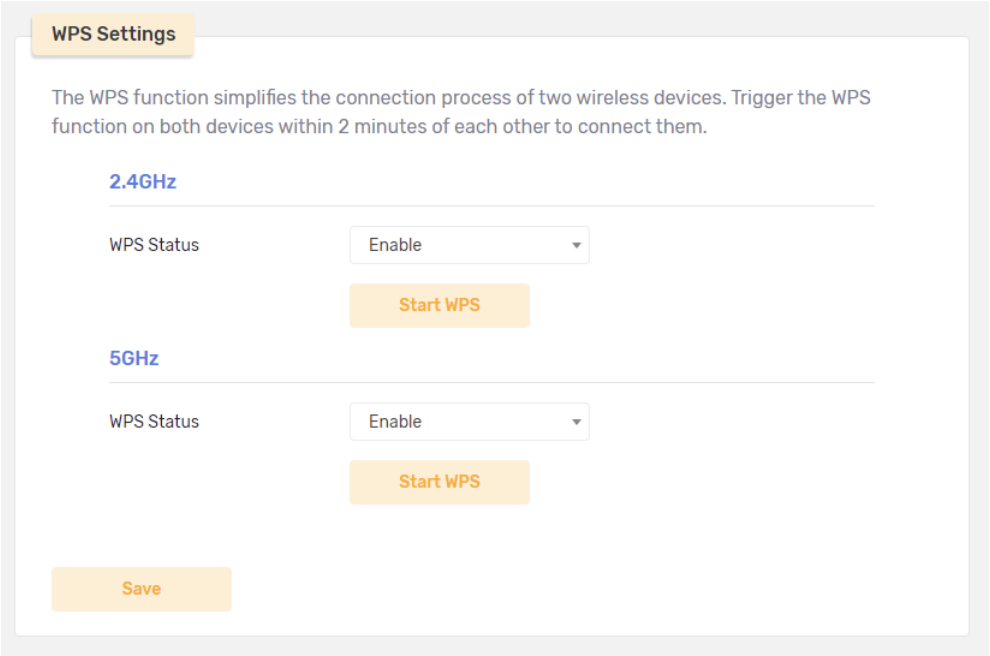


Figure 19 - WiFi - MAC Filter

To ensure the WPS functionality is working, select **Enable** from the **WPS Status** drop down list for either 2.4GHz or 5GHz or both.

For either the 2.4GHz or 5GHz WiFi press the WPS function button both devices within 2 minutes of each other to connect them.

MAC Filter

You can filter access for devices based on the unique MAC address of each electronic device. The MAC Filter function allows you to either Allow the specified MAC addresses or Block other specified MAC addresses.

To access this page, from the menu on the left, select WiFi, then MAC Filter.

The first step is to open the MAC Restrict Mode drop-down list and select either Allow list or Block list and add a new rule that either allows or blocks the specific MAC address of a unique device.

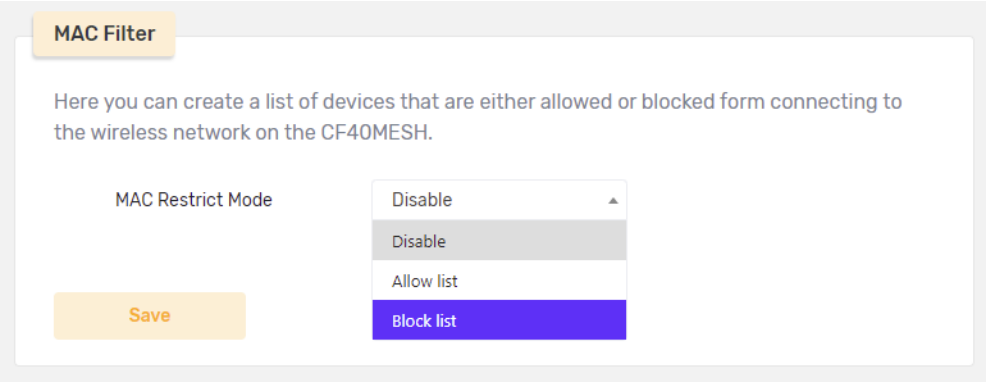


Figure 20 - WiFi - MAC Filter – Select Mode

The Add Rule page requires the entry of a meaningful Device Name for the rule as well as the device's unique MAC address.

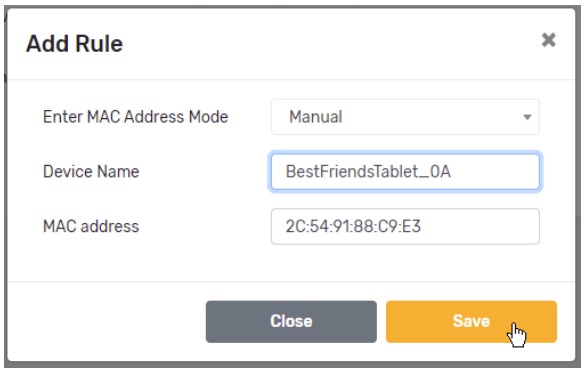


Figure 21 - WiFi - MAC Filter – Add Rule

The new rule will be added to either the Allow or Block list.

Existing rules can be either edited or deleted from each list by clicking the respective button on the rule's row in the Device List table.

Network Setting

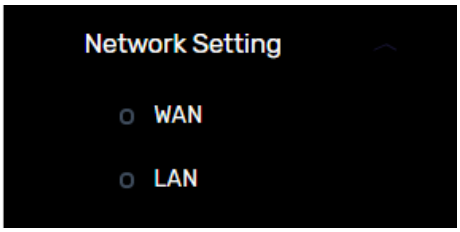


Figure 22 – Network Setting menu

This section provides a variety of options for configuring your WAN or LAN connections.

WAN

To access this page, Network Setting from the menu on the left, then choose WAN.

There are three separate sections on the WAN page:

- WAN Info
- WAN Setting
- Default Gateway & Default DNS

WAN Info

The topmost section of the WAN page contains the WAN Info table.

WAN Info

Status	Interface	Type	IP Version	IP Address	VlanID	IGMP/MLD	NAT	Firewall	Delete
Disconnected	wan0_1	IPOE	IPv4/IPv6	N/A	N/A	Disabled	Enabled	Enabled	
Disconnected	wan0_2	IPOE	IPv4/IPv6	N/A	10	Disabled	Enabled	Enabled	

Figure 23 - Network Setting – WAN Info table

The WAN Info table provides details of the WAN connections of your Wi-Fi 6 Gateway.

WAN Setting

On this page configure standard WAN interface settings.

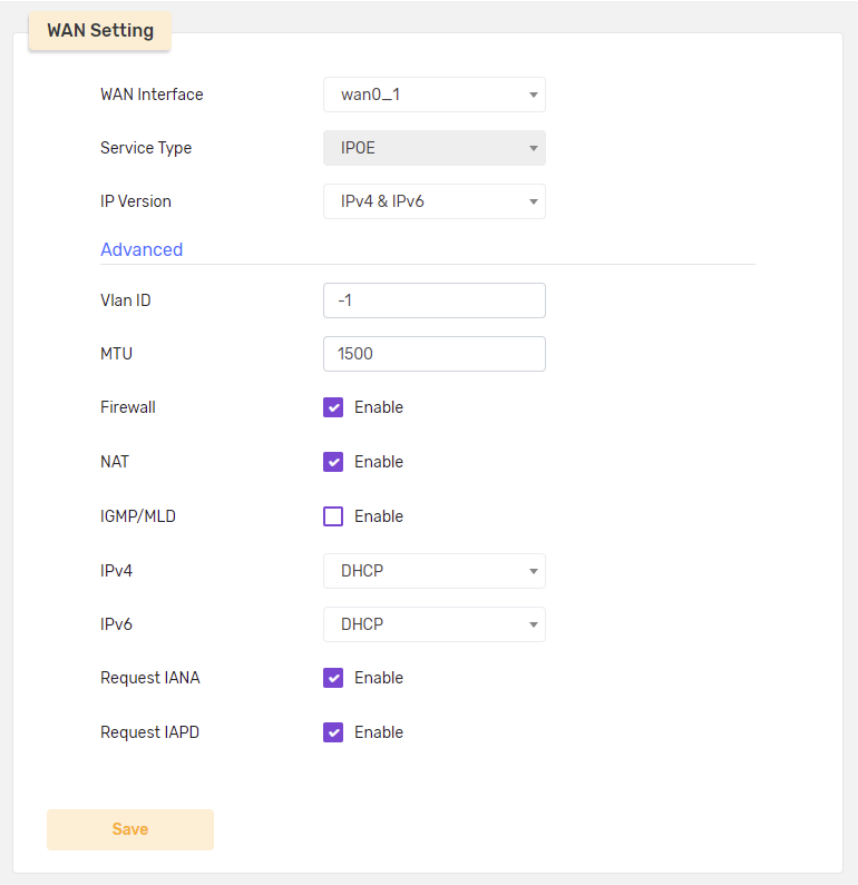


Figure 24 - Network Setting – WAN Setting page

Click the Advanced link to drop down more settings for the WAN.

Default Gateway & Default DNS

Select either IPv4 or IPv6 to view the respective gateway details.

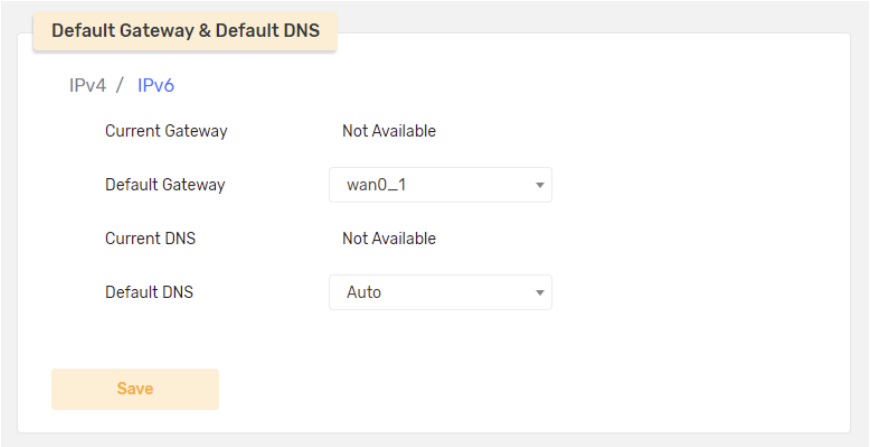


Figure 25 - Network Setting – Default Gateway & Default DNS

LAN

To access this page, **Network Setting** from the menu on the left, then choose **LAN.**

There are three separate sections on the **LAN** page:

- LAN Setting
  - IPv4
  - IPv6
- IP/MAC Binding
- VLAN Setting

LAN Setting

This page lets you configure the local network settings of the router for both of the protocols that are supported by the device: **IPv4** or **IPv6**

IPv4

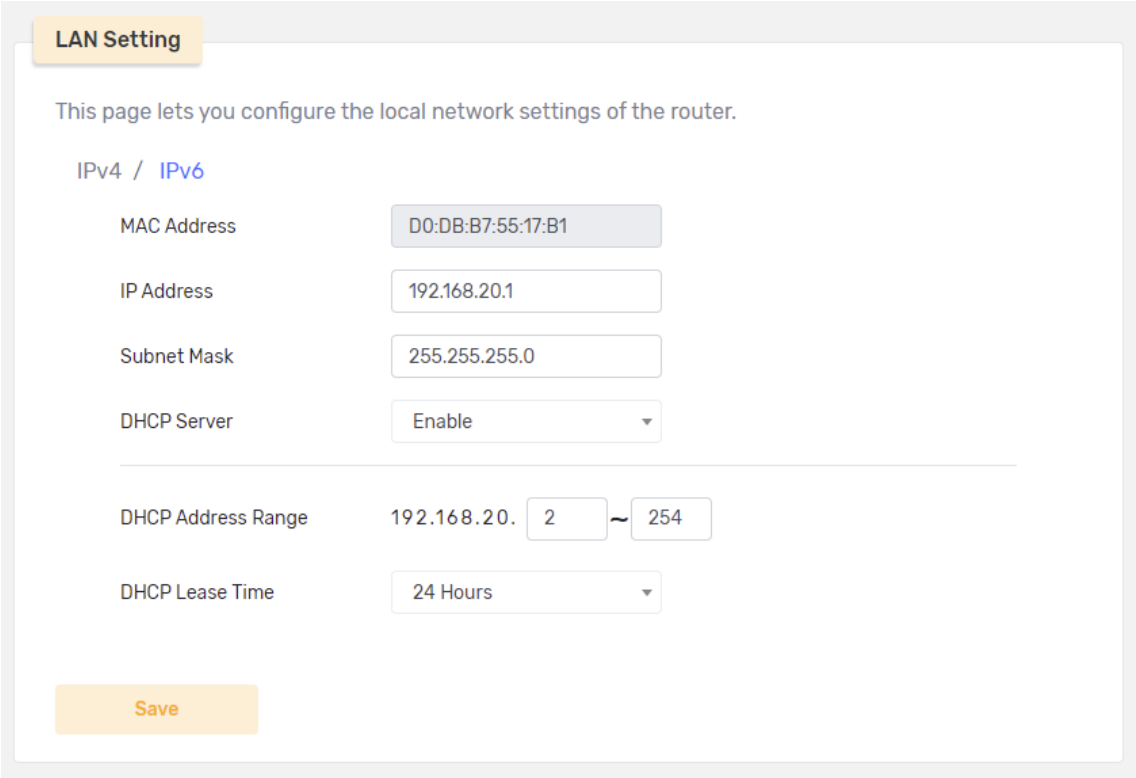


Figure 26 - Network Setting – LAN settings for IPv4

The **LAN Setting** page provides details of the WAN connections of your Wi-Fi 6 Gateway.

