LANTRONIX®

NTC-550 Series User Guide

NTC-551
NTC-552

Part Number PMD-00305
Revision A July 2025

Trademark Notice

This product may reference NetComm. On December 26, 2024, Lantronix, Inc. acquired the Industrial Internet of Things (IIoT) product portfolio from NetComm Wireless Pty Ltd and is authorized to use the NetComm trademark in association with this product.

Intellectual Property

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

Patented: https://www.lantronix.com/legal/patents/. Additional patents pending.

Warranty

For details on the Lantronix warranty policy, please go to our web site at https://www.lantronix.com/support/warranty/.

Contacts

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: www.lantronix.com/technical-support/

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix website at https://www.lantronix.com/about-us/contact/.

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

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. Lantronix accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Lantronix NTC-550 Series to transmit or receive such data.

Safety and Hazards

Warning: *Do not connect or disconnect cables or devices to or from the USB port, SIM card tray, Ethernet port or the terminals of the power connector in hazardous locations such as those in which flammable gases or vapours may be present, but normally are confined within closed systems; are prevented from accumulating by adequate ventilation; or the location is adjacent to a location from which ignitable concentrations might occasionally be communicated.*

Revision History

Date	Rev.	Comments
July 2025	A	Initial document

For the latest revision of this product document, please check our online documentation at https://www.lantronix.com/support/documentation/.

Contents

1. Overview

Introduction

This document provides you all the information you need to set up, configure and use the Lantronix NTC-550 Series router.

Target audience

This document is intended for system integrators or experienced hardware installers who understand telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NTC-550 Series router, please confirm that you have the following:

- An electronic computing device with a working Ethernet network adapter
- A web browser such as Mozilla Firefox® or Google Chrome™

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 to avoid damage or injury.*

2. Product introduction

Product overview

The NTC-550 Series routers are high-end, high-speed industrial-grade 5G routers. Designed with critical and complex applications in mind, it provides ultra-reliable, high bandwidth throughput even in extremely demanding environments.

The NTC-550 Series features support the latest wireless technologies including Release 16 5G and Wi-Fi 6 to ensure access to the latest innovations and the best possible throughput at a world-leading price point.

Ideal for use in emergency vehicles, trucks, and buses, or as the core of complex systems to monitor and control critical infrastructure in remote, unmanned locations.

Product features

- 5G with failover to 4G
- Wi-Fi 6 and Bluetooth support (Bluetooth support not available in current firmware.)
- Multiple gigabits per second ports
- Built-in GPS
- Serial port, I/Os and Ignition sensing
- Robust, ruggedized industrial-grade metal housing and a wide operating temperature range
- Designed, assembled, and tested for unmanned locations in extreme environments

Package contents

The Lantronix NTC-550 Series router package contains:

- 1 x NTC-550 Series router
- 1 x Six-way terminal block
- 1 x 1 m Ethernet cable
- 1 x DIN rail mounting kit
- 1 x Welcome Card
- 1 x Compliance sheet

If any of these items are missing or damaged, please contact your sales representative or the support team.

Ordering Information

Model	Lantronix Part Number	Description
NTC-551	NTC-551-01-01	5G Release 16 Sub 6 Industrial Grade 5 Port Router with Wi-Fi for North America
NTC-552	NTC-552-01-01	5G Release 16 Sub 6 Industrial Grade 5 Port Router with Wi-Fi, Global

Product Label

Figure 2-1 NTC-552 Product Label

3. Physical dimensions and indicators

Physical dimension

Figure 3-1 NTC-550 Series top and side views

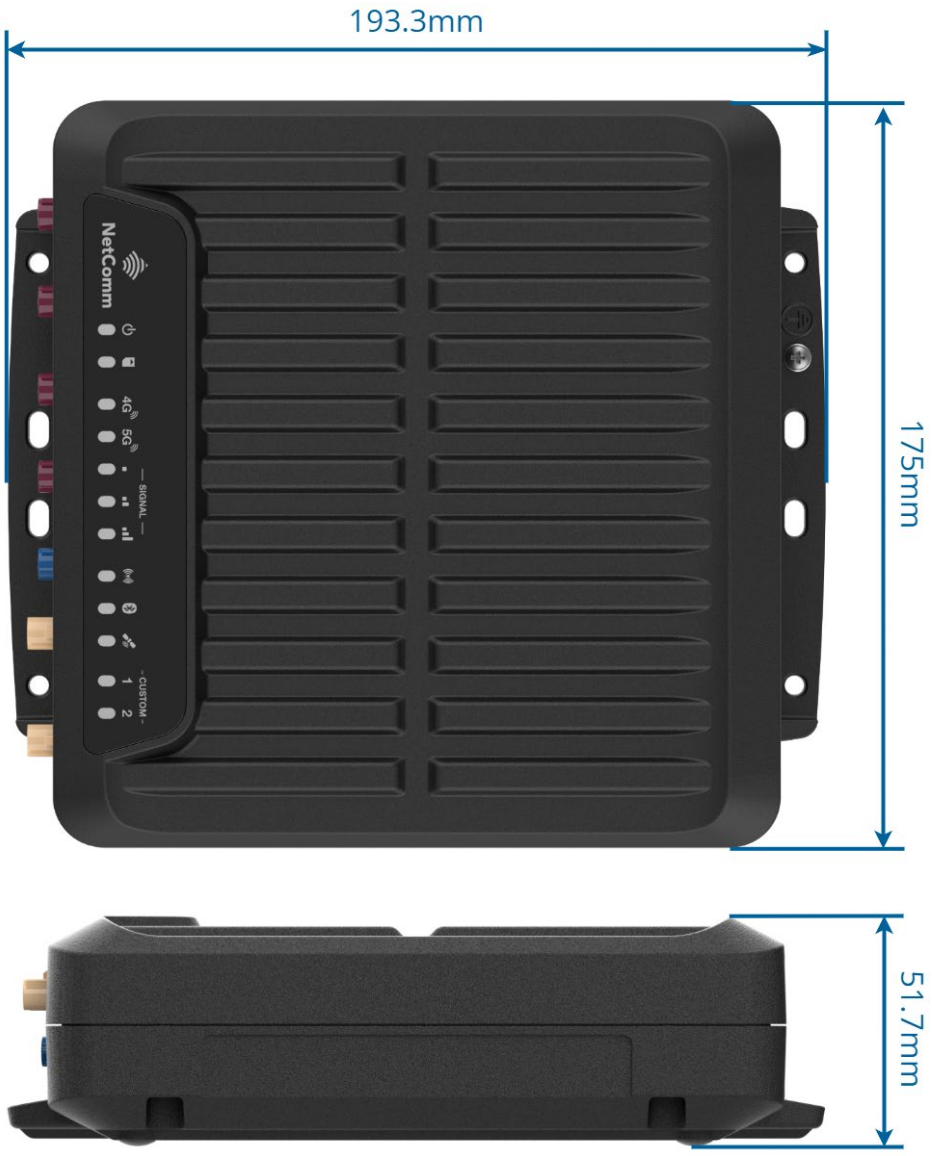


Table 3-1 NTC-550 Series Router Dimensions

NTC-550 Series Router Dimensions	
Length	175 mm
Depth	193.3 mm
Height	51.7 mm
Weight	1.050 kg

Interfaces

The following interfaces are available on the NTC-550 Series router:

Figure 3-2 Interfaces

Table 3-2 Interfaces

No.	ITEM	DESCRIPTION
1	2.5Gbps WAN Ethernet Port	Connect a wired WAN connection here.
2	Gigabit LAN Ethernet ports	Connect local Ethernet compatible devices here.
3	Serial Port	Configurable RS232 DE-9 serial port used to connect serial devices to the router.
4	Factory reset button	Press and hold for less than 5 seconds to reboot to normal mode. The LEDs are green and extinguish in sequence to indicate that the router will reboot normally if the button is released during this period. Press and hold for 5 to 10 seconds to reboot to another partition for recovery purpose. The LEDs are amber and extinguish in sequence to indicate that the router will load the recovery image. Press and hold for 10 to 15 seconds to reset the router to factory default settings. The LEDs are red and extinguish in sequence to indicate that the router will reset to factory default settings if the button is released during this period.
5	Bluetooth pairing button	Press for one second then release to initiate Bluetooth pairing.
6	Six-way terminal block connector	Connect power source wires here. Power wires may be terminated on optional terminal block and connected to DC input jack. Refer to Powering the Router section for further information.
7	Cellular antenna connectors (claret violet)	FAKRA connectors for cellular antennas.
8	GNSS antenna connector (signal blue)	FAKRA connector for GNSSS antenna.
9	Wi-Fi antenna connectors (beige)	FAKRA connectors for Wi-Fi antennas.
10	SIM card tray	Insert SIM card (2FF size) here.
11	SIM eject button	Press to eject the SIM card tray.
12	microSD card slot	Insert microSD card here. Remove the cover using a Phillips head screwdriver to access the slot.
13	USB-C port	Provides USB connectivity for debugging. Remove the cover using a Phillips head screwdriver to access the slot.

LED indicators

The NTC-550 Series router uses LEDs to display the current system and connection status.

Figure 3-3 LED Indicators

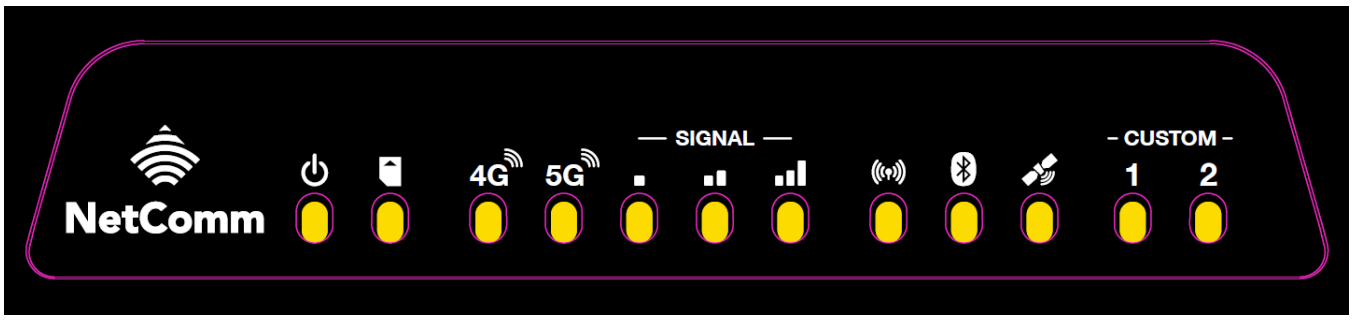


Table 3-3 LED Indicators

LED	NAME	COLOUR	STATE	DESCRIPTION
⏻	Power	⃠	Off	Power off
		■	Blinking	Router starting up
		■	On	Power on
	SIM	⃠	Off	No SIM detected
		■	Blinking	SIM error
		■	On	SIM installed and working
4G	4G Network	⃠	Off	No 4G connection
		■	Blinking	Connecting to 4G network
		■	On	4G connected
5G	5G Network	⃠	Off	No 5G connection
		■	Blinking	Connecting to 5G network
		■	On	5G connected
SIGNAL	Signal Strength	⃠	Off	No signal
		■	One Lit	Poor signal
		■ ■	Two Lit	Fair signal
		■ ■ ■	Three Lit	Good signal
	Wireless	⃠	Off	Wireless off

LED	NAME	COLOUR	STATE	DESCRIPTION
			Blinking	Client mode enabled
			On (Amber)	Connected to Wi-Fi network as client device
			On	Wireless Access Point enabled
	Bluetooth		Off	Bluetooth off
			Blinking	Bluetooth pairing mode
			On	Bluetooth on
	GPS		Off	GPS off
			Blinking	Acquiring GPS location
			On	GPS on
CUSTOM	Custom 1	Customizable		Programmable LED for custom use
CUSTOM	Custom 2	Customizable		Programmable LED for custom use

Signal strength LEDs

The following table lists the signal strength range corresponding to the number of lit signal strength LEDs.

Table 3-4 Signal strength LED indicators

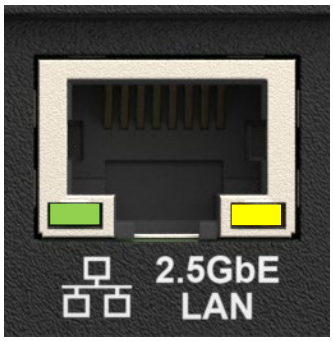
NUMBER OF LIT LEDS	SIGNAL STRENGTH
All LEDs unlit	No signal
1	> -120 dBm
2	> -105 dBm
3	> -90 dBm

LED update interval

The signal strength LEDs update within a few seconds with a rolling average signal strength reading. When selecting a location for the router or connecting and positioning an external antenna, please allow up to 20 seconds for the signal strength LEDs to update before repositioning.

Ethernet port LED indicators

Figure 3-4 NTC-550 Series Ethernet port LED indicators



The table below describes the status of each light and their meanings.

Table 3-5 Ethernet port LED indicators

LED	STATUS	DESCRIPTION
Green	On	Valid network link.
	Blinking	Activity on the network link.
	Off	No valid network detected.
Amber	On	Ethernet port is operating at a speed of 100 Mbps or 1000 Mbps or 2500 Mbps.
	Off	Ethernet port is operating at a speed of 10 Mbps or no ethernet cable is connected

4. Placement of the router

Antenna Installation

The NTC-550 Series router is fitted with multiple FAKRA antenna connectors to connect cellular, Wi-Fi, and GNSS antennas. Attach antennas fitted with FAKRA connectors to the corresponding antenna connectors on your router. Refer to the Interfaces section for the antenna connector layout.

Figure 4-1 Connecting Antenna

Note: *The antennas are not shipped with the device and have to be ordered separately.*

If you find the signal strength is weak, try adjusting the orientation of the antennas. If you are unable to get an acceptable signal, try moving the router to a different place or mounting it differently.

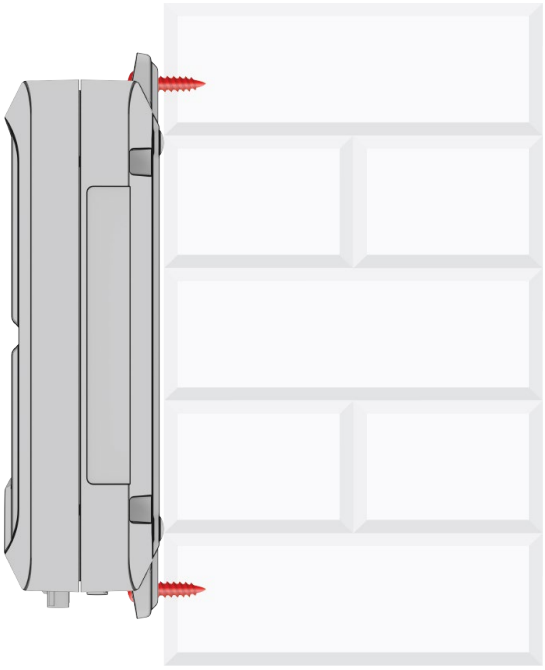
Note: *When selecting a location for the router, allow at least 20 seconds for the signal strength LEDs to update before trying a different location.*

Mounting Options

You have multiple options to mount the NTC-550 Series router.

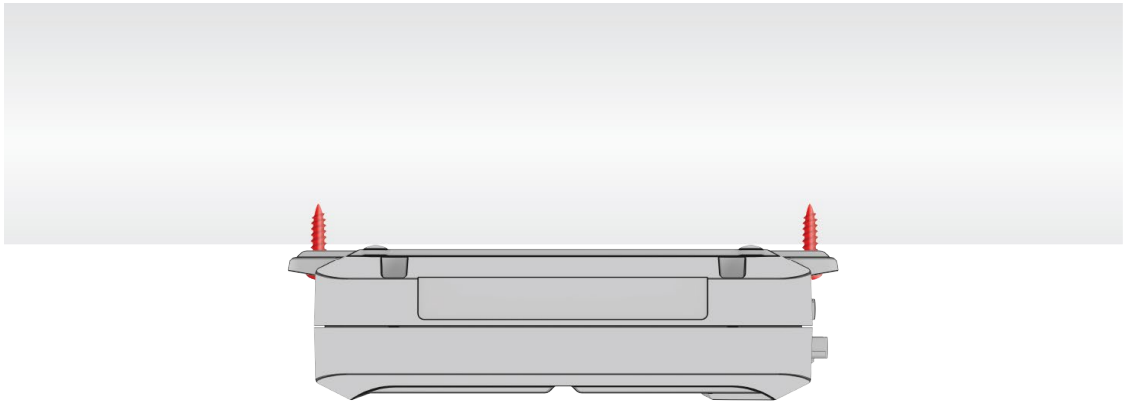
Wall Mount

Figure 4-2 NTC-550 Series Router Wall Mount



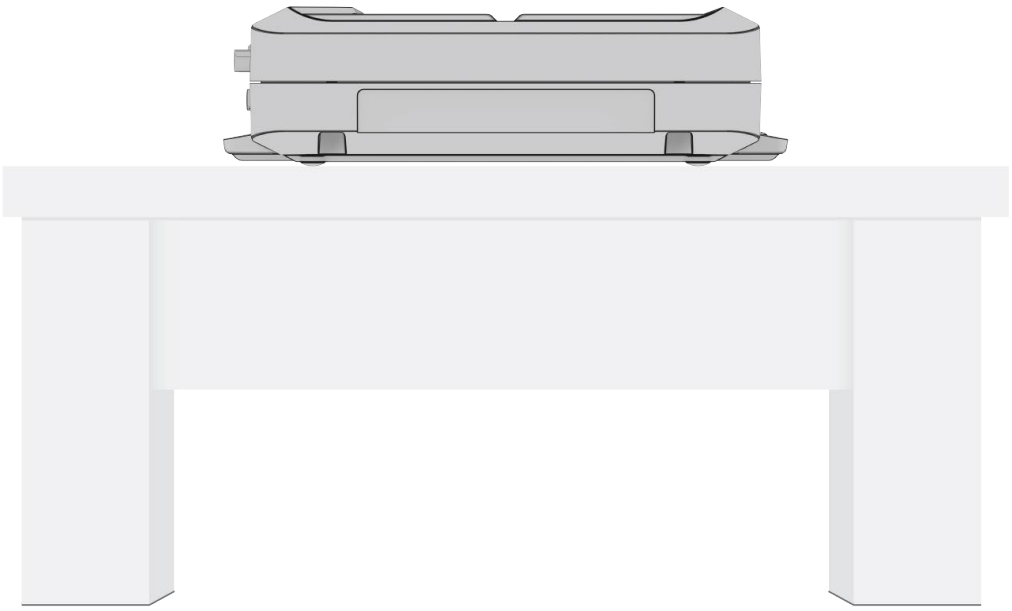
Ceiling Mount

Figure 4-3 NTC-550 Series Router Ceiling Mount



Desk Mount

Figure 4-4 NTC-550 Series Router Desk Mount



Mounting Using DIN Rail Mounting Kit

The DIN rail mounting kit allows you to install the device in two orientations. Install the DIN rail mounting kit by screwing the DIN rail mounts into the locations as shown below.

Figure 4-5 Installing DIN Rail Mounts

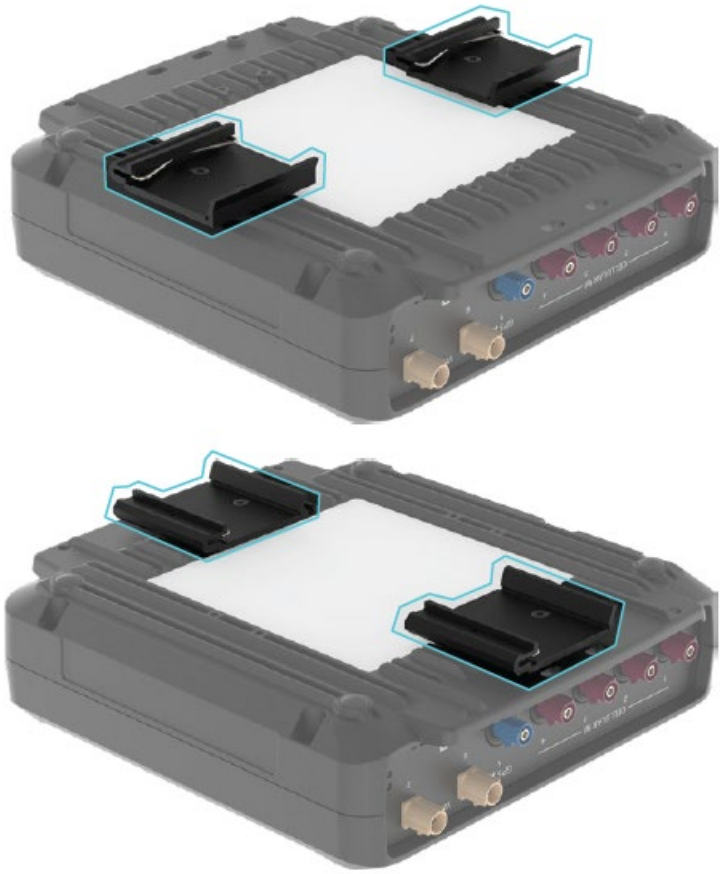
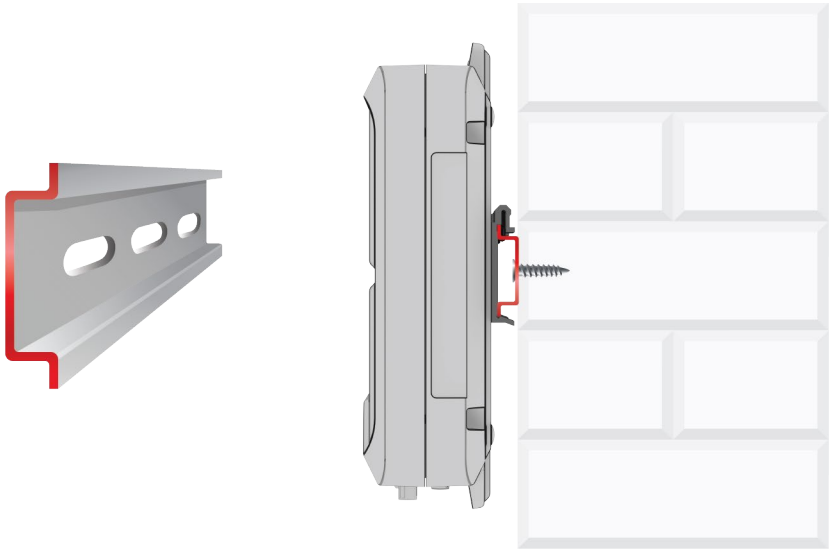


Figure 4-6 Mounting Using DIN Rail Kit



5. Installation and configuration of the NTC-550 Series router

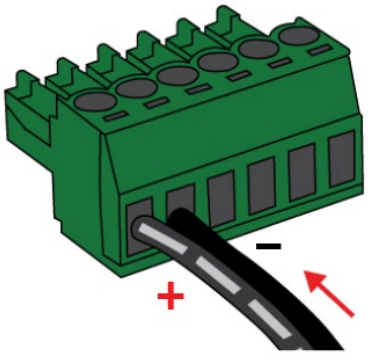
Powering the router

DC power via 6-way connector

The positive and ground terminals on the 6-pin connector can accept power from a separately sold DC power supply. Both a standard temperature range DC power supply and an extended temperature range DC power supply are available to purchase as accessories.

If you have purchased an optional DC power supply, first remove the terminal block from the connector. The terminal block connector uses rising cage clamps to secure the wires and ships with the cages lowered and ready for wire insertion. Inspect the cage clamps and use a flathead screwdriver to lower the cage clamps if they have moved during transportation. Insert the wires into the terminal block as shown below, noting the polarity of the wires, then use a flathead screwdriver to raise the cage clamp to secure the wires in the terminal block. Insert the wired terminal block into the terminal block connector of the router and then connect the adapter to a wall socket.

Figure 5-1 Terminal block wiring diagram



DC power via field terminated power source

If an existing 8-40V DC power supply is available, you can insert the wires into the supplied terminal block to power your router. Use a flathead screwdriver to tighten the terminal block screws and secure the power wires, making sure the polarity of the wires is correctly matched, as illustrated below. You should avoid using DC cables greater than 2 metres in length.

Figure 5-2 Locking Power Terminal block pinout

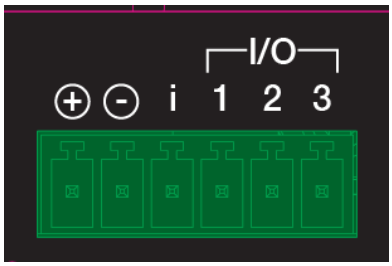


Table 5-1 Locking Power Terminal Block Pinout Description

Terminal	Description
+	Positive wire for power
_	Ground wire
i	Dedicated terminal for ignition detection
I/O	Used for general purpose input/output (refer to IO configuration section for more information)

Installing the router

After you have mounted the router and connected a power source, follow the below steps to complete the installation process:

1. Connect equipment that requires network access to the Ethernet port of your router. This may be your computer for advanced configuration purposes, or your end equipment which requires data access via the NTC-550 Series router. You can connect one device directly, or several devices using a network switch.
2. Connect the antennas, if required.
3. If your router does not come with a SIM pre-installed, insert a SIM card into the SIM card slot by pressing the SIM Eject button to eject the SIM card tray. Place the SIM card in the tray and then insert the loaded tray into the SIM slot with the gold side facing up.
4. Ensure the external power source is switched on and wait 2 minutes for your NTC-550 Series router to start up and connect to the mobile network. Your router arrives with preconfigured settings that should suit most customers. Your router is now connected. To check the status of your router, compare the LED indicators on the device with those listed in the LED indicators table.

6. Advanced configuration

To access the web-based user interface, open a web browser (e.g., Mozilla Firefox or Google Chrome), type https://192.168.1.1 into the address bar and press Enter.

The router's web user interface is displayed.

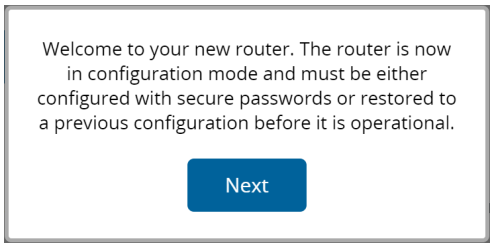
⚠ ***Important:*** *The HTTP protocol is disabled by default, secure HTTP (HTTPS) is the default protocol. HTTP access is available but must be manually enabled.*

Initialization

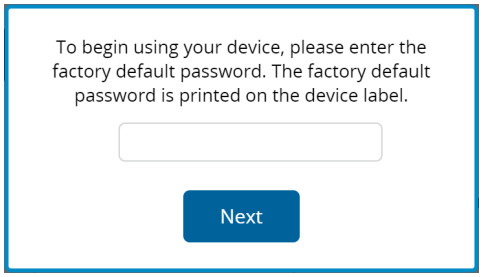
The first time the device is booted (or booted after a factory reset), the device enters configuration mode. In configuration mode, the router runs a setup wizard which must be completed before the device boots into live mode. This is a security feature which enables you to set strong passwords for the web UI users root, admin, and user, and Telnet/SSH access or restore a previous configuration from a file.

To complete the setup:

1. Click **Next** on the first dialogue box.



2. Enter the factory default password which is printed on the device label, then click **Next**.



3. Select whether to configure the router as a new device or restore a previous configuration backup.

Configure as a new device (create new passwords)

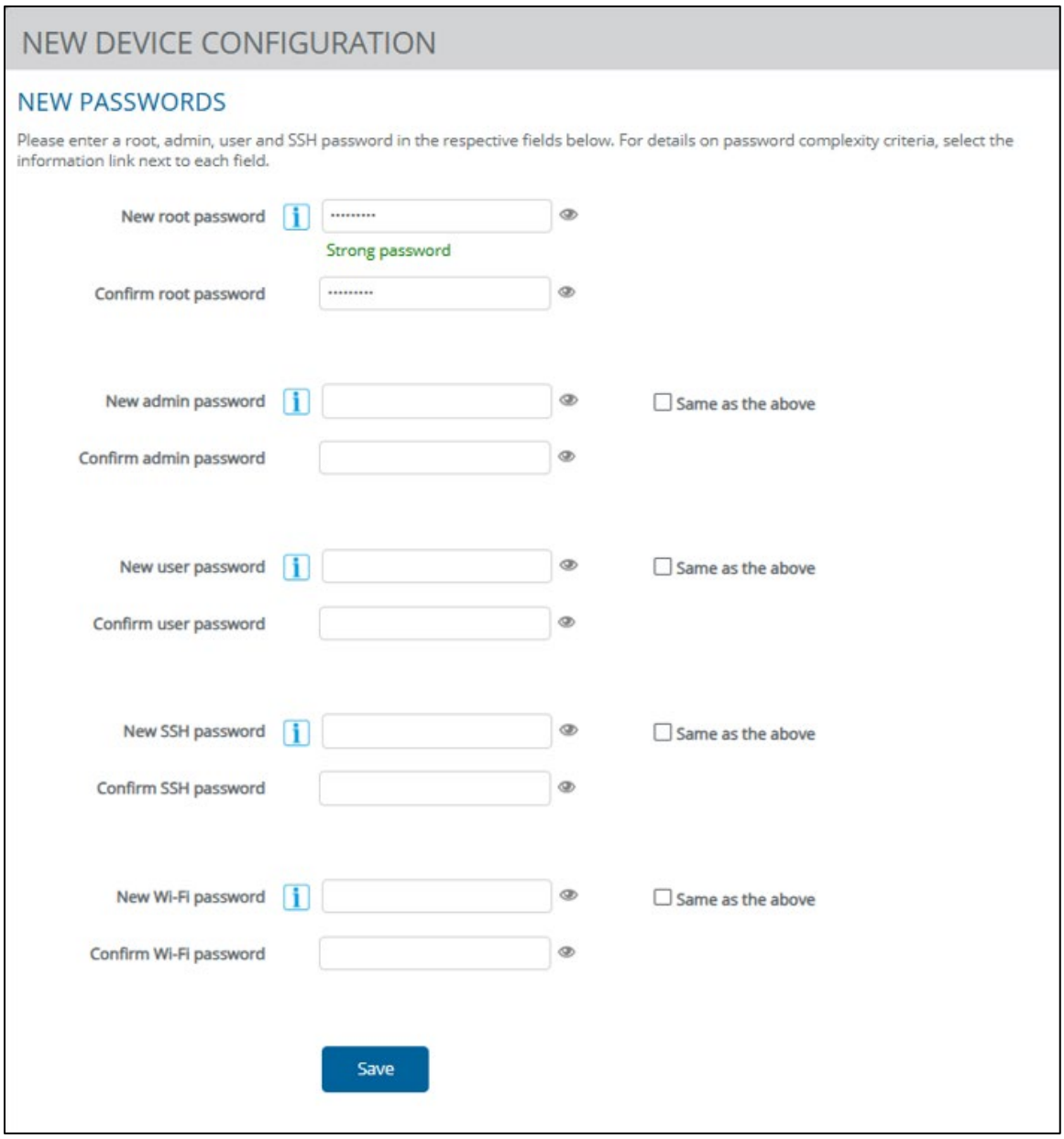
Select **I want to configure this as a new device**, then click **OK**.

In the **NEW PASSWORDS** section, enter a strong password in each field. You may configure the same password for all three accounts, but it must meet the following security requirements:

- The password must be a minimum of eight characters and no more than 128 characters in length.
- The password must contain at least one upper case, one lower case character, and one number.
- The password must contain at least one special character, such as: ` ~ ! @ # $ % ^ & * ( ) - _ = + [{] } \ | ; : ' " , < > / ?

- Additionally, the password must satisfy an algorithm which analyses the characters as you type them, searching for commonly used patterns, passwords, names, and surnames according to US census data, popular English words from Wikipedia, US television, movies, and other common patterns such as dates, repeated characters (aaa), sequences (abcd), keyboard patterns (qwertyuiop), and substitution of numbers for letters.

Figure 6-1 New device configuration dialog page

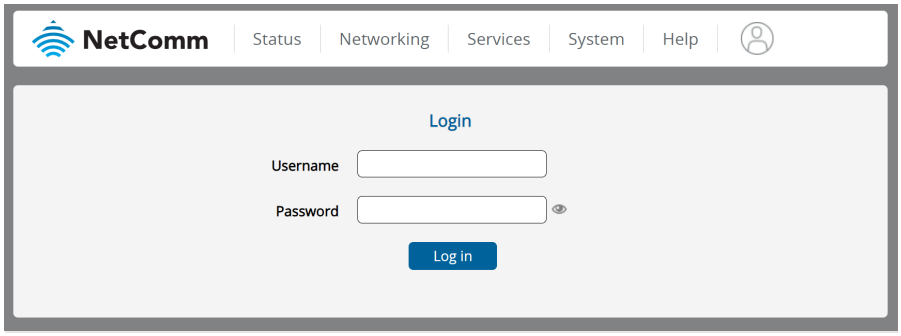


When you have entered values for all password fields, Click **Save** button. If the passwords meet the security requirements, they are saved and the router reboots to Live mode automatically. See below for further instructions on logging in.

Logging In

To login into the router, enter the login username (root, admin or user) and the password that you configured for that user during the initialisation process.