IPv6

Click the IPv6 link to display the LAN settings specific to the IPv6 connection.

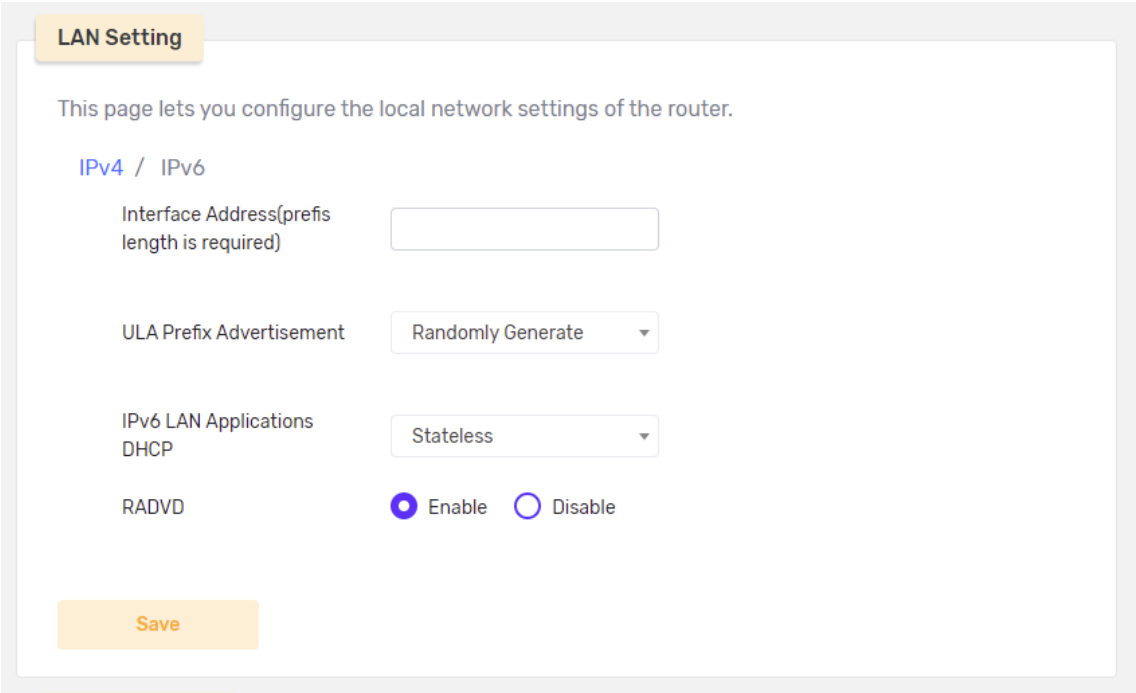


Figure 27 - Network Setting – LAN settings for IPv6

The LAN settings for IPv6page provides configuration options for the Wi-Fi 6 Gateway.

IP/MAC Binding

Use IP/MAC binding to reserve a static IP assignment for a client.

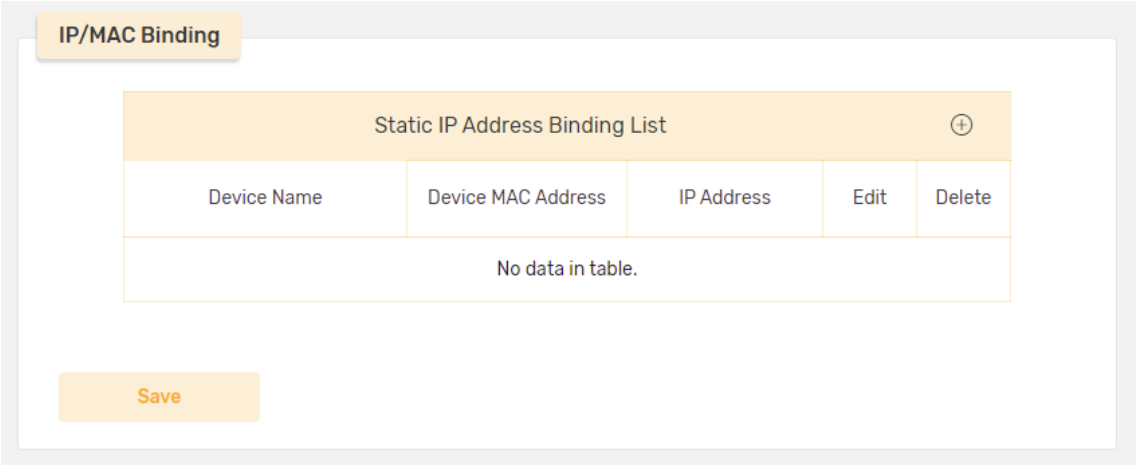


Figure 28 - Network Setting – LAN – Static IP Address Binding list

Add Static IP Address Binding

Select the add button ⊕ in the Static IP Address Binding List heading bar to open the configuration popup box:

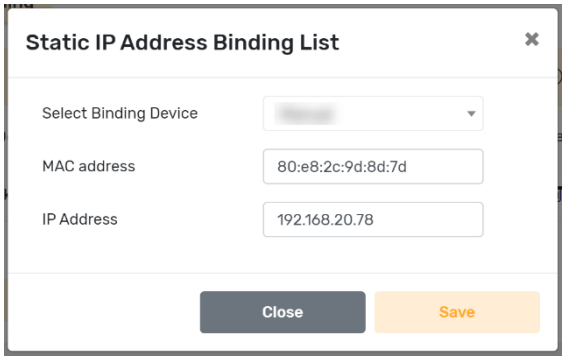


Figure 29 - Advanced Setup – Add Static IP Address Binding list dialog

Enter the device MAC address and IP address, then select the Save button to add the binding. The device appears in the Static IP Address Binding List. Select the Save button below the list to finalise the addition of the new binding.

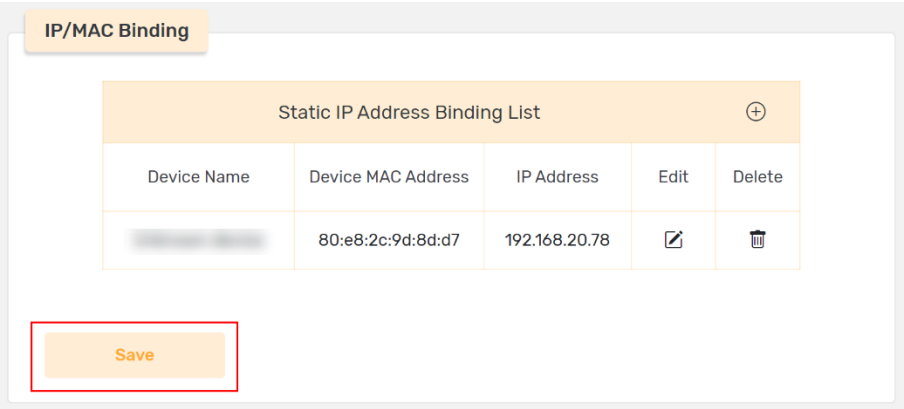


Figure 30 - Advanced Setup – Add Static IP Address Binding list - Save

VLAN Settings

Create a Virtual Local Area Network (VLAN) custom network from one or more existing LANs.

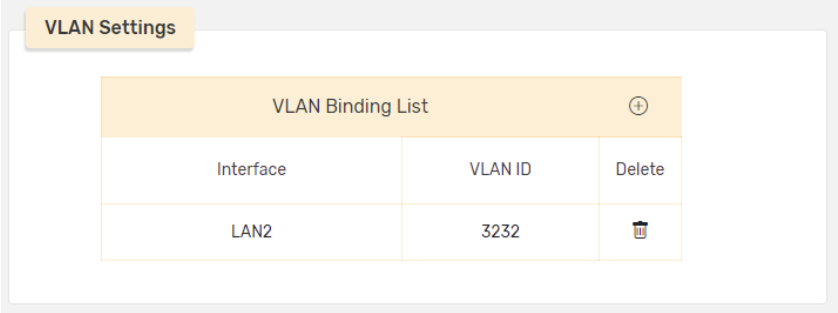


Figure 31 - Network Setting – LAN – VLAN Settings

Add a VLAN Binding

Click the add button ⊕ in the VLAN Binding List heading bar to open the Add Rule popup box:

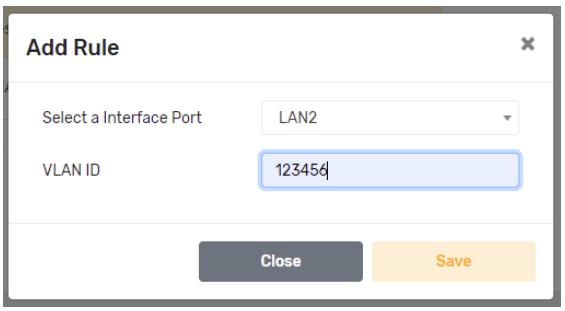


Figure 32 - Advanced Setup – Add VLAN Binding Rule dialog

Enter the new VLAN details. Select an Interface Port from the drop down list and create a VLAN ID [the ID must be a number between 3-4094].

Click the Save button to add the rule to the VLAN Binding List.

Advanced Setup

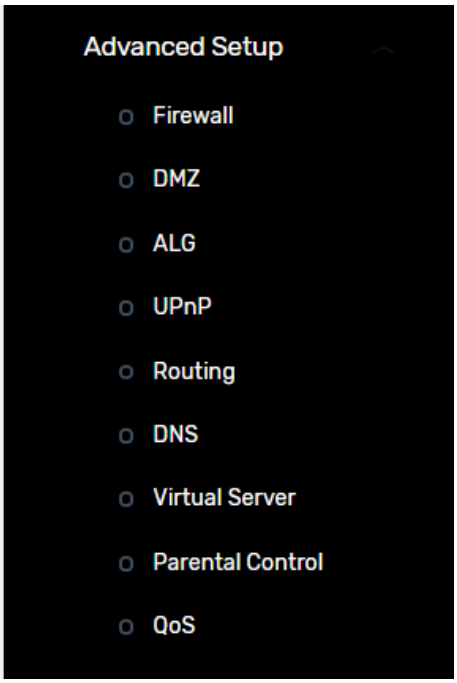


Figure 33 – Advanced Setup menu

This section provides a variety of options for configuring system related settings.

Firewall

The Stateful Packet Inspection (SPI) Firewall and Denial of Service (DOS) Protection options provide you with important protection from malicious attacks.

To access this page, Network Setting from the menu on the left, then choose Firewall.

There are two separate sections on the LAN page:

- Firewall
- Firewall Rules

Firewall

To access this page, select **Advanced Setup** from the menu on the left, then choose **Firewall** from the submenu.

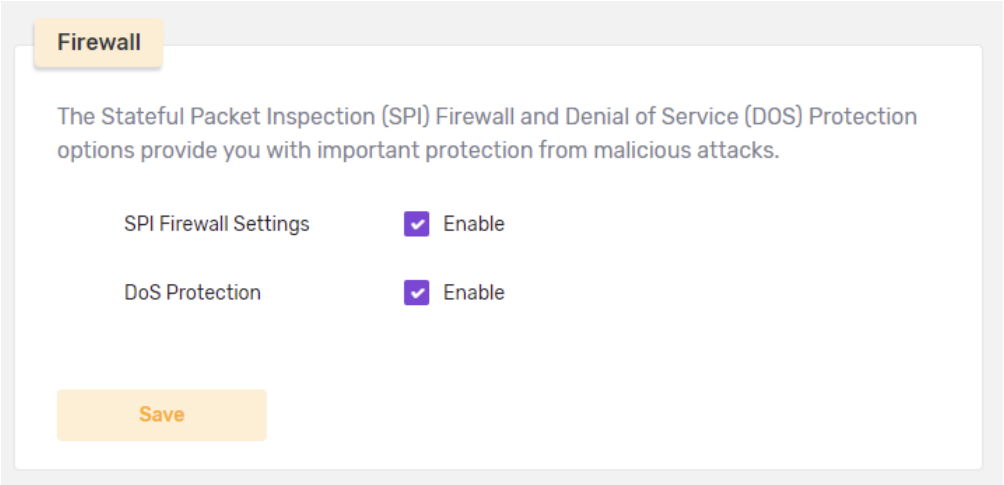


Figure 34 - Advanced Setup – Firewall

The **Firewall** section provides two options for protection from malicious attacks.

Select ☑ **Enable** to apply Stateful Packet Inspection (SPI) measures to your firewalls.

You can also select ☑ **Enable** to apply Denial of Service (DOS) Protection.

Click the **Save** button to apply the selected protective measures to all the **Firewalls**.

Firewall Rules

Firewall Rules may be created to allow or block traffic on your network.

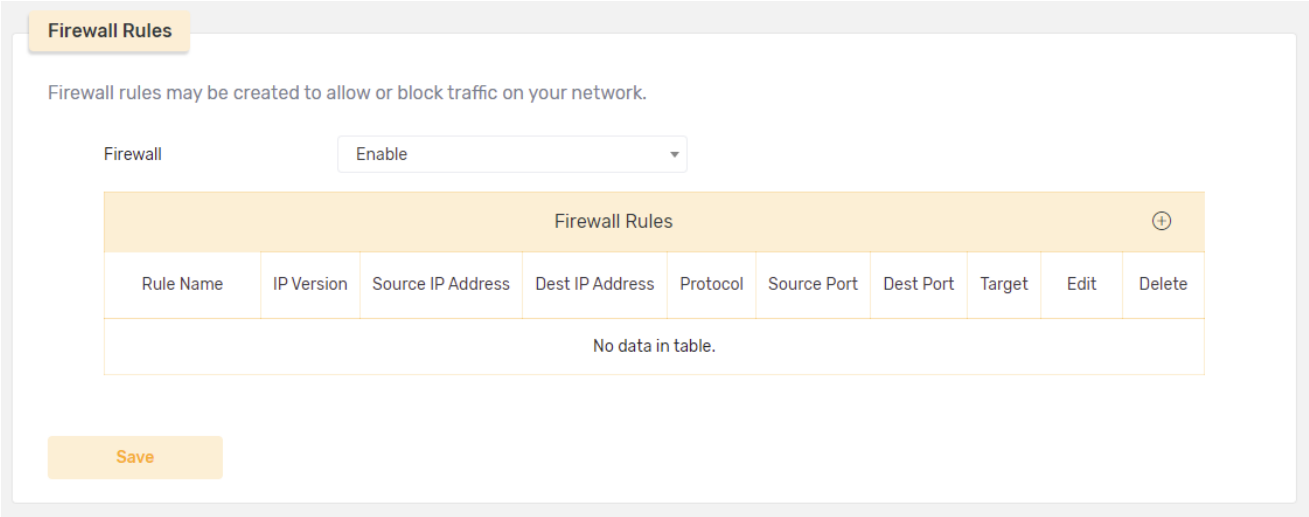


Figure 35 - Advanced Setup – Firewall Rule list

This table provides configuration details of all **Firewall Rules**.

Add Firewall Rule

Click the add button ⊕ in the **Firewall Rule List** heading bar to open the **Add Firewall Route** popup box:

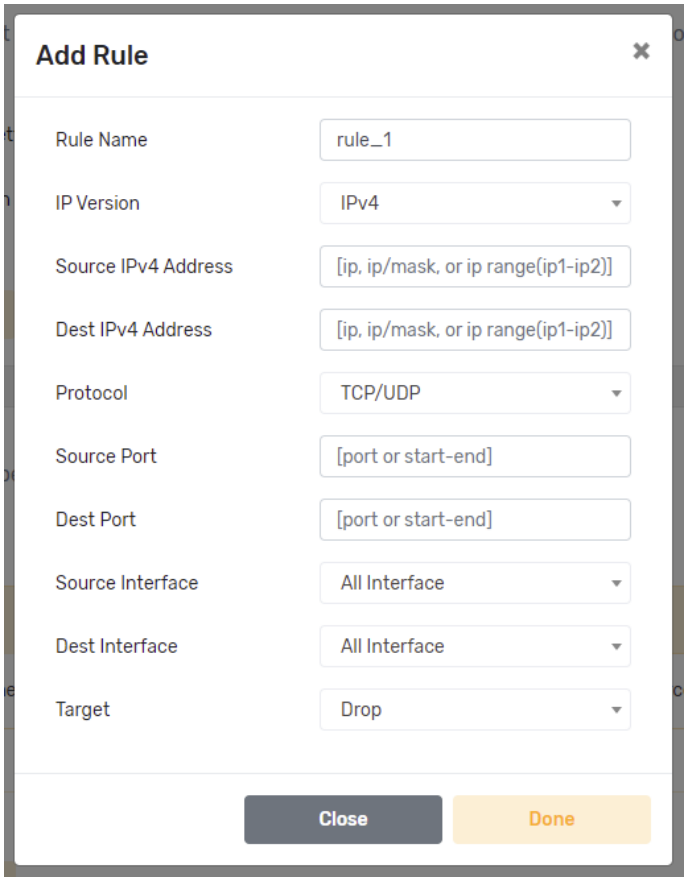


Figure 36 - Advanced Setup – Add Firewall Rule

Create a meaningful **Rule Name** and enter the Firewall configuration options for the new rule.

Click the **Done** button to add the rule to the **Firewall Rules** list.

Edit/Delete Rule

To edit an existing rule in the list, click the rule's edit button, a popup box with he same fields as the Add Rule dialog will open.

To permanently remove an existing rule in the list, click the rule's delete button.

DMZ

The DMZ function allows you to place a specific local device in a “Demilitarized Zone”, i.e. fully open to the internet.

Important – Be aware that this carries risks as all packets are forwarded directly to this device.

To access this page, select Advanced Setup from the menu on the left, then choose DMZ from the submenu.

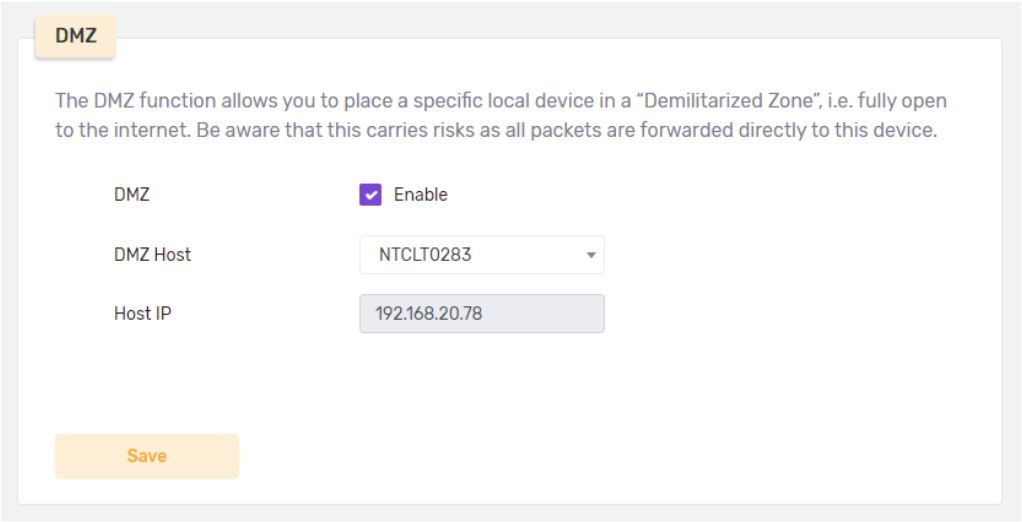


Figure 37 - Advanced Setup – DMZ

To enable a DMZ on a specific, select the Enable button, then select its DMZ Host and enter its Host IP address.

Click the Save button to apply the DMS to the specified device.

ALG

The device supports a number of Application Layer Gateways (ALGs).

To access this page, select Advanced Setup from the menu on the left, then choose LAN from the submenu.

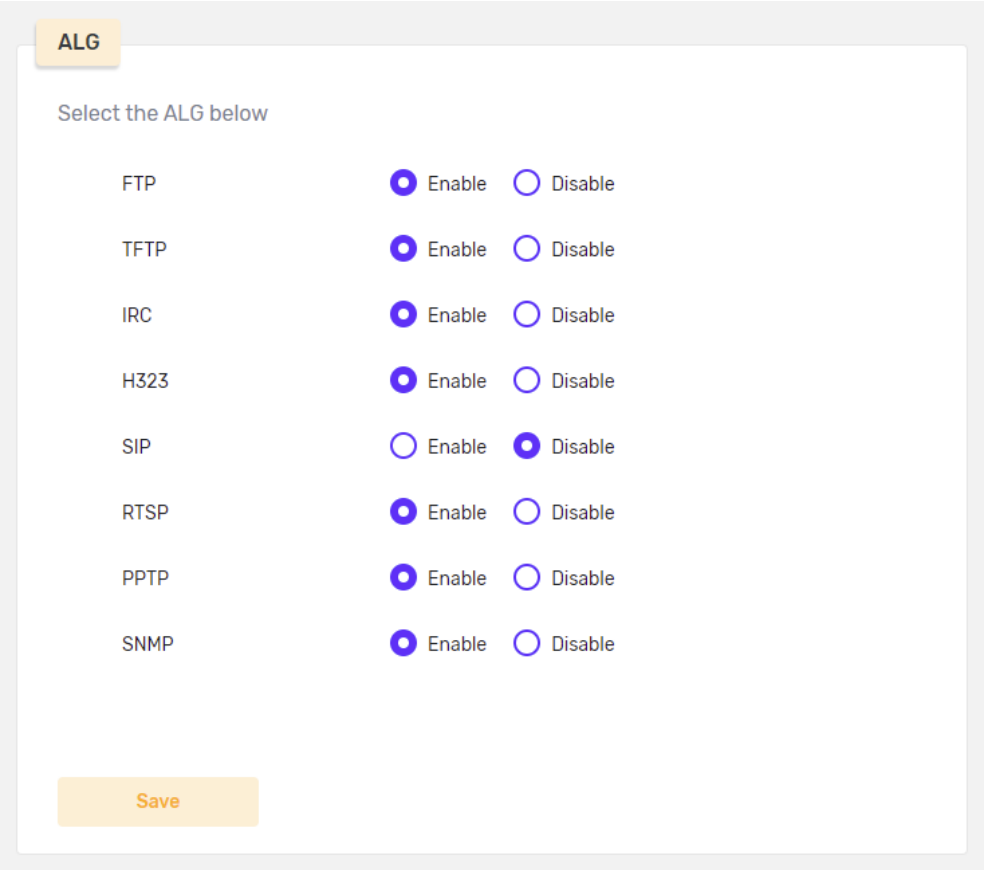


Figure 38 - Advanced Setup – ALG

To enable a gateway type, select the Enable radio button.

UPnP

Universal Plug and Play (UPnP) is a way of quickly forwarding the ports in use to other devices on a network automatically with one setting change and no additional configuration needed.

UPnP Port Forwarding is widely used by many network devices, allowing them to communicate with each other more efficiently and to automatically create workgroups for data sharing, among other applications.

Warning – Important – Security issue
UPnP is not a secure protocol.
It uses network UDP multicasts, no encryption and no authentication.
Despite its convenience, using UPnP may expose your device to public networks and malicious attacks.

To enable this service, select **Advanced Setup** from the menu on the left, then choose **UPnP** from the submenu.

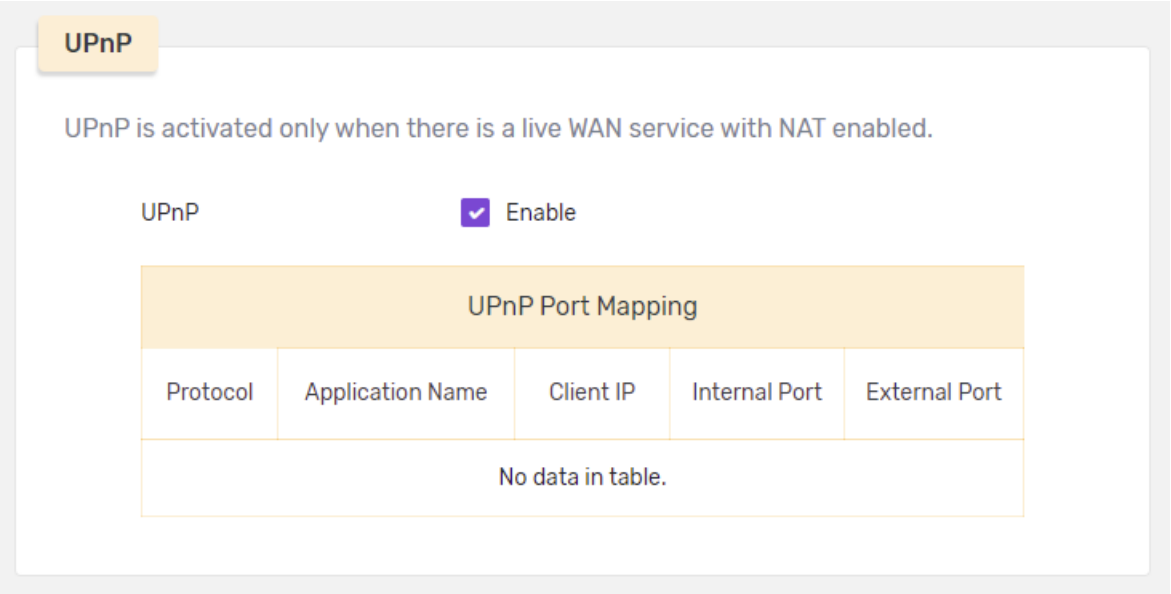


Figure 39 - Advanced Setup – UPnP

Important – UPnP is activated only when there is a live WAN service with NAT enabled.