Figure 6-2 Log in prompt for web-based user interface



Note: *If logging in as user, the account allows you to manage all settings of the router except functions such as firmware upgrade, device configuration backup and restore and reset to factory default settings, which are privileged only to the root manager account.*

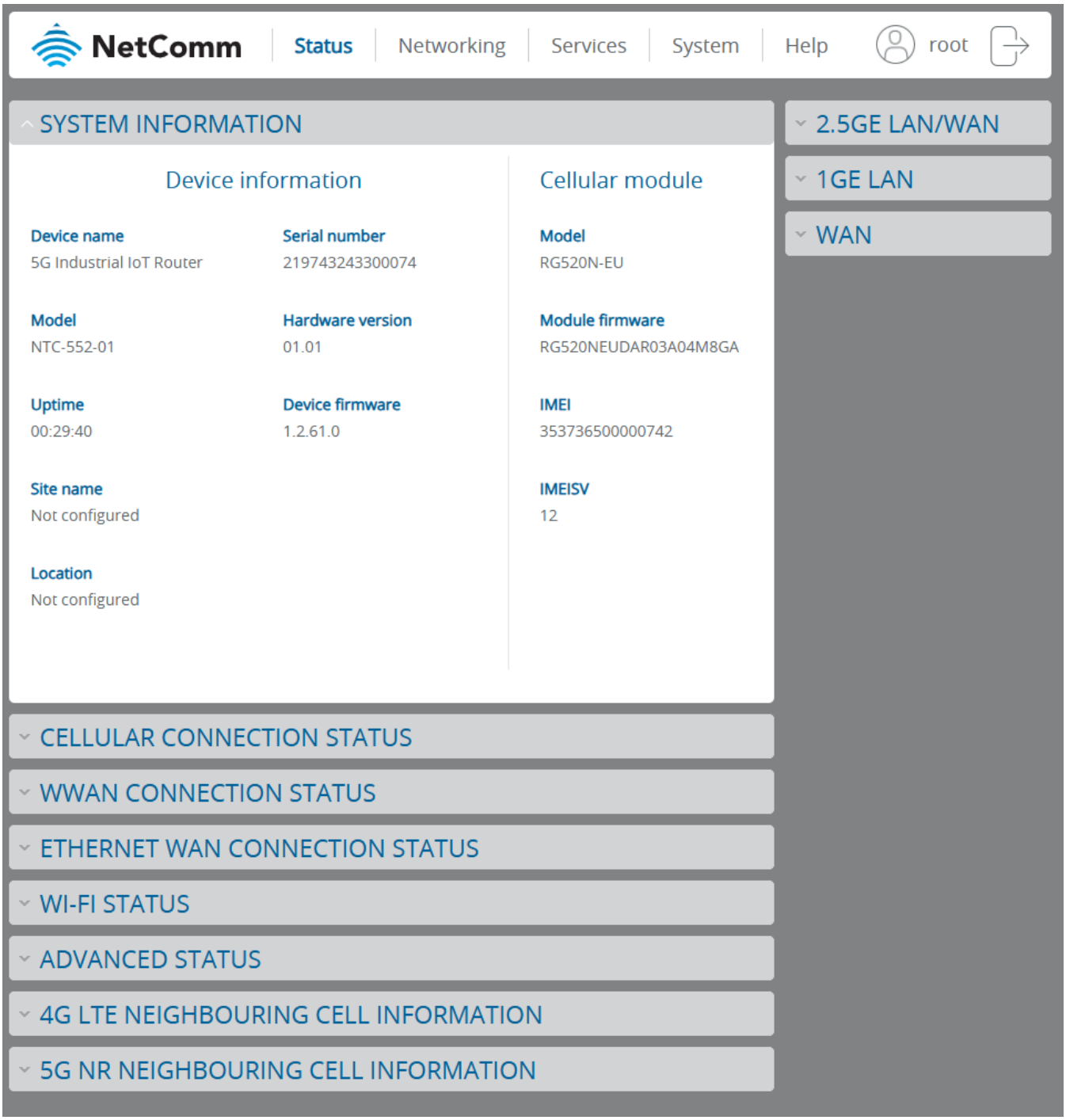
7. Status

The Status page displays once you login into the NTC-550 Series router web interface. The Status page displays the following details:

- System Information
- Cellular Connection Status
- WWAN Connection Status
- Ethernet WAN Connection Status
- Wi-Fi Status
- Advanced Status
- 4G LTE Neighboring Cell Information
- 5G NR Neighboring Cell Information
- 2.5GE LAN/WAN
- 1GE LAN
- WAN

Click or buttons in each section tab to show or hide the details in that section. Extra sections will appear as additional software features are enabled.

Figure 7-1 NTC-550 Series router status page



System Information

The table below lists the System Information details:

Table 7-1 System Information details

Item	Definition
Device Information	
Device name	The device name of the NTC-550 Series router
Model	The commercial product name which helps to identify the available features of the router.
Uptime	The current up time (the time since the router was last turned on) of the router.
Site name	The configured site name.
Location	The configured location.
Serial number	The serial number of the router.
Hardware version	The hardware version of the router.
Device Firmware	The firmware version of the router
Cellular Module	
Model	The type of cellular module
Module firmware	The firmware revision of the cellular module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
IMEISV	International Mobile Equipment Identity and Software Version. It is a 16-digit code that uniquely identifies a mobile device and its software version.

Cellular Connection Status

The table below lists the Cellular Connection Status details.

Table 7-2 Cellular Connection Status Items

Item	Definition
SIM status	Displays the SIM status of the NTC-550 Series router. This includes information about whether there is a SIM inserted or if the SIM card has an error.
Signal strength	The current signal strength measured in dBm.
Network registration status	The status of the NTC-550 Series router registration for the current network.
Operator selection	The mode used to select an operator network.

Item	Definition
Provider	The current operator network in use.
Roaming status	The roaming status of the NTC-550 Series router.
Enabled bands	The bands to which the NTC-550 Series may connect.
Current band	The current band being used by the NTC-550 Series.
Connection (RAT)	The radio access technology in use.
Coverage	The type of mobile coverage being received by the NTC-550 Series router.
Service options	The network options provided by the current service in use.

WWAN Connection Status

The table below lists the WWAN Connection Status details.

Table 7-3 WWAN Connection Status Items

Item	Definition
Profile	The name of the active profile.
APN	The Access Point name currently in use, If the APN has been manually entered by you. Auto-assigned is displayed if the APN is assigned by the network.
Connection uptime	The duration of the current mobile connection session.
Default profile	Indicates whether the current profile in use is the default profile.
IPv4 status	The IPv4 connection status of the active profile.
IPv4 WWAN	The IPv4 address assigned by the mobile broadband carrier network.
IPv4 DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection.
IPv4 MTU	The current IPv4 Maximum Transmission Unit (MTU) of the WWAN connection.
IPv6 status	The IPv6 connection status of the active profile.
IPv6 WWAN	The IPv6 address assigned by the mobile broadband carrier network.
IPv6 DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection.
IPv6 MTU	The current IPv6 Maximum Transmission Unit of the WWAN connection.

Ethernet WAN Connection Status

The table below lists the Ethernet WAN Connection Status details.

Table 7-4 Ethernet WAN Connection Status Items

Item	Definition
#	Index umber of the WAN interface.
Name	The interface name as it is shown on the system.
Status	Displays whether interface is up or down.
IP address	IP address assigned to the ethernet interface.
Gateway	Gateway address for the ethernet interface.

Wi-Fi Status

The table below lists Wi-Fi Status details.

Table 7-5 Wi-Fi Status Items

Item	Definition
Wi-Fi client	
Network name (SSID)	Network name (SSID) of the Wi-Fi access point.
Channel	The frequency band used for the Wi-Fi communication.
State	Status of the Wi-Fi network.
IP	IP address assigned to the Wi-Fi interface by the access point to which it is connected.
5GHz AP	
Network name (SSID)	Network name (SSID) of the router that is broadcasted in the network.
Channel	The frequency band used for the Wi-Fi communication.
State	Status of the Wi-Fi network.
Broadcast SSID	Status the SSID broadcast.
2.4GHz AP	
Network name (SSID)	Network name (SSID) of the router that is broadcasted in the network.
Channel	The frequency band used for the Wi-Fi communication.
State	Status of the Wi-Fi network.
Broadcast SSID	Status the SSID broadcast.

Advanced Status

The table below lists the Advanced Status details.

Table 7-6 Advanced Status Items

Item	Definition
Mobile country code	The Mobile Country Code (MCC) of the NTC-550 Series router.
Mobile network code	The Mobile Network Code (MNC) of the NTC-550 Series router.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the NTC-550 Series router, a unique number up to 19 digits in length.
IMSI	The International Mobile Subscriber Identity is a unique identifier of the user of a cellular network.
Packet service status	Displays whether the packet service is attached or detached. When APN or username/password is changed, the device detaches and reattaches to the network.
4G LTE	
ECGI	E-UTRAN Cell Global Identifier. The globally unique identity of a cell in E-UTRA. The ECGI concatenates the PLMN-Id and the ECI (E-UTRAN Cell Identifier). The ECI concatenates the eNodeB ID and the Cell ID
eNodeB	Also known as the Evolved Node B,5G this is the hardware element in the LTE network that communicates directly with mobile devices.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile LTE network signal.
PCI	Physical Cell ID of the LTE Cell.
Channel number (EARFCN)	The channel number of the current cellular connection.
Reference Signal Received Power (RSRP)	Average power received from a single reference signal within a specific bandwidth.
Reference Signal Received Quality (RSRQ)	RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by N x RSRP / RSSI where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.
Signal to Interference plus Noise Ratio (SINR)	The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.
CQI	Channel Quality Indicator. This is a value between 1 and 15 with 15 being the highest rating.

Item	Definition
5G NR	
NCGI	NR Cell Global Identifier. This concatenates the PLMN-Id (PLMN Identifier) and the 36bit NCI (NR Cell Identity). This information is not available when the device is operating in LTE or 5G non-standalone mode.
gNodeB	The gNodeB (gNB) is the term given to network equipment that transmits and receives wireless communications between UE and a mobile network
gNB Cell ID	A unique code that identifies the base station from within the location area of the current mobile 5G network signal. This is not available when the device is operating in LTE or 5G non-standalone mode.
gNB PCI	Physical Cell ID of the 5G NR Cell.
Channel number (NR ARFCN)	The channel number of the current 5G cellular connection.
SSB Channel number (SSB ARFCN)	The Synchronization Signal Block (SSB) channel number of the current 5G cellular connection.
SCS	The size of the current Subcarrier Spacing (SCS) expressed in KHz.
Reference Signal Received Power (SS-RSRP)	Synchronization Signal Reference Signal Received Power (SS-RSRP). The linear average over the power contributions (in Watts) of the resource elements that carry Secondary Synchronization Signal (SSS).
Reference Signal Received Quality (SS-RSRQ)	Secondary Synchronization Signal Reference Signal Received Quality (SS-RSRQ). It calculates signal quality taking into consideration the RSSI. It is calculated by N x SS-RSRP / NR carrier RSSI where N is the number of Physical Resources Blocks (PRBs) over which the NR RSSI is measured.
Signal to Interference plus Noise Ratio (SS-SINR)	Synchronization Signal – Signal to interference plus noise ratio. The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.
NR CQI	The 5G NR Channel Quality Indicator (CQI).
Synchronisation Signal Block (SSB) Index	This is a key part of beam management. It is a value comprised of Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS) and the Physical Broadcast Channel (PBCH).

4G LTE Neighboring Cell Information

The table below lists the 4G LTE Neighboring Cell Information details.

Table 7-7 4G LTE Neighboring Cell Information Items

Item	Definition
PCI	The Physical Cell ID.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
RSRP	Reference Signal Received Power.
RSRQ	Reference Signal Received Quality.
RAT	The radio signal being served e.g., 5G NR, LTE.

5G NR Neighboring Cell Information

The table below lists the 5G NR Neighboring Cell Information details.

Table 7-8 5G NR Neighboring Cell Information Items

Item	Definition
PCI	The Physical Cell ID.
NR ARFCN	Absolute radio-frequency channel number
SS-RSRP	Synchronization Signal Reference Signal Received Power.
SS-RSRQ	Secondary Synchronization Signal Reference Signal Received Quality.
Type	Serving or neighbor
Role	
SSB ARFCN	The Synchronization Signal Block (SSB) channel number of the current 5G cellular connection.
RAT	The radio signal being served e.g., 5G NR, LTE.

2.5GE LAN/WAN

The table below lists the 2.5GE LAN/WAN details.

Table 7-9 2.5GE LAN/WAN Items

Item	Definition
Interface assignment	Displays the current interface assignment, whether LAN or WAN.
IP	The IP address and subnet mask assigned to the interface.
MAC address	The MAC address of the interface.
Ethernet port status	The status of the port and its current operating speed.

1GE LAN

The table below lists the 1GE LAN details.

Table 7-10 1GE LAN Items

Item	Definition
IP	The IP address and subnet mask assigned to the interface.
MAC address	The MAC address of the interface.
Ethernet port status #1	The status of the port and its current operating speed.
Ethernet port status #2	The status of the port and its current operating speed.
Ethernet port status #3	The status of the port and its current operating speed.
Ethernet port status #4	The status of the port and its current operating speed.

WAN

WAN section displays the priority and status of the available WAN connections.

8. Networking

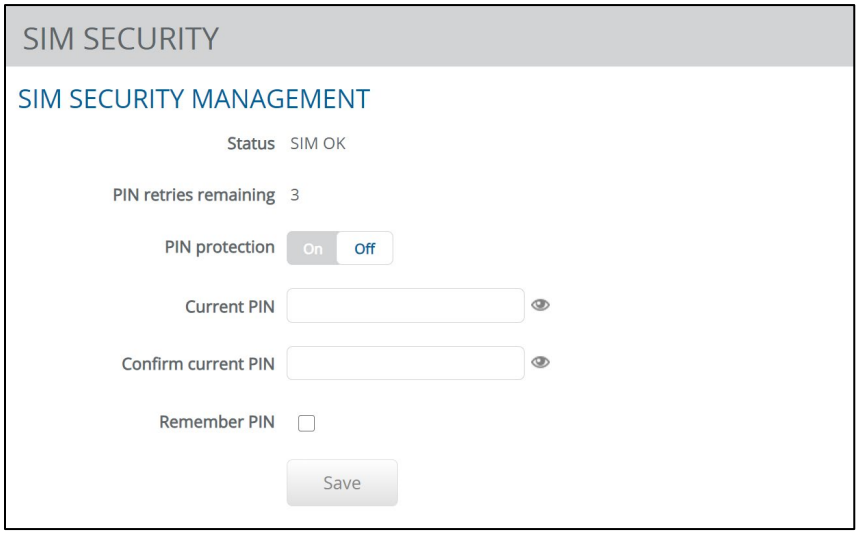
The Networking page provides configuration options for Cellular Settings, LAN Settings, Wi-Fi settings, WAN settings, Routing Settings, and VPN Settings

Cellular settings

SIM security

The SIM Security settings page is used for authenticating SIM cards that have been configured with a security PIN.

Figure 8-1 SIM security settings



If the SIM card is locked, you will receive a notice when you access the Status page after which you will be directed to the PIN settings page to enter the PIN. The PIN settings page lists the status of the SIM at the top of the page.

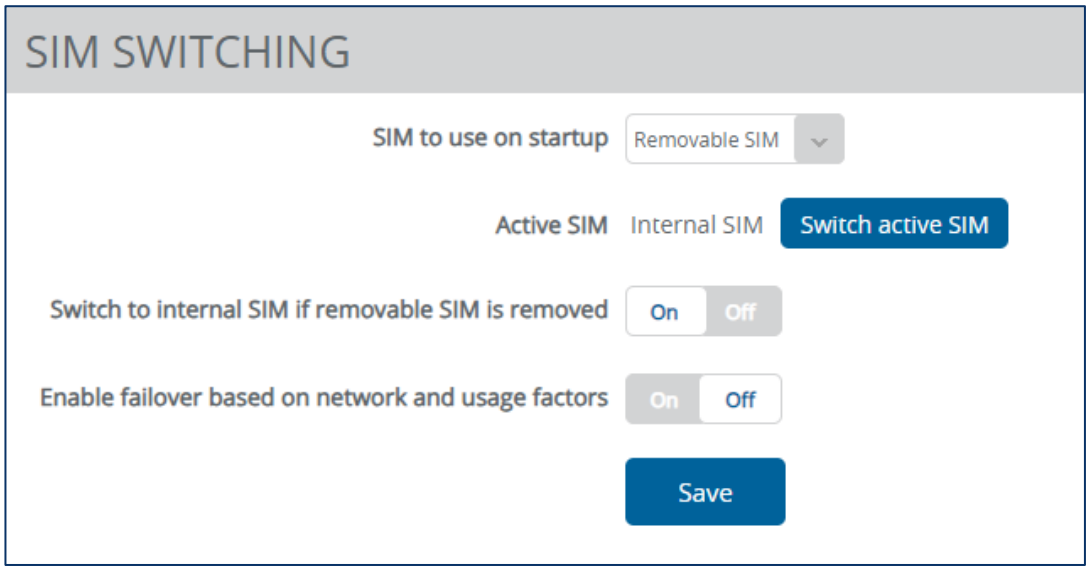
If you are not redirected to the PIN settings page, to unlock the SIM:

1. Click **Networking** tab on the top menu bar, and then click **SIM security**.
2. Enter the PIN in the **Current PIN** field (enter numbers only).
3. Click **Save** to save the PIN and unlock access.
4. Once unlocked, you may toggle the **PIN protection** switch to the **Off** position if you do not wish to have access locked by a PIN.

SIM switching

The NTC-550 Series router is equipped with both a removable and an internal SIM. To configure and switch between the two SIMs, the SIM switching page is used. The SIM switching page also provides several failover options to switch between the SIM cards.

Figure 8-2 SIM management



To select the SIM which should be used on startup, set the **SIM to use on startup** field to either **Internal SIM** or **Removable SIM**.

Active SIM displays the SIM that is currently in use. Click **Switch active SIM** to use the other SIM.

To automatically switch to the internal SIM if the removable SIM card is removed, set the **Switch to internal SIM if removable SIM is removed** toggle to **On.**

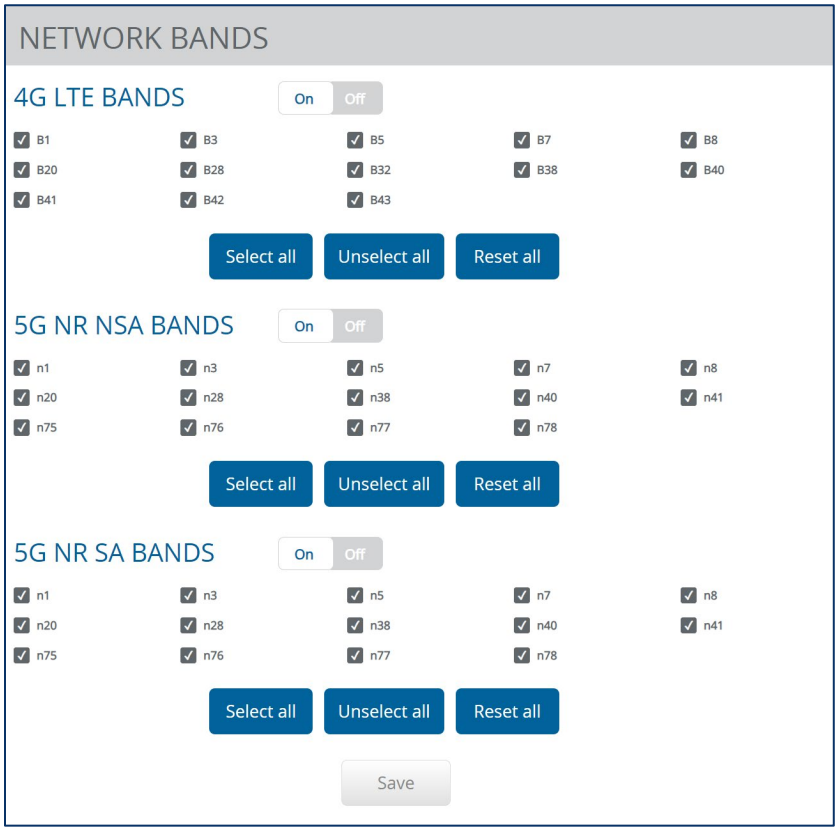
To configure **Failover** options, set the **Enable failover based on network and usage factors** to **On**, then set the relevant toggles for each condition that you would like to meet.

Click **Save** to apply any changes to this page.

Network bands

This page allows you to select individual bands from the following band groupings: **LTE, NR5G NSA, NR5G SA.**

Figure 8-3 NTC-550 Series band selection

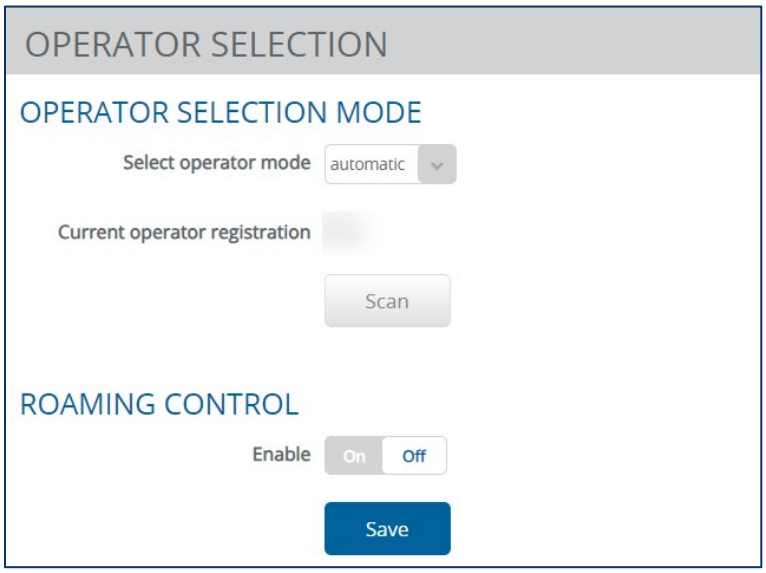


To setup a device for different LTE, 5G non-standalone (NR5G NSA) and 5G Standalone (NR5G SA) modes, refer to Appendix A – Configuring Radio Access Technologies

Operator selection

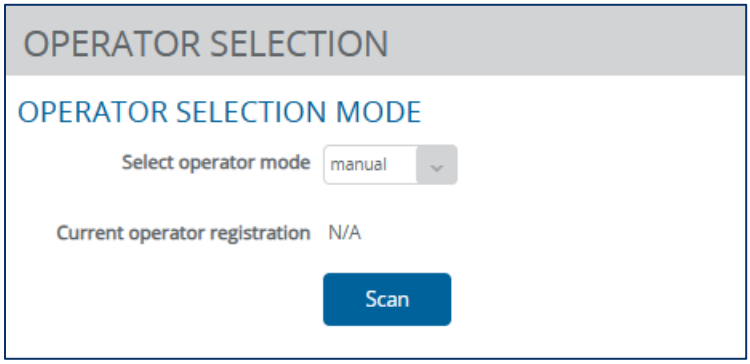
The Operator selection page allows you to set how the NTC-550 Series router selects the operator, whether automatically or manually. If you set it to manual, you can override and lock it to a particular carrier or access technology. The operator setting page also contains roaming controls.

Figure 8-4 Operator setting



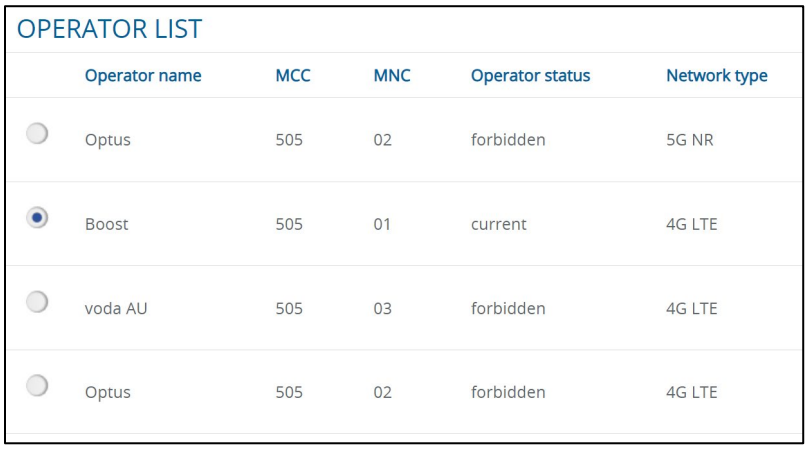
Operator selection mode

Figure 8-5 Operator selection mode



To scan for available networks, set the **Select operator mode** to manual and click **Scan** button. This operation can take a few minutes and requires that the packet data session be disconnected prior to scanning. A list of the detected service carriers in your area is displayed.

Figure 8-6 Operator list



Select the required service from the list and click **Apply**.

When **Select operator mode** is set to Automatic, the router selects the most appropriate operator based on the inserted SIM card. This is the default option and is sufficient for most users.

Roaming control

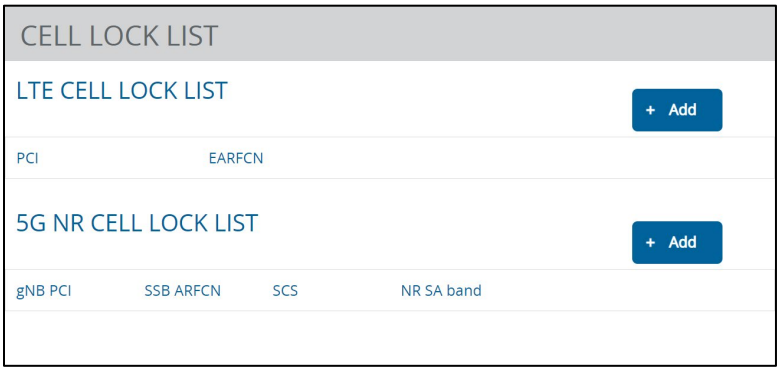
The roaming control function allows roaming to be enabled or disabled on the NTC-550 Series router. Enable roaming by setting the **Enable** toggle to On, then click **Save.**

Figure 8-7 Roaming control toggle

Cell lock list

The Cell lock function allows you to specify a list of cells that the NTC-550 Series router will not deviate from. The cells are separated on the basis of LTE and NR5G networks.

Figure 8-8 Cell lock

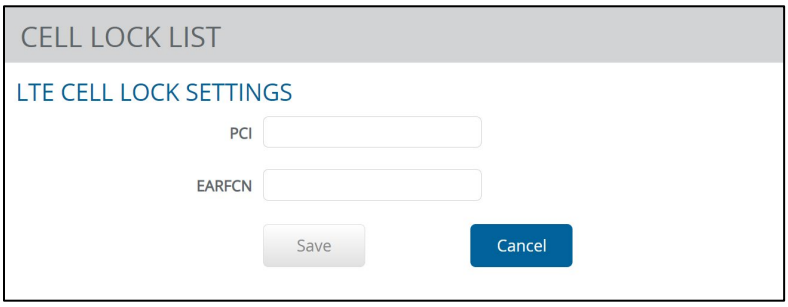


Adding to LTE cell lock list

To add a cell to the LTE cell lock list:

1. Click **Add,** next to **LTE Cell Lock List**.
2. Enter the **PCI** and **EARFCN** values of the cell that you want to lock.

Figure 8-9 Cell lock – Adding cell to LTE cell lock list



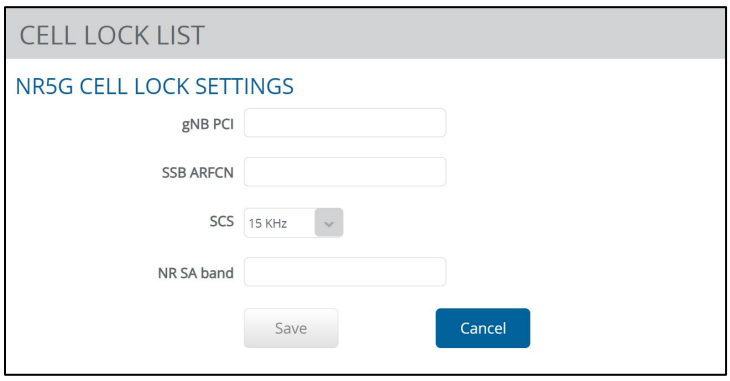
3. Click **Save** button. Repeat steps 1 to 3 for all the LTE cells that you wish to add.

Adding to NR cell lock list

To add a cell to NR cell lock list:

1. Click **Add**, next to **NR5G Cell Lock List**.
2. Enter the **gNB PCI**, **SSB ARFCN** values, select SCS value, and enter **NR SA band** value for the NR5G cell that you want to lock to.

Figure 8-10 Cell lock – Add NR5G cell lock



3. Click **Save** button. Repeat steps 1 to 3 for all the NR5G cells that you wish to add.

WAN profiles

The WAN profiles page allows you to configure and enable or disable connection profiles.

Each profile refers to a set of configuration items which are used by the router to activate a Packet Data Protocol (PDP) context. Under normal scenarios, you may have a single profile enabled. Multiple profiles can be used for simple fast switching of PDP settings such as APN or advanced networking configuration where multiple simultaneous PDP contexts may be required.

Figure 8-11 WAN profiles

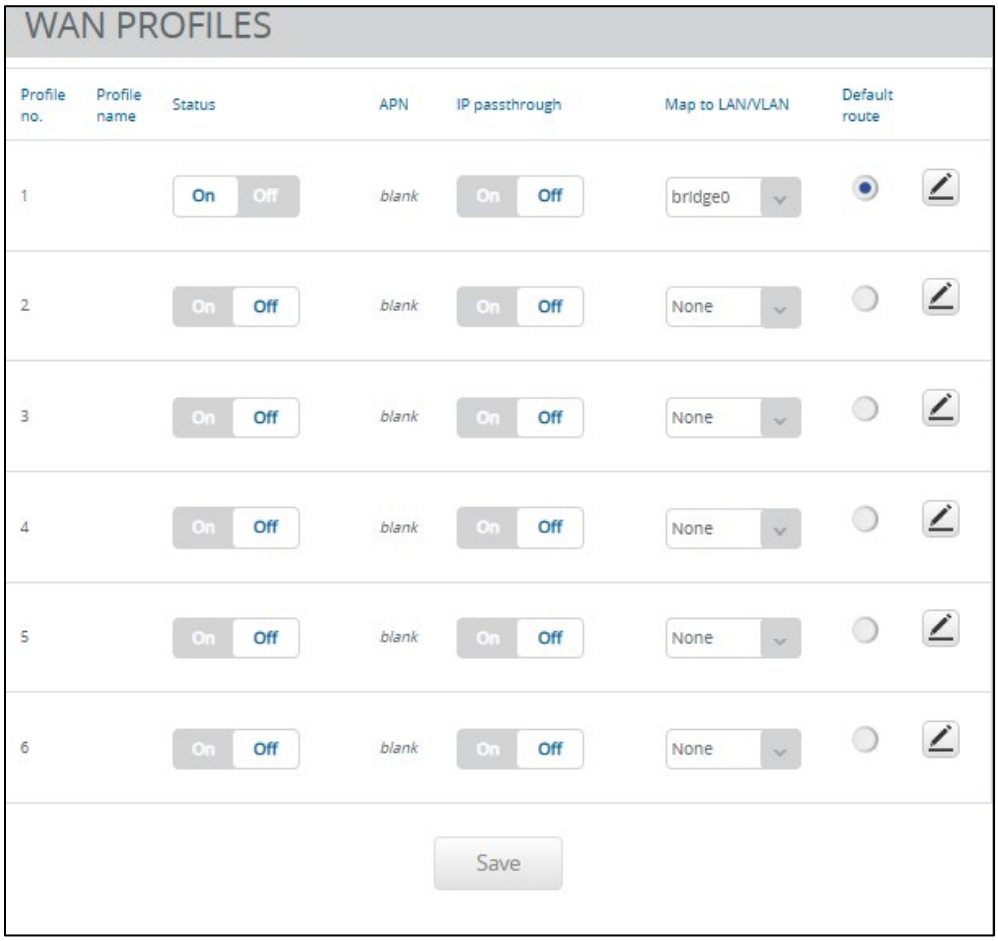


Table 8-1 WAN profile item details

ITEM	DEFINITION
Profile no.	Number of the profile.
Profile name	Name of the profile.
Status	Toggles the corresponding profile on or off. Only one profile may be turned on at any time.
APN	The APN configured for the corresponding profile.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device. Internet traffic is still terminated at the gateway (NTC-550 Series router) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Map to LAN/VLAN	The LAN or VLAN that the profile is assigned to.

ITEM	DEFINITION
Default Route	Sets the profile as the default route for traffic.

Connecting to the mobile broadband network

The NTC-550 Series router supports the configuration of up to six APN profiles. These profiles allow you to configure the settings that the router will use to connect to the 5G/4G network and switch easily between different connection settings.

For advanced networking purposes, you may activate a maximum of two profiles simultaneously (dependent on network support). When activating two connection profiles, you should avoid selecting two profiles with the same APN as this can cause only one profile to connect. Similarly, activating two profiles which are both configured to automatically determine an APN can cause a conflict and result in neither profile establishing a connection. It is recommended that the two active connection profiles have differing, manually configured APNs to avoid connection issues and ensure smooth operation.

Manually configuring a connection profile

To manually configure a connection profile:

1. Click button corresponding the profile that you wish to modify.
2. The **Wireless WAN Profile Settings** page is displayed.

Figure 8-12 WWAN profiles – WWAN profile settings

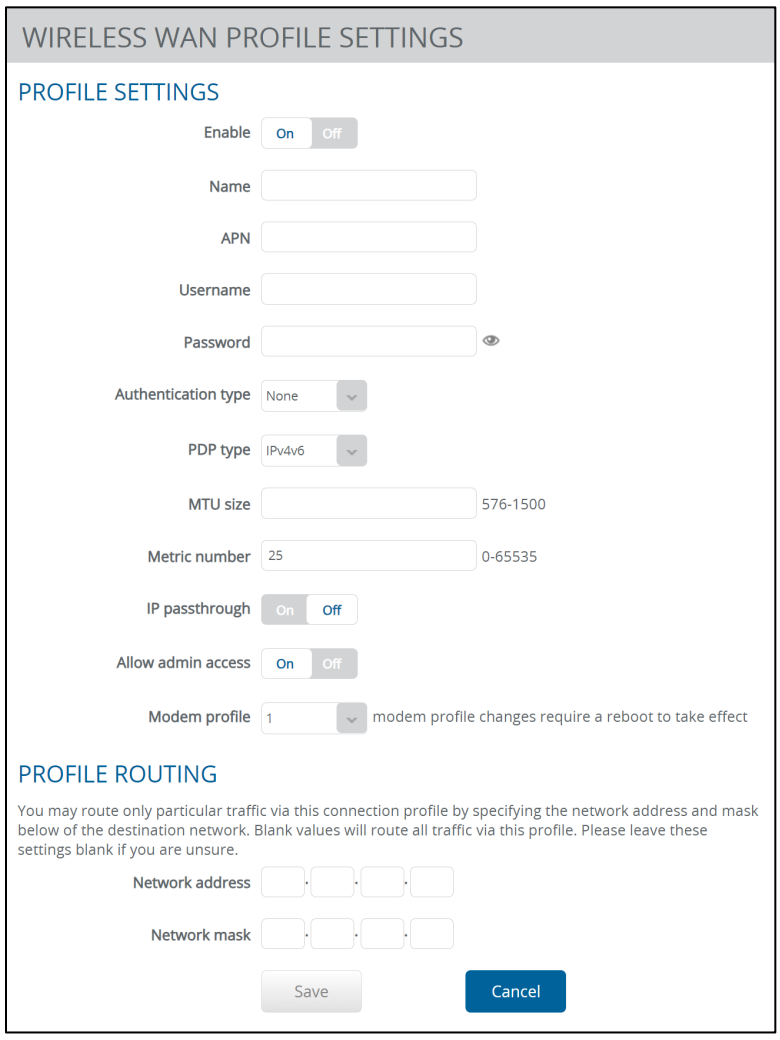


Table 8-2 WWAN profiles – WWAN profile settings details

Item	Definition
Enable	Toggle the enable button to **On** or **Off**, as desired.
Name	The name of the profile for easy identification on the Wireless WAN profile page. This name is only used to identify the profile on the NTC-550 Series.
APN	Enter the APN (Access Point Name) configured for the corresponding profile.
Username	The username used to log on to the corresponding APN (if required).
Password	The password used to log on to the corresponding APN (if required).