To enable a UPnP, select the **Enable** button.

Details of UPnP port mapping appear in the data table.

Routing

To access this page, select **Advanced Setup** from the menu on the left, then choose **Routing** from the submenu.

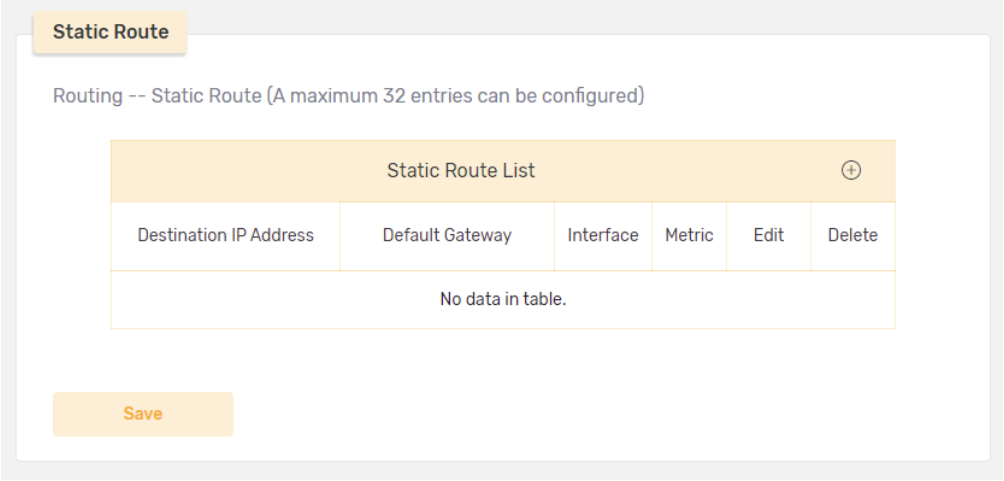


Figure 40 - Advanced Setup – Static Route Rule list

This table provides configuration details of all **Static Routes**. A maximum of 32 routes can be specified.

Add Static Route

Click the add button ⊕ in the Static Route List heading bar to open the Add Static Route popup box:

Figure 41 - Advanced Setup – Add Static Route

Click the Save button to add the rule to the Static Route list.

Edit/Delete Rule

To edit an existing route in the list, click the rule's edit button ✎, a popup box with he same fields as the Add Static Route dialog will open.

To permanently remove an existing rule in the list, click the rule's delete button 🗑.

DNS

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

To access this page, Network Setting from the menu on the left, then choose DNS.

There are two separate sections on the DNS page:

- Dynamic DNS
- DNS Proxy

Dynamic DNS

On this page you can set your own domain name.

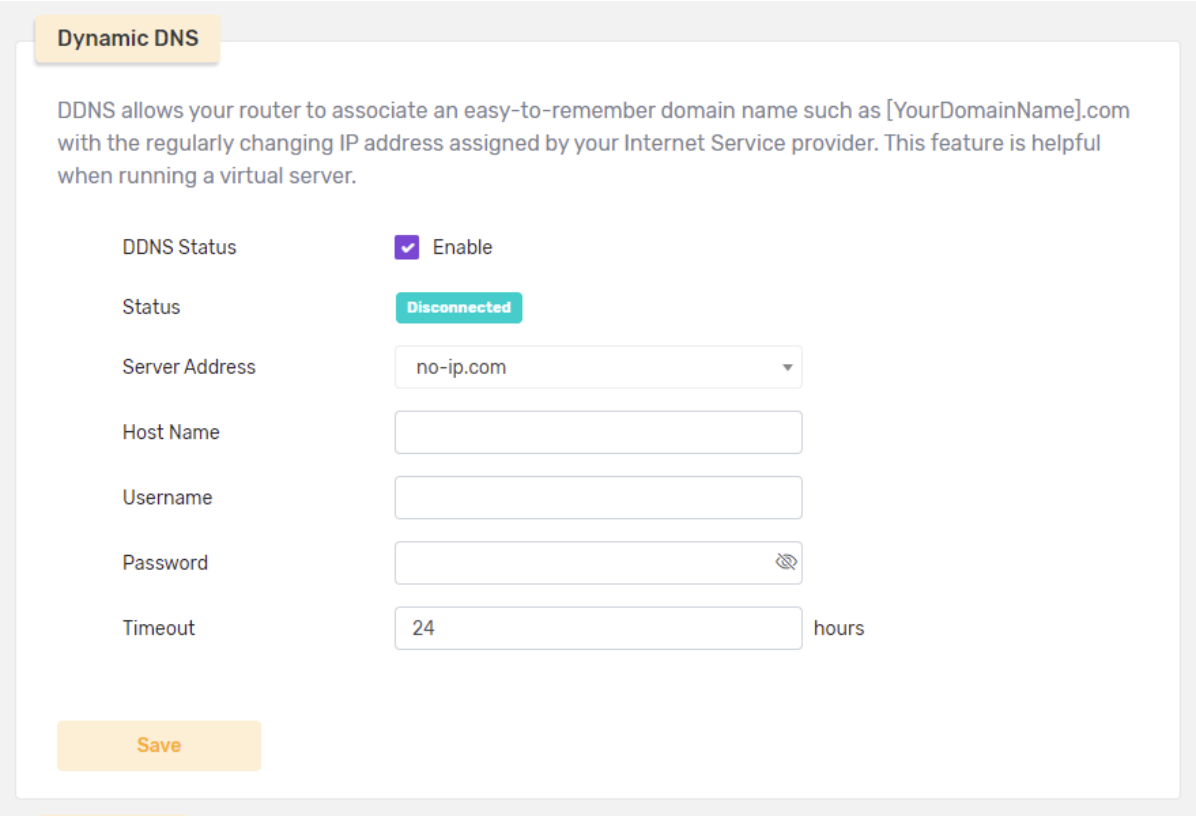


Figure 42 - Advanced Setup – Dynamic DNS

You can also add a password and set a period after which the account will time out and close if there is no activity.

DNS Proxy

To access this page, from the menu on the left, select Advanced Setup, then LAN.

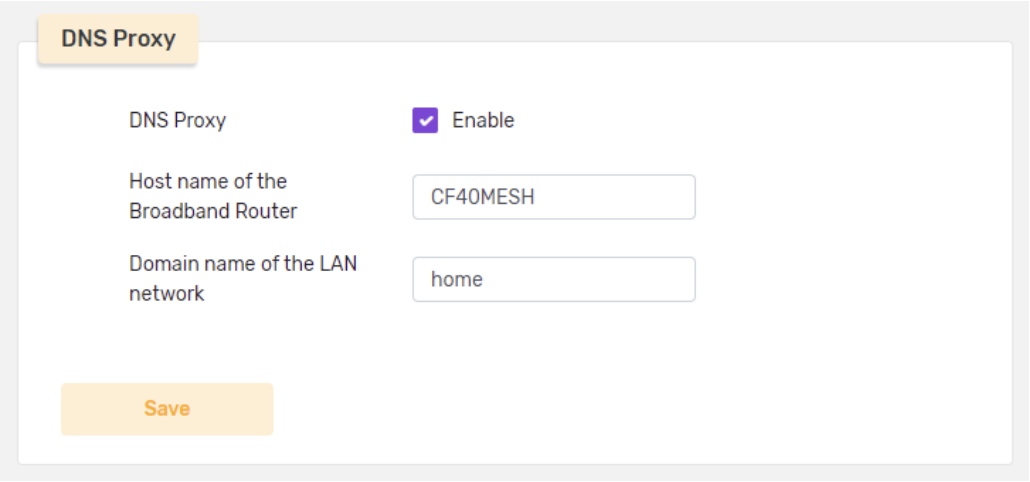


Figure 43 - Advanced Setup – DNS Proxy

Virtual Server

A Virtual Server allows you to direct incoming traffic from the WAN interface (identified by its Protocol and External port) to the Internal server with a private IP address on the LAN interface.

To access this page, select **Advanced Setup** from the menu on the left, then choose **Virtual Server** from the submenu.

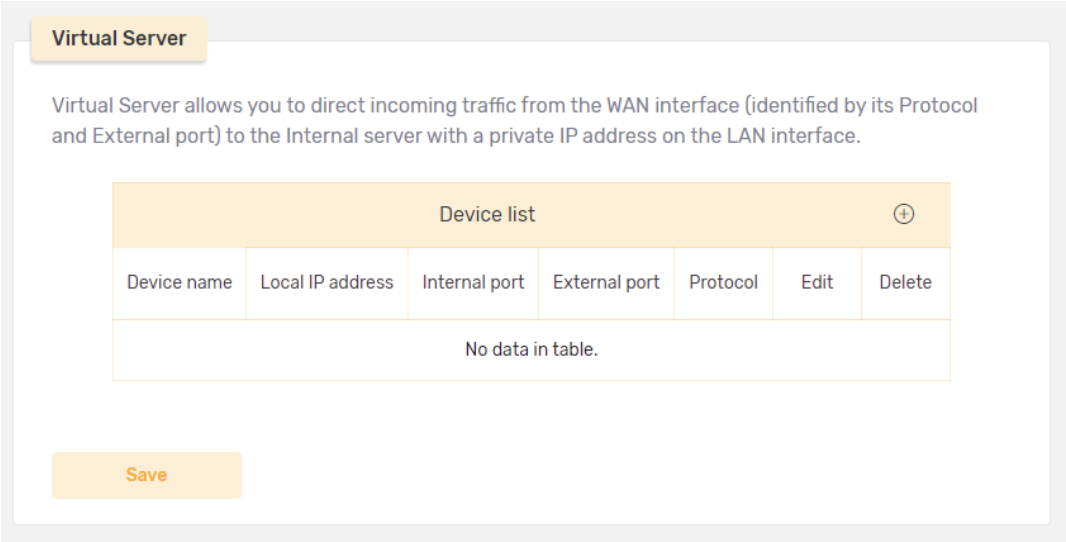


Figure 44 - Advanced Setup – Virtual Server Device List table

The **Device List** provides details of each virtual server.

Add Virtual Server Rule

Click the add button ⊕ in the **Device List** heading bar to open the **Add Rule** popup box:

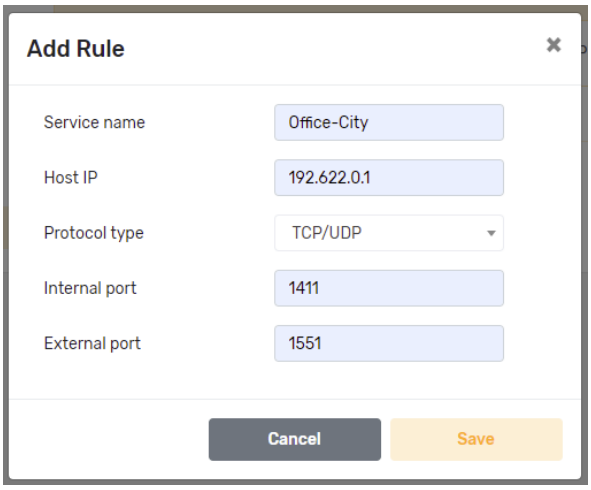


Figure 45 - Advanced Setup – Add Virtual Server Rule dialog

Click the **Save** button to add the rule to the Virtual Server Device list.

Edit/Delete Rule

To edit an existing rule in the list, click the rule's edit button, a popup box with he same fields as the **Add Rule** dialog will open.

To permanently remove an existing rule in the list, click the rule's delete button.

Parental Control

Parental control can be used to restrict internet access to certain website and also based on time.

To access this page, select **Advanced Setup** from the menu on the left, then choose **LAN** from the submenu.