Item	Definition
Authentication type	The authentication type required by your provider. This can be set to: **None**, **PAP** or **CHAP**
PDP Type	Select the PDP type (IP protocol) to use for the connection. • **IPv4** – Sets a single stack IPv4 connection through which the NTC-550 Series router receives only IPV4 network and DNS addresses. • **IPv6** – Sets a single stack IPv6 connection through which the NTC-550 Series router receives only IPV6 network and DNS addresses. ***Note:*** *Before selecting this PDP type, check with your carrier to confirm that single stack IPV6 connectivity is supported.* • **IPv4v6** – Sets a dual stack connection allowing simultaneous IPV4 and IPV6 network connectivity. The NTC-550 Series router receives both IPv4 and IPV6 network and DNS addresses. This is the default **PDP type**
MTU size	Enter the Maximum Transmission Unit size. This may be from 1 to 1500 bytes.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device. Internet traffic is still terminated at the gateway (NTC-550 Series) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Allow Admin Access	Set to on, if you want to allow remote SSH, TR-069, and WebGUI access to the device via this Wireless WAN profile. ***Note:*** *SSH/HTTP/HTTPS can be individually restricted in the* ***Access Control*** *menu. Note also that this will automatically be enabled if the profile is selected in the* ***TR-069 settings*** *menu.*
Modem profile	Assigns the WWAN profile to a specific modem profile, which may be required by your carrier.
Profile Routing (See the **Profile Routing** section below)	
Network address	Enter network address of the remote network.
Network mask	Enter the network mask of the remote network.

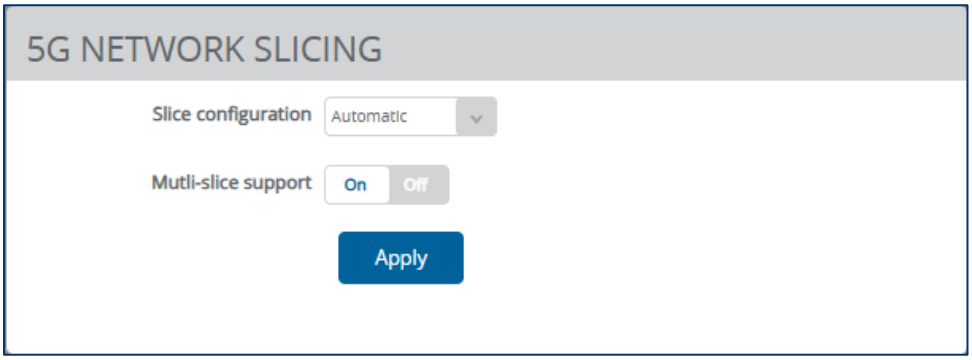
Profile routing

For advanced networking such as using dual simultaneous PDP contexts, you can configure a particular profile to route only certain traffic via that profile by with a custom address and mask of traffic to send via that profile. To do this, in the **Profile Routing** section, enter the **Network address** and **Network mask** of the remote network. If you do not want to use this feature, or are unsure, please leave these fields blank. This will not designate any particular traffic to be routed via this profile.

5G Network Slicing

The 5G Network Slicing page allows to perform network slice configuration.

Figure 8-13 Network slice configuration



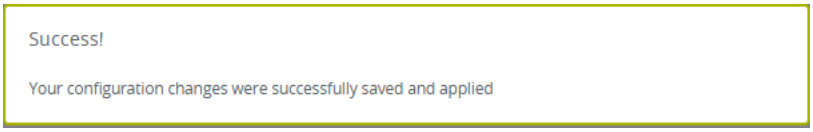
You can perform automatic or manual network slice configuration.

Automatic Network Slice Configuration

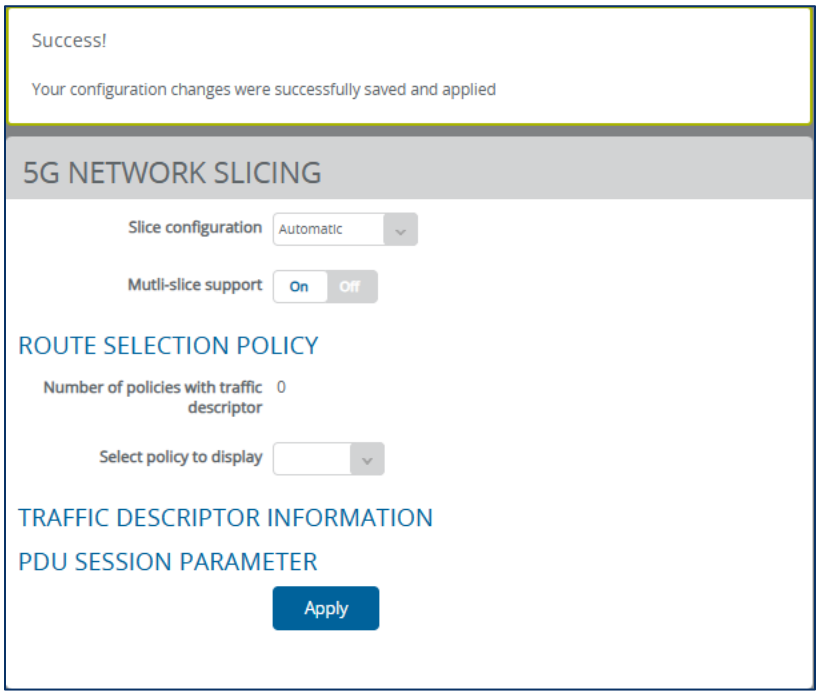
To perform automatic network slice configuration:

1. Select option Automatic for **Slice configuration** in the 5G Network Slicing page.
2. Set Muti-slice support to On or Off.
3. Click **Apply**

In the case **Multi-slice support** is set to **Off**, the below success message displays.



In the case **Multi-slice support** is set to **On**, the below success message and settings display.

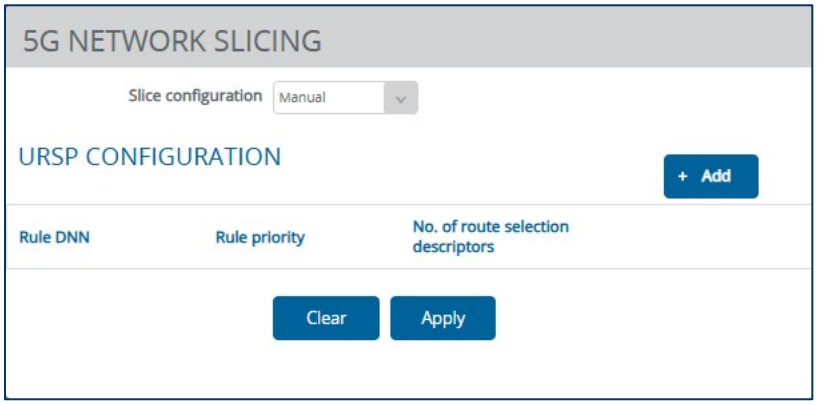


Manual Network Slice configuration

To perform manual network slice configuration:

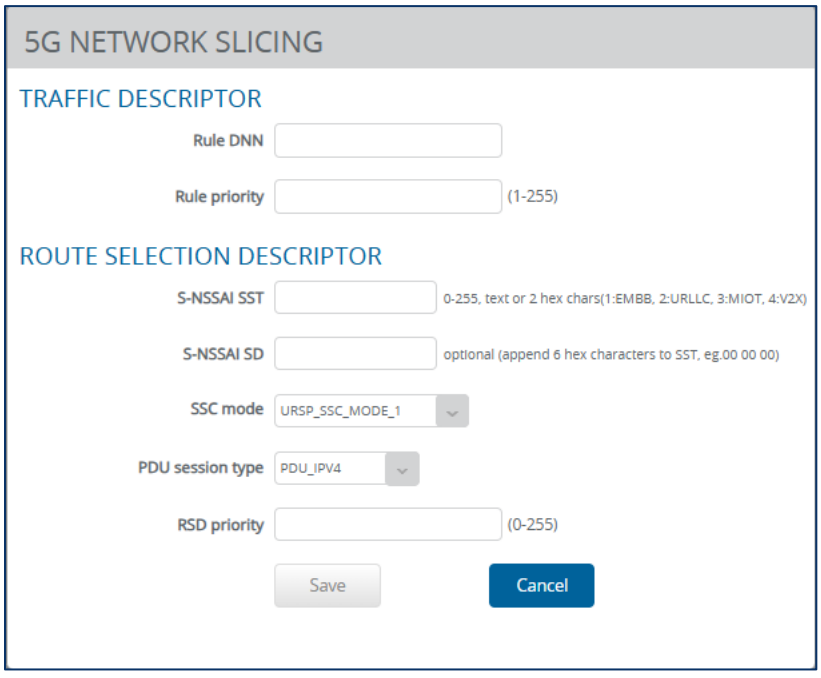
1. Select option Manual for **Slice configuration** in the 5G Network Slicing page. The below page displays.

Figure 8-14 Manual Network Slicing



2. Click **Add** for **URSP Configuration**, then click **Add** for **Route Selection Descriptor**. The below settings display.

Figure 8-15 Manual Network Slicing Configuration



The table below lists the manual network slicing configuration details.

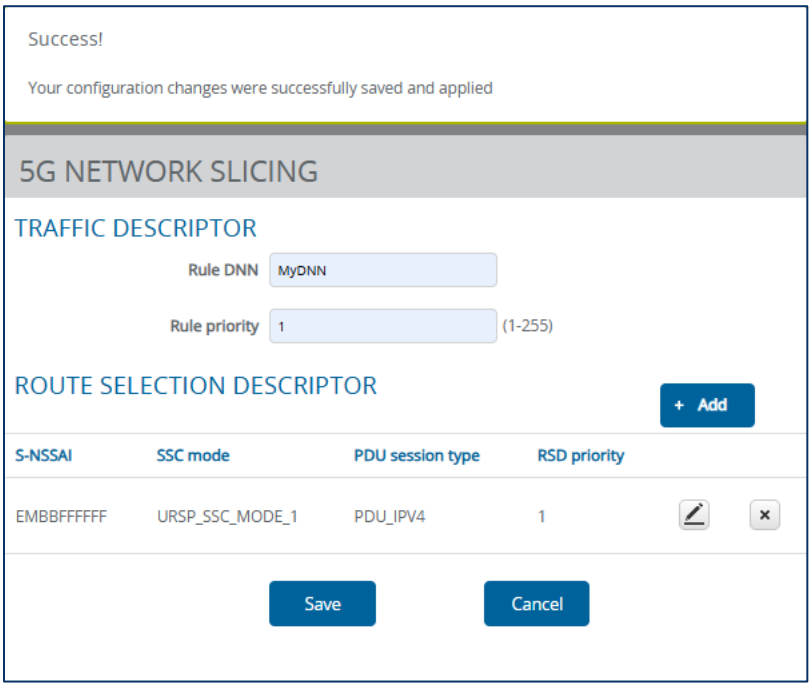
Table 8-3 Manual Network Slicing Configuration Items

Item	Definition
Traffic Descriptor	
Rule DNN	Enter the Data Network Name. It identifies the external data network (e.g., "internet" or an enterprise APN) that a PDU session should connect to.

Item	Definition
Rule priority	Enter a number from 1 to 255. It Determines the order in which URSP rules are evaluated (lower number = higher priority)
Route Selection Descriptor	
S-NSSAI SST	Enter the required value. Single-Network Slice Selection Assistance Information SST (Slice/Service Type) indicates the category or type of service the slice is intended to provide.
S-NSSAI SD	Enter the required value. Single-Network Slice Selection Assistance Information SD (Slice Differentiator) complements the mandatory SST (Slice/Service Type) to further differentiate between multiple network slices that share the same SST value.
SSC mode	Select a mode. Options are: • **URSP_SSC_MODE_1**: The network preserves the UE's connectivity and retains the same IP address throughout the session. • **URSP_SSC_MODE_2**: The network may release the PDU session and re-establish a new session, possibly assigning a new IP address. • **URSP_SSC_MODE_3**: The network allows the PDU Session Anchor (PSA) to be relocated while the session remains active, which can result in the IP address being changed.
PDU session type	Select an option. It specifies the kind of data connectivity established between a user device (UE) and the data network (DN) for a given PDU (Packet Data Unit) session. Options are: • PDU_IPV4 • PDU_IPV6 • PDU_IPV4V6
RSD priority	Enter a number from 0 to 255. It refers to the order in which Route Selection Descriptors (RSDs) are evaluated within a UE Route Selection Policy (URSP) rule.

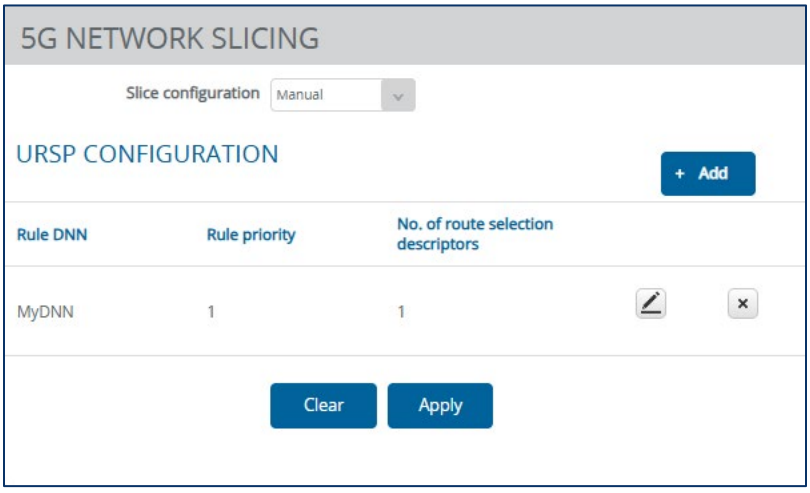
3. Click **Save** to save the settings. The above configuration is added to Route Selection Descriptor.

Figure 8-16 Manual Network Slicing – Route Selection Descriptor



4. Click to edit the Route Selection Descriptor, click to delete it.
5. Click **Save** to save the configuration. The configuration displays in the URSP Configuration.

Figure 8-17 Manual Network Slicing – URSP Configuration

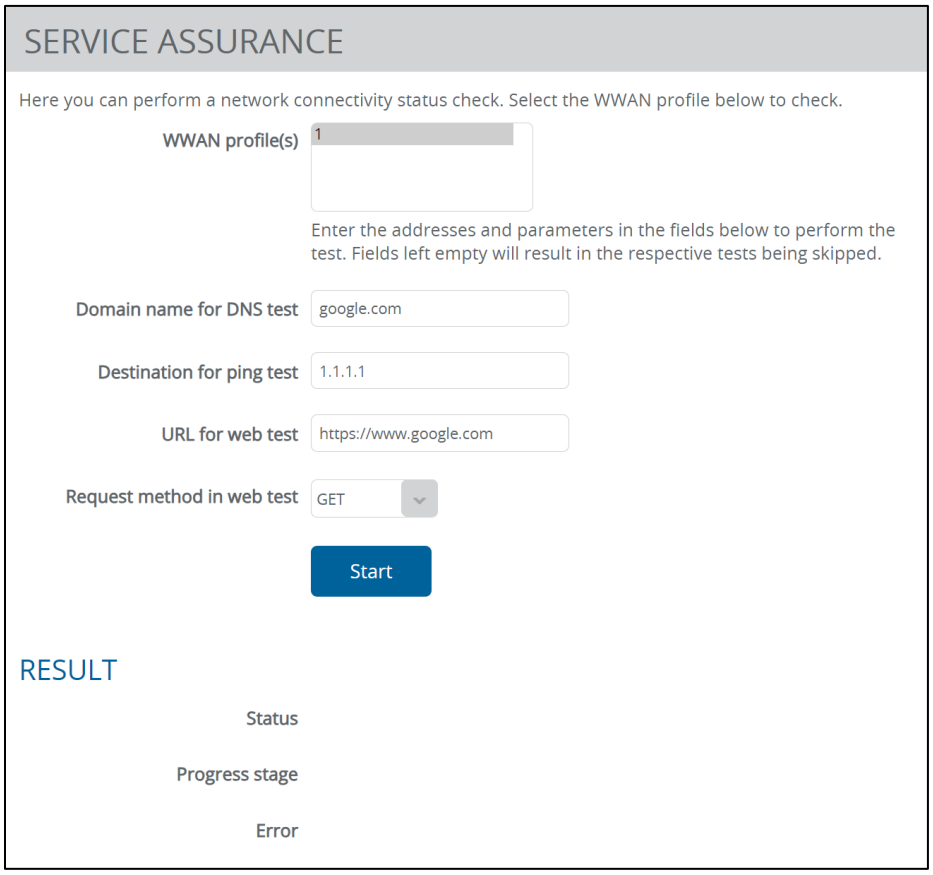


6. Click to edit that URSP configuration, click to delete it.

Service assurance

The service assurance page allows you to run a number of tests to confirm connectivity on different WWAN profiles.

Figure 8-18 Service assurance



To run a service assurance test:

1. In the **WWAN profiles** field select the WWAN profile you wish to test.
2. In the **Domain name for DNS test** field enter a Domain name to check the DNS connectivity.
3. In the **Destination for ping test** field enter an IPv4 IP address to test the ping.
4. In the **URL for web test** field enter a full URL to test a web page download.
5. In the **Request method in web test** dropdown, select either GET or PUT as the request method.
6. Press the **Start** button to run the test.

In the **Results** section, a successful test will show a **Passed** whilst a failed test will show **Failed** and which of the tests did not pass.

LAN Settings

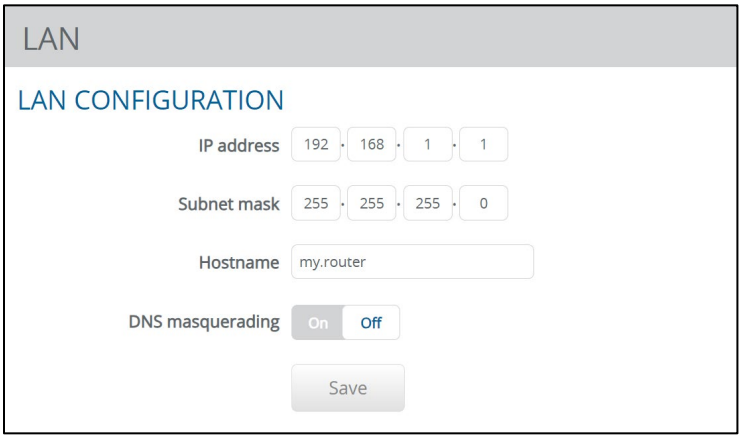
LAN

The **LAN Configuration** page allows you to configure the LAN settings of the NTC-550 Series router. To access the LAN configuration page, go to **Networking > LAN settings > LAN**

The default IP of the LAN port is 192.168.1.1 with subnet mask 255.255.255.0. To change the IP address, Subnet mask or Hostname enter the appropriate value into the respective field and select the **Save** button.

Note: *If you change the IP address, remember to refresh the Ethernet interface of your device, or set an appropriate IP address range, then enter the new IP address into your browser address bar to access the NTC-550 Series router.*

Figure 8-19 LAN configuration



DNS masquerading

DNS masquerading allows the device to proxy DNS requests from LAN clients to dynamically assigned DNS servers. When enabled, clients on the local LAN network can use the router as a DNS server without needing to know the dynamically assigned cellular network DNS servers.

The DNS masquerading toggle key is OFF by default.

With DNS masquerading OFF, the DHCP server hands out the upstream cellular DNS server IP addresses to downstream clients directly, so that downstream clients can send DNS requests directly to the upstream DNS servers without being proxied by the NTC-550 Series router.

With DNS masquerading ON, the DHCP server embedded in the NTC-550 Series router hands out its own IP address (e.g., 192.168.1.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NTC-550 Series router, which proxies them to the upstream DNS servers.

You may also override the DNS Masquerading option by specifying custom DNS Server IP addresses in the DNS server configuration, detailed in DNS server section. In this case the DHCP server assigns downstream devices the manually configured addresses and the DNS Masquerading option is ignored.

The DNS masquerading toggle key is OFF by default.

DHCP

The **DHCP configuration** page is used to configure the DHCP settings of the NTC-550 Series router. You can manually set the IP address range, the lease time of the assigned address, the default domain name suffix, primary and secondary DNS server, the primary and secondary WINS server, as well as the advanced DHCP settings such as NTP, TFTP and Option 150/Option 160 (VoIP options).

Figure 8-20 DHCP configuration

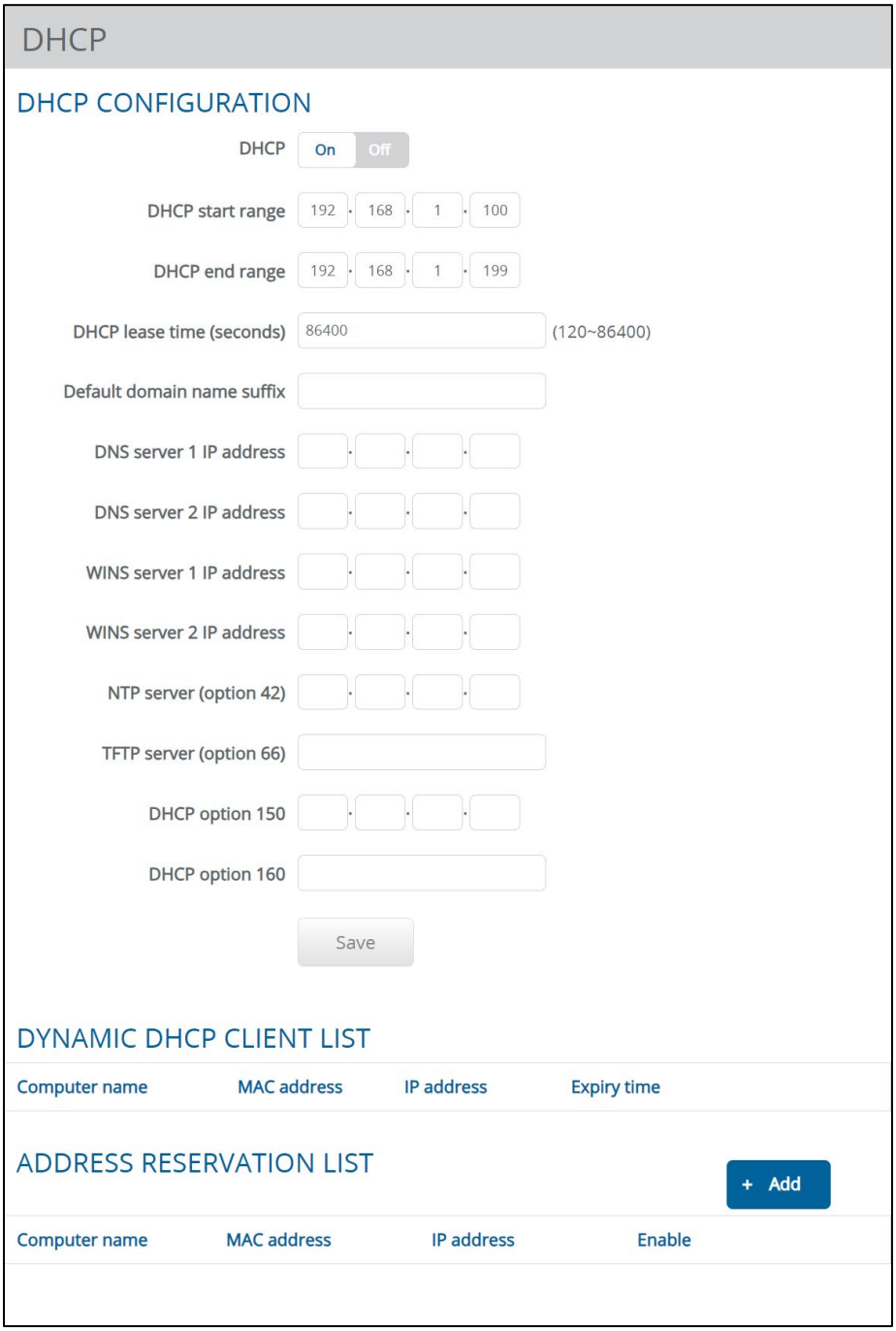


Table 8-4 DHCP configuration items

Option	Description
DHCP start range	Sets the first IP address of the DHCP range
DHCP end range	Sets the last IP address of the DHCP range
DHCP lease time (seconds)	The duration in seconds that DHCP allocated IP addresses are valid.
Default domain name suffix	Specifies the default domain name suffix for the DHCP clients. A domain name suffix enables users to access a local server, for example, server1, without typing the full domain name server1.domain.com
DNS server 1 IP address	Specifies the primary DNS (Domain Name System) server's IP address.
DNS server 2 IP address	Specifies the secondary DNS (Domain Name System) server's IP address.
WINS server 1 IP address	Specifies the primary WINS (Windows Internet Name Service) server's IP address
WINS server 2 IP address	Specifies the secondary WINS (Windows Internet Name Service) server's IP address
NTP server (Option 42)	Specifies the IP address of the NTP (Network Time Protocol) server
TFTP Server (Option 66)	Specifies the TFTP (Trivial File Transfer Protocol) server
DHCP option 150	This is used to configure Cisco IP phones. When a Cisco IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 150 request.
DHCP option 160	This is used to configure Polycom IP phones. When a Polycom IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 160 request.

Enter required values for DHCP items and click **Save** button.

Dynamic DHCP client list

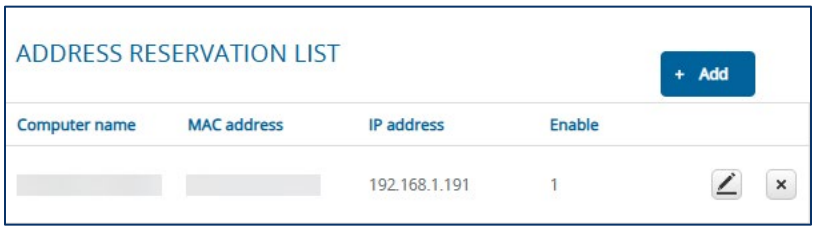
The **Dynamic DHCP Client List** displays a list of the DHCP clients that have been allocated IP addresses. If you want to reserve the current IP address for a particular device, click **Clone** button corresponding to the device details. The device details are added to the Address Reservation List.

Figure 8-21 Dynamic DHCP client list

Address Reservation List

The Address Reservation List displays the list of DHCP clients whose IP address has been reserved and add devices to the list by reserving their IP address.

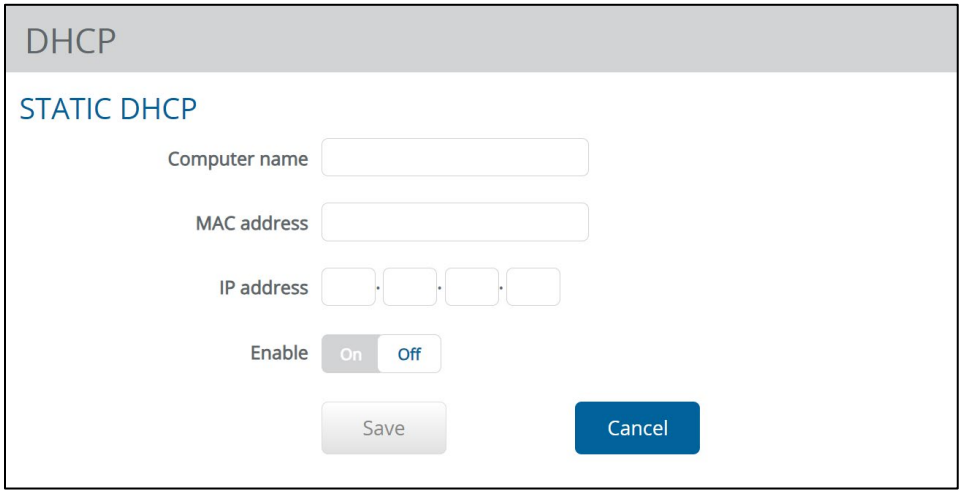
Figure 8-22 Address reservation list



To add a device to the address reservation list:

1. Select the **+Add** button. The Static DHCP page appears.

Figure 8-23 Address reservation list – Add Static DHCP settings



2. In the **Computer name** field enter a name for the device.
3. In the **MAC address** field, enter the device's MAC address.
4. In the **IP address** field, enter the IP address that you wish to reserve for the device.
5. Set the **Enable** toggle to **On** to enable the setting.
6. Select the **Save** button to save the settings.

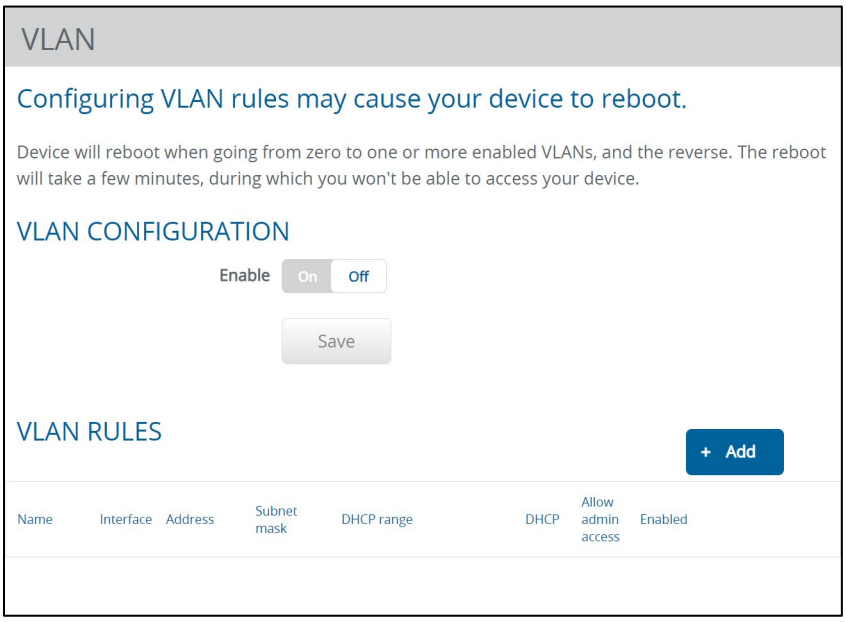
The device is added to the Address Reservation List.

Click **Edit** button to edit the details of that device and button to delete that device from the Address Reservation List.

VLAN

A Virtual Local Area Network (VLAN) is a subnetwork used to group devices located on separate physical networks. This is useful since it allows you to partition your network without the need for additional cabling or wireless access.

Figure 8-24 VLAN

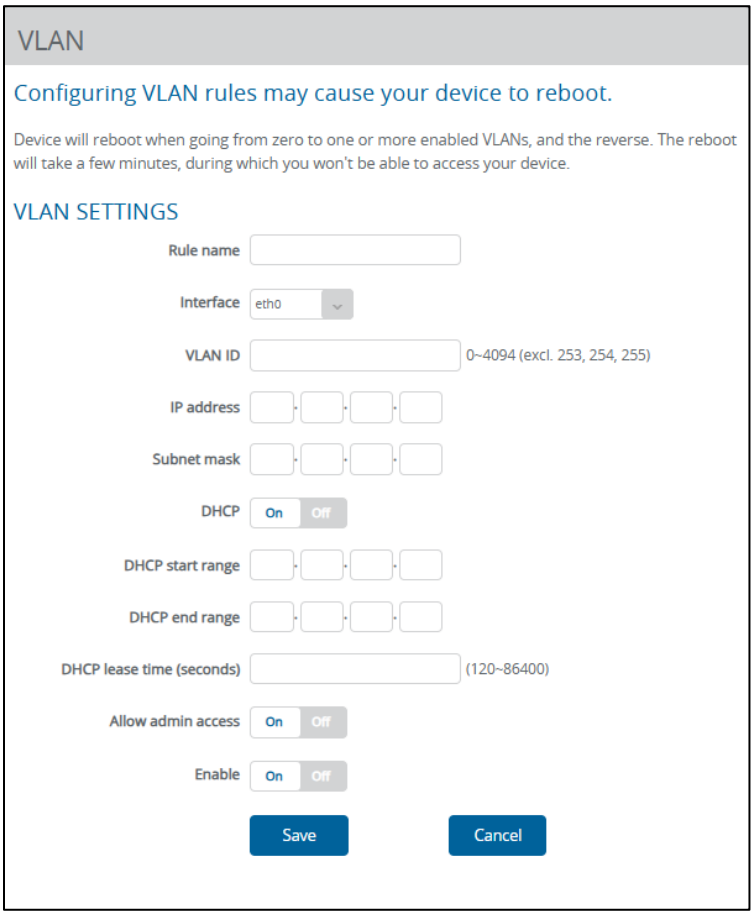


VLAN Settings

To create a VLAN:

1. Click **+Add** button on the VLAN Configuration page. The **VLAN Settings** display.

Figure 8-25 VLAN Settings

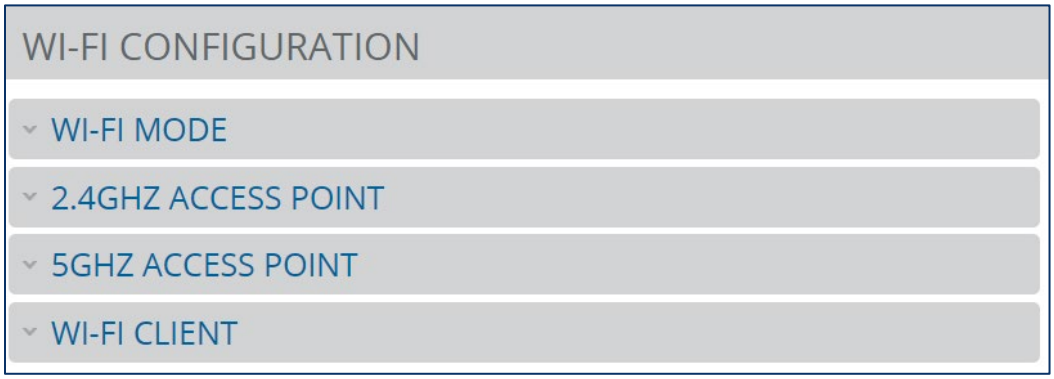


2. In the **Rule name** field, enter a name for the VLAN rule. This is a name that allows you to easily identify the VLAN.
3. In the **VLAN ID** field, enter a number between 0 and 4094 which will be used by the network to identify the VLAN uniquely.
4. In the **IP address** field, enter the IP address for this device on the VLAN.
5. In the **Subnet mask** field, enter the Subnet mask for the device on the VLAN.
6. To use DHCP, set the **DHCP** to On position. Enter values for **DHCP start range** and **DHCP end range** fields. Addresses within this range will be assigned automatically to devices connecting to this VLAN.
7. In the **DHCP lease time (seconds)** field, enter the number of seconds for which the DHCP lease is valid. This value must be 120 or higher.
8. To allow access to the administration web interface, set the **Allow admin access** toggle to **On** position.
9. Set the **Enable** toggle to the **ON** position.
10. Select on the **Save** button to apply the settings.

Wi-Fi Settings

The Wi-Fi configuration allows you to configure settings for Wi-Fi functionality of the NTC-550 Series router. Click each section to display the fields and configure that section.

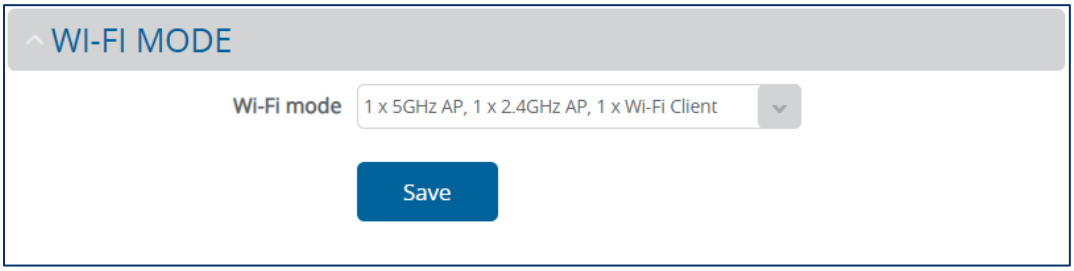
Figure 8-26 Wi-Fi configuration



Wi-Fi mode

The Wi-Fi mode allows you to configure the Wi-Fi mode that the NTC-550 Series router should operate in. To configure each of the modes once the selection has been made, click the required section in the **Wi-Fi configuration** page

Figure 8-27 Wi-Fi configuration – Wi-Fi mode



Two modes are available:

1 x 5GHz AP, 1 x 2.4GHz AP, 1 x Wi-Fi Client

In this mode, the NTC-550 Series router will broadcast one 5GHz Wi-Fi network, one 2.4GHz network and will be able to connect to another Wi-Fi network to act as a WAN connection for the gateway.

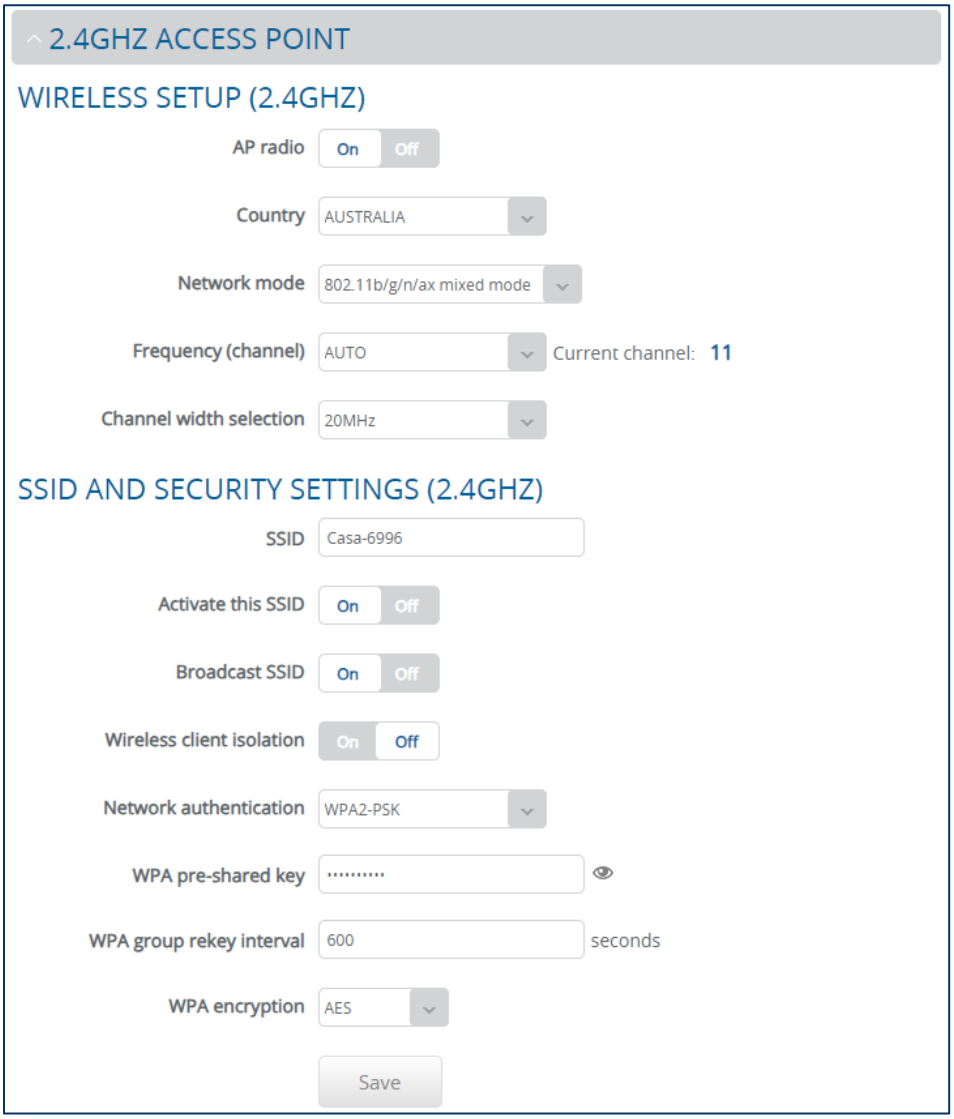
2 x 5GHz AP, 1 x 2.4GHz AP

In this mode, the NTC-550 Series router will broadcast two 5GHz Wi-Fi networks and one 2.4GHz Wi-Fi network.

Access Point configuration

Both the 2.4 GHz and 5GHz access points provide the same configuration settings for their relevant band.

Figure 8-28 Wi-Fi configuration – 2.4GHz access point



Wireless Setup

To configure the Wireless Setup of the access point:

1. Set the **AP radio** toggle to **On** to enable the access point.
2. Set the **Country** field to the country where the NTC-550 Series router is located.
3. Set the **Network mode** to the Wi-Fi version which should be broadcast. The default is 802.11b/g/n/ax mixed mode, which covers most modern devices.
4. Set the **Frequency (channel)** to the appropriate channel. The default is **Auto,** for which the router will analyze the surrounding networks and choose the most appropriate channel.
5. Set the **Channel Width** to the most appropriate width. Lower channel widths will generally provide better stability in an environment with many other interfering Wi-Fi networks or with high levels of frequency interference.
6. Select the **Save** button at the bottom of the page to apply any changes.

SSID and security settings

To configure the SSID and security settings of the Wi-Fi access point:

1. Set the **SSID** (Wi-Fi name) of the network as required.
2. Set the **Activate SSID** toggle to **On** to enable the SSID. If the toggle is set to off, clients will be unable to connect to the access point.
3. Set the **Broadcast SSID** toggle to **On** to broadcast the SSID and allow it to be seen by clients. If the toggle is set to **Off** the SSID will not appear in the list of networks for clients to connect.
4. Set the **Wireless client isolation** toggle to **On** to only allow Wi-Fi clients to access the internet via the Wi-Fi network. They will not be able to access other devices on the network. Set the toggle to **Off** to allow clients to find and connect to network resources connected to the NTC-550 Series router.
5. Set the **Network authentication** field to the required level of security for the Wi-Fi network. Options are **Open, WPA2-PSK,** and **WPA3-SAE**. If you select **Open** any Wi-Fi device will be able to access the network, which may compromise the security of the router and any other connected devices.
6. Enter a value for **WPA shared key** field. This key should be used by Wi-Fi clients to connect to the network.
7. Enter a value for **WPA group rekey interval**. It is the number of seconds between WPA key rotations. The default is 600 seconds.
8. Set the **WPA encryption** type field to either **AES** or **None**. Selecting none may reduce the security of the network key.
9. Select the **Save** button to apply the changes.

Wi-Fi client

The Wi-Fi client section allows you to configure the NTC-550 Series router to connect an existing Wi-Fi network, allowing you to rebroadcast an internet connection via the NTC-550 Series router.

Figure 8-29 Wi-Fi configuration – Wi-Fi Client

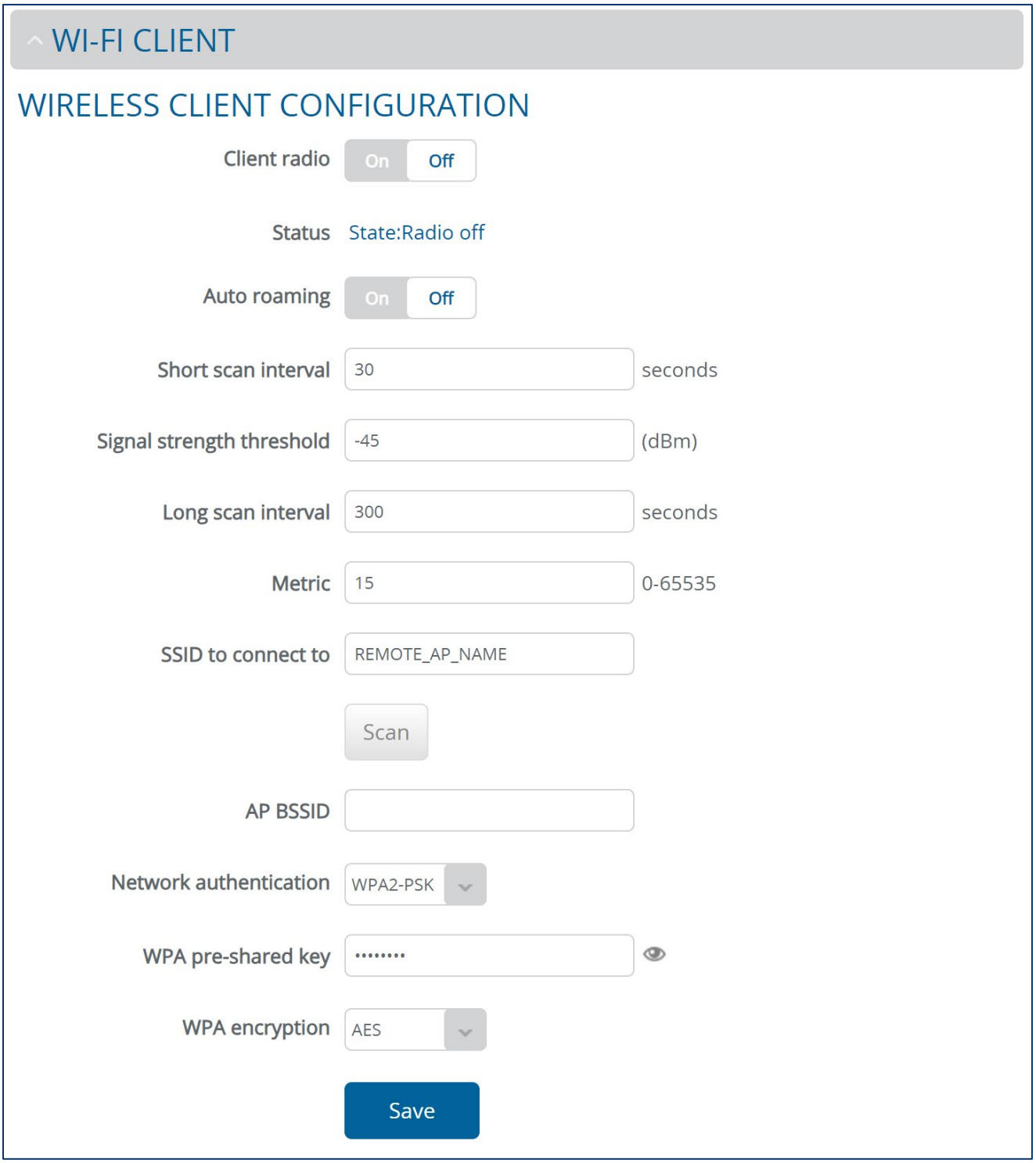


Table 8-5 Wireless Client Configuration Items

Item	Definition
Client radio	Set to **On** to enable.
Status	Displays the current channel and connection status of the wireless client.
Auto roaming	Set to **On** to enable. Auto roaming allows the router to scan for other access points with the same SSID at regular intervals to determine whether the signal strength is below the Signal strength threshold and switch to an access point with a stronger signal if it is below the threshold at the time of the scan.
Short Scan Interval	Enter the time in seconds. The interval at which the router will scan all access points with the same SSID when the signal strength is below the Signal strength threshold.
Signal strength threshold	Enter the value. The signal strength value in dBm that determines whether the router should use the Short scan interval or the Long scan interval
Long scan interval	Enter the time in seconds. The interval at which the router will scan all access points with the same SSID when the signal strength is above the Signal strength threshold.
Metric	Enter the metric value is used by the router to prioritise routes.
SSID to connect to	Enter the SSID of the network you wish to connect to. Click **Scan** to discover nearby networks.
AP BSSID	Enter the BSSID or MAC address of the access point to which you are connecting.
Network authentication	Select type of authentication in use on the network from the available options.
WPA pre-shared key	Enter the pre-shared key required to join the wireless network.
WPA encryption	Select the type of encryption in use on the network.

Click **Save** to save the settings.

Figure 8-30 Wi-Fi configuration – Wi-Fi Client - Connected

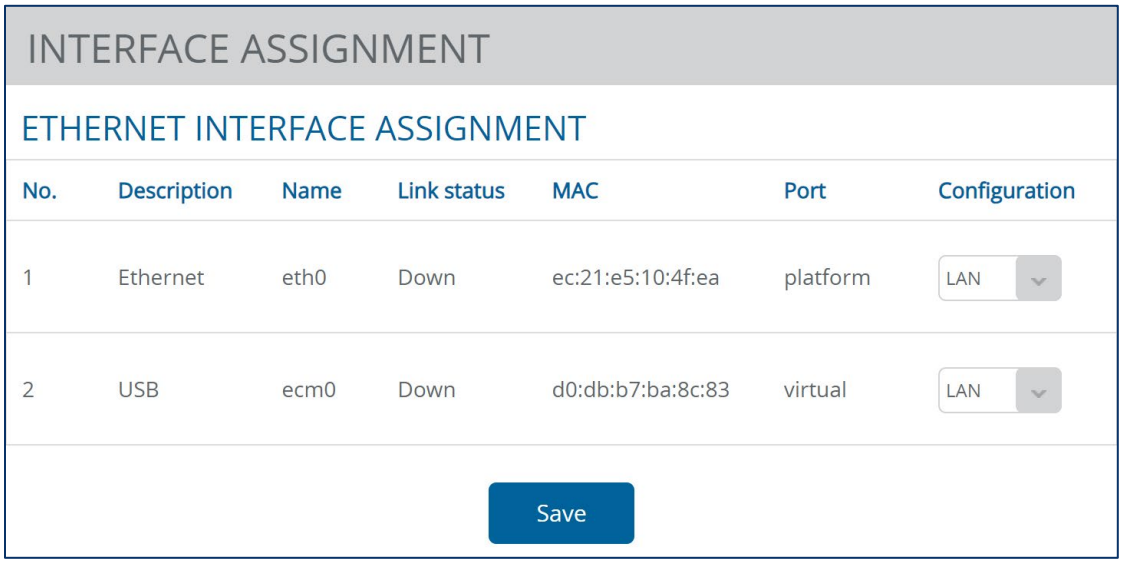
WAN Settings

The WAN Settings section allows you to configure the WAN port on the NTC-550 Series router.

Interface assignment

The Interface assignment page allows you to configure the functionality of the WAN port or the virtual USB port.

Figure 8-31 WAN Settings – Interface assignment

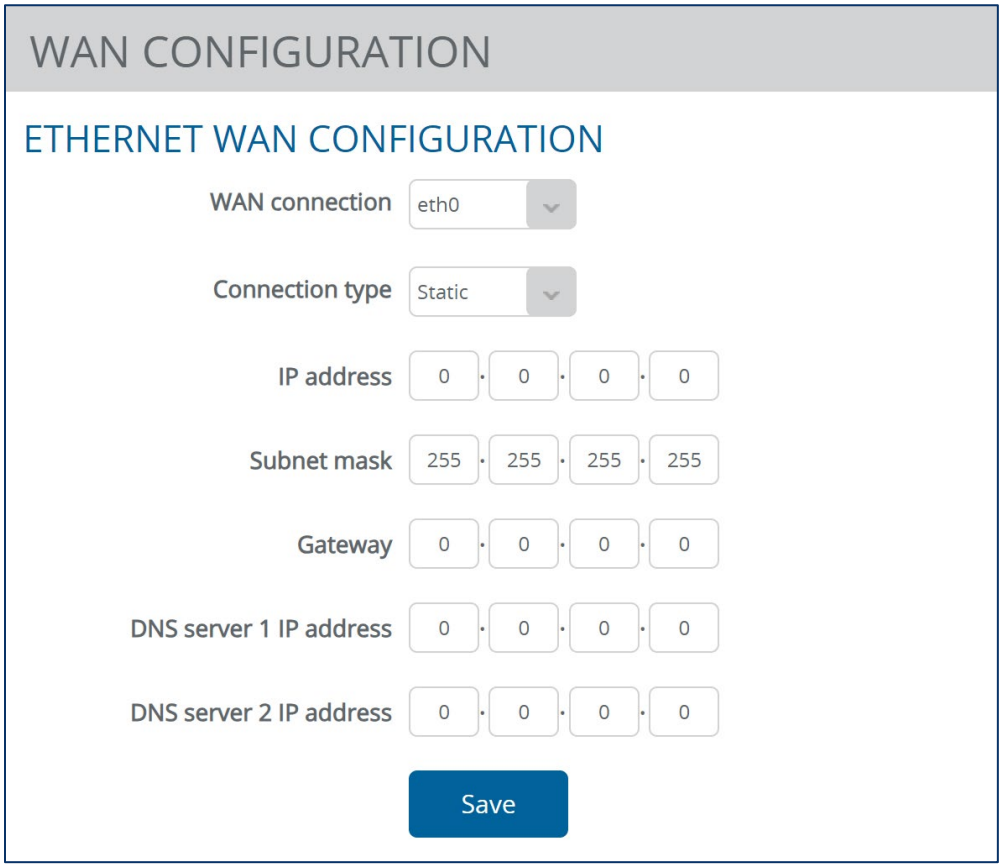


Use the dropdown under the **Configuration** column to set the function of the port. Set the field to **LAN** for the port to function as a **LAN** port. Set the field to **WAN** for the port to function as a WAN port, which allows you to configure it as an incoming connection. Set the field to **Disable** to disable the port. Select **Save** to apply the change.

WAN configuration

The **WAN configuration** allows you to configure the WAN connection.

Figure 8-32 WAN Settings – WAN configuration



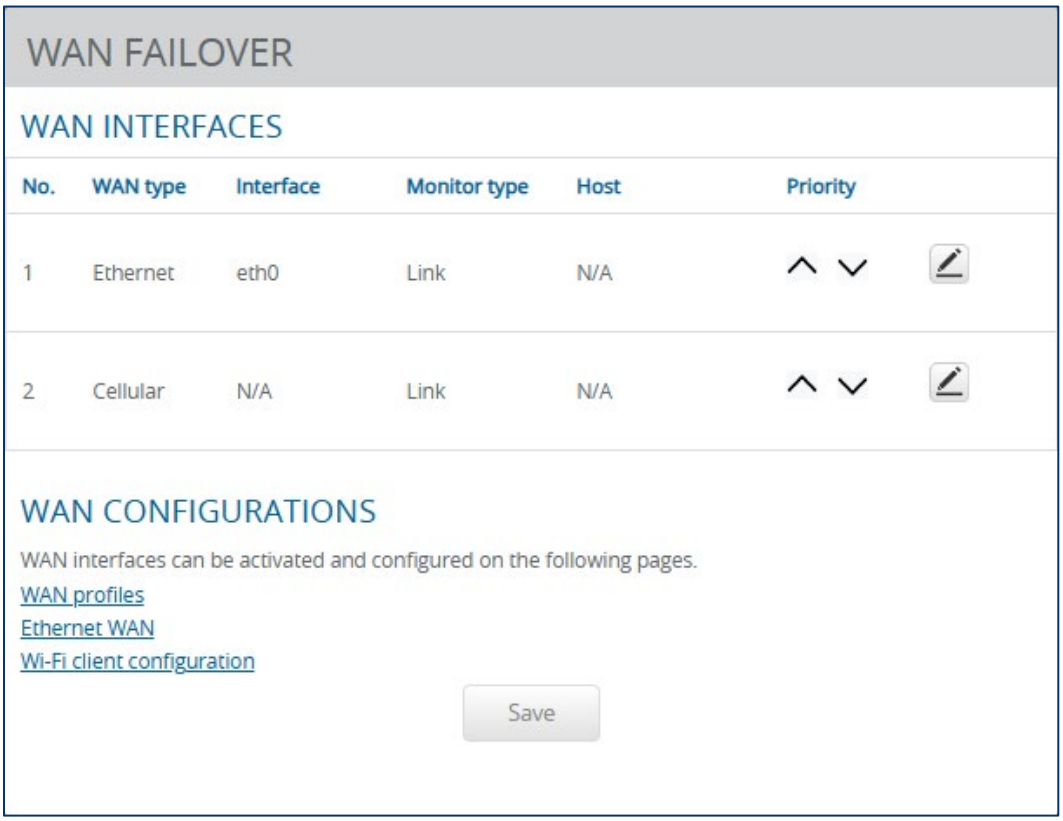
To configure the WAN connection:

1. Set the **WAN connection** field as the ethernet interface you want to use for WAN connection.
2. Set the **Connection type** field to match the requirements of the WAN connection, either **DHCP** or **Static.**
3. If using **Static**, enter required values for the following fields:
   - **IP address**
   - **Subnet mask**
   - **Gateway**
   - **DNS server 1 IP address**
   - **DNS server 2 IP address**
4. Select the **Save** button to apply the changes.

Failover

The WAN failover page allows you to configure the priority of failover for WAN connections on the NTC-550 Series router. When multiple connections are active, one can be prioritised over another. The method by which the connection can be monitored can also be configured.

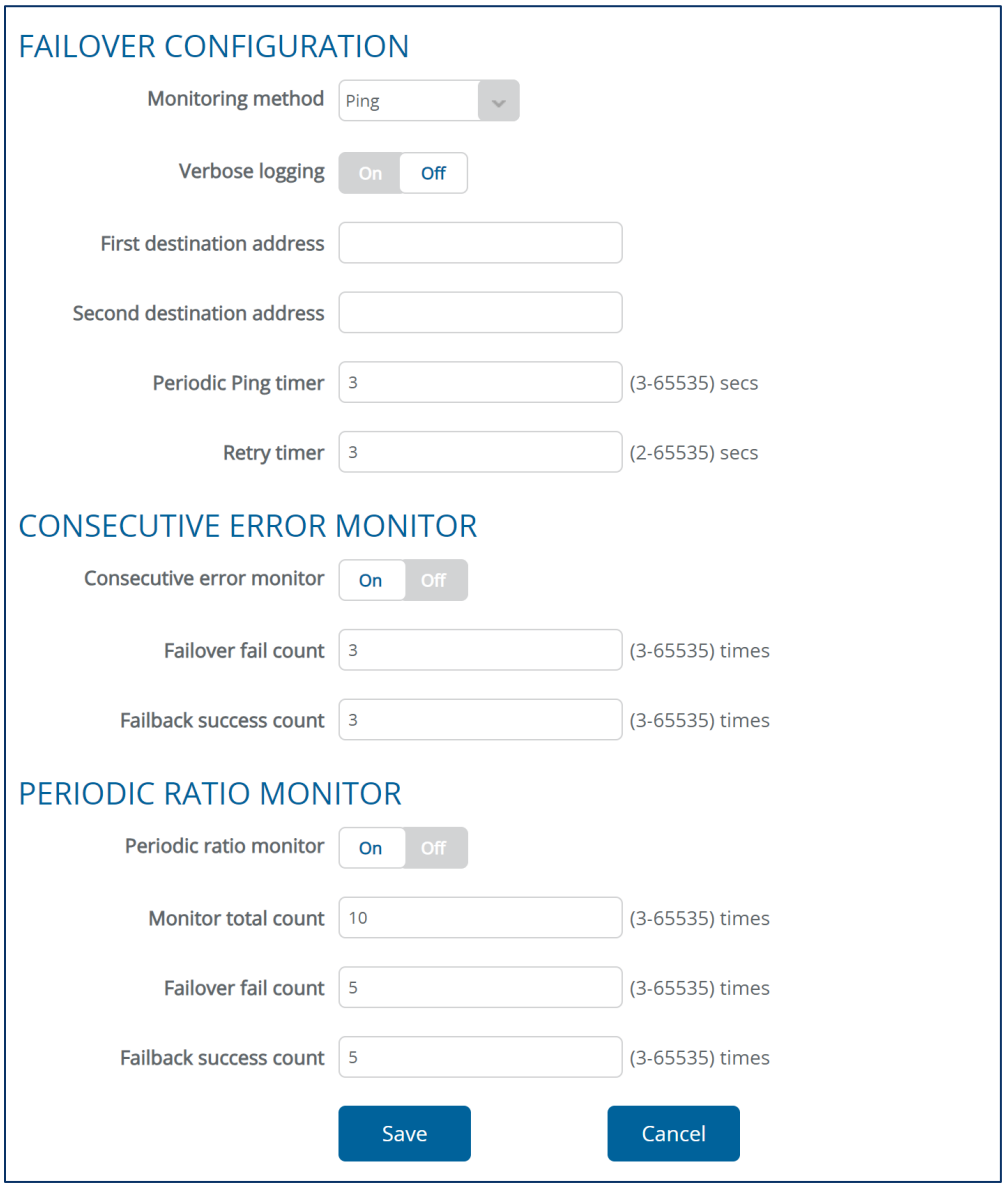
Figure 8-33 WAN Settings – Failover



Use the **Priority** arrows to move each connection to the appropriate position on the **Failover** table. The interface at the top will receive priority over the connections which follow it. When a connection becomes disconnected, the router will try to failover to the next connection.

Click button to manage the connection monitoring method.

Figure 8-34 WAN Settings – Failover – Failover configuration



Monitoring Methods

The following methods are available:

- **Physical link**: If the monitoring method is set to Physical link, the failover mechanism is controlled by the physical detection of the link. When the physical link to eth.0 is broken (i.e. the cable is disconnected, or some other hardware fault causes the physical connection to fail), the router fails over to the WAN interface with the next highest priority.
- **Ping**: If the monitoring method is set to Ping, controlled ping packets can be used to determine the status of the link. These are small packets of data that the router sends to a remote address and if the connection is up, a reply is received. They are sent indefinitely at regular intervals that you specify. At each interval, a set of 3 pings are sent to the first destination address and 3 pings are sent to the second destination address configured for each WAN interface to test the availability of the interface.

Methods of evaluating ping responses

The following methods are available:

- **Consecutive Error Monitor** - using this method, the router will determine the availability of an interface based on a set number of consecutive ping instance responses.
- **Periodic Ratio Monitor** - using this method, the router will determine the availability of an interface based on a set ratio of ping instance successes or failures to the number of attempts.

It should be noted that the Periodic ratio monitor evaluates an interface over a Series of ping instances (defined by the Total monitor count) and when the Series has completed, the success and fail counts are reset. For example, with the default Total monitor count value set to 10 and Failover fail count set to 5, the router sends 10 ping instances and if 4 of those instances fail and the first instance of the next Series of 10 fails, the router will not fail over because the 5 failed instances occurred across a different Series.

To simplify configuration, we recommend using only one of the monitor types at any point in time.

Table 8-6 Ping Monitoring Configuration Items

Item	Definition
Failover Configuration	
Monitoring method	Select **Ping**.
Verbose logging	When enabled, this logs verbose comments in the system log related to the failover monitoring.
First destination address	Enter the first address that the router should ping in order to confirm the connection is up. This may be an IP address or a domain name.
Second destination address	Enter the second address that the router should ping in order to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	The time in seconds between ping attempts.
Retry timer	The time in seconds between attempts when a ping failure occurs.
Consecutive Error Monitor	
Consecutive error monitor	Set to **On** to enable.
Failover fail count	The number of failed pings that must occur before the monitor fails the connection over to the next interface.
Failback success count	The number of successful pings that must occur before the monitor fails the connection back to the higher priority interface.
Periodic Ratio Monitor	
Periodic ratio monitor	Set to **On** to enable.
Monitor total count	This field specifies a Series of pings to consider when calculating whether to fail over or fail back. When the Series is completed, the router repeats the ping test and resets the Failover fail count/Failback success count, therefore, in order for

Item	Definition
	the failover or failback ratio to be met, the number of Failover fail counts/Failback success counts must occur within a particular Series.
Failover fail count	This field specifies the number of failed ping results that must occur within a Series of pings configured in the Monitor total count before the router fails over to the next highest priority interface. For example, at the default setting of 5, the router fails over to the next interface when 5 out of 10 ping attempts in a particular Series have failed. The failures need not be consecutive to meet the failover criteria. If any 5 of the 10 pings in a Series have failed, the router deems the interface connection to be down and fails over.
Failback success count	Like the Failover fail count field, this field specifies the number of ping successes that must be registered on a higher priority interface within a Series of pings configured in the Monitor total count before the router fails back to that interface.

To configure Failover for Ping monitoring method:

1. In the **First destination address** field, enter a website address or IP address to which the router should send the first round of ping requests.
2. In the **Second destination address** field, enter a website address or IP address to which the router should send the second round of ping requests.
3. In the **Periodic Ping timer** field, enter an integer between 3 and 65535 for the number of seconds the router should wait between ping attempts.
4. In the **Retry timer** field, enter an integer between 2 and 65535 for the number of seconds the router should wait between retry ping attempts, i.e. pings to the second destination address.
5. Configure Consecutive Error Monitor.
    a. Set the **Consecutive error monitor** toggle to **On** position.
    b. In the **Failover fail count** field, enter an integer between 3 and 65535 for the number of times a retry ping should fail before the router fails over to the next WAN interface.
    c. In the **Failback success count** field, enter an integer between 3 and 65535 for the number of times a periodic ping should succeed before the router fails back to the higher priority interface.
    d. Click **Save** to Save the settings.
6. Configure Periodic ratio Monitor.
    a. Set the **Periodic ratio monitor** toggle to On,
    b. In the **Monitor total count** field, enter an integer between 3 and 65535 for the number of previous ping instances to consider for failover and failback.
    c. In the **Failover fail count** field, enter the number of pings out of the total count that must fail before the router fails over to the next highest priority WAN interface.
    d. In the **Failback success count** field, enter the number of pings out of the total count that must succeed before the router fails back to the higher priority WAN interface.
    e. Click **Save** to save the settings.

To simplify configuration, we recommend using only one of the monitor types at any point in time i.e. either the **Consecutive error monitor** or the **Periodic ratio monitor**.

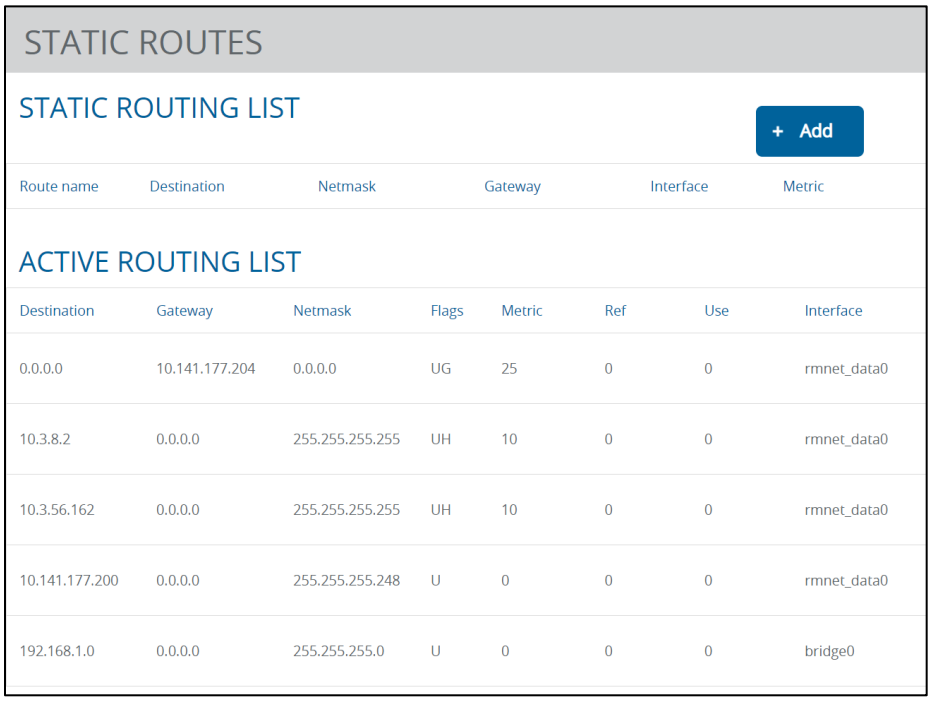
Routing settings

Static routes

Static routing is the alternative to dynamic routing used in more complex network scenarios and is used to facilitate communication between devices on different networks. Static routing involves configuring the routers in your network with all the information necessary to allow the packets to be forwarded to the correct destination. If you change the IP address of one of the devices in the static route, the route will be broken.