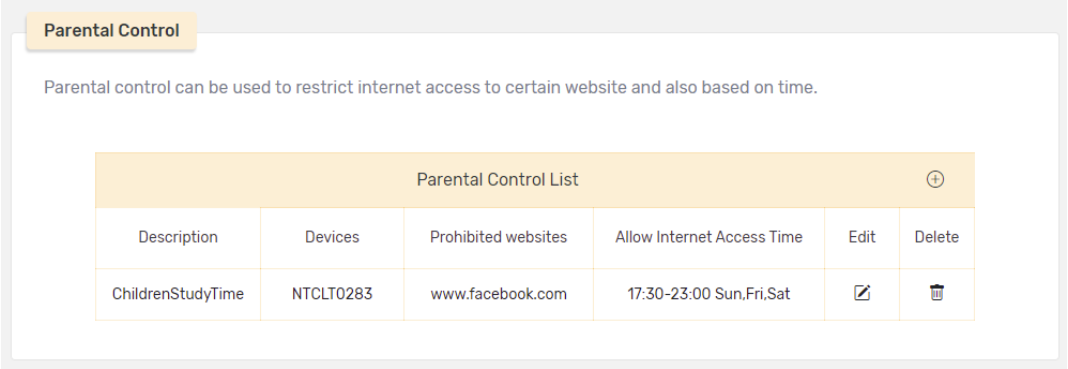


Figure 46 - Advanced Setup – Parental Control List table

The **Parental Control List** provides details of each control rule that you have created.

Add Parental Control Rule

Click the add button in the **Parental Control List** heading bar to open the **Add Rule** popup box:

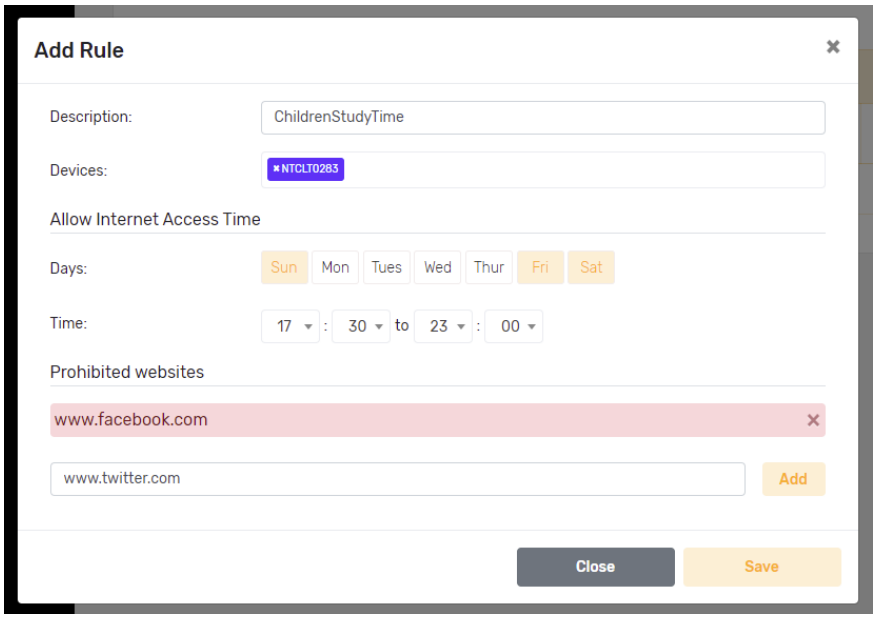


Figure 47 - Advanced Setup – Add Parental Control Rule

Click the **Save** button to add the rule to the **Parental Control List**.

Edit/Delete Rule

To edit an existing rule in the **Parental Control List**, click the rule's edit button, a popup box with he same fields as the **Add Rule** dialog will open.

To permanently remove an existing rule in the list, click the rule's delete button.

QoS

To access this page, **Network Setting** from the menu on the left, then choose **QoS.**

There are four separate sections on the **QoS** page:

- Basic QoS
- Queue
- Classification
- Port Shaping

Basic

To access this page, from the menu on the left, select **Advanced Setup**, then **QoS.**

The first section allows you to **Enable** or **Disable** the QoS functionality and select a default **DSCP Mark.**

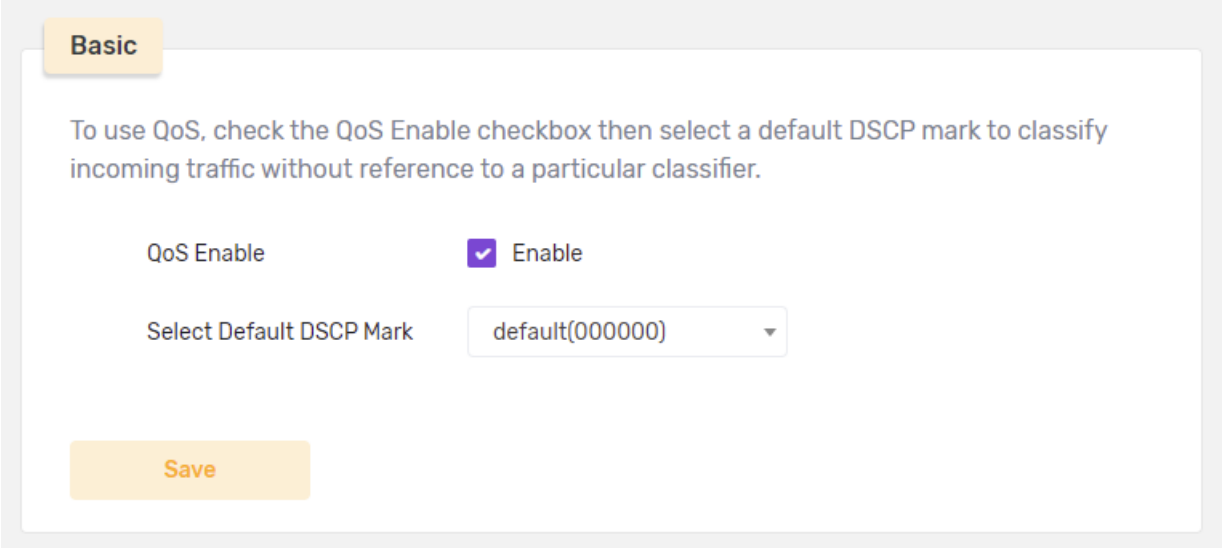


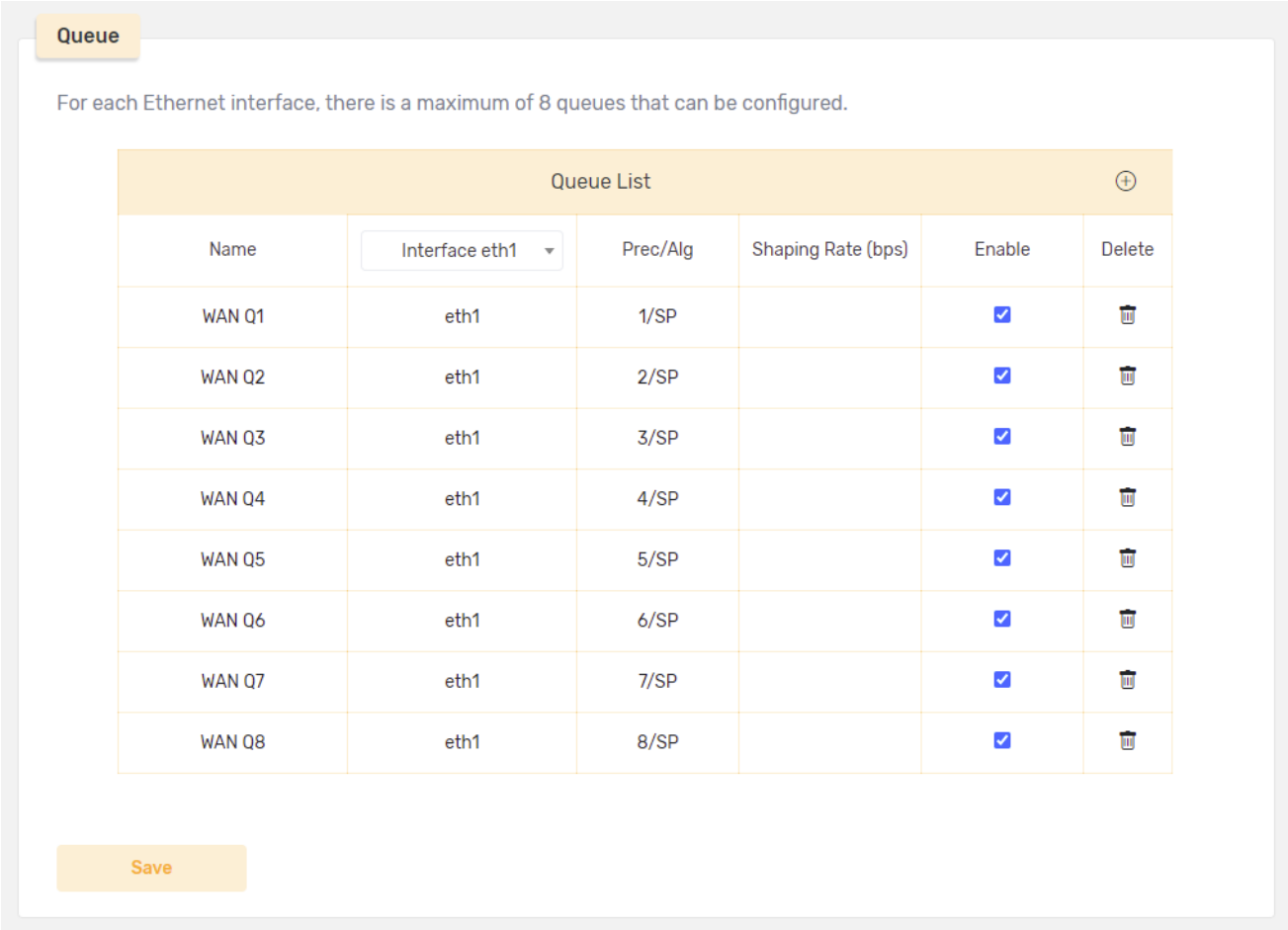
Figure 48 - Advanced Setup – Basic QoS section

Click the **Save** button to add the rule to the apply those settings.

Queue

To access this functionality select **Advanced Setup** from the menu on the left, then **QoS** from its submenu.

The second section of the page contains a **Queue List** showing a maximum of eight queues that can be configured. for each Ethernet interface.



Name	Interface eth1	Prec/Alg	Shaping Rate (bps)	Enable	Delete
WAN Q1	eth1	1/SP		☑	
WAN Q2	eth1	2/SP		☑	
WAN Q3	eth1	3/SP		☑	
WAN Q4	eth1	4/SP		☑	
WAN Q5	eth1	5/SP		☑	
WAN Q6	eth1	6/SP		☑	
WAN Q7	eth1	7/SP		☑	
WAN Q8	eth1	8/SP		☑	

Figure 49 - Advanced Setup – LAN

Select ☑ **Enable** to apply the queue to the selected Ethernet interface.

To permanently remove an existing rule in the list, click the rule's delete button 🗑.

Add Queue Rule

Click the add button ⊕ in the **Queue List** heading bar to open the **Add Rule** popup box:

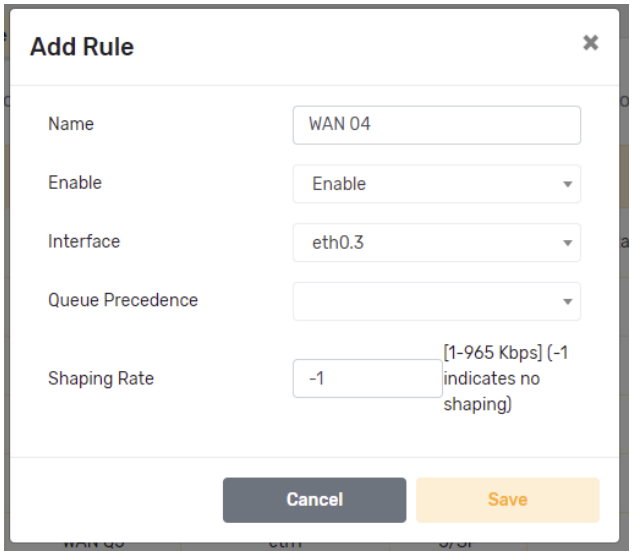


Figure 50 - Advanced Setup – LAN

As a maximum number of eight queues are allowed at any time, select one of the eight **Interfaces** to edit.

Click the **Save** button to make changes to the queue.

Classification

To access this functionality select **Advanced Setup** from the menu on the left, then **QoS** from its submenu.

The third section of the page contains a **Classification List**.