To access the Static routing page, select on the **Networking** menu at the top of the screen, select on the **Routing** menu on the left, then select on the **Static** menu item.

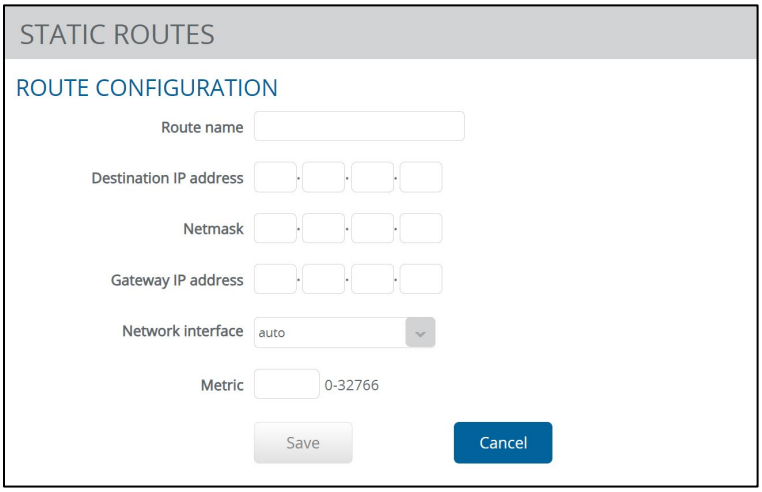
Figure 8-35 Static routing



Adding Static Routes

To add a new route to the static routing list, select the **+Add** button. The **Static routes** page displays.

Figure 8-36 Static routing – Route configuration

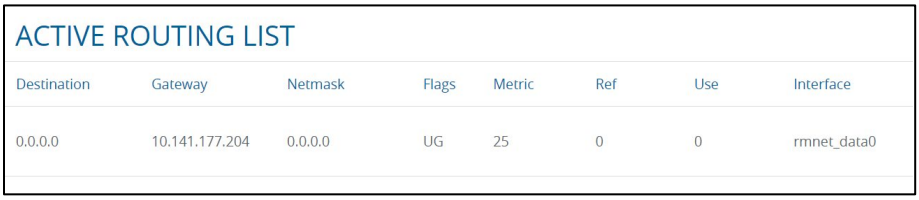


1. In the **Route name** field, type a name for the route so that it can be identified in the static routing list.
2. In the **Destination IP address** field, enter the IP address of the destination of the route.
3. In the **Destination netmask** field, enter the subnet mask of the route.
4. In the **Gateway IP address** field, enter the IP address of the gateway that will facilitate the route.
5. From the **Network interface** drop-down list, select the interface for which you would like to create a static route.
6. In the **Metric field** enter the metric for the route. The metric value is used by the router to prioritize routes. The lower the value, the higher the priority. To give the route the highest priority, set it to 0.
7. Click the **Save** button to save your settings.

Active Routing List

Static routes are displayed in the **Active routing list**.

Figure 8-37 Static routing – Active routing list



Static Routing List

From the static routing list, click the **Delete** icon to the right of the entry you wish to delete.

Figure 8-38 Static routing – Static routing list

Firewall

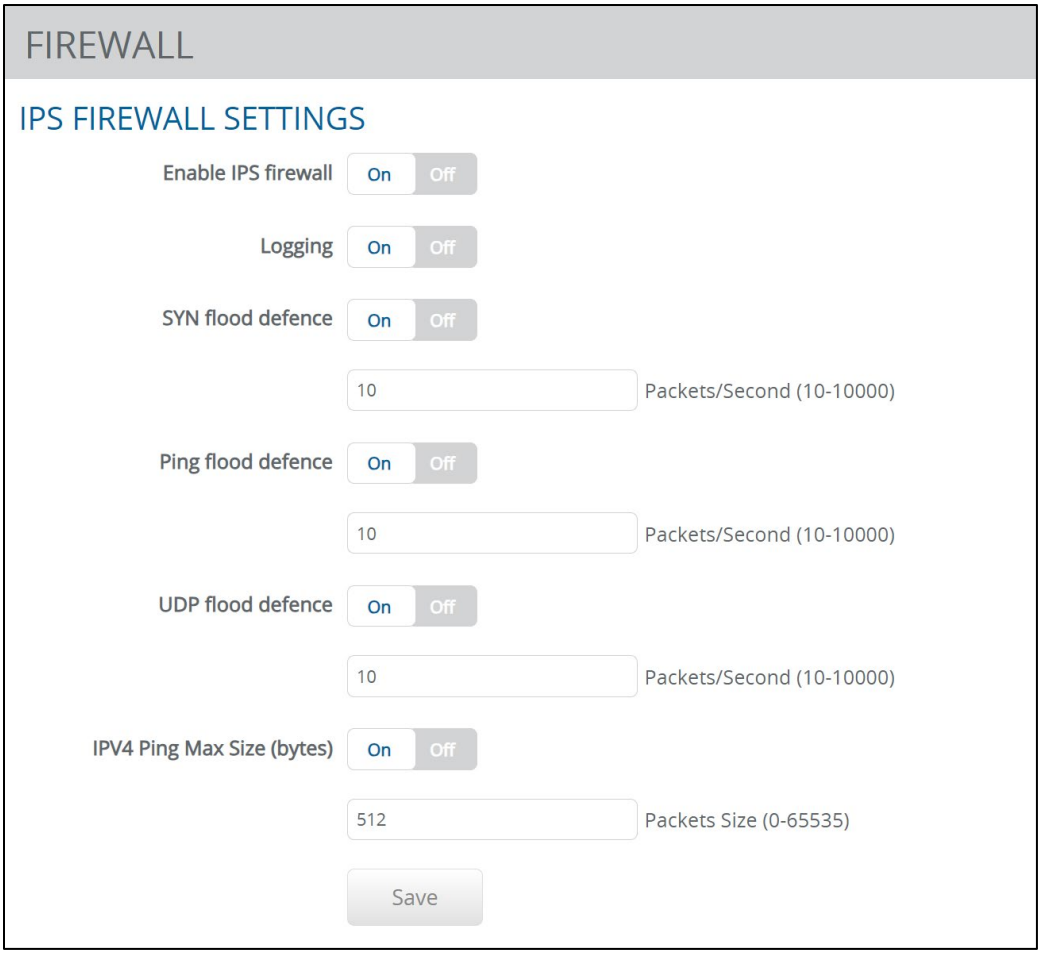
The Firewall on the NTC-550 Series router implements an Intrusion Prevention System (IPS). The IPS works together with system firewalls, but in a different manner, to prevent unauthorised access to your network and potentially malicious attacks. It provides a few more levels of security protection for your system from external threats.

Firewalls are rules-based and allow or exclude broad ranges of traffic that do not meet the criteria. IPS monitors and analyses individual inbound data packets to identify threats. Be aware that an IPS should not be considered a replacement for a well-defined firewall but should be seen as one more defensive weapon in your network security arsenal: firewalls, anti-virus software, etc.

IPS filters are interposed between the firewall and the other NTC-550 Series router functionality. It uses a variety of sophisticated techniques to monitor traffic flows and analyse inbound packets to determine whether they constitute network threats and, if so, deny them access. The IPS firewall allows different levels of protection to be selectively applied, to thwart a specifically identified threat.

IPS Firewall Settings

Figure 8-39 IPS router firewall



The table below lists the IPS Firewall Settings configuration details

Table 8-7 IPS Firewall Settings Configuration Items

Item	Description
Enable IPS Firewall	Enables or disables IPS Firewall
Logging	Enables or disables logging of network activity.
SYN flood defense	Enables or disables SYN flood defense which restricts the number of SYN requests processed by the router during a given time frame. When enabled enter the number of packets/second. Default value is 10, range (10-10000)
Ping flood defense	Enables or disables Ping flood defense. When enabled enter the number of packets/second accepted. Default value is 10, range (10-10000)
UDP flood defense	Enables or disables UDP flood defense. When enabled enter the number of packets/second allowed from a single source. Default value is 10, range (10-10000)

Item	Description
IPV4 Ping Max Size (bytes)	Enables or disables IPV4 Ping Max Size which allows you set maximum size for an IPv4 packet. When enabled enter the maximum packet size. Default value is 512, range (0-65535)

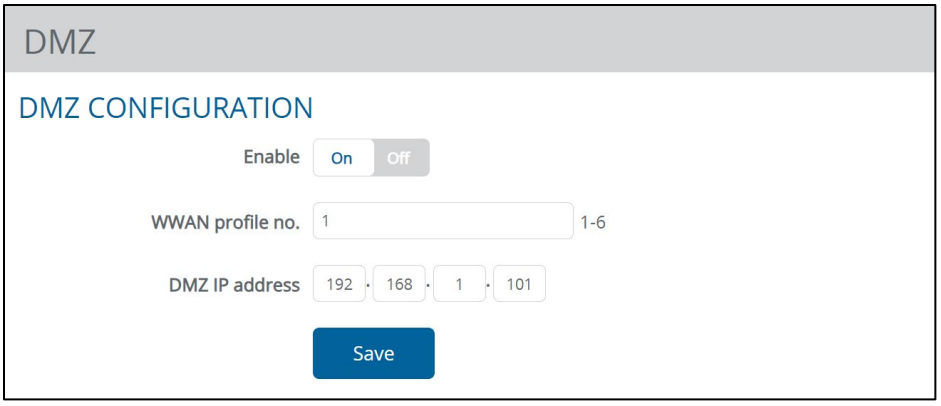
Click **Save** to save the settings.

DMZ

The Demilitarized Zone (DMZ) allows you to configure all incoming traffic on all protocols to be forwarded to a selected device behind the router. This feature can be used to avoid complex port forwarding rules, but it exposes the device to untrusted networks as there is no filtering of what traffic is allowed and what is denied. The DMZ configuration page is used to specify the IP Address of the device to use as the DMZ host.

To access the DMZ page, select on the **Networking** menu at the top of the screen, select on the **Routing** menu on the left, then select on the **DMZ** menu item.

Figure 8-40 DMZ configuration



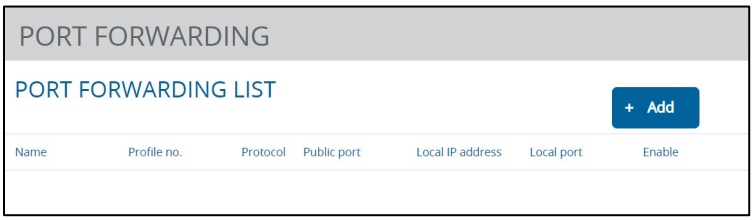
To configure DMZ:

1. Set **Enable** to On.
2. Enter the WWAN profile number with which you want to associate the DMZ configuration.
3. Enter the IP Address of the device to be the DMZ host in the **DMZ IP Address** field.
4. Select the **Save** button to save your settings.

Port forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the NTC-550 Series router. To access the Port forwarding page, select on the **Networking** menu at the top of the screen, select on the **Firewall** menu on the left.

Figure 8-41 NAT



The purpose of the port forwarding feature is to allow mapping of inbound requests to a specific port on the WAN IP address to any connected device.

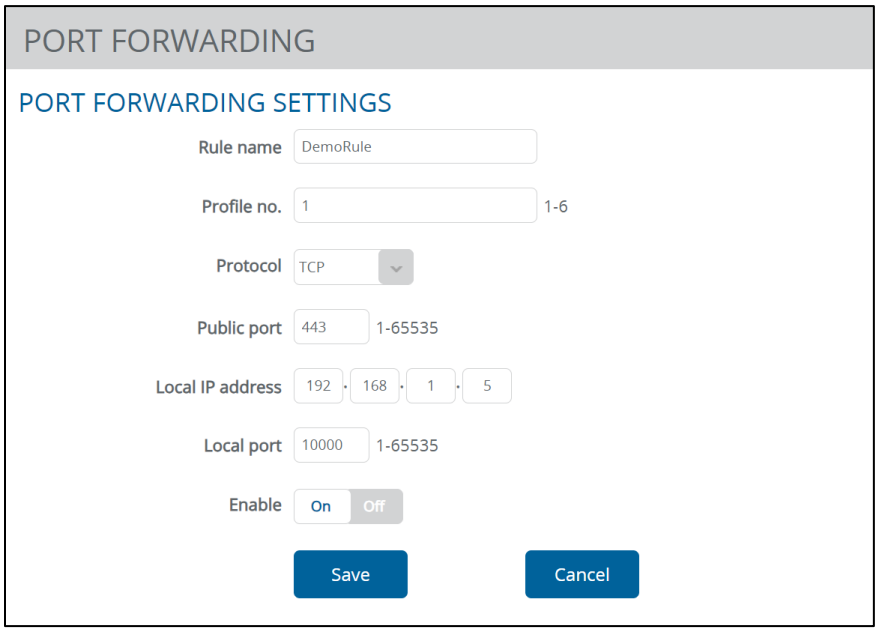
Note: *Some carriers block inbound connections or require a public IP address to get inbound requests.*

Adding a port forwarding rule

To create a new port forwarding rule:

1. Click **+Add** button in the Port Forwarding List page. The Port Forwarding Settings page displays.

Figure 8-42 IPv4 Port Forwarding Settings



2. In the **Rule name** field, enter a name for the rule so that it can be easily identified.
3. In the **Profile no.** field, enter the of the Wireless WAN Profile that you want to use for the rule.
4. Use the **Protocol** drop-down list to select the type of protocol you want to use for the rule. The protocols selections available are **TCP**, **UDP** and **TCP/UDP**.
5. In the **Public port** field, enter port number to use for the communication between the NTC-550 Series and the mobile network, range (1-65535)
6. In the **Local IP Address** field, enter the IP address of LAN equipment to which traffic should be routed or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the traffic.

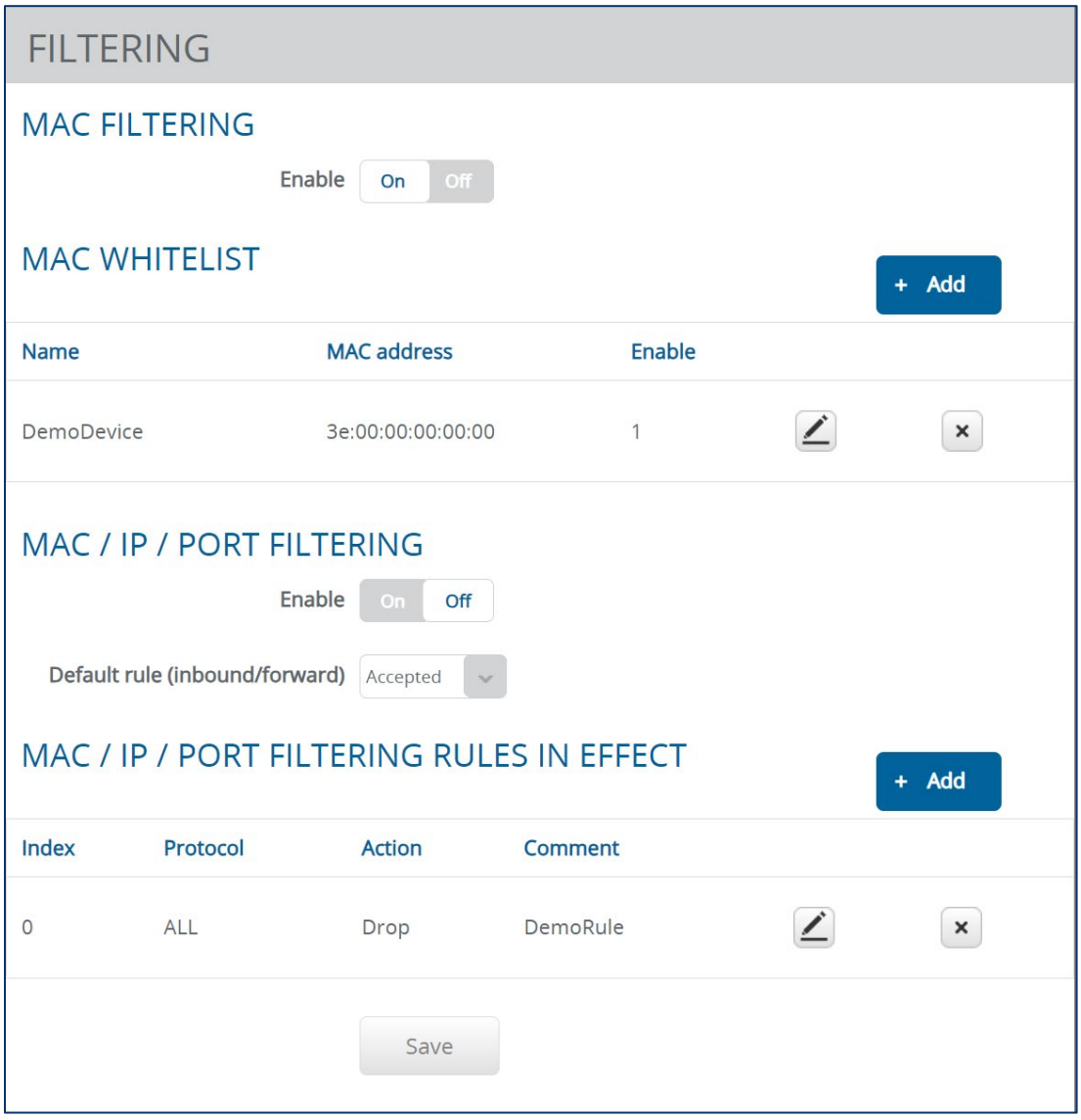
7. In the **Local port** field, enter the port number to use for traffic to the local device, range (1-65535).
8. Set the **Enable** toggle to **On** position.
9. Click **Save** to save your settings.

To delete a port forwarding rule, click the button in the **Port forwarding list** for the rule that you want to delete. To edit an existing rule, select on the button for that rule.

Filtering

The Filtering feature allows you to restrict devices that are allowed to connect to the NTC-550 Series router bases on their MAC address.

Figure 8-43 Filtering



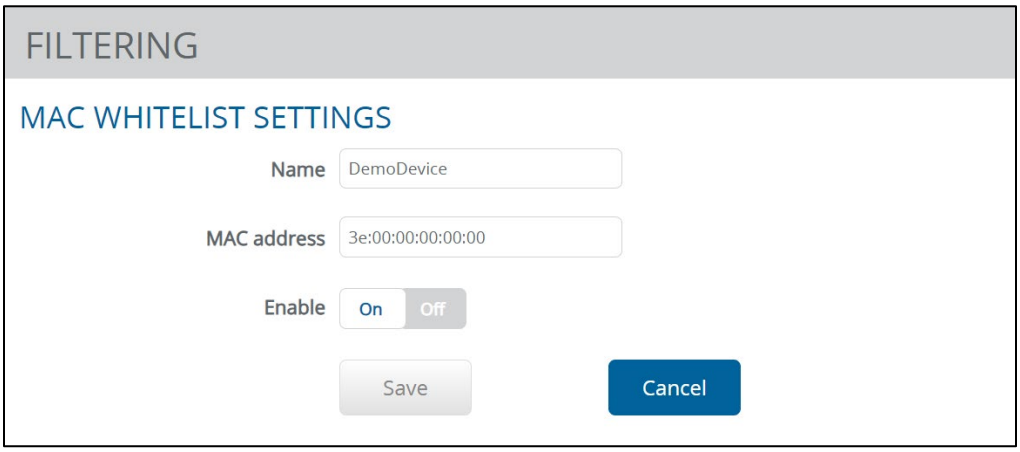
To enable MAC filtering, set the **Enable** toggle to **On**, then click **Save.**

MAC whitelist

To add a device to the MAC whitelist:

1. Click **+Add** button in MAC Whitelist. The **MAC whitelist settings** page displays.

Figure 8-44 MAC - MAC filtering whitelist settings



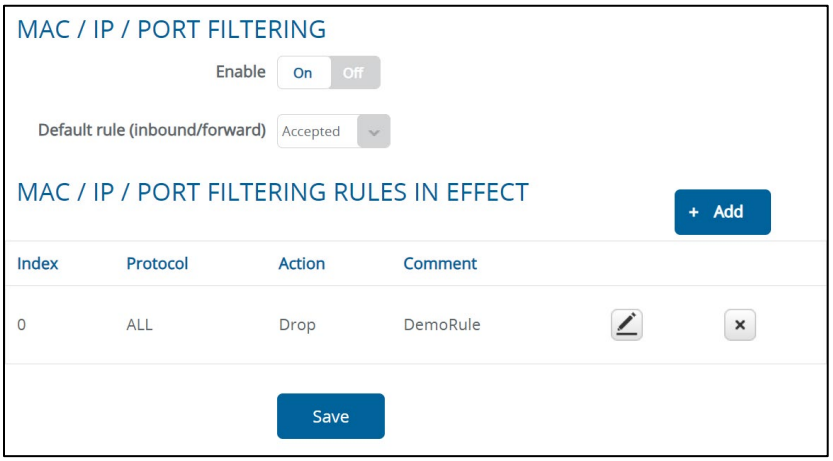
2. In the **Name** field, enter a name for the device.
1. In the **MAC address** field, enter the MAC address of the device.
2. Set the Enable toggle to **On.**
3. Click **Save** button.
4. The device displays in the **MAC Whitelist** section.

To remove a device, select the button for that device. To edit the device, including temporarily disabling it, Click the button.

MAC / IP / Port filtering

The MAC/IP/Port filtering allows you to apply a policy to the traffic that passes through the router, both inbound and outbound, so that network access can be controlled. When the filter is enabled with a default rule of "Accepted", all connections will be allowed except those listed in the "Current MAC / IP / Port filtering rules in effect" list. Conversely, when the default rule is set to "Dropped", all connections are denied except for those listed in the filtering rules list.

Figure 8-45 Firewall Filtering



Important: *When enabling MAC / IP / Port filtering and setting the default rule to "Dropped", you should ensure that you have first added a filtering rule which allows at least one known MAC/IP to access the router, otherwise you will not be able to access the user interface of the router without resetting the router to factory default settings.*

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

1. Set the **MAC / IP / Port** filtering toggle key to ON position.
2. Use the **Default rule (inbound/forward)** drop-down list to select the default action for the router to take when traffic reaches it. By default, this is configured to Accepted. If you change this to Dropped, you should first configure a filter rule that allows at least one device access to the router, otherwise you will effectively be locked out of the router.
3. Click the **Save** button to confirm the default rule.
4. In the Current MAC / IP / Port Filtering Rules In Effect section, click the **+Add** button. The Filter Settings display.

Figure 8-46 MAC/IP/Port Filter Settings

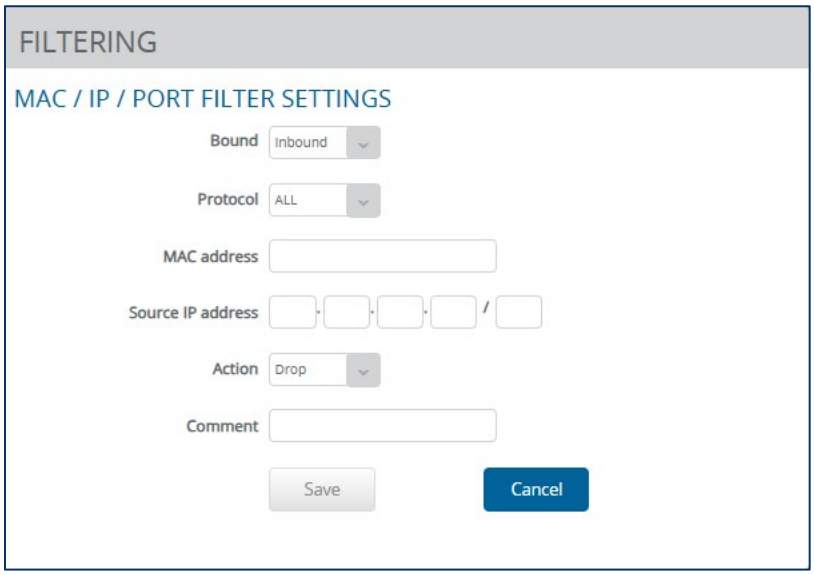


Table 8-8 MAC/IP/Port Filter Settings Configuration Details

Item	Description
Bound	Select the direction of traffic. The options available are: • **Inbound** • **Outbound** • **Forward**
Protocol	Select the protocol of the traffic. The options available are: • **All** • **UDP/TCP** • **UDP** • **TCP**

Item	Description
	• **ICMP**
MAC Address	Enter MAC Address of the source device.
Source IP address	Enter IP address of the source device.
Action	Select the action to be taken. The options available are: • **Drop** • **Accept**
Comment	Add comments for the rule

Enter, select the required values for all the fields and click **Save**.

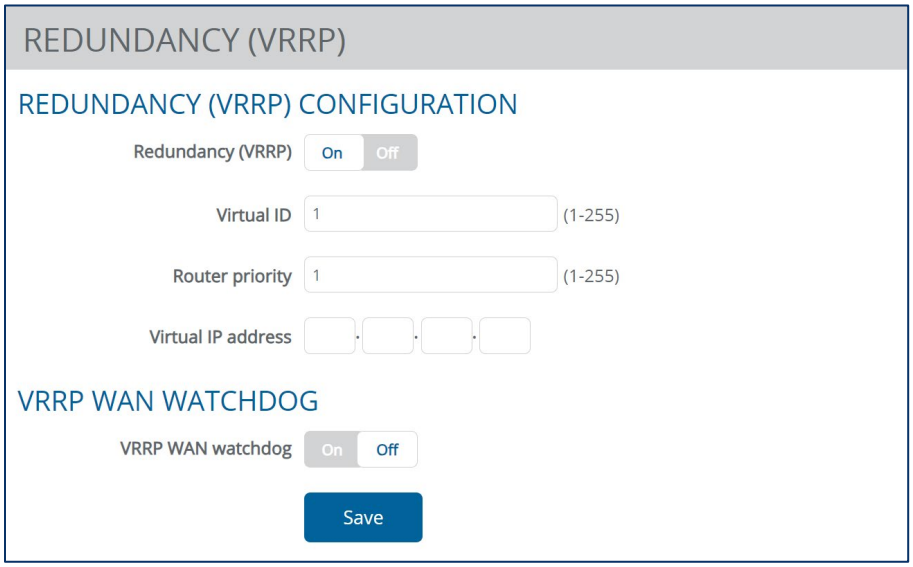
5. The new rule is displayed in the filtering rules list. To edit the rule click the Edit button and to delete the rule click the button.

Redundancy (VRRP)

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a "virtual router" (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, an arrangement is made for another physical router to automatically replace it. The physical router that is currently forwarding data on behalf of the virtual router is called the master router. Routers are given a priority of between 1 and 255 and the router with the highest priority is assigned as the master.

A virtual router must use 00-00-5E-00-01-XX as its (MAC) address. The last byte of the address (XX) is the Virtual Router Identifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time and is the only way that other physical routers can identify the master router within a virtual router.

Figure 8-47 Redundancy



Configuring VRRP

To configure VRRP, configure multiple devices as follows and connect them together via an Ethernet network switch to downstream devices.

1. Set the **Redundancy (VRRP)** toggle to **On** to enable VRRP.
2. In the **Virtual ID** field, enter an ID between 1 and 255. This is the VRRP ID which is different for each virtual router on the network.
3. In the **Router priority** field, enter a value for the priority – a higher value is a higher priority.
4. The **Virtual IP address** field is used to specify the VRRP IP address – this is the virtual IP address that both virtual routers share.
5. Click **Save** button to apply the new settings.

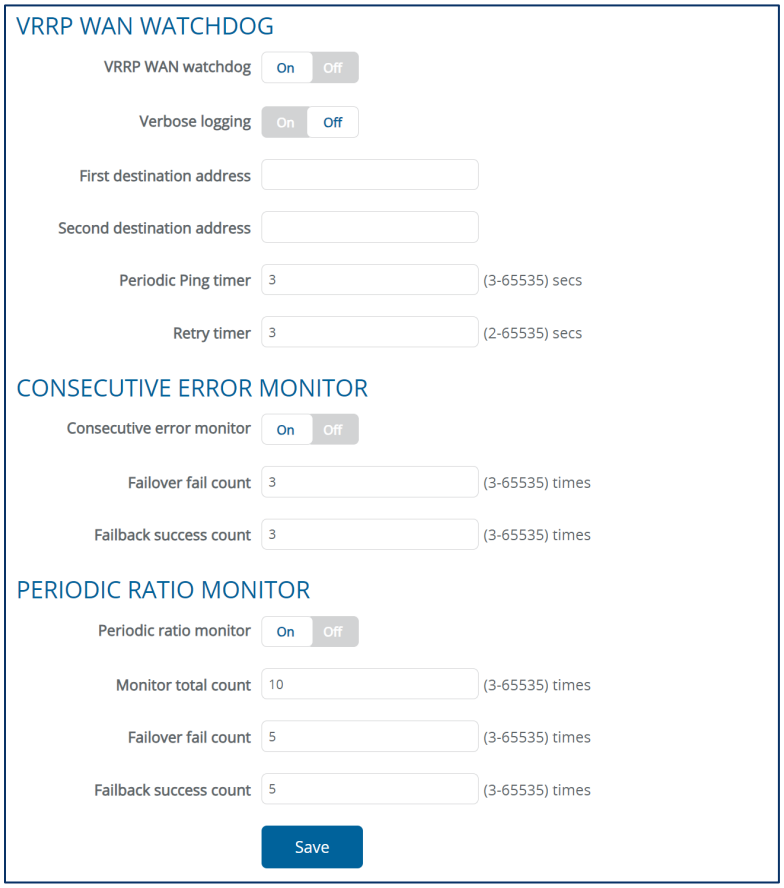
Note: *Configuring VRRP changes the MAC address of the Ethernet port which may interrupt the connection to the router. If you want to resume with the web configuration you must use the new IP address (VRRP IP) or clear the arp cache (old MAC address). On Windows, run the following command in command prompt:*

```
arp -d <ip address> (i.e. arp -d 192.168.1.1)
```

Configuring the VRRP WAN watchdog

The VRRP WAN watchdog is disabled by default. When it is enabled, VRRP monitors the status of the primary and secondary by the physical link. When enabled, the VRRP WAN watchdog feature monitors the status of the connection by both the physical link and controlled ping packets.

Figure 8-48 Redundancy – VRRP WAN Watchdog



The following table details each field on the VRRP WAN Watchdog page.

Table 8-9 VRRP WAN Configuration Items

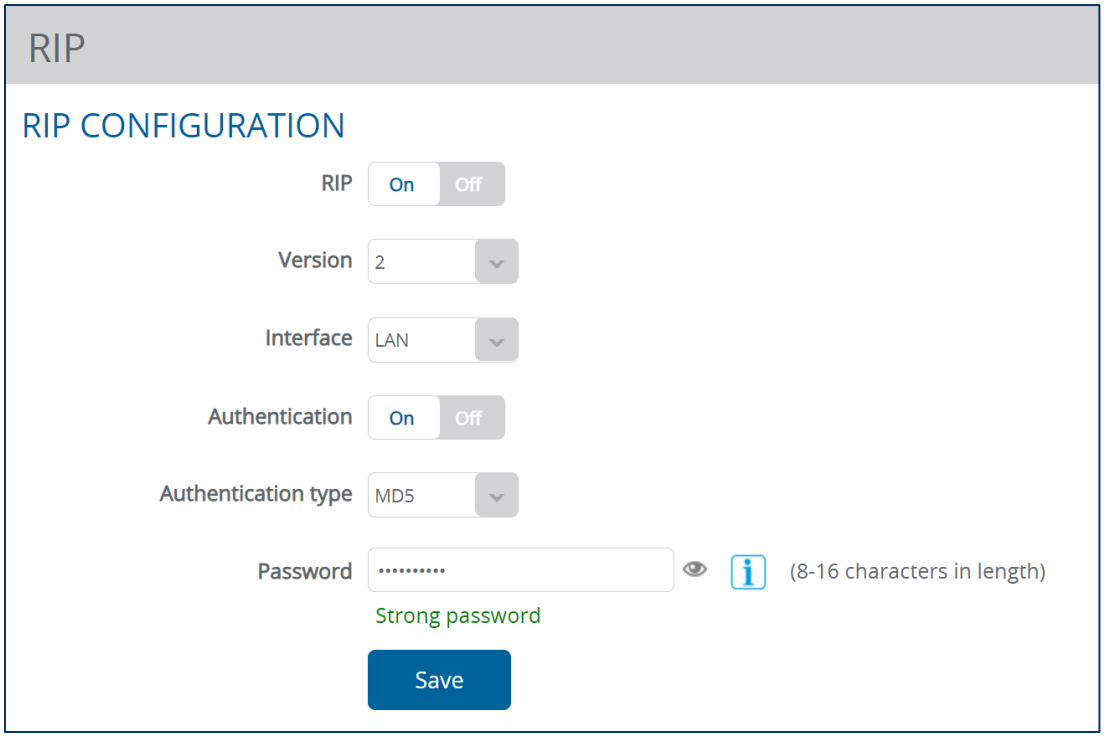
Parameter	Description
VRRP WAN Watchdog	Set to **On** to enable the watchdog.
Verbose logging	When enabled verbose comments are logged in the system log related to the failover monitoring.
First destination address	The first address the router that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Second destination address	The second address the router that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	The time in seconds between ping attempts.
Retry timer	The time in seconds between attempts when a ping failure occurs.
Consecutive error monitor	
Consecutive Error Monitor	Set to **On** to enable the consecutive error monitor. Using this method, the router will determine the availability of an interface based on a set number of consecutive ping instance responses.
Failover fail count	The number of failed pings that must occur before the monitor fails the connection over to the next interface.
Failback success count	The number of successful pings that must occur before the monitor fails the connection back to the higher priority interface.
Periodic ratio monitor	
Periodic ratio monitor	Set to **On** to enable the Periodic ratio monitor. Using this method, the router will determine the availability of an interface based on a set ratio of ping instance successes or failures to the number of attempts.
Monitor total count	This field specifies a series of pings to consider when calculating whether to fail over or fail back. When the series is completed, the router repeats the ping test and resets the Failover fail count/Failback success count. Therefore, for the failover or failback ratio to be met, the number of Failover fail counts/Failback success counts must occur within a particular Series.
Failover fail count	This field specifies the number of failed ping results that must occur within a series of pings configured in the Monitor total count before the router fails over to the next highest priority interface. For example, at the default setting of 5, the router fails over to the next interface when 5 out of 10 ping attempts in a particular Series have failed. The failures need not be consecutive to meet the failover criteria. If any 5 of the 10 pings in a Series have failed, the router deems the interface connection to be down and fails over.

Parameter	Description
Failback success count	Like the Failover fail count field, this field specifies the number of ping successes that must be registered on a higher priority interface within a Series of pings configured in the Monitor total count before the router fails back to that interface.

RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. By enabling RIP all the routes in the router's routing table will be advertised to other nearby routers. For example, the route for the router's Ethernet subnet could be advertised to a router on the PPP interface side so that a router on this network will know how to route to a device on the router's Ethernet subnet. Static routes must be added manually according to your requirements. See Adding Static Routes for more information.

Figure 8-49 RIP configuration



Note: *Other routers may ignore RIP.*

To enable Routing Information Protocol (RIP)

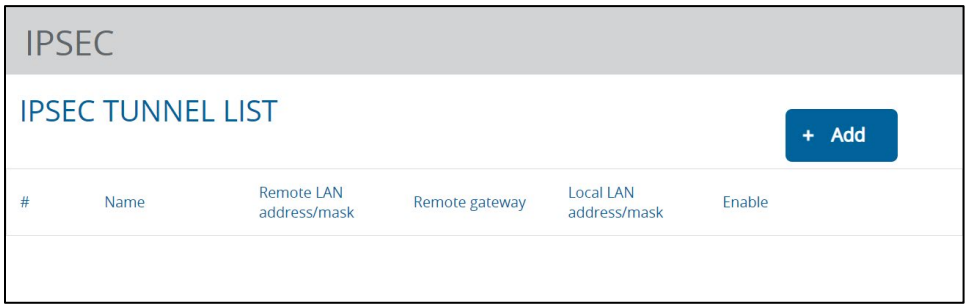
1. Set the **RIP** toggle to **On** to enable RIP.
2. Using the **Version** drop-down list, select the version of RIP to use.
3. Select the **Interface** that RIP should apply on. Options are **LAN**, **WWAN** or **Both**.
4. If you want to turn on authentication, toggle the **Authentication** toggle key to the **ON** position. Use the Authentication type drop-down list to select the method of authentication then enter password in the Password field.
5. Click **Save** button to save your settings.

VPN

IPSec

IPSec operates on Layer 3 of the OSI model and can protect higher layered protocols. IPSec is used for both Site-to-Site VPN and Remote Access VPN. The NTC-550 Series router supports IPsec end points and can be configured with Site-to-Site VPN tunnels for third party VPN routers.

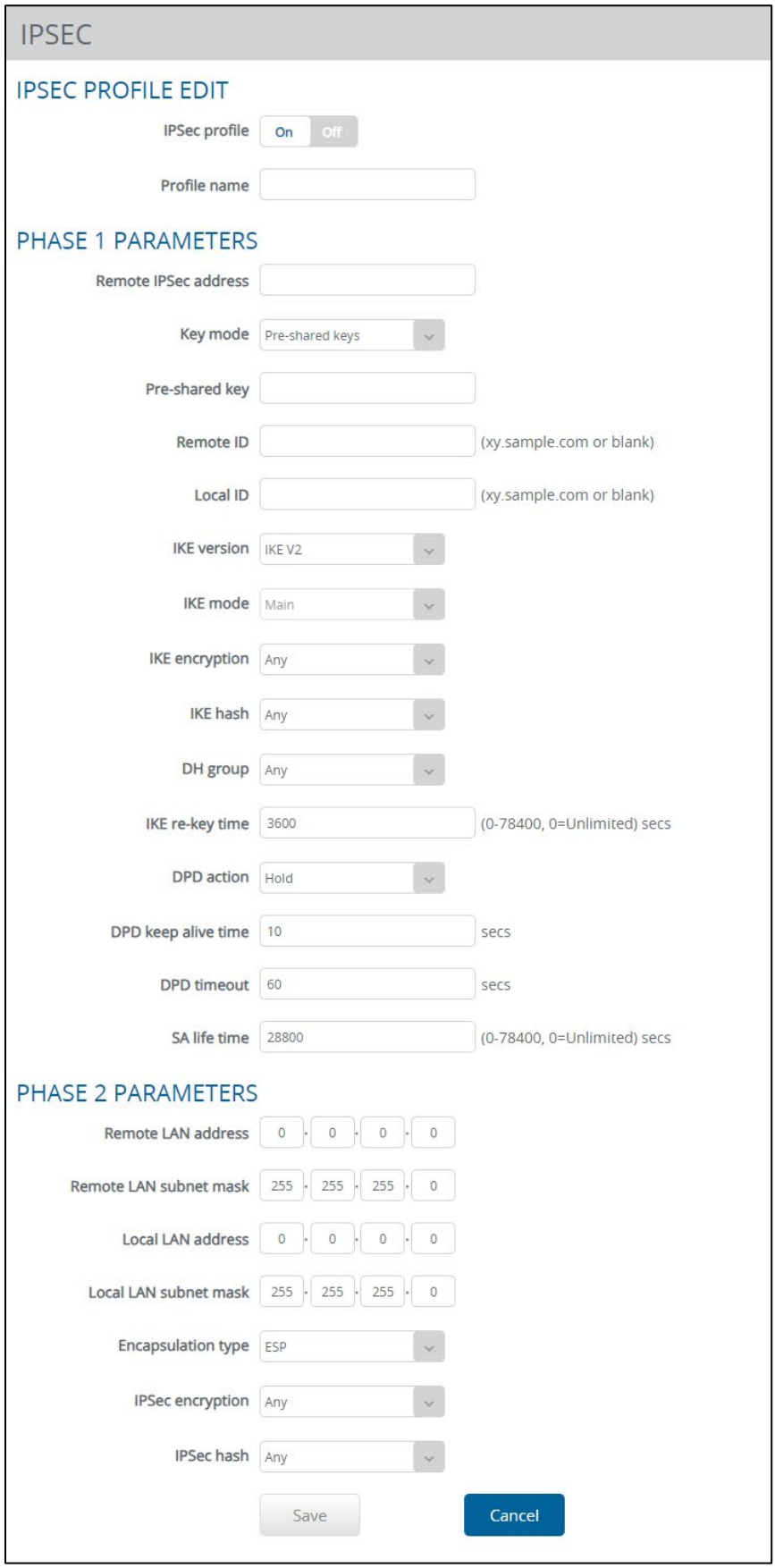
Figure 8-50 VPN – IPSec



Configuring an IPSec VPN

From the menu at the top of the screen, click **Networking** and under the VPN section, click **IPSec**. A list of configured IPSec VPN connections is displayed. Click the **+Add** button to begin configuring an IPSec VPN connection.

Figure 8-51 VPN – IPSec Profile Edit



The following table describes each of the fields of the IPSec VPN configuration page.

Table 8-10 IPSec configuration items

Parameter	Description
IPSec profile	Enables or disables the VPN profile.
Profile name	A name used to identify the VPN connection profile.
Phase 1 parameters	
Remote IPSec address	The IP address or domain name of the IPSec server.
Key mode	Select the type of key mode in use for the VPN connection. You can select from: • **Pre-Shared Keys** • **RSA keys** • **Certificates** • **SCEP client**
Pre-shared key	The pre-shared key is the key that peers use to authenticate each other for Internet Key Exchange. The pre-shared key must meet the requirements for a strong password. See the Configuring a strong password section. This field appears if Pre-shared keys is used as the key mode.
Remote ID	Remote ID of the connection. Refer to the documentation of the remote IPSec server for further details. This field may be left blank.
Local ID	Local ID of the connection. Refer to the documentation of the remote IPSec server for further details. This field may be left blank.
Local RSA key upload	Upload the Local RSA key if RSA Keys is used as the Key mode.
Remote RSA key upload	Upload the Remote RSA key if RSA Keys is used as the Key mode.
Private key passphrase	The Private key passphrase is required if Certificates is used as the Key mode.
Key / Certificate	Select the Key / Certificate type for the IPSec connection if Certificates is used as the Key mode.
IPSec certificate upload	Upload the IPSec certificate if Certificates is used as the Key mode.
SCEP remote id	Enter the SCEP remote ID if SCEP client is used as the Key mode.
IKE version	Set the IKE version for the connection. There are two options available **IKE V1** and **IKE V2.**
IKE mode	Set the IKE mode for the connection. There are three options **Any, Main** and **Aggressive.**
IKE encryption	Select the cipher type to use for the Internet Key Exchange.
IKE hash	Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.

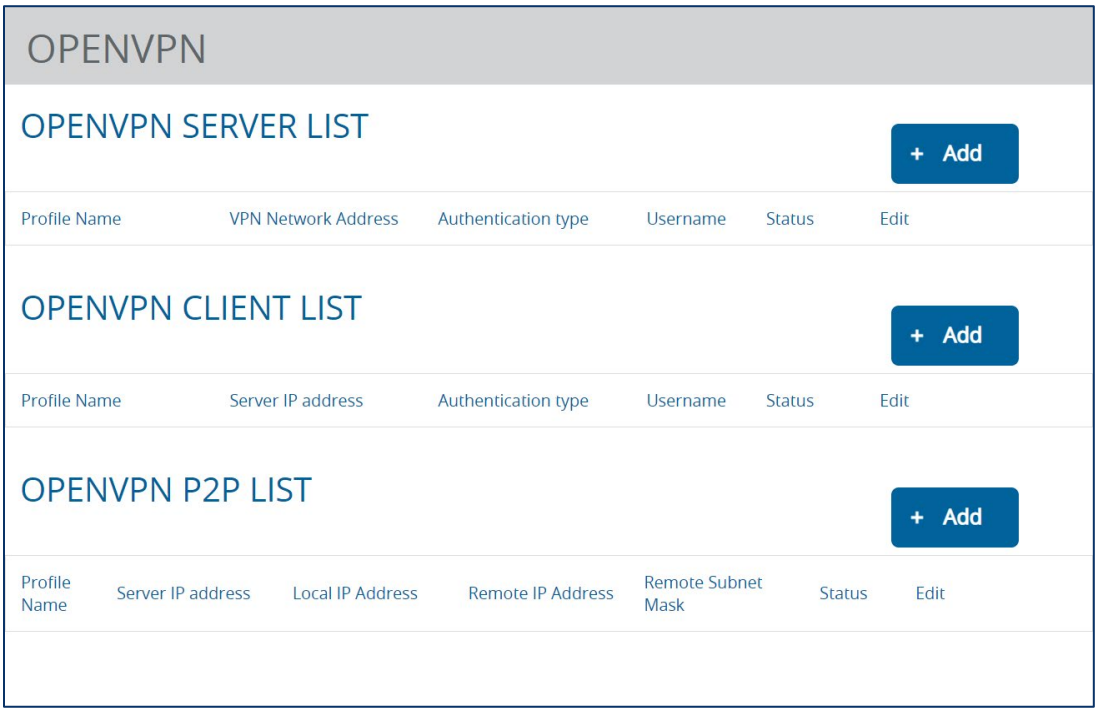
Parameter	Description
DH group	Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.
IKE re-key time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.
DPD action	Select the required Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.
DPD keep alive time	Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.
DPD timeout	Enter the time in seconds of no response from a peer before Dead Peer Detection times out.
SA life time	Enter the time in seconds for the security association lifetime.
Phase 2 parameters	
Remote LAN address	Enter the IP address of the remote network for use on the VPN connection.
Remote LAN subnet mask	Enter the subnet mask in use on the remote network.
Local LAN address	Enter the IP address of the local network for use on the VPN connection.
Local LAN subnet mask	Enter the subnet mask in use on the local network.
Encapsulation type	Select the encapsulation protocol to use with the VPN connection. You can choose **ESP**, **AH** or **Any**.
IPSec encryption	Select the IPSec encryption type to use with the VPN connection.
IPSec hash	Select the IPSec hash type to use for the VPN connection. The hash is used for authentication of packets for the VPN connection.

OpenVPN

OpenVPN is an open-source virtual private network (VPN) program for creating point-to-point or server-to-multi-client encrypted tunnels between host computers. It can traverse network address translation (NAT) and firewalls and allows authentication by certificate, pre-shared key or username and password. OpenVPN works well through proxy servers and can run over TCP and UDP transports. Support for OpenVPN is available on most operating systems, including Windows, Linux, macOS, Solaris, OpenBSD, FreeBSD, NetBSD and QNX.

From the menu at the top of the screen, select **Networking**, then from the VPN section on the left, select **OpenVPN**. A list of configured OpenVPN VPN connections is displayed.

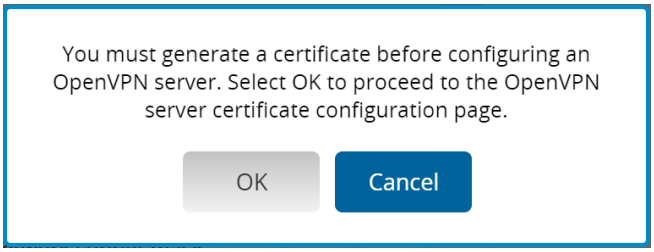
Figure 8-52 VPN - OpenVPN



Configuring an OpenVPN Server

To add an OpenVPN server, select the **+Add** button to the right of the OpenVPN Server List heading. Each time the **+Add** button is selected, the router checks if there are existing server certificates. If no server certificate is found, you are prompted to generate a certificate before configuring the OpenVPN server.

Figure 8-53 VPN – OpenVPN – Generate server certificate prompt



Select the **OK** button, the Server Certificate page displays. For more information on generating server certificates, refer to the Server Certificate section of this guide. When you have created the certificate, return to the OpenVPN server configuration page to continue the setup.

To configure an OpenVPN server:

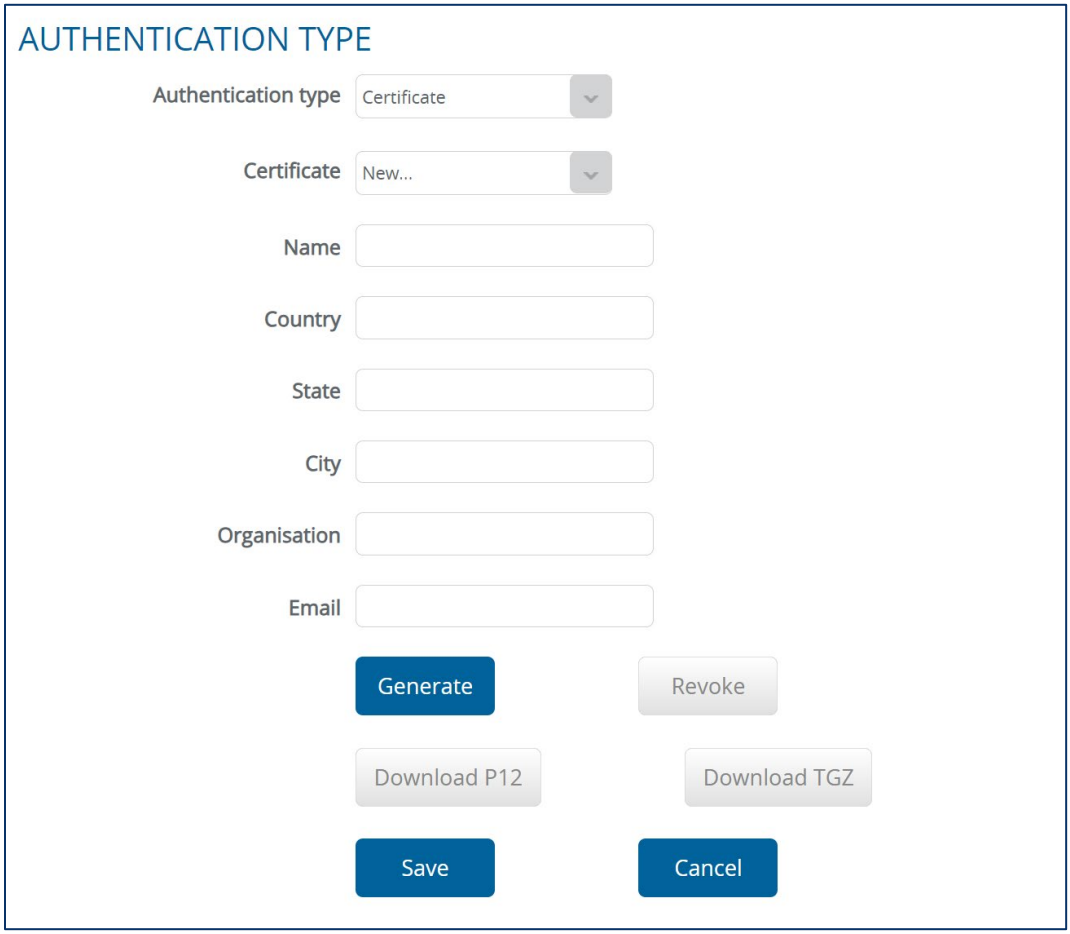
1. Set the **OpenVPN profile** toggle key to **ON** position.
2. In the **Profile name** field, enter a name for the OpenVPN server profile you are creating.
3. In the **Type** filed, select the OpenVPN connection type (**TUN**/**TAP**). Default is **TUN**.
4. In the **Port type** field, select a packet type to use for your OpenVPN Server and in the **Server port** field, enter a port number. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **Encryption cipher** field, select the encryption type for the connection. The default is **AES-256** as this is the strongest encryption level.
6. Enter a maximum transmission unit value into the **MTU** field. The default is 1500.

7. In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
8. The Server certificates section displays the details of the certificate. If you wish to change the certificate, click the **Change** button.
9. HMAC or Hash-based Message Authentication Code is a means for calculating a message authentication code using a cryptographic hash function and a cryptographic key. If you wish to use the HMAC signature as an additional key and level of security, under the SSL/TLS handshake section, set the **Use HMAC Signature** toggle key to **On** position, then click the **Generate** button so that the router can randomly generate the key. The **Server key timestamp** field is updated with the time that the key was generated. Click the **Download** button to download the key file so that it can be uploaded on the client.
10. Select an **Authentication type**. Authentication may be done using a Certificate or Username / Password. See the below sections for information on each of the certificate types.

Certificate authentication

In the Authentication Type section select **Authentication type** as **Certificate**. Enter the required details to create a client certificate. All fields are required. After filling out the required fields, click **Generate** button.

Figure 8-54 VPN – OpenVPN – Certificate Authentication type



Once the certificate is generated, click **Download P12 button** or**Download TGZ button** to save the certificate file, depending on which format you would like. If for some reason the integrity of your network has been

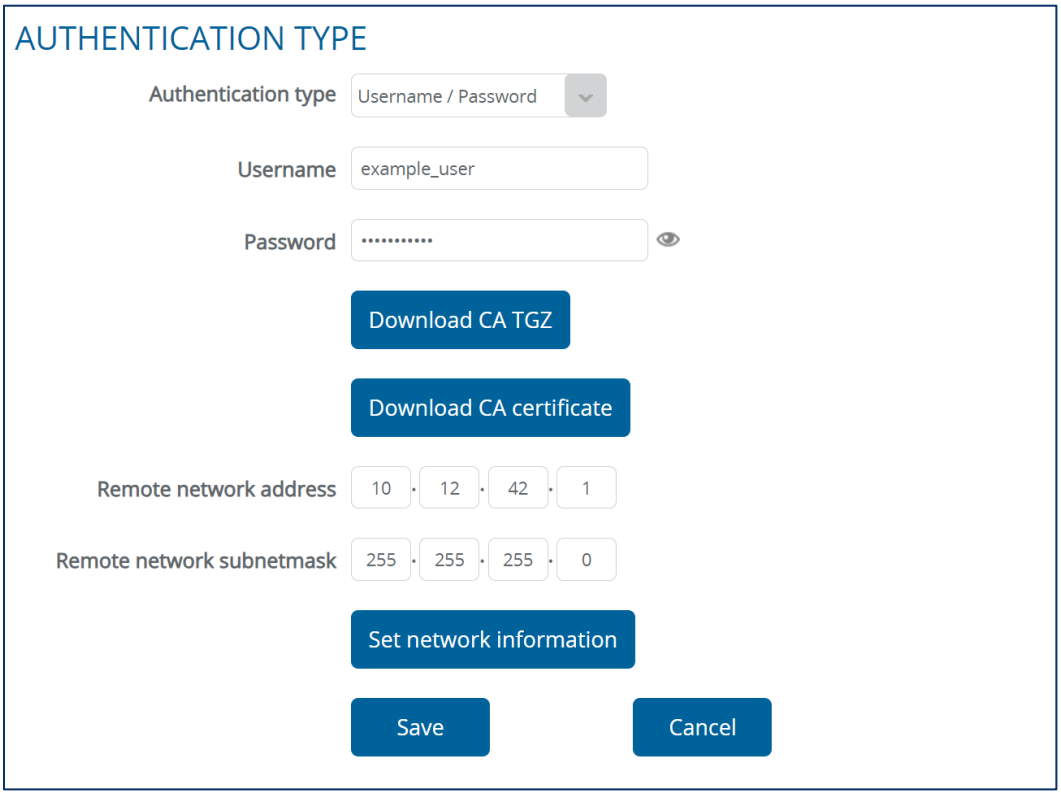
compromised, return to this screen, use the Certificate drop-down list to select the certificate and then select the Revoke button to make the certificate invalid.

Username / Password Authentication

In the Username/Password section, enter the username and password you would like to use for authentication on the OpenVPN Server. Click t**he Download CA certificate** or **Download CA TGZ** depending on file format to save the ca.crt file. This file will need to be provided to the client.

Note: *If you wish to have more than one client connect to this OpenVPN server, you must use Certificate authentication mode as Username/Password only allows for a single client connection.*

Figure 8-55 VPN – OpenVPN – Username / Password Authentication type



Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the network address and network subnet mask in the respective fields and click the **Set Network Information** button. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client's subnet.

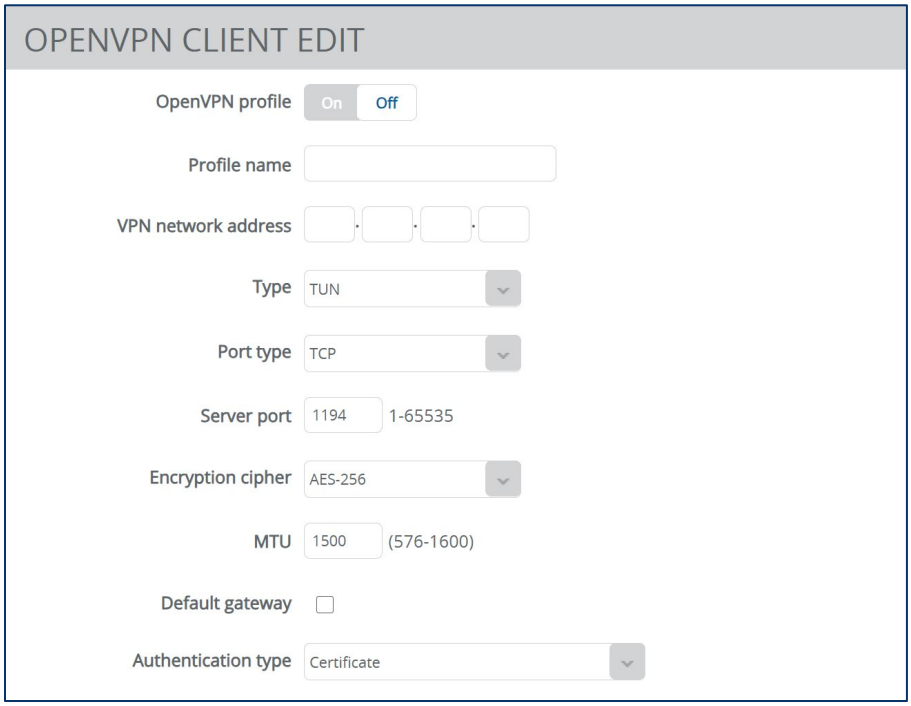
When you have finished entering all the required information, click **Save** to save the settings and finish configuring the OpenVPN server.

Configuring an OpenVPN client

To configure and Open VPN client:

1. In the OpenVPN page click the **+Add** button in the **OpenVPN Client List** section**.** The OpenVPN Client Edit page displays

Figure 8-56 VPN – OpenVPN – Configure OpenVPN client



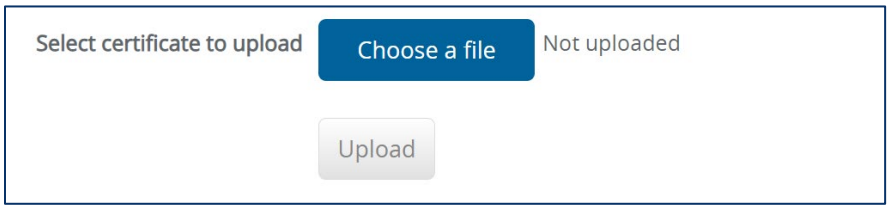
2. Set the **OpenVPN profile** toggle key to the **On** position.
3. In the **Profile name** field, enter a name for the OpenVPN client profile you are creating.
4. In the **VPN network address** field, enter the WAN IP address / host domain name of the OpenVPN server.
5. Select **Type** (**TUN/TAP**). Default is **TUN**.
6. In the **Server port** field enter a port number and for **Encryption cipher** select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
7. Enter a maximum transmission unit value in the **MTU** field
8. If the **Default gateway** option is applied on the OpenVPN client page, the OpenVPN server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between this router and the remote OpenVPN server only.
9. Select the **Authentication type** to use for the OpenVPN client. The available options are **Certificate, Username and Password,** or **Combination Certificate and Username / Password.** See the below sections to understand the different authentication types.

Certificate Authentication

To use Certificate Authentication:

1. Set the **Authentication Type** field to **Certificate**.
2. Scroll down to the **Select certificate to upload** field and click **Choose a file** button.

Figure 8-57 OpenVPN – Certificate upload



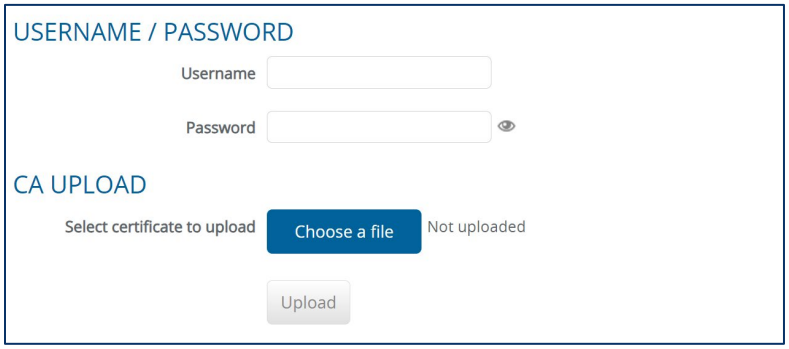
3. Locate the certificate on your computer, click **Open,** then click **Upload**.
4. Once the certificate is uploaded, click the **Save** button to confirm the connection.

Username / Password Authentication

To use Username / Password Authentication:

1. Set the **Authentication Type** field to **Username / Password**.

Figure 8-58 OpenVPN – Username / Password Authentication



2. In the **Username** field, enter the username of the OpenVPN server.
3. In the **Password** field, enter the password of the OpenVPN server.
4. Click **Choose a file** button to locate the CA certificate file you saved from the OpenVPN Server and then click the **Upload** button.
5. If you have an additional SSL/TLS key created on the server, set the **Use HMAC Signature** toggle key to **ON** position. Click **Choose a file** button then locate the key file on your computer. Click the **Upload** button to upload it to the router.
6. Click **Save** button to confirm the connection.

Certificate and Username / Password authentication

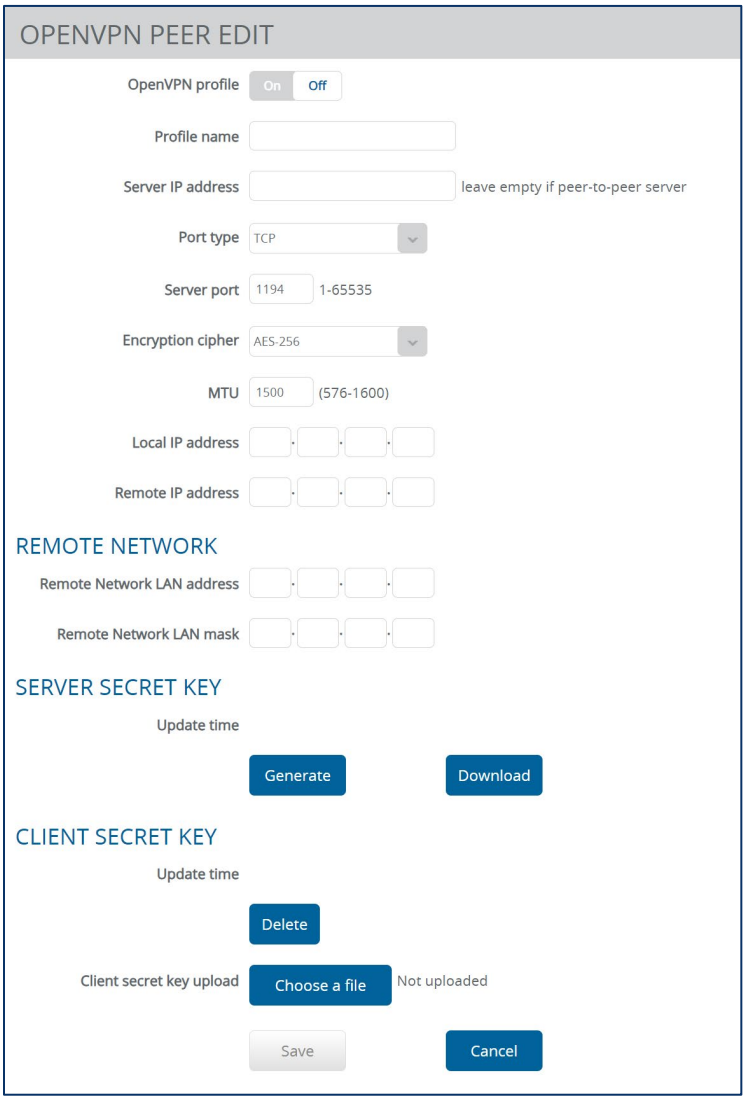
The Certificate and Username / Password Authentication option is a combination of both the Certificate and Username / Password authentication methods. This provides additional levels of security since the client must know the username / password combination and be in possession of the certificate. Set the **Authentication type** to **Certificate and Username / Password Authentication**, then follow the instructions in both the above sections to complete the configuration.

Configuring an OpenVPN P2P Connection

The OpenVPN P2P connection allows you to create a Peer-to-peer VPN connection with another router. One router should be the primary router, and the other router should be a secondary router.

1. In the OpenVPN page click the **+Add** button in the OpenVPN P2P List section . The OpenVPN Peer Edit page displays.

Figure 8-59 OpenVPN – P2P Peer Edit Page



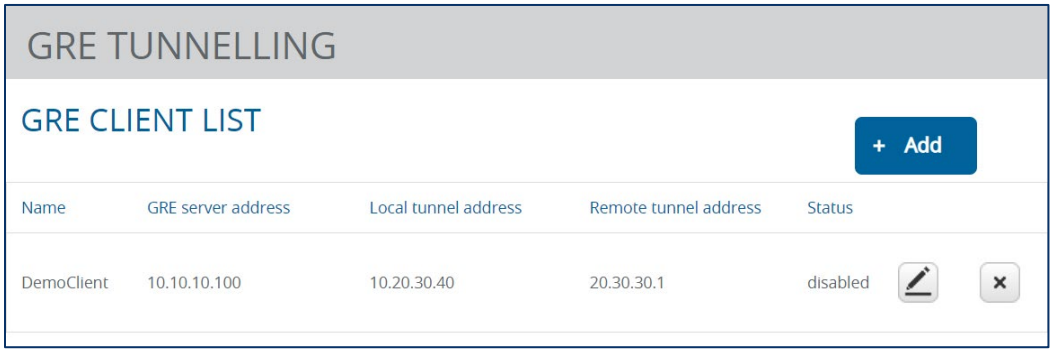
2. Set the **OpenVPN profile** toggle key to **ON** position.
3. In the **Profile** name field, enter a name for the OpenVPN P2P profile you are creating.
4. In the router designated as the server, leave the **Server IP address** field empty. In the router designated as the client, enter the WAN IP address/host domain name of the server.
5. In **Port type** and **Server port** fields enter port number and select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
6. In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The secondary router should have the reverse settings of the primary router.

7. In the **Remote network** section, in the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The secondary router should have the reverse settings of the primary router.
8. Click **Generate** button to create a secret key to be shared with the other router. When the timestamp displays, you can click the **Download** button to save the file to exchange with the other router.
9. When you have saved the secret key file on each router, click the **Choose a file button** to locate the secret key file for the master and then click the **Upload** button to send it to the secondary router. Perform the same for the other router, uploading the secondary secret key file to the primary router.
10. Click **Save** button to confirm the Peer-to-peer VPN connection.

GRE Tunnelling

The Generic Route Encapsulation (GRE) protocol creates a point-to-point connection similar to a VPN between clients and servers or between clients only. GRE is used to encapsulate the data or payload.