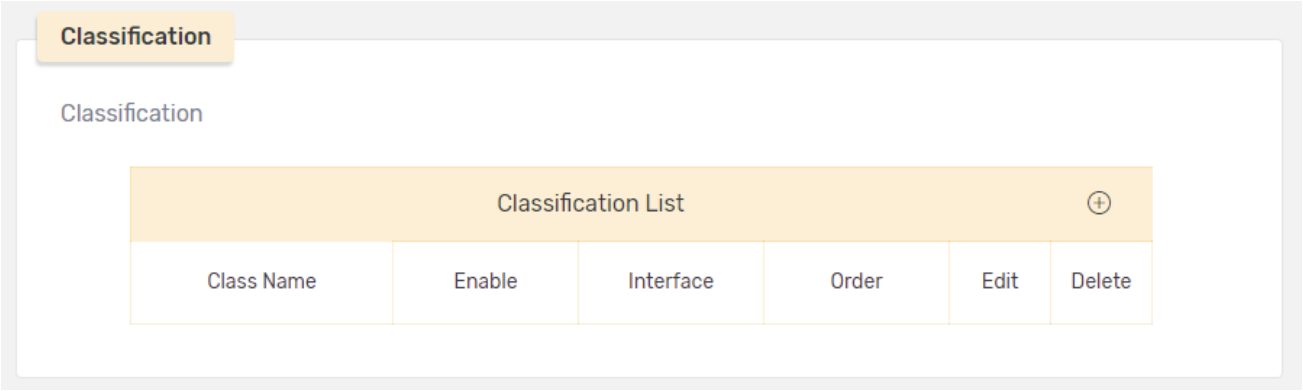


Figure 51 - Advanced Setup – LAN

Add Classification Rule

Click the add button ⊕ in the **Classification List** heading bar to open the **Add Rule** popup box:

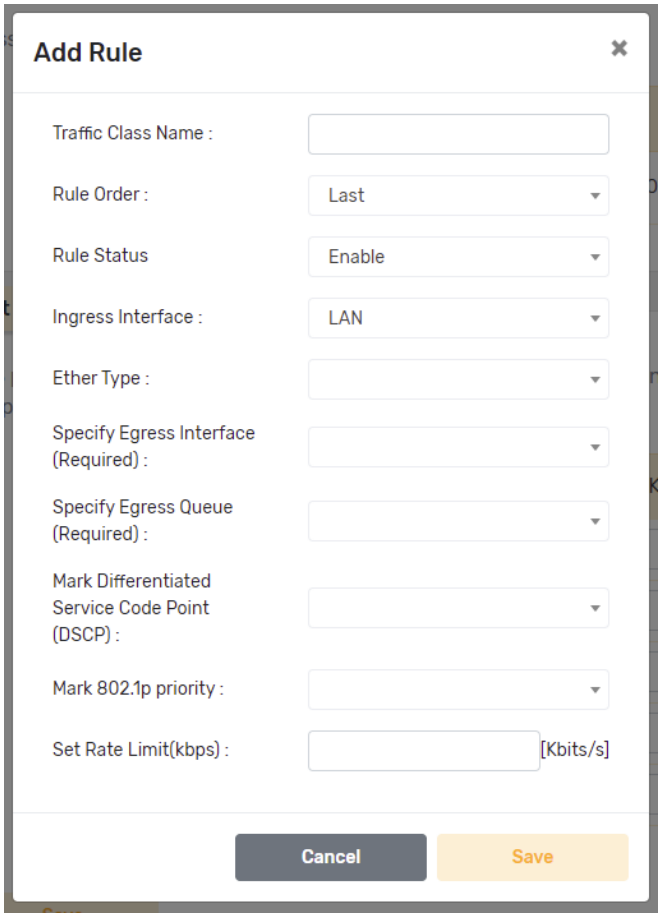


Figure 52 - Advanced Setup – LAN

Click the **Save** button to make changes to the classification rule.

Port Shaping

QoS port shaping supports traffic shaping of Ethernet interface.

To access this functionality select **Advanced Setup** from the menu on the left, then **QoS** from its submenu.

The fourth section of the page contains a table showing **Port Shaping** details.

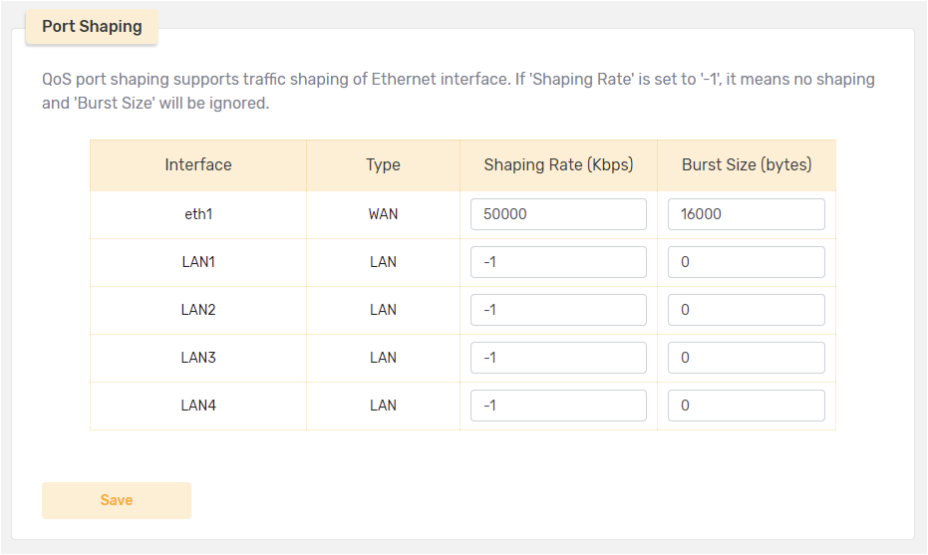


Figure 53 - Advanced Setup – LAN

Note that if **Shaping Rate (Kbps)** is set to '**-1**', it means no shaping and **Burst Size (bytes)** will be ignored.

Enter new settings into the fields and click the **Save** button to make changes to the **Port Shaping** settings.

Management

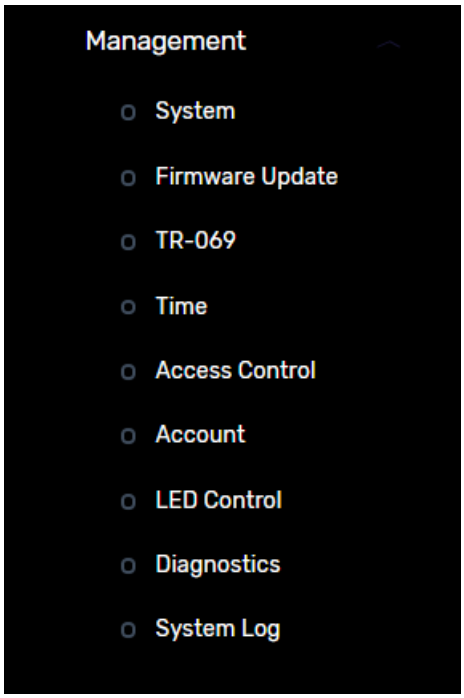


Figure 54 – Management menu

This section provides a variety of options for configuring system related settings.

System

To access this page, select Management from the menu on the left, then choose System from the submenu.

There are three separate sections on the System page:

- Reboot and Reset
- Backup and Restore
- Timeout

Reboot and Reset

Click the Reboot button to turn the device off and then back on using the existing settings.

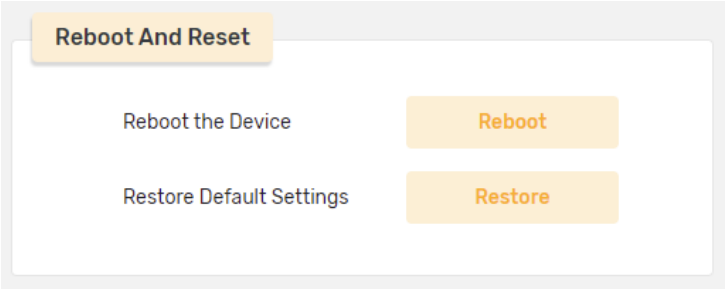


Figure 55 - Management – System – Reboot and Reset page

If the problem you are troubleshooting persists, click the Reset button to delete current user defined settings and reapply all factory default settings. This will permanently delete all current settings.

Note – We recommend that prior to clicking the Restore button you create a backup file which you can later use to restore those settings should the problem not be solved by restoring the factory default settings.
See next section for the Backup and Restore process.

Backup and Restore

Backup

Click the Backup button to create a backup file which contains all the current settings.

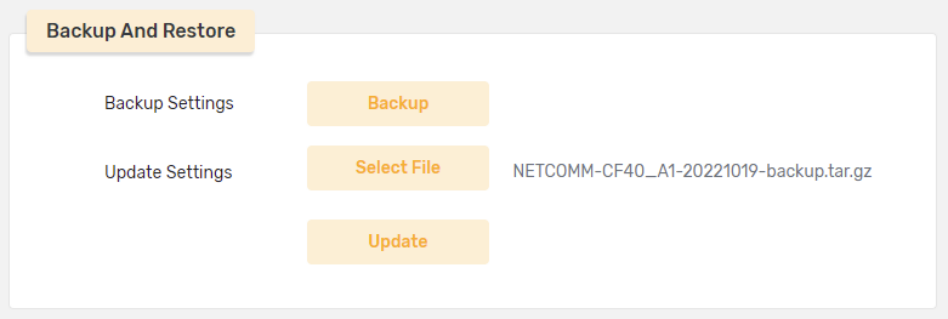


Figure 56 - Management – System –Backup and Restore page

A file with device details and the **`-backup.tar.gz`** file extension will be downloaded into your browser's default download folder.

Restore

If required to return the system's configuration to what it was prior to Resetting the device, first click the Select File button to select the backup file from the browser's default download folder [or another location if you have moved it].

When a valid backup file has been selected, the Update button will appear.

Click the Update button to reapply the previously defined user settings.

The process will take a few minutes and the following progress indicator will appear:

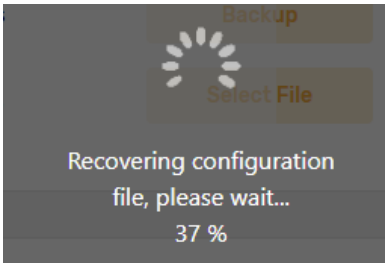


Figure 57 – Restore progress indicator

When the process is over the backup file's settings will over-write any differing factory default settings.

Timeout

Enter the amount of time that the device can remain logged up when no interaction has occurred.

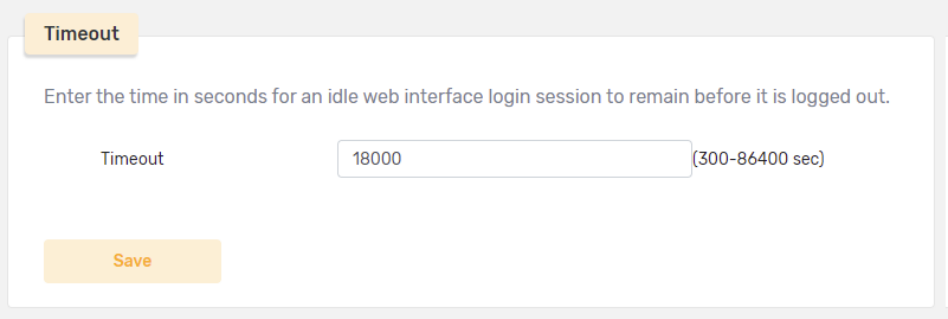


Figure 58 - Management – System –Timeout page

The time is entered in seconds, for example if you want to set the unattended **Timeout** time to 5 hours enter:

18,000 seconds which = 300 minutes (seconds/minutes) which = 5 hours (minutes/hours)

Firmware Update

From time to time the firmware on the device will be updated by the manufacturer and distributed to current users in an image file.

If you become aware of a new firmware version image file, download it and put it into a known location.

To access this page, select **Management** from the menu on the left, then choose **Firmware Update** from the submenu.

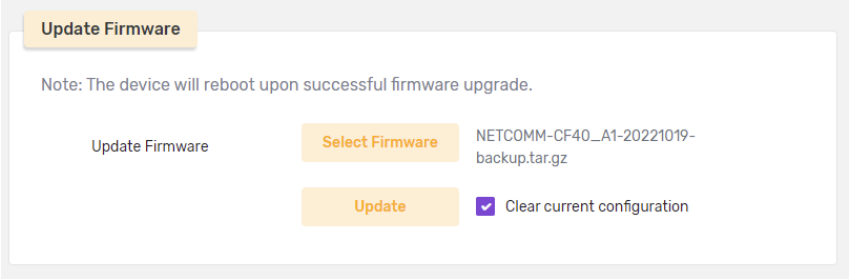


Figure 59 - Management – LAN

Click **Select Firmware** button, navigate to the folder where the downloaded file was saved.

Select the firmware update image file and click the **Open** button. Once successfully uploaded, the filename will appear to the left of the **Select Firmware** button and the **Update** button to install the firmware.

If you want to remove the existing firmware image files select ☑ **Clear current configuration** permanently delete the previous firmware files.

TR-069

The WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to remotely perform auto-configuration, provision, collection, and diagnostics to this device.

To access this page, select **Management** from the menu on the left, then choose **TR-069** from the submenu.

By default the TR-069 functionality is disabled, select ☑ **Enable** to display the following settings fields:

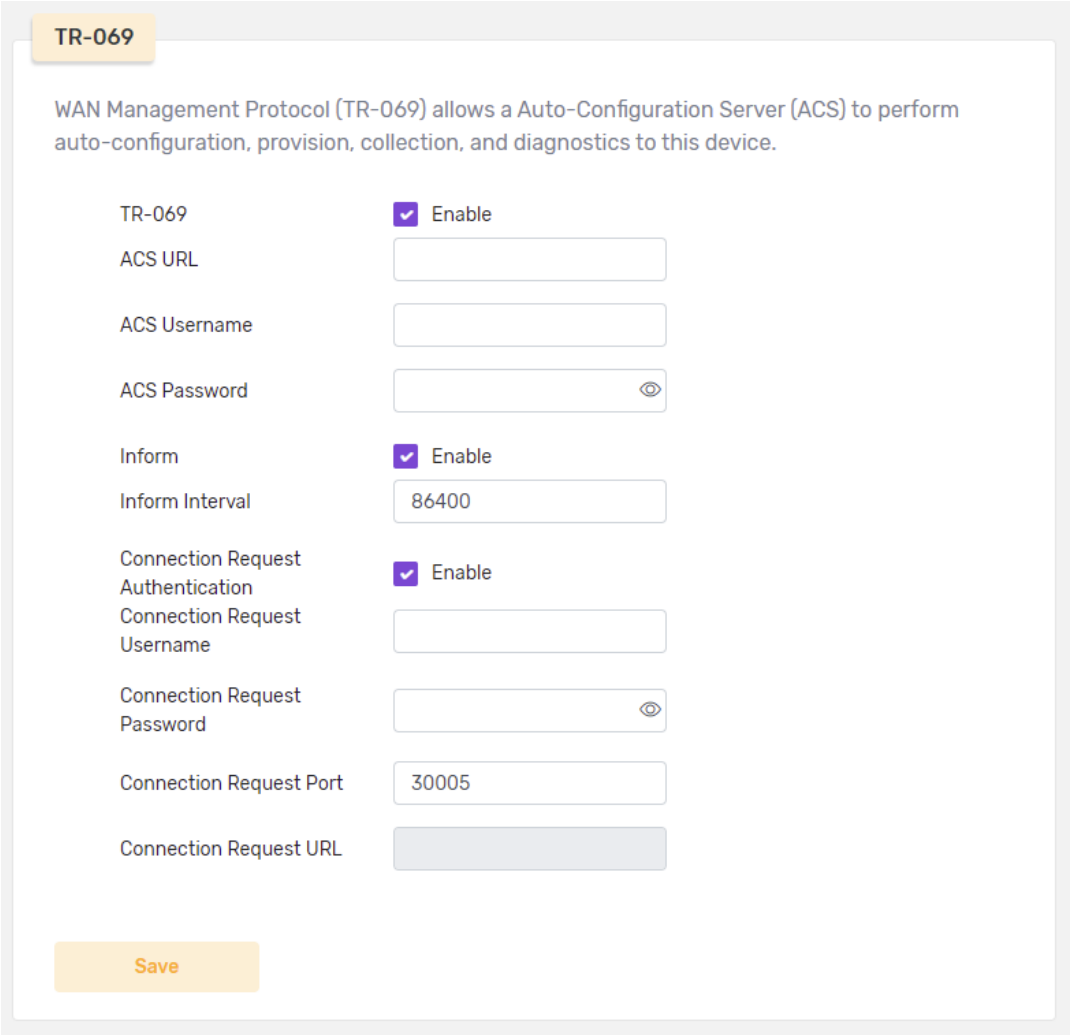


Figure 60 - Management –TR-069 – display settings

Select ☑ **Enable** for either Inform or Connection Request Authentication to apply additional security settings.

Click the **Save** button to allow TR-069 access based on those settings.

Time

To ensure the accuracy of the system time, synchronize the router's system time with the network time. You can also elect to use **Daylight Saving Time** if it applies to your area.

To access this **Time Setting** page, select **Management** from the menu on the left, then choose **Time** from the submenu.

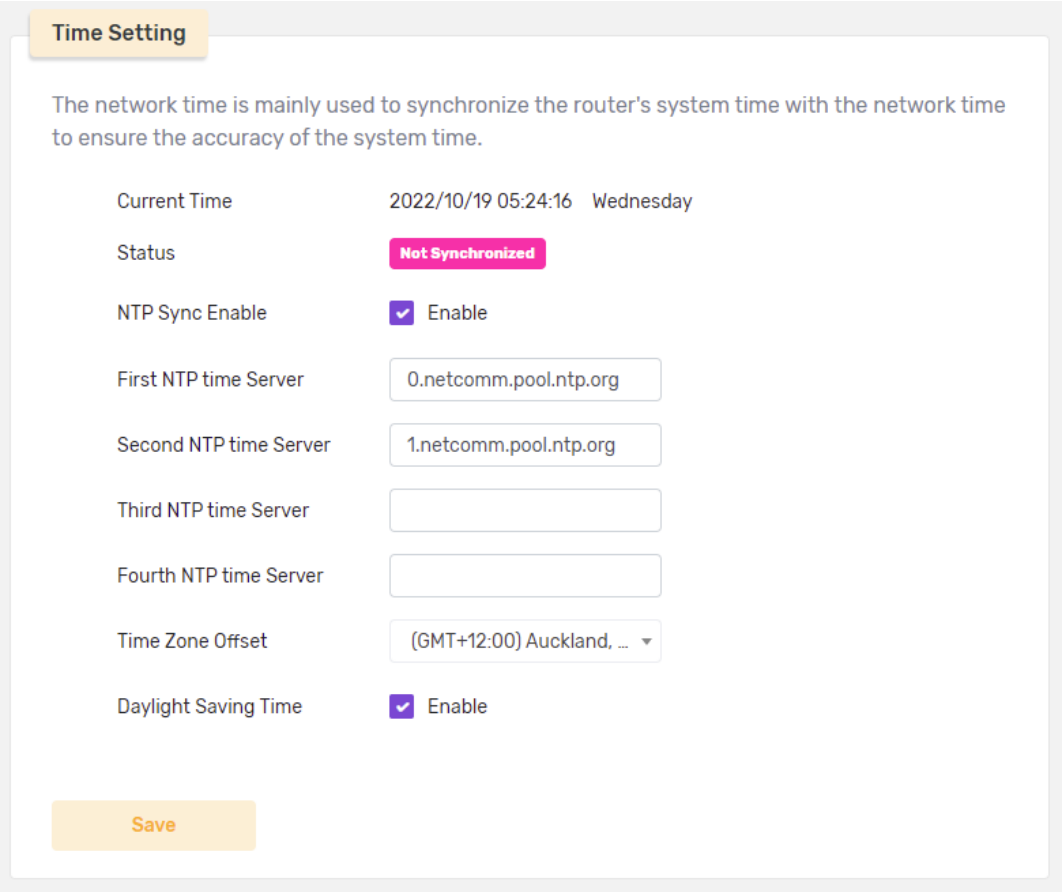


Figure 61 - Management – Time Setting page

Click the **Save** button to add the rule to the apply those settings.

Access Control

To access this page, Management from the menu on the left, then choose Access Control from the submenu.

There are two separate sections on the Access Control page:

- Services Control
- Access List

Services Control

The Services Control page allows you to enable or disable the services running on the router:

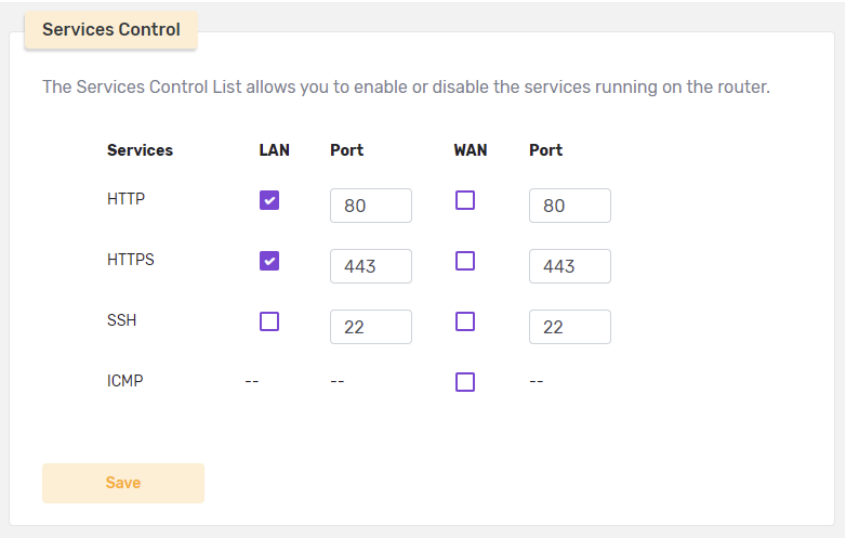


Figure 62 - Advanced Setup – Access Services Control page

Click the Save button to add the rule to the apply those settings.

Access List

The IP Address Access Control mode, if enabled, permits access to local management services from the WAN side IP addresses contained in the Access Control List.

If the Access Control mode is disabled, the system will not validate the WAN side IP addresses for incoming packets. The services affected are the system applications listed in the Service Control List.

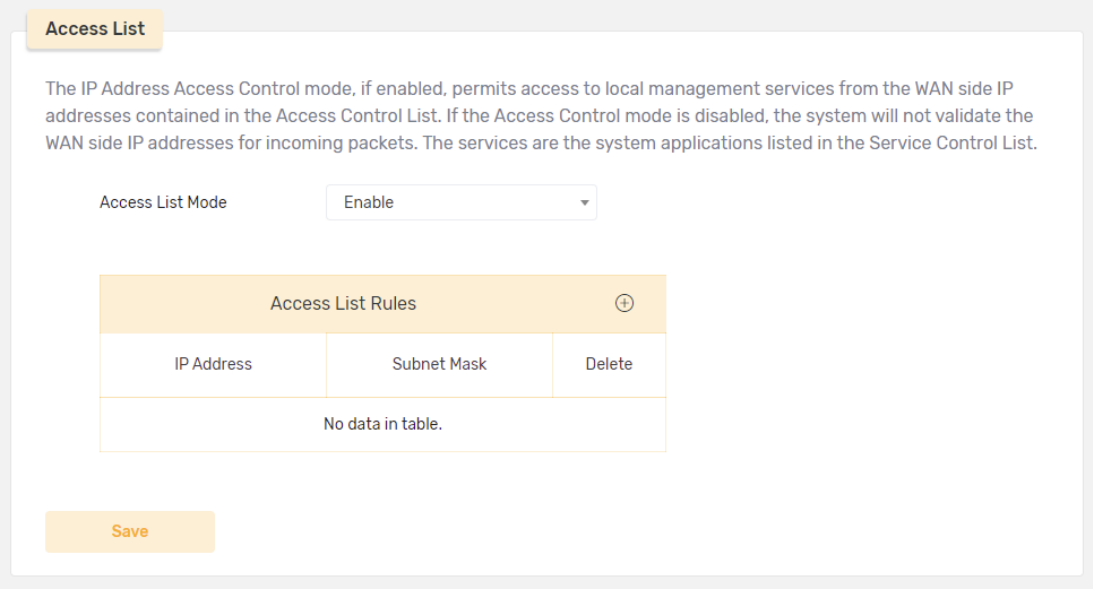


Figure 63 - Management – Access Rules List

Click the **Save** button to **Enable** or **Disable** the rules described in the table for this functionality.

Add Access Rule

Click the add button ⊕ in the **Access List** heading bar to open the **Add Rule** popup box:

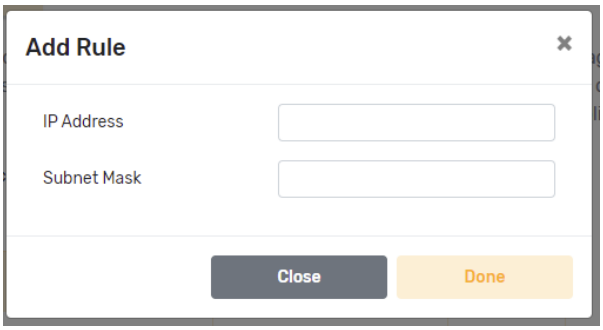


Figure 64 - Advanced Setup – Add Access Rule dialog

Click the **Done** button to add the new rule to the **Access List** table.

Account

Access to your broadband router is controlled through your admin account.

The username 'admin' has unrestricted access to change and view configuration of your Broadband Router.

To access this page, select **Management** from the menu on the left, then choose **Account** from the submenu.