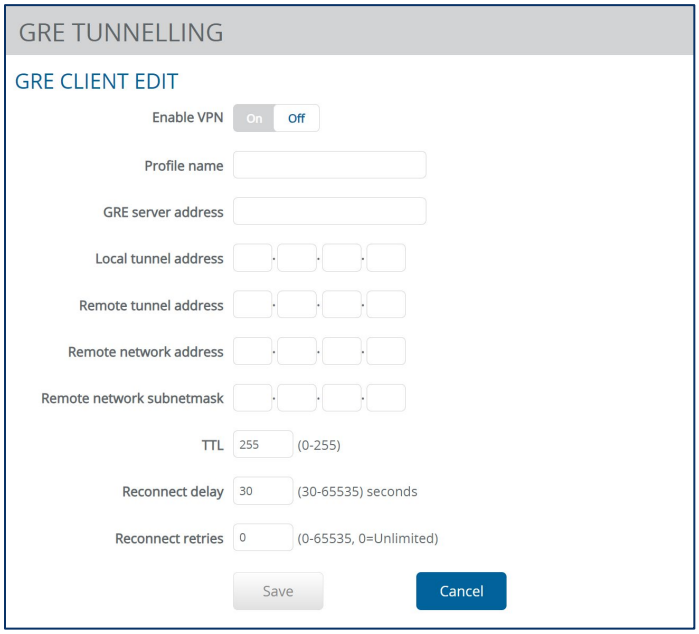
Figure 8-60 VPN – GRE Tunnelling



To configure GRE tunnelling:

1. In the GRE client list section, click the **+Add** button. The **GRE Client Edit** screen displays.

Figure 8-61 VPN – GRE Tunnelling – GRE Client Edit



2. Set the **Enable VPN** toggle to **On**.
3. In the **Profile name** field, enter a profile name for the tunnel. This name is used to identify the tunnel on the router.
4. In the **GRE server address** field, enter the IP address or domain name of the GRE server.
5. In the **Local tunnel address** field, enter the IP address you want to assign the tunnel locally.
6. In the **Remote tunnel address** field, enter the IP address you want to assign to the remote tunnel.
7. In the **Remote network address** field, enter the IP address scheme of the remote network.
8. In the **Remote network subnetmask** field, enter the subnet mask of the remote network.
9. The **TTL** (Time To Live) field is an 8-bit field used to remove an undeliverable data packet from a network to avoid unnecessary network traffic across the internet. The default value of 255 is the upper limit on the time that an IP datagram can exist. The value is reduced by at least one for each hop the data packet takes to the next router on route the datagram's destination. If the TTL field reaches zero before the datagram arrives at its destination the data packet is discarded and an error message is sent back to the sender.
10. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the GRE server if the connection is broken. The minimum time to wait is 30 seconds so as to not flood the GRE server with connection requests, while the maximum time to wait is 65335 seconds.
11. The **Reconnect retries** is the number of connection attempts that the router will make if the GRE connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.
12. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Select the Status button at the top left of the interface to return to the status window and monitor the VPN's connection state.

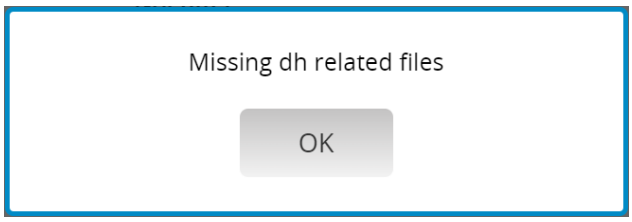
Server Certificate

The Server Certificate page is used to generate a certificate for use with OpenVPN.

Generating Diffie-Helman files

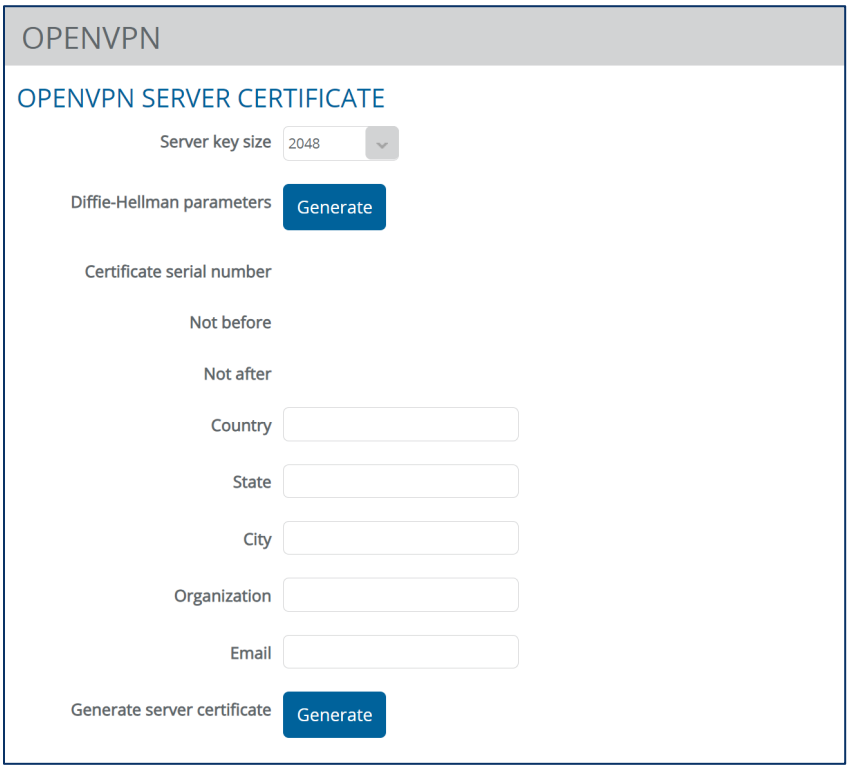
On first use of the certificate page, you will see the following prompt, where **dh** refers to **Diffie-Hellman.**

Figure 8-62 VPN – Server Certificate – Missing dh related files



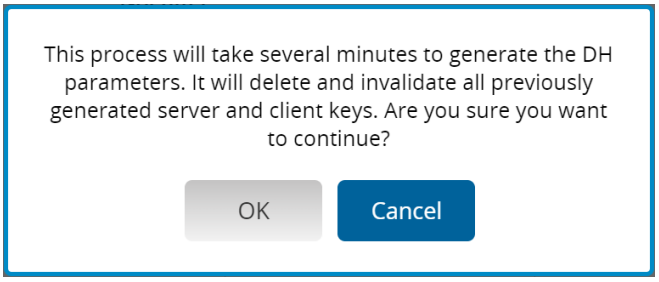
To proceed with generating the certificate, the Diffie-Hellman parameters must first be generated. Click **OK** on the prompt to close it. The OpenVPN Server Certificate page is shown.

Figure 8-63 VPN – Server Certificate – Missing dh related files



Click **Generate** for the **Diffie-Hellman parameters filed.** The following prompt displays.

Figure 8-64 VPN – Server Certificate – Generate Diffie-Hellman prompt



Selecting the **OK** button will delete and invalidate all previous server and client keys, if they exist, and generates new parameters. This process will take up to five minutes to complete. Once the files are generated, the Success prompt is shown.

Figure 8-65 VPN – Server Certificate – Missing dh related files

The Server Certificate can now be generated.

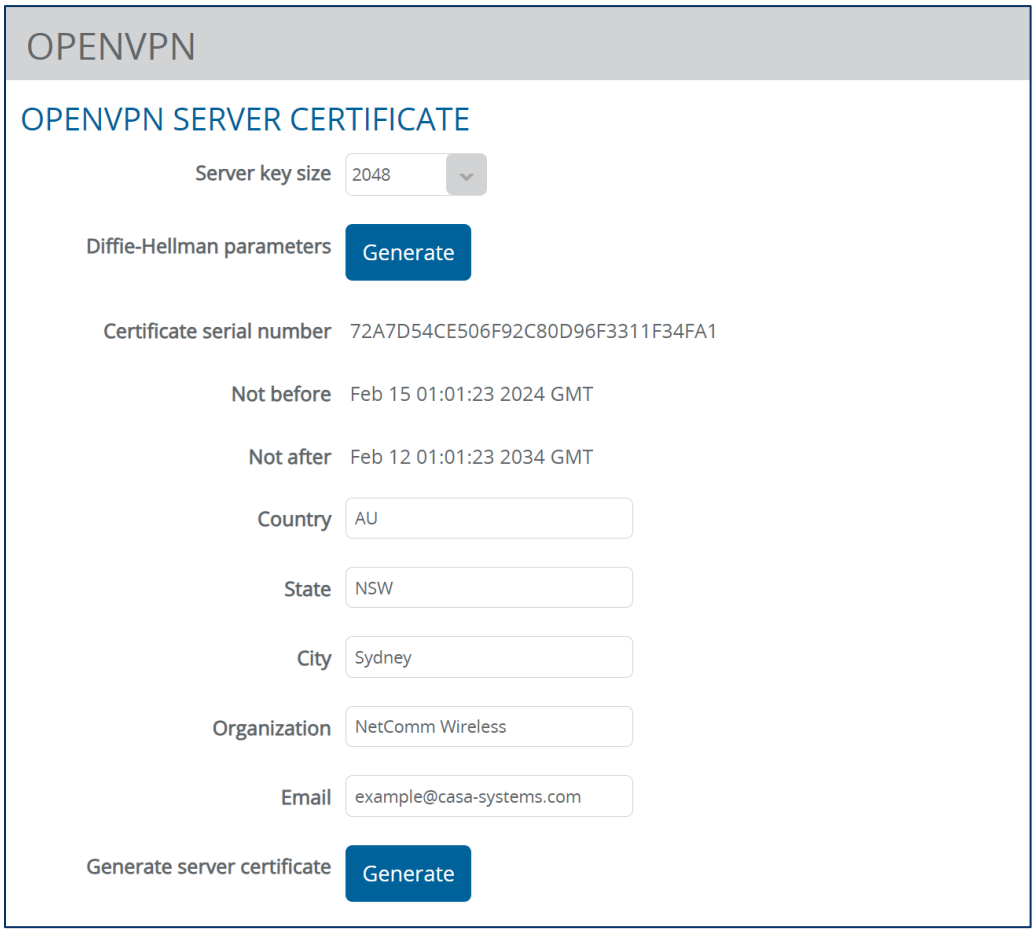
Generating the OpenVPN Server Certificate

To generate an OpenVPN Server Certificate:

1. In the **Country** field, enter the SSL Country code for the country the certificate is issued for.
2. In the **State** field, enter the state the certificate is issued for.

3. In the **City** field, enter the city the certificate is issued for.
4. In the **Organization** field, enter the name of the organization for the certificate.
5. In the **Email** field, enter a contact email for the certificate.
6. For the **Generate Server Certificate** filed click **Generate** to generate the certificate. A success prompt is shown, and the certificate serial number and validity dates are shown in **Certificate serial number**, **Not before** and **Not after fields**.

Figure 8-66 VPN – Server Certificate – Generate certificate



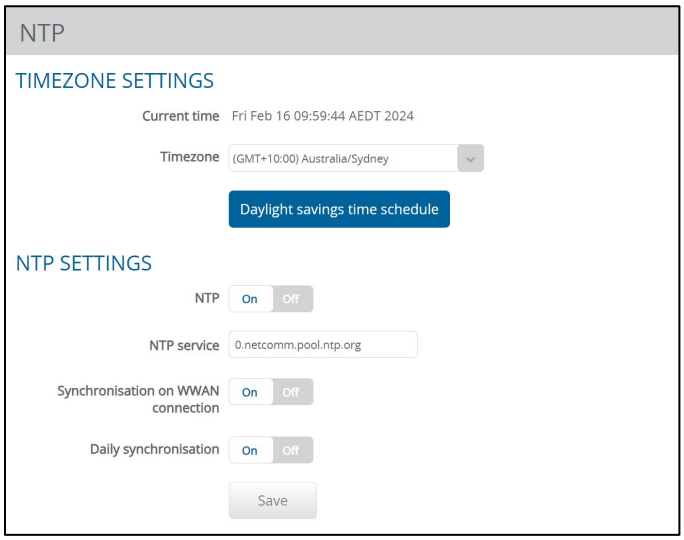
9. Services

Network time (NTP)

The NTP Network (NTP) page allows you to configure the NTC-550 Series router to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded. Any Network Time Protocol (NTP) server available publicly on the internet may be used.

To access the Network time (NTP) page, click the **Services** tab at the top of the screen then click **Network time (NTP)** tab on the left.

Figure 9-1 NTP



Timezone Settings

The **Current time** field shows the time and date configured on the router. If this is not accurate, use the Timezone drop-down list to select the correct time zone for the router.

If the selected zone observes daylight savings time, a **Daylight savings time schedule** button displays below the drop-down list. Click **Daylight savings time schedule**, a window displays the start and end times for daylight savings. Click **OK** and click **Save** to save the settings.

Configuring NTP settings

To configure NTP settings:

1. Set the **Network time (NTP) toggle** key to switch it to the **On** position.
2. In the **NTP service** field, enter the address of the NTP server you want to use.
3. Set the **Synchronization on WWAN connection** toggle key to **On** or **Off** ad require. It enables or disables the router to perform time synchronization, each time a mobile broadband connection is established.
4. Set the **Daily synchronization** toggle key to **On** or **Off** as required. It enables or disables the router to perform time synchronization each day.
5. Click **Save** to save the settings.

SMS messaging

The NTC-550 Series router offers an advanced SMS feature set, including sending messages, receiving messages, redirecting incoming messages to another destination, and supporting remote commands and diagnostics messages.

Some of the functions supported are:

- Ability to send a text message via a cellular network and store it in permanent storage.
- Ability to receive a text message via a cellular network and store it in permanent storage.
- Ability to forward incoming text messages via a cellular network to another remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to receive run-time variables from the device (e.g. uptime) on request via SMS.
- Ability to change live configuration on the device (e.g. network username) via SMS.
- Ability to execute supported commands (e.g. reboot) via SMS.
- Ability to trigger the NTC-550 Series router to download and install a firmware upgrade.
- Ability to trigger the NTC-550 Series router to download and apply a configuration file.

To access the SMS messaging functions of the NTC-550 Series router, click the **Services** tab on the top menu bar, and then click an option under the **SMS messaging** section.

Setup

The **SMS Setup** page allows you to perform SMS and SMS forwarding configurations of the router. SMS messaging is enabled by default.

Figure 9-2 SMS - SMS setup configuration

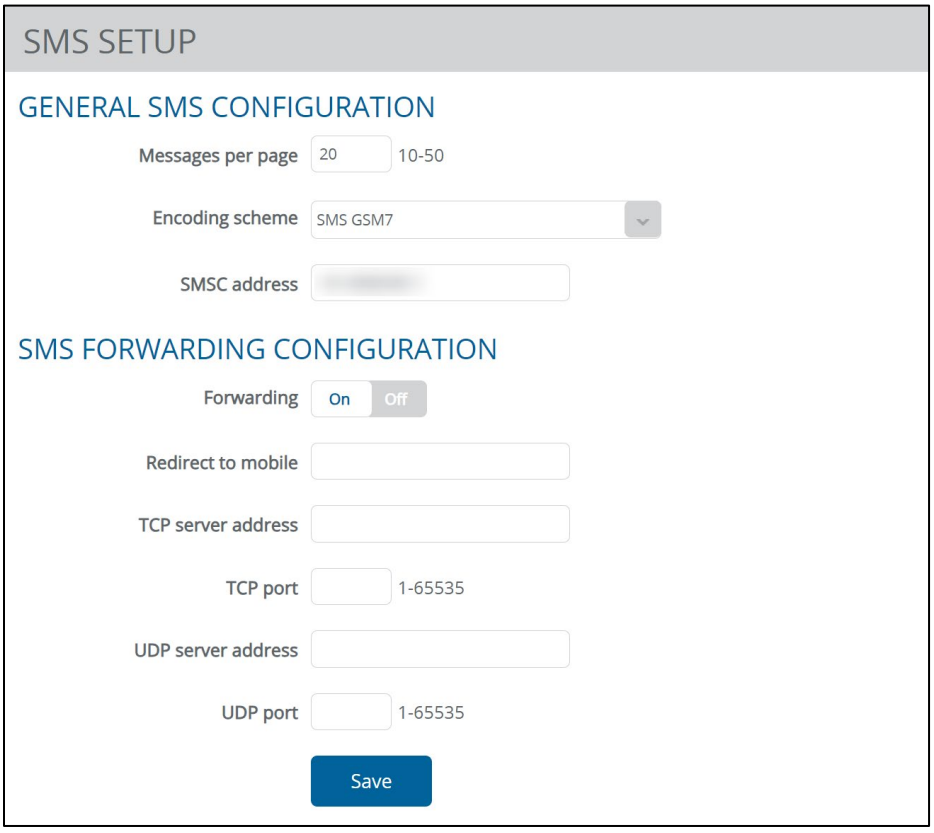


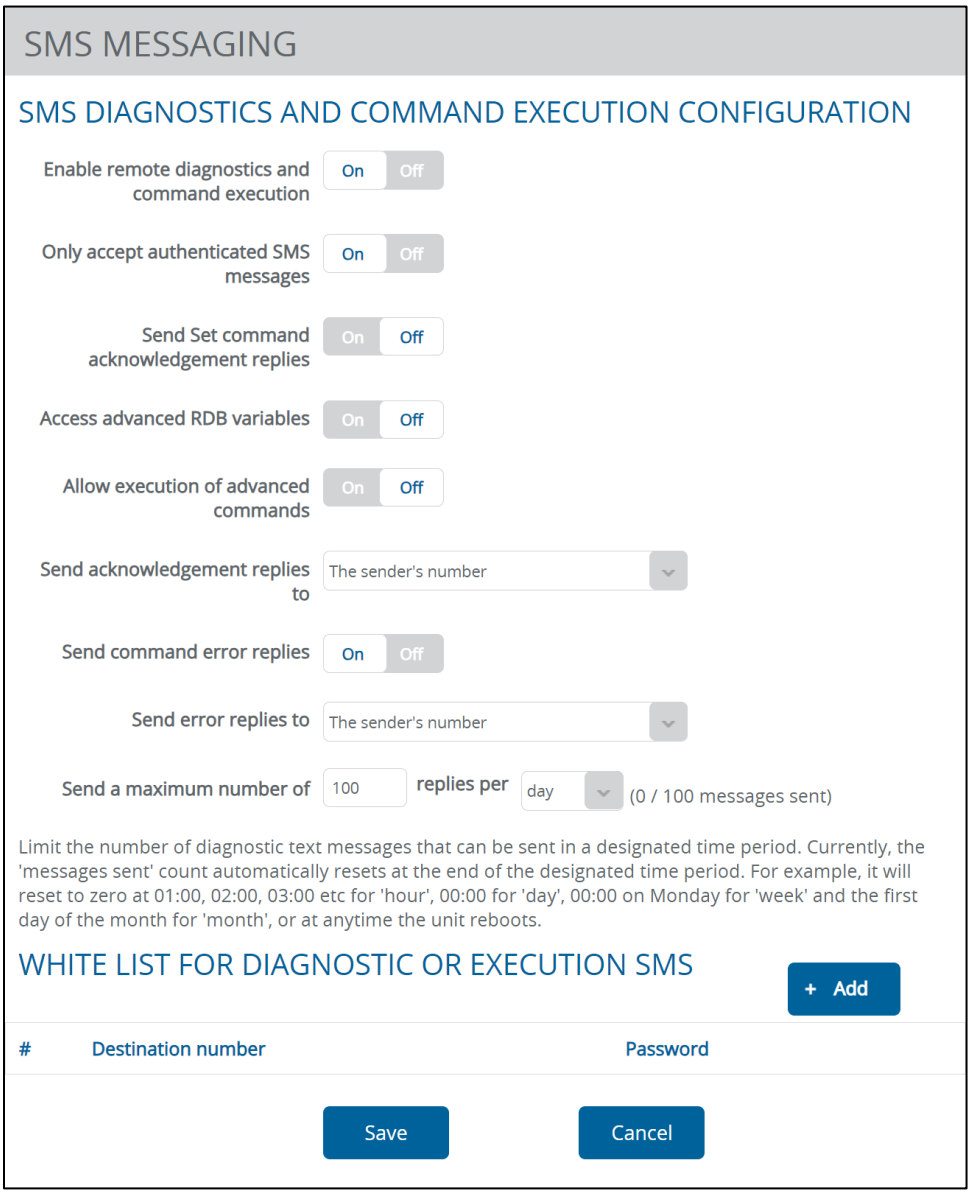
Table 9-1 SMS - SMS setup configuration items

Option	Definition
General SMS configuration	
Messages per page	Enter the number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding scheme	Enter the encoding method used for outbound SMS messages. GSM 7-bit mode permits up to 160 characters per message but drops to 50 characters if the message includes special characters. UCS-2 mode allows to send Unicode characters and permits a message to be up to 50 characters in length.
SMS forwarding configuration	
Forwarding	Set to **On**, to enable forwarding. Incoming text messages can be redirected to another mobile device and/or a TCP/UDP message server.
Redirect to mobile	Enter a mobile number as the destination for forwarded SMS messages. You can forward incoming text messages to a different destination number. This destination number can be another mobile phone or a router phone number. The text message is stored on the router and forwarded to the mobile number at the same time.
TCP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP. You can also forward incoming text messages to a TCP based destination. The TCP server can be any kind of public or private server if the server accepts incoming text-based messages. The TCP address can be an IP address or domain name. The text message is stored on the router and forwarded to the TCP server at the same time.
TCP port	The TCP port on which to connect to the remote destination. The port number range is from 1 to 65535. Please refer to your TCP based SMS server configuration for which port to use.
UDP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP. You can also forward incoming text messages to a UDP based destination. The UDP server can be any kind of public or private server if the server accepts incoming text-based messages. The UDP address can be an IP address or domain name. The text message is stored on the router and forwarded to the UDP server at the same time.
UDP port	The UDP port on which to connect to the remote destination. The port number range is from 1 to 65535. Please refer to your UDP based SMS server configuration for which port to use.

Diagnostics

The Diagnostics page is used to configure the SMS diagnostics and command execution configuration. This allows you to change the configuration, perform functions remotely, and check on the status of the router via SMS commands.

Figure 9-3 SMS – SMS diagnostics configuration



The table below lists the SMS Diagnostics Configuration details.

Table 9-2 SMS – SMS Diagnostics and Command Execution Configuration Items

Item	Description
SMS Diagnostics and Command Execution Configuration	
Enable remote diagnostics and command execution	Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands. If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox. ***Note:*** *It is possible to adjust settings and prevent your router from functioning correctly using remote diagnostics. If this occurs, you will need to perform a factory reset to restore normal operation.*
Only accept authenticated SMS messages	Enables or disables checking the sender's phone number against the allowed sender white list for incoming diagnostics and command execution SMS messages. If authentication is enabled, the router will check if the sender's number exists in the white list. If it exists, the router then checks the password (if configured) in the incoming message against the password in the white list for the corresponding sending number. If they match, the diagnostic or command is executed. If the number does not exist in the white list or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message. This is enabled by default and it is strongly advised that you leave this feature enabled to maintain security. ***Important:*** *We highly recommended that you use the white list and a password when utilising this feature to prevent unauthorised access. See the White list description for more information.*
Send Set command acknowledgement replies	The NTC-550 Series router will automatically reply to certain types of commands received, such as get commands, or execute commands. However, acknowledgement replies from the NTC-550 Series router are optional with set commands and the Wakeup command. This option enables or disables sending an acknowledgment message after execution of a set command or SMS Wakeup command. If disabled, the router does not send any acknowledgement after execution of a set command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they

Item	Description
	have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.
Access advanced RDB variables	This option allows access to the full list of RDB variables via SMS. When it is turned off, you are only allowed access to the basic RDB variables listed later in this guide.
Allow execution of advanced commands	This option allows execution of advanced commands such as those which are common to the Linux command line. For example: “execute ls /usr/bin/sms*” to list the contents of the /etc folder on the router. When it is turned off you are only allowed to execute the basic commands listed later in this guide.
Send acknowledgement replies to	Select **A fixed number** or **The sender’s number**. This option allows you to specify where to send acknowledgment messages after the execution of a set, get, or exec command. If a fixed number is selected, the acknowledgement message will be sent to the number defined in the Fixed number to send replies to field. If the sender’s number is selected, the acknowledgement message will be sent to the number that the SMS diagnostic or command message originated from. The default setting is to use the sender’s number.
Send command error replies	Allows to enable or disable the option to send replies to error messages.
Send error replies to	Select **A fixed number** or **The senders’s number**. This is the destination number to which error messages are sent after the execution of a get, set, or exec command whether a fixed number or the sender’s number. This field is only displayed when it set to Fixed Number.
Send a maximum number of, replies per	Allows you to set the maximum number of acknowledgement and error messages sent when an SMS diagnostic or command is executed. The maximum limit can be set per hour, day, week or month. The router will send a maximum of 100 replies per day by default.

Click **Save** to save the settings.

The white list is a list of mobile numbers that you can create which are considered “friendly” to the router. If **Only accept authenticated SMS** messages is enabled in the diagnostics section, the router will compare the mobile number of all incoming diagnostic and command messages against this white list to determine whether the diagnostic or command should be executed. You must configure a password for each number added to the white list to give an additional level of security.

The Whitelist For Diagnostic Or Execution SMS displays the list of mobile numbers added to white list and their details.

The table below lists the details of the Whitelist For Diagnostic Or Execution SMS

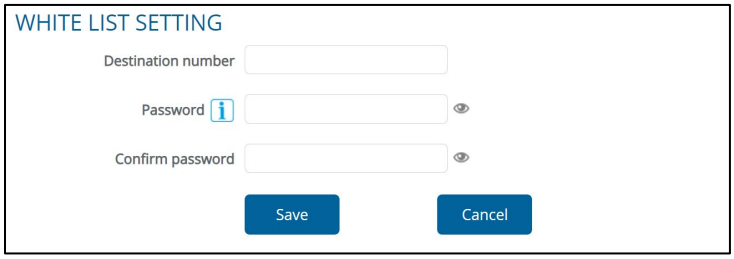
Table 9-3 Whitelist For Diagnostic Or Execution SMS Items

Item	Description
#	Serial number
Destination number	Mobile number added to white list
Password	Password associated with mobile number
	Click to edit the details of the white list number
	Click to delete the number from the white list

To configure a White List for Diagnostic or Execution SMS:

1. Click **+Add** button, the **Whitelist Setting** page displays.

Figure 9-4 SMS - SMS diagnostics configuration – White list settings



2. Enter a number in the **Destination number** field to add it to the White List.
3. In the Password field, enter a password. The password must meet the following requirements:
   Must contain a minimum of eight characters and no more than 128 characters in length.
   Must contain at least one upper case character, one lower case character and one number.
   Must contain least one of the following special characters: !*()?/
4. In the Confirm password field, re-enter the password.
5. Click **Save** to save the settings.

Sending an SMS diagnostic command

Follow the steps below to configure the router to optionally accept SMS diagnostic commands only from authenticated senders and learn how to send SMS diagnostic commands to the router.

1. Navigate to the **Services > SMS messaging > Diagnostics** page.
2. Confirm that the Enable remote diagnostics and command execution toggle key is set to the ON position. If it is set to OFF select the toggle key to switch it to the ON position.
3. If you wish to have the router only accept commands from authenticated senders, ensure that Only accept authenticated SMS messages is set to the ON position. In the White list for diagnostic or execution SMS messages section, select the +Add button and enter the sender's number in international format into the Destination number field that appears. You must enter a password in the Password field corresponding to the destination number.
4. If you would prefer to accept SMS diagnostic commands from any sender, set the Only accept authenticated SMS messages toggle key to the OFF position.

Note: *An alternative method of adding a number to the white list is to send an SMS message to the router, navigate to Services > SMS messaging > Inbox and then select the button next to the message which corresponds to the sender's number.*

You will then need to set a Password in the White list for diagnostic execution SMS list.

5. Select the **Save** button.

Types of SMS diagnostic commands

There are three types of commands that can be sent; execute, get and set. The basic syntax is as follows:

- execute COMMAND
- get VARIABLE
- set VARIABLE=VALUE

If authentication is enabled, each command must be preceded by the password:

- PASSWORD execute COMMAND
- PASSWORD get VARIABLE
- PASSWORD set VARIABLE=VALUE

The following are some examples of SMS diagnostic commands:

```
password6657 execute reboot
get rssi
set apn1=testAPNvalue
```

SMS acknowledgement replies

The router automatically replies to get commands with a value and execute commands with either a success or error response. Set commands will only be responded to if the Send Set command acknowledgement replies toggle key is set to ON. If the Send command error replies toggle key is set to ON, the router will send a reply if the command is correct but a variable or value is incorrect, for example, due to misspelling.

SMS command format

Generic Format for reading variables:

```
get VARIABLE
PASSWORD get VARIABLE
```

Generic Format for writing to variables:

```
set VARIABLE=VALUE
PASSWORD set VARIABLE=VALUE
```

Generic Format for executing a command:

```
Execute COMMAND
PASSWORD execute COMMAND
```

Replies

Upon receipt of a successfully formatted, authenticated (if required) command, the gateway will reply to the SMS in the following format:

Table 9-4 SMS – SMS diagnostics command syntax

Type	SMS Contents	Notes
get command	**"VARIABLE=VALUE"**	
set command	**"Successfully set VARIABLE to VALUE"**	Only sent if the acknowledgment message function is enabled
execute command	**"Successfully executed command COMMAND"**	

Where "VARIABLE" is the name of the value to be read

Where "VARIABLE (x)" is the name of another value to be read

Where "VALUE" is the content to be written to the "VARIABLE"

Where "COMMAND" is a supported command to be executed by the device (e.g. reboot)

Where "PASSWORD" is the password (if configured) for the corresponding sender number specified in the White List

Multiple commands can be sent in the same message, if separated by a semicolon.

For Example:

```
get VARIABLE1; get VARIABLE2; get VARIABLE3
PASSWORD get VARIABLE1; get VARIABLE2
set VARIABLE=VALUE1 ; set VARIABLE2=VALUE2
PASSWORD set VARIABLE1=VALUE1; set VARIABLE2=VALUE2; set VARIABLE3=VALUE3
```

If required, values can also be bound by an apostrophe, double apostrophe, or back tick.

For Example:

```
"set VARIABLE='VALUE'"
"set VARIABLE="VALUE""
"set VARIABLE=`VALUE`"
"get VARIABLE"
```

A password (if required), only needs to be specified once per SMS, but can be prefixed to each command if desired.

```
"PASSWORD get Variable1"; "get VARIABLE2"
"PASSWORD set VARIABLE1=VALUE1"; "set VARIABLE2=VALUE2"
```

If the command sent includes the "reboot" command and has already passed the white list password check, the device keeps this password and executes the remaining command line after the reboot with this same password.

For Example:

```
"PASSWORD execute reboot; getVariable1"; "get VARABLE2"
"PASSWORD execute reboot; PASSWORD get Variable1"; "get VARABLE2"
```

⚠ ***Important:*** *Commands, variables and values are case sensitive.*

List of basic commands

A list of basic commands which can be used in conjunction with the execute command are listed below:

"pdpcycle", "pdpdown" and "pdpup" commands can have a profile number suffix 'x' added. Without the suffix specified, the command operates against the default profile configured on the profile list page of the Web-UI.

Table 9-5 List of basic SMS diagnostic commands

Item	Command	Definition
1	**reboot**	Immediately performs a soft reboot.
2	**pdpcycle**	Disconnects (if connected) and reconnects the data connection. If a profile number is selected in the command, try to disconnect/reconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect/reconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
3	**pdpdown**	Disconnects the PDP. If a profile number is selected in the command, the router tries to disconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
4	**pdpup**	Reconnects the PDP. If a profile number is selected in the command, the router tries to connect with the specified profile. If no profile number is selected, the router tries to connect to the last active profile. The gateway will check the currently activated profile and disconnect this profile before executing the command. The router reports an error if no profile number is selected and there is no stored last active profile number.
5	**factorydefaults**	Performs a factory reset on the router. Be aware that this command also clears the SMS white list on the router.
6	**download**	Performs a download and install of a Firmware Upgrade (.cdi), Config File (.tar.gz) or a help document (.pdf) file. If the file is a firmware image as in the case of a .cdi file, the router will apply the recovery image first and then the main firmware image. The download location is specified immediately after the command and may be from an HTTP or FTP source URL. If the file is a .cdi file, the router will apply the file as a configuration file update for the device and reboot afterwards. If the file is a .pdf, the router will assume this is a user guide document and save it to the router and make the file available for viewing via the help menu on the Web-UI. Note: If your download URL includes any space characters, please encode these prior to transmission according to RFC1738, for example:

Item	Command	Definition
		ftp://username:password@serveraddress/directory%20with%20spaces/filename.cdi Note: Authenticated FTP addresses may be used following the format as defined in RFC1738, for example: ftp://username:password@serveraddress/directory/filename.cdi
10	**ssh.genkeys**	Instructs the router to generate new public SSH keys.
11	**ssh.clearkeys**	Instructs the router to clear the client public SSH key files.

List of get/set commands

The following table is a partial list of get and set commands which may be performed via SMS.

Table 9-6 SMS - List of get/set commands

Command name	Example	Description
get status	**get status**	Returns the Module firmware version, LAN IP Address, Network State, Network operator and Signal strength.
get sessionhistory	**get sessionhistory**	Returns the time and date of recent sessions along with the total amount of data sent and received for each session.
set syslogserver	**set syslogserver=123.45.67.89:514**	Sets a remote syslog server IP or hostname and port.
get plmnscan	**get plmnscan**	Instructs the router to perform a network scan and returns the results by SMS.
set forceplmn	**set forceplmn=505,3**	Sets the operator to a manual selection made by the user where “505” is the Mobile Country Code for Australia. As no network type (e.g.. LTE/5G) is specified, it is selected automatically.
get forceplmn	**get forceplmn**	Returns the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values
get ledmode	**get ledmode**	Returns the status of the LED operation mode.
set ledmode	**set ledmode=10**	Sets the LED operation mode to be always on or to turn off after the specified number of minutes.
get ssh.proto	**get ssh.proto**	Returns the SSH protocol in use.
set ssh.proto	**set ssh.proto=1,2**	Sets the SSH Protocol to protocol 1, 2 or both (1,2).

Command name	Example	Description
get ssh.passauth	`get ssh.passauth`	Returns the status of the SSH Enable password authentication option.
set ssh.passauth	`set ssh.passauth=1`	Sets the SSH Enable password authentication option on or off.
get ssh.keyauth	`get ssh.keyauth`	Returns the status of the SSH Enable key authentication option.
set ssh.keyauth	`Set ssh.keyauth=1`	Sets the SSH Enable key authentication option on or off.
get download.timeout	`get download.timeout`	Returns the time in minutes that the router waits before a download times out.
set download.timeout	`set download.timeout=20`	Sets the time in minutes that the router waits before a download times out. This is set to 10 minutes by default. Supported range is 10 – 1440 minutes.
get install.timeout	`get install.timeout`	Returns the time in minutes that the router waits before a file that is being installed times out.
set install.timeout	`set install.timeout=5`	Sets the time in minutes that the router waits before a file that is being installed times out. This is set to 3 minutes by default. Supported range is 3 – 300 minutes.
get sw.version	`get sw.version`	Returns the software version of the router.