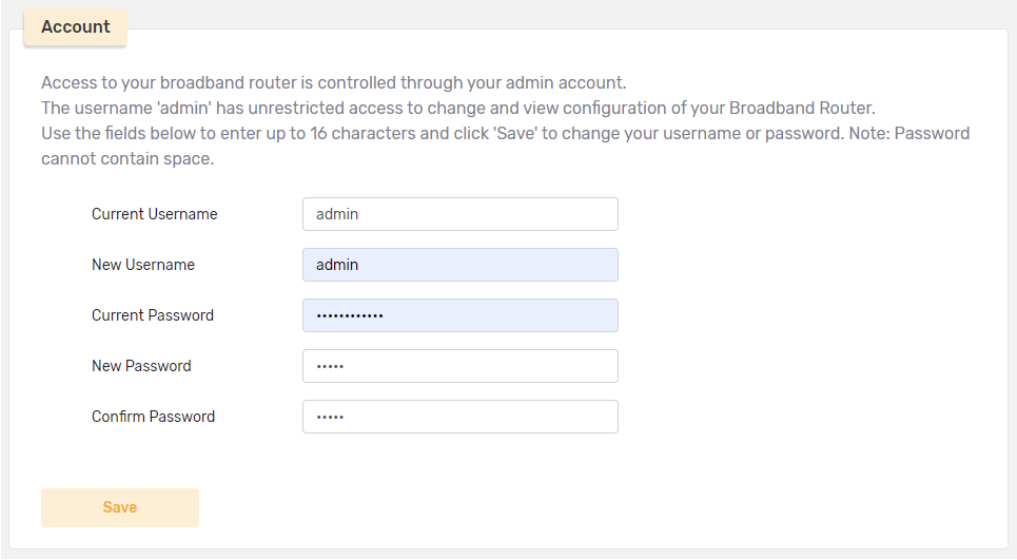


Figure 65 - Management – Account access settings

Enter up to 16 characters in each of the fields.

Note – The **Passwords** cannot contain spaces.
Also the **Passwords** are case-sensitive.

Click the **Save** button to add the rule to change your username and/or password.

LED Control

In some environments, for example is a bedroom, the continuous display of LED lights can be undesirable. The LED Control setting allows you to turn on or off LED indicator display on the top panel of the router.

To access this page, select **Management** from the menu on the left, then choose **LED Control** from the submenu.

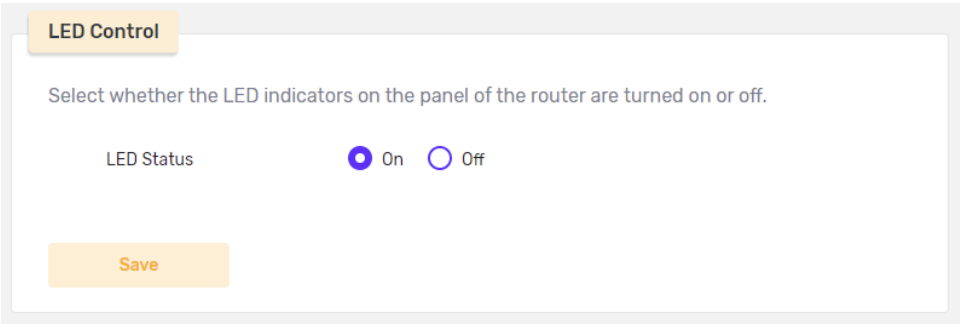


Figure 66 - Management – LED display controls

To allow the LEDs to display select the On radio button.

To turn off the LED display select the Off radio button.

Click the Save button to apply the setting.

Diagnostics

To check the connection automatically, type in a host name or an IP Address and the perform either a Ping or Traceroute diagnosis and click the Start button.

To diagnose any connection issues, select Management from the menu on the left, then choose Diagnostics from the submenu.

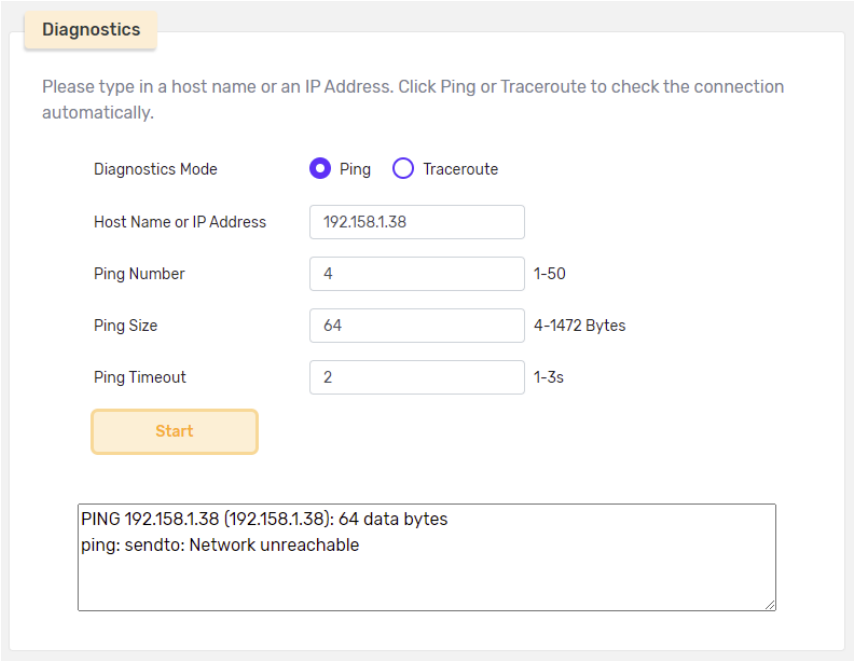


Figure 67 - Management – Diagnostics

The following progress indicator will appear while the test is in progress.

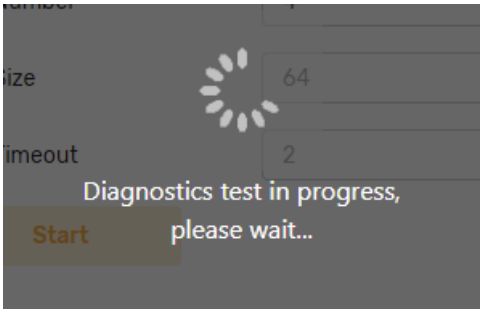


Figure 68 – Diagnosis in progress icon

System Log

The **Systems Log** records a range of types of the device's operation and equipment exceptions

To access this page, select **Management** from the menu on the left, then choose **System Log** from the submenu.

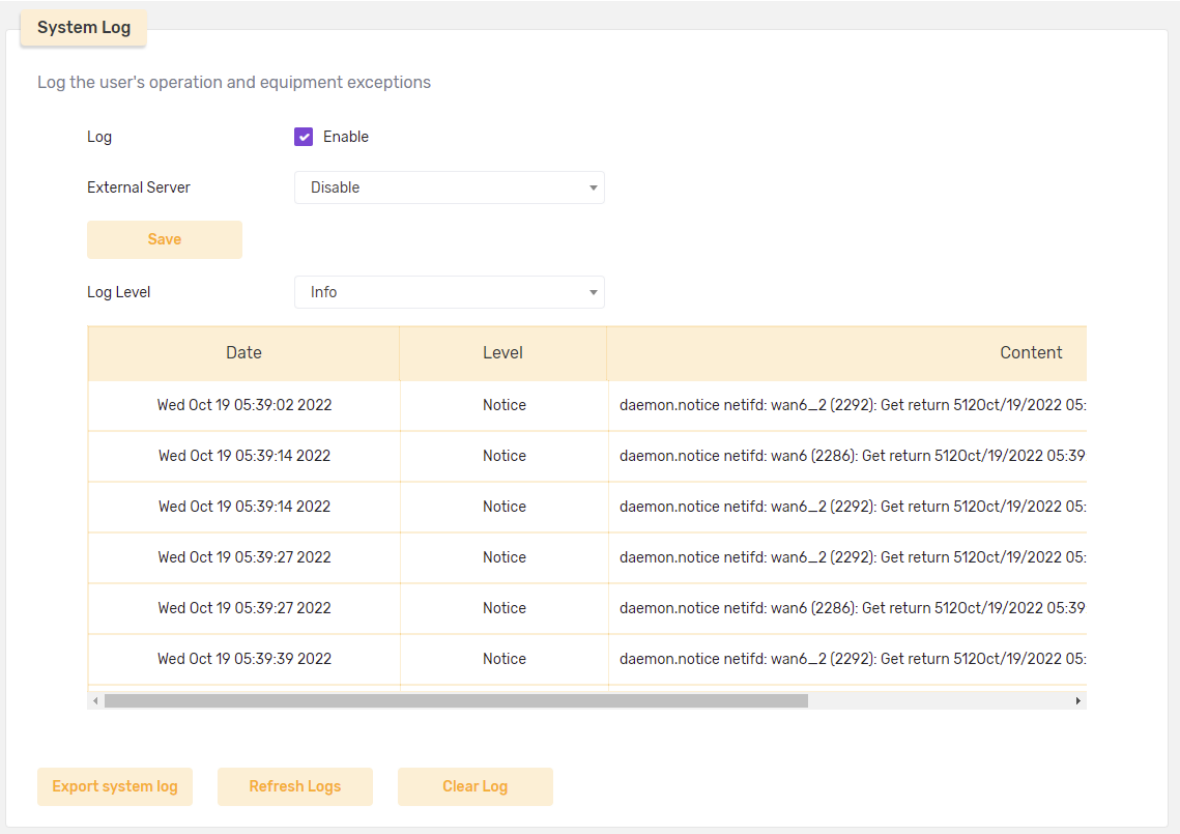


Figure 69 - Management – System Log

This page allows you to ☑ **Enable** or ☐ disable the log and to specify what **Log Level** (type of information) you want to display in the table (**Debug**, **Info**, **Notice**, **Warning**, **Error**, **Critical**, **Alert** or **Emergency**).

Three buttons at the bottom of the page control logging operations:

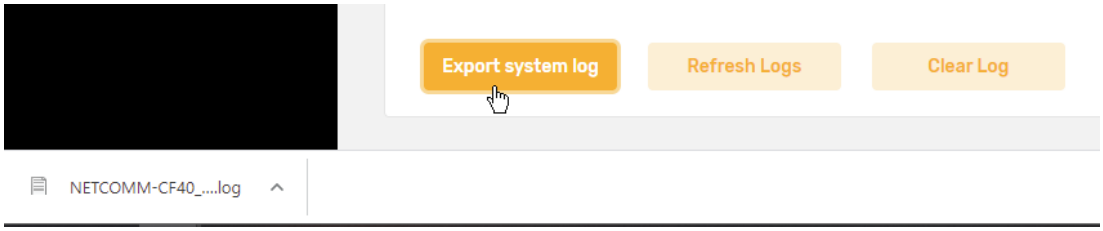


Figure 70 - Management – Logging option buttons

Refresh

After changing the Log Level click the Refresh Logs button to update the log with the most recent data for that type of data.

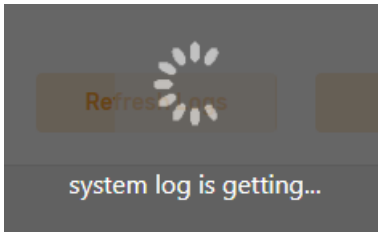


Figure 71 – Refreshing logs progress indicator

Export System Log

Once the logging is complete, click the Export System Logs button to save a text .log file into your browser's default Download folder.

Clear

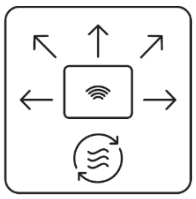
Click the Clear Logs button to delete all current logged data.

Appendix A – Safety and Compliance

Location

- The device is designed for indoor use only.
- Place the device in a central location for the best WiFi performance.

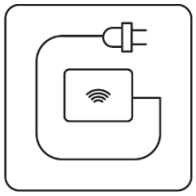
Airflow



- Do not restrict airflow around the device.
- The device is air-cooled and may overheat if airflow has been restricted.
- Always allow minimum clearance of 5cm around all sides and the top of the device.
- The device may become warm during normal use.
- Do not cover, do not put in an enclosed space, do not put under or behind large items of furniture.

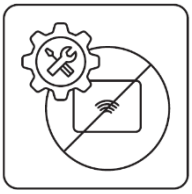
Environment

- Do not place the device in direct sunlight or any hot areas.
- The safe operating temperature of the device is between 0° and 40°C
- Do not allow the device to come in contact with any liquid or moisture.
- Do not place the device in any wet or humid areas such as kitchen, bathroom or laundry rooms.



Power Adaptor

- Always use the power adaptor that came with the device.
- You should immediately stop using the power adaptor if the cable or power adaptor is damaged.



Service

- Do not attempt to disassemble, repair, or modify the device.
- There are no user-serviceable components in the device.

Small Children

- Do not leave the device or its accessories within the reach of small children or allow them to play with it.
- The device may contain small parts with sharp edges that could cause an injury or which could become detached and create a choking hazard.

RF Exposure

- The device contains a transmitter and a receiver. When it is on, it receives and transmits RF energy.
- The device conforms with the radio frequency (RF) exposure limits adopted by the Australian Communications and Media Authority (ACMA), when used at a distance of not less than 20 cm from the body.

Product Handling

- Always treat the device and its accessories with care and keep them in a clean and dust-free place.
- Do not expose the device or its accessories to open flames.
- Do not drop, throw or try to bend the device or its accessories.
- Do not use harsh chemicals, cleaning solvents, or aerosols to clean the device or its accessories.
- Do not paint the device or its accessories.
- Please check local regulations for disposal of electronic products.
- Arrange power and network cables in a manner such that they are not likely to be stepped on or have items placed on them.