List of basic RDB variables

The following table lists valid variables where “x” is a profile number (1-6). If no profile is specified, variables are read from or written to for the current active profile. If a profile is specified, variables are read from or written to for the specified profile number (‘x’).

Table 9-7 SMS - List of basic SMS diagnostics RDB variables

#	RDB variable name	SMS variable name	Read/ Write	Description	Example VALUE
0	link.profile.1.enable link.profile.1.apn link.profile.1.user link.profile.1.pass link.profile.1.auth_type	profile	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,apn,username,password, chap,202.44.185.111,up

#	RDB variable name	SMS variable name	Read/ Write	Description	Example VALUE
	link.profile.1.iplocal link.profile.1.status				Write: (apn, user, pass,auth) apn,username,password
2	link.profile.1.user	username	RW	Cellular broadband username	Guest, could also return “null”
3	link.profile.1.pass	password	RW	Cellular broadband password	Guest, could also return “null”
4	link.profile.1.auth_type	authtype	RW	Cellular broadband Authentication type	”pap” or”chap”
5	link.profile.1.iplocal	wanip	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rssi	R	Cellular signal strength	-65 dBm
7	wwan.0.imei	imei	R	IMEI number	3.57347E+14
8	statistics.usage_current	usage	R	Cellular broadband data usage of current session	“Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes” or “Rx 0 byte, Tx 0 byte, Total 0 byte” when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current cellular broadband session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current band	NR5G BAND 78

Network scan and manual network selection by SMS

Performing a network scan:

The get plmnscan SMS command enables you to perform a scan of the cellular networks available at the time of the scan.

It returns the following semi-colon separated information for each network in range:

- MCC
- MNC
- Network Type (LTE, 5G)

- Provider's Name
- Operator Status (available, forbidden, current)

The following is an example of a response from the get plmnscan SMS command:

```
plmnscan=505,03,7,vodafone AU,1;505,03,1,vodafone AU,1;505,03,9,vodafone AU,4;505,01,7,Telstra
Mobile,1;505,01,1,Telstra Mobile,1;505,02,9,YES OPTUS,1;505,02,1,YES OPTUS,1;505,01,9,Telstra
```

Table 9-8 Operator status codes returned by get plmnscan SMS command

Operator status	Description
1	Indicates an available operator which may be selected.
2	Indicates a forbidden operator which may not be selected (applies only to generic SIM cards).
4	Indicates the currently selected operator.

Note:

- *If the connection status is Up and connection mode is Always on, the get plmnscan SMS will cause the connection to disconnect, perform the scan, send the result through SMS and then bring the connection back up again. If the connection status is Down, the router will perform the PLMN scan, send the result and keep the connection status down.*
- *If the connection status is Waiting and connection mode is Connect on demand, the get plmnscan SMS will change the connection status to Down, perform the scan, send the result through SMS and then restore the connection status to the Waiting state.*
- *If the connection status is Up and connection mode is Connect on demand, the get plmnscan SMS will cause the connection to disconnect, perform the scan, send the result through SMS, and then restore the connection status to the Waiting state unless there is a traffic which triggers a connection in which case the connection status will be set to Up.*

Setting the router to connect to a network

The router can be instructed by SMS to connect to one of the networks returned by the get **plmnscan** command. The **set forceplmn** command forces the router to connect to a specified operator network (if available) while the **get forceplmn** command retrieves the currently configured network on the router.

The command format for the **set forceplmn** command is:

```
set forceplmn=0|MCC,MNC| MCC,MNC,Network Type
```

For example:

```
set forceplmn=0
```

Sets the selection of operator and network type to automatic mode.

```
set forceplmn=505,9
```

Sets the operator to a manual selection made by the user where “505” is the Mobile Country Code for Australia and “1” is the Mobile Network Code for Telstra. As no network type (e.g. LTE/5G) is specified, it is selected automatically.

```
set forceplmn=505,1,9
```

Sets the operator and network type to a manual selection made by the user where “505” is the Mobile Country Code for Australia, “1” is the Mobile Network Code for Telstra and “9” is the LTE network type.

Table 9-9 SMS - Mobile Network Provider codes (Australia)

Mobile Network Code	Mobile Network Provider
1	Telstra
2	Optus
3	Vodafone

Confirming the currently configured operator and network type

You can retrieve the currently configured operator and network type using the **get forceplmn** command.

The **get forceplmn** command returns the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values, for example:

```
Automatic,505,1
```

This response indicates that the operator/network selection mode is Automatic, and the network used is Telstra.

SMS diagnostics examples

The examples below demonstrate various combinations of supported commands. This is not an exhaustive list and serves as an example of possibilities only.

If the default setting of **Only accept authenticated SMS messages** is enabled then password authentication is required. Add your password followed by a space as a prefix to the command, for example

If authentication required:

```
PASSWORD set username= ”<username>”
```

If authentication not required:

```
set username=’<username>’
```

Note: *The authentication setting is located in the user interface at Services > SMS messages> Diagnostics.*

Table 9-10 SMS – SMS diagnostics example commands

Description	Input Command (without PASSWORD prefix)
Send SMS to change the data connection username	`set username=’<username>’`
Send SMS to change the data connection password	`set password= `<password>` `
Send SMS to change the data connection authentication	`set authtype= ‘pap’`
Send SMS to reboot	`execute reboot`

Description	Input Command (without PASSWORD prefix)
Send SMS to check the WAN IP address	**get wanip**
Send SMS to check the mobile signal strength	**get rssi**
Send SMS to check the IMEI number	**get imei**
Send SMS to check the current band	**get band**
Send SMS to Disconnect (if connected) and reconnect the data connection	**execute pdpcycle**
Send SMS to disconnect the data connection	**execute pdpdown**
Send SMS to connect the data connection	**execute pdpup**
Send multiple get command	**get wanip; get rssi**
Send multiple set command	**set ssh.genkeys=1; set username=test; set auth=pap**
Send SMS to reset to factory default settings	**execute factorydefaults**
Send SMS to retrieve status of router	**get status**
Send SMS to retrieve the history of the session, including start time, end time and total data usage	**get sessionhistory**
Send SMS to configure the router to send syslog to a remote syslog server	**set syslogserver=123.209.56.78**
Send SMS to perform firmware upgrade when firmware is located on HTTP server	**execute download http://download.com:8080/firmware_image.cdi** **execute download http://download.com:8080/firmware_image_r.cdi**
Send SMS to perform firmware upgrade when firmware is located on FTP server	**execute download ftp://username:password@download.com/firmware_image.cdi** **execute download ftp://username:password@ download.com/firmware_image_r.cdi**
Send SMS to download and install IPK package located on HTTP server	**execute download http://download.com:8080/package.ipk**
Send SMS to download and install IPK package located on FTP server	**execute download ftp://username:password@ download.com:8080/package.ipk**
Send SMS to set the LED mode timeout to 10 minutes	**set ledmode=10**
Send SMS to retrieve the current LED mode	**get ledmode**
Retrieve current SSH protocol	**get ssh.proto**
Select SSH protocol	**set ssh.proto=1**
Retrieve password authentication status	**get ssh.passauth**

Description	Input Command (without PASSWORD prefix)
Enable/disable password authentication on host	`set ssh.passauth=1 or set ssh.passauth=0`
Generate set of public/private keys on the host	`execute ssh.genkeys`
Clear client public keys stored on host	`execute ssh.clearkeys`
Send SMS to initiate a Network Quality test	`get networkquality`

Inbox

The Inbox displays all received messages that are stored on the router.

Figure 9-5 SMS – Inbox

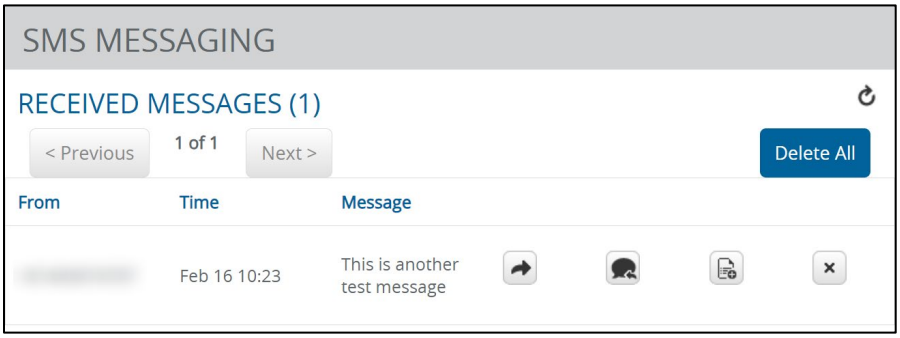


Table 9-11 SMS - Inbox

Icon	Name	Description
	Forward	Opens a new message window where you can forward the corresponding message to another recipient.
	Reply	Opens a new message window where you can reply to the sender.
	Add to White list	Add the sender's mobile number to the white list on the router.
	Delete	Delete the corresponding message.
	Refresh	Refresh the inbox to see new messages.

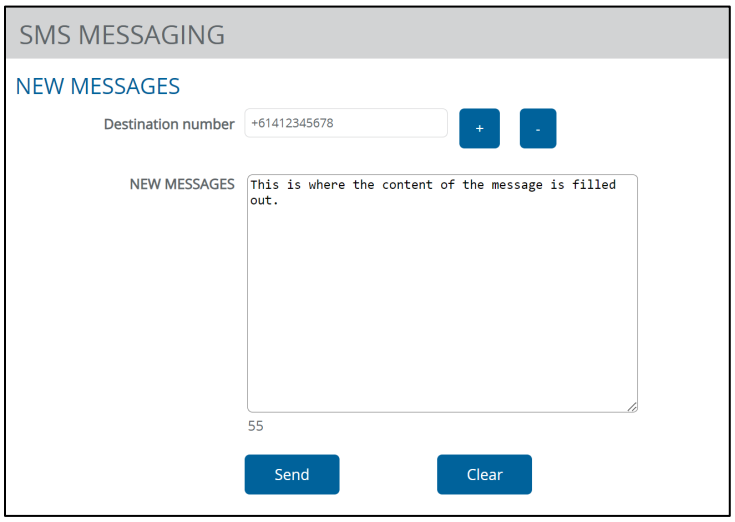
Compose Message

The Compose Message page can be used to send SMS text messages to a single or multiple recipients. To access the Compose message page, click **Services** tab on the menu bar, click **SMS messaging**, and in the dropdown click **Compose Message**.

A new SMS message can be sent to a maximum of 9 recipients at the same time. After sending the message, the result is displayed next to the destination number as "Success" or "Failure". By default, only one destination number field is displayed. Additional destination numbers may be added one at a time after entering a valid

number for the current destination number field. To add a destination number, select the + button and to remove the last destination in the list, select the - button.

Figure 9-6 SMS – New message



Enter recipient number in the **Destination number** field. It should begin with the "+" symbol followed by the country calling code.

For example:

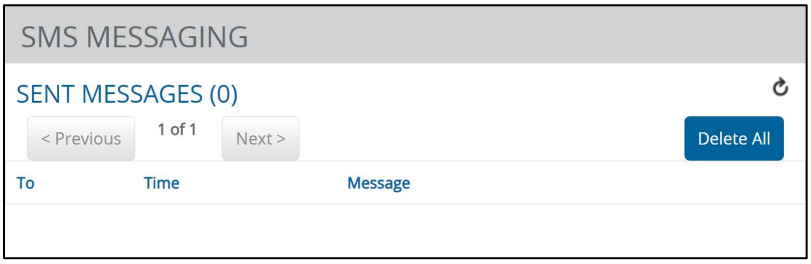
To send a message to the mobile destination number 0412345678 in Australia (country calling code 61), enter "+61412345678".

After entering the required recipient numbers, type your SMS message in the **New Messages** field. As you type your message, a counter shows how many characters you have entered out of the total number available for your chosen encoding scheme. When you have finished typing your message and you are ready to send it, click **Send** button.

Outbox

The outbox displays all sent messages.

Figure 9-7 SMS - Outbox

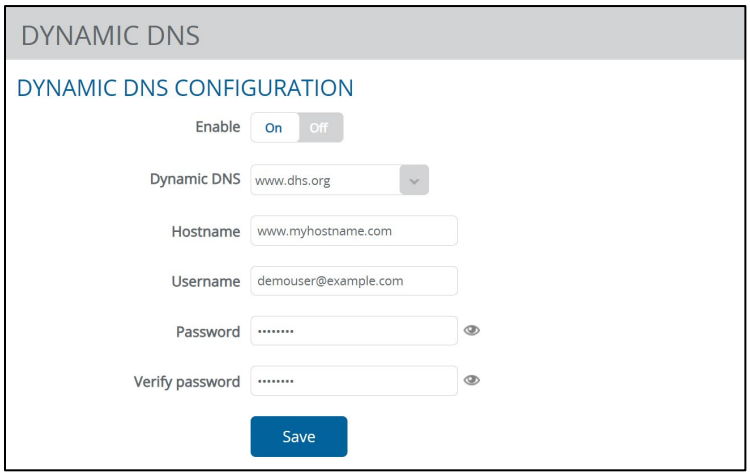


Click **Delete All** to delete all messages and empty the outbox.

Dynamic DNS

Dynamic DNS (DDNS) allows your NTC-550 Series router to associate an easy-to-remember domain name such as **[yourdomainname].com** with the regularly changing IP address assigned by your carrier. This feature allows you to connect to the NTC-550 Series router and its internal network more easily for maintenance.

Figure 9-8 Services – Dynamic DNS



To use DDNS, you will need to sign up for a DDNS provider which is supported by the NTC-550 Series router. The supported providers are DHS.org, No-IP, DynDNS, easyDNS, and ZoneEdit. To configure DDNS on the NTC-550 Series router you will require your unique hostname from the provider, as well as your username and password which you used to sign up with the provider.

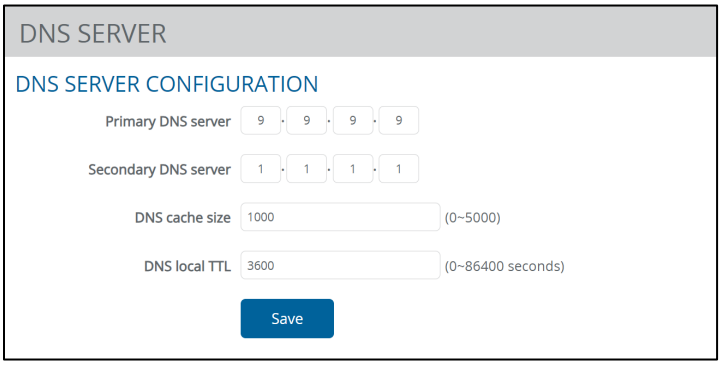
To configure DDNS:

1. Set the **Enable** toggle to **On.**
2. In the **Dynamic DNS** field select the provider you have signed up with.
3. In the **Hostname** field, enter the custom hostname which you added to your provider.
4. In the **Username** field, enter the username which you used to sign up to your provider.
5. In the **Password** field, enter the password which you used to sign up to your provider.
6. In the **Verify Password** field, re-enter the password which you used to sign up to your provider.
7. Click **Save** button to apply the configuration.

DNS Server

The NTC-550 Series router can be configured to use custom DNS servers if required.

Figure 9-9 DNS configuration



To set the DNS servers:

1. In the **Primary DNS server** field, enter the primary DNS server.
2. In the **Secondary DNS server** field, enter the secondary DNS server.
3. In the **DNS Cache Size** field, enter the size of the cache that should be kept on the router.
4. In the **DNS local TTL** field, enter the time to live (TTL) , which is the duration for which a cached request remains in the router.
5. Click the **Save** button to save the configuration.

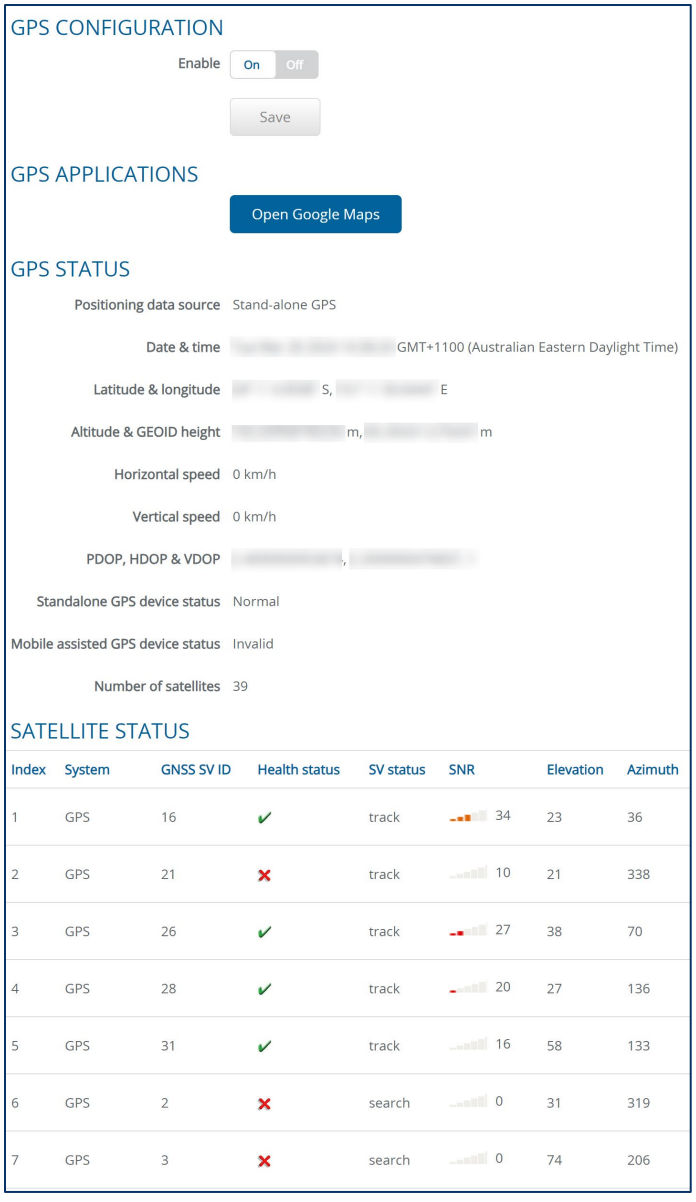
GPS

The NTC-550 Series router is equipped with GPS which allows the use of location-based services, to monitor field deployed hardware or find the current location of the NTC-550 Series router. The GPS Status window provides up to date information about the current location and the current GPS signal conditions (Position Dilution of Precision (PDOP), Horizontal Dilution of Precision (HDOP), and Vertical Dilution of Precision (VDOP)) of the router.

GPS Configuration

The GPS Configuration page allows you to configure the settings related to GPS and displays information about the GPS connection.

Figure 9-10 GPS – GPS configuration



To enable GPS, set **Enable** toggle to **On** and click **Save** button.

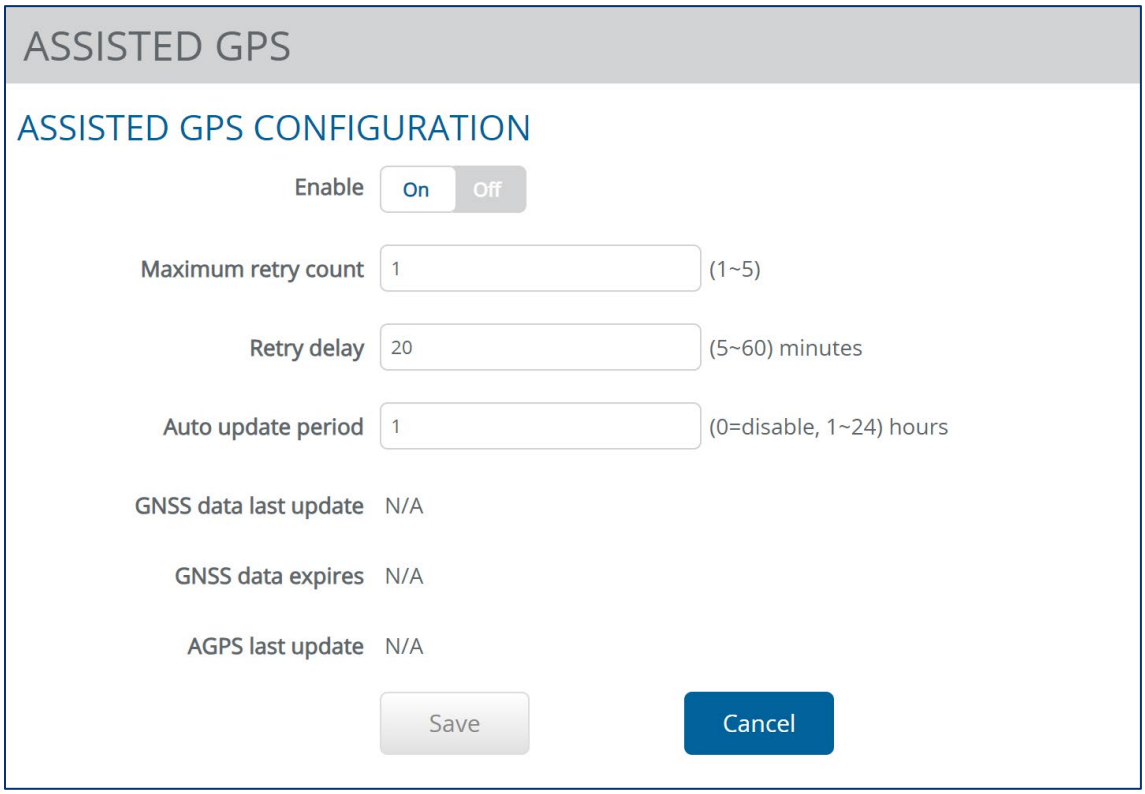
Clicking the **Open Google Maps** button opens a Google Maps page with the current GPS location pinned.

The **GPS Status** and **Satellite Status** sections provide an overview of the current GPS details and details of the satellites which are in use.

Assisted GPS

Assisted GPS enables your router to download GNSS data which supplies orbital data to the GPS receiver, enabling it to lock to the satellites more rapidly. The GNSS data is stored on the router to assist the GPS in locating the router.

Figure 9-11 GPS – Assisted GPS



To setup automatic updates of GNSS data, set the **Enable** toggle key to the **ON** position and then set the automatic retry options. For each retry, the router checks for an updated GNSS data file and downloads the GNSS data if newer than the currently stored data.

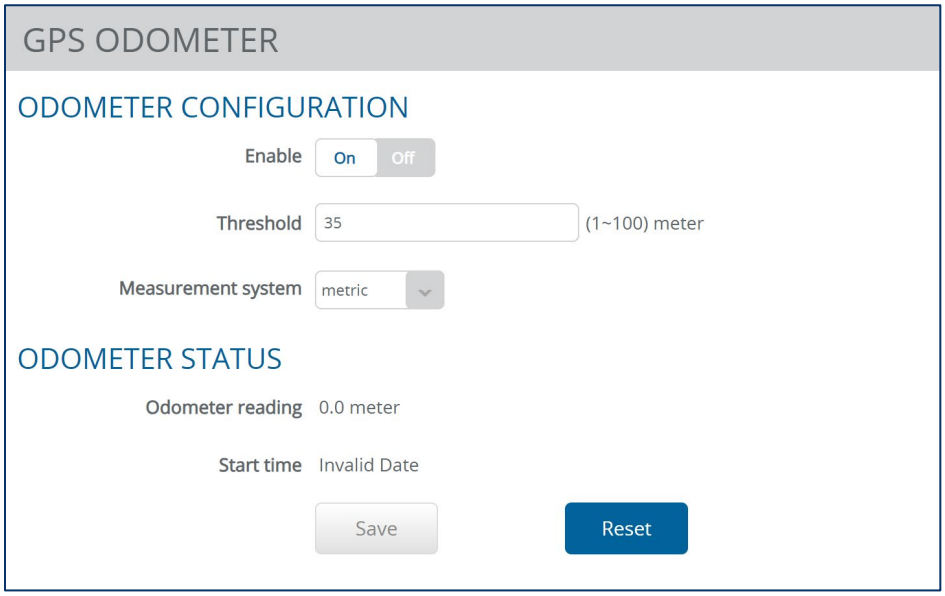
The **GNSS data last update** field represents the time that the GNSS data file was created, the **GNSS data expires** field indicates the time until this data is valid, and the **A-GPS last update** field specifies the last time the router attempted to retrieve an update to the GNSS data.

When you have finished configuring the settings, click **Save** button to save the settings.

GPS Odometer

The GPS Odometer is used to record the distance that the router has travelled.

Figure 9-12 GPS – GPS odometer



The table below lists the GPS Odometer details.

Table 9-12 GPS – GPS Odometer Items

Item	Description
Odometer Configuration	
Enable	Set to **On** to enable GPS Odometer
Threshold	Enter the required value. It pecifies the minimum distance that the router must travel from its current position before the Odometer reading increases.
Measurement system	Select the unit of measurement for the Odometer reading. The options are **metric** and **imperial**.
Odometer Status	
Odometer reading	The distance that the device has travelled since the time listed in the Odometer start time field.
Odometer start time	The time that recording of distance travelled began.

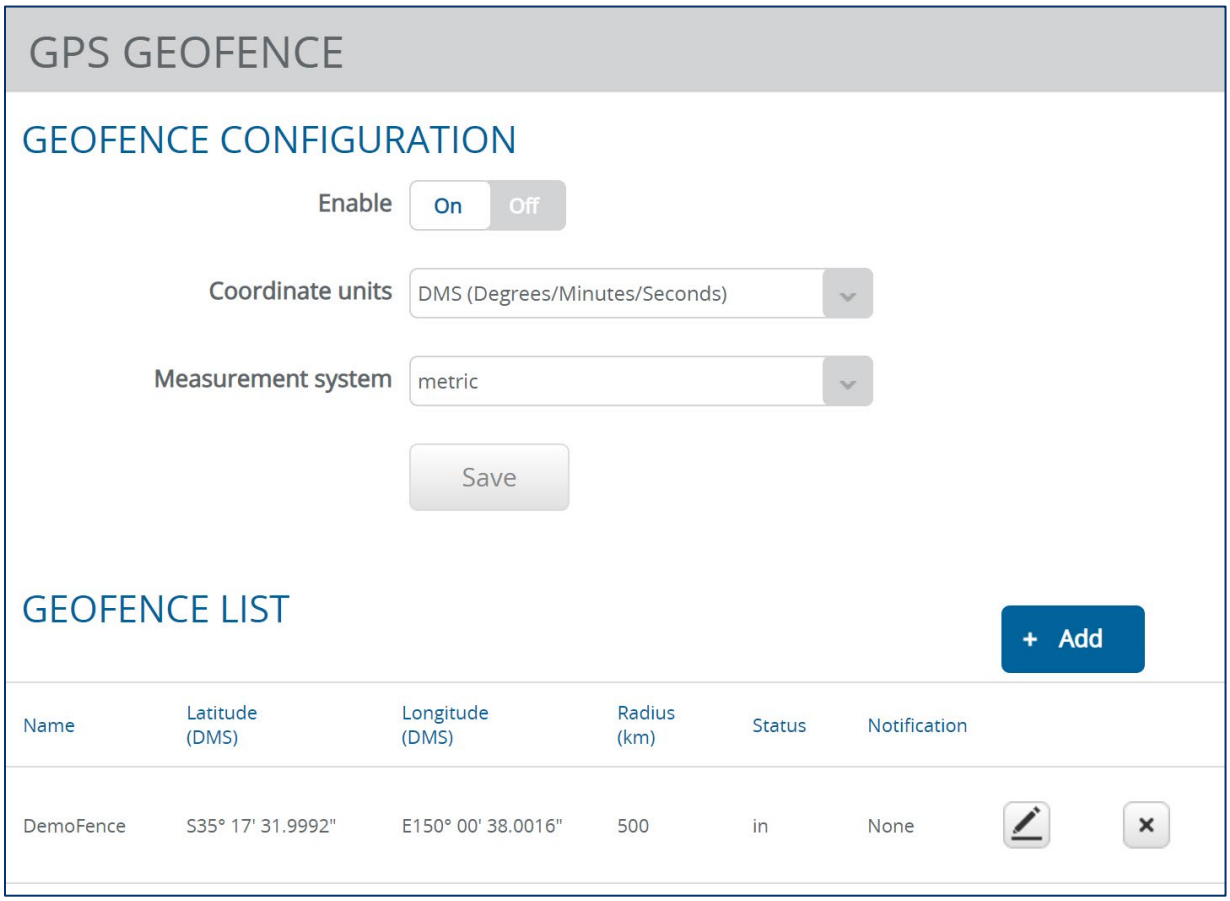
Click **Save** to save the settings.

Click **Reset** to reset the odometer reading to zero and the odometer start time to the current time.

GPS Geofence

The GPS Geofence allows you to designate a circular area and then use the router's GPS position to monitor when the NTC-550 Series router moves out of or into that area. You can configure notifications to be sent when the unit enters or exits the area. Notification types are set on the Event notification configuration page.

Figure 9-13 GPS – GPS Geofence



The table below lists the GPS Geofence Configuration details

Table 9-13 GPS – GPS Geofence Configuration Items

Item	Description
Enable	Set to **On** to enable GPS Geofence. When On, your currently defined Geofences appear in the Geofence list, see below.
Coordinate units	Select how to display the Coordinate units. The options are **Decimal degrees** and **DMS (Degrees/Minutes/Seconds)**
Measurement system	Select the type of Measurement system to display the radius of the geofence. Options are **metric** (kilometres) and **imperial** (miles).

Click **Save** to save the settings.

The Geofence List displays the list of the Configured geofences and their details.

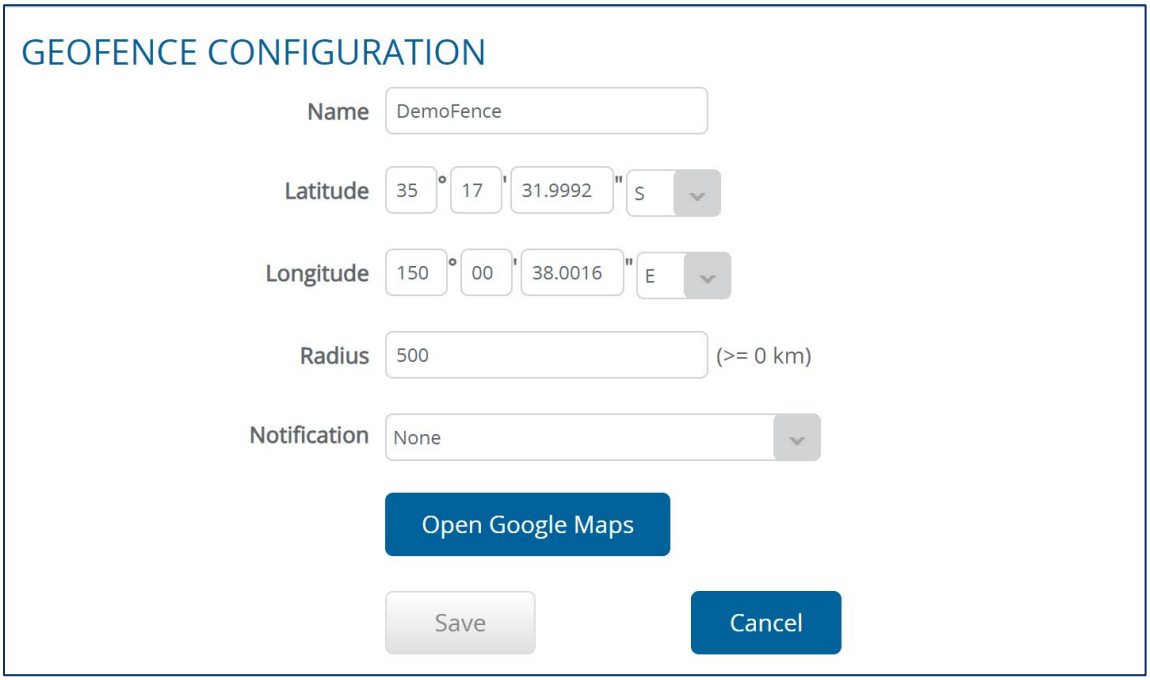
The table below lists the details of the Geofence List.

Table 9-14 GPS Geofence List Items

Item	Description
Name	Name given to the geofence during configuration.
Latitude (decimal degrees)	Latitude of the center of the geofence.
Longitude (decimal degrees)	Longitude of the center of the geofence.
Radius (km)	Radius of the geofence.
Status	**In**, if the router is inside the radius. **Out**, if the router is outside the radius.
Notification	The event that triggers a notification. See Add Geofence in next section for the available notification types.
	Click to edit that Geofence. The user interface is the same as the add Geofence configuration screen, see next section below.
	Click to delete that geofence.

To add a new geofence click **+Add** button in the Geofence List.The Geofence configuration page displays.

Figure 9-14 GPS – GPS Geofence – Geofence configuration



The table below lists the new geofence configuration details.

Table 9-15 GPS – New Geofence Configuration Items

Item	Description
Name	Enter a name for the geofence. The geofence is added to the Geofence List with this name.
Latitude	Enter the latitude of the center of the geofence.
Longitude	Enter the longitude of the center of the geofence.
Radius	Set the radius of the Geofence.
Notification	Select an event to trigger a notification. The options are: **None** – This effectively turns the Geofence function off, although the router continues to monitor the location of the device with respect to the Geofence settings. To properly disable the Geofence function, set the Geofence operation toggle key to the off position. **Entry** – A notification is triggered when the router enters the Geofence radius. **Exit** – A notification is triggered when the router leaves the Geofence radius. **Entry/Exit** – A notification is triggered when the router crosses the Geofence radius line.
Open Google maps button	The **Open Google Maps** button serves the following purposes: • When no latitude and longitude has been entered, the Google maps button displays the router's current location on the map. • When coordinates have been entered, clicking on the Google maps button checks that your coordinates go to where you expect them to be.

Click **Save** to save the settings and add new geofence or complete editing a geofence.

To configure event notifications, click **Event Notification Configuration** link. It will direct you to Event Configuration section.

Remote management

OMA-LWM2M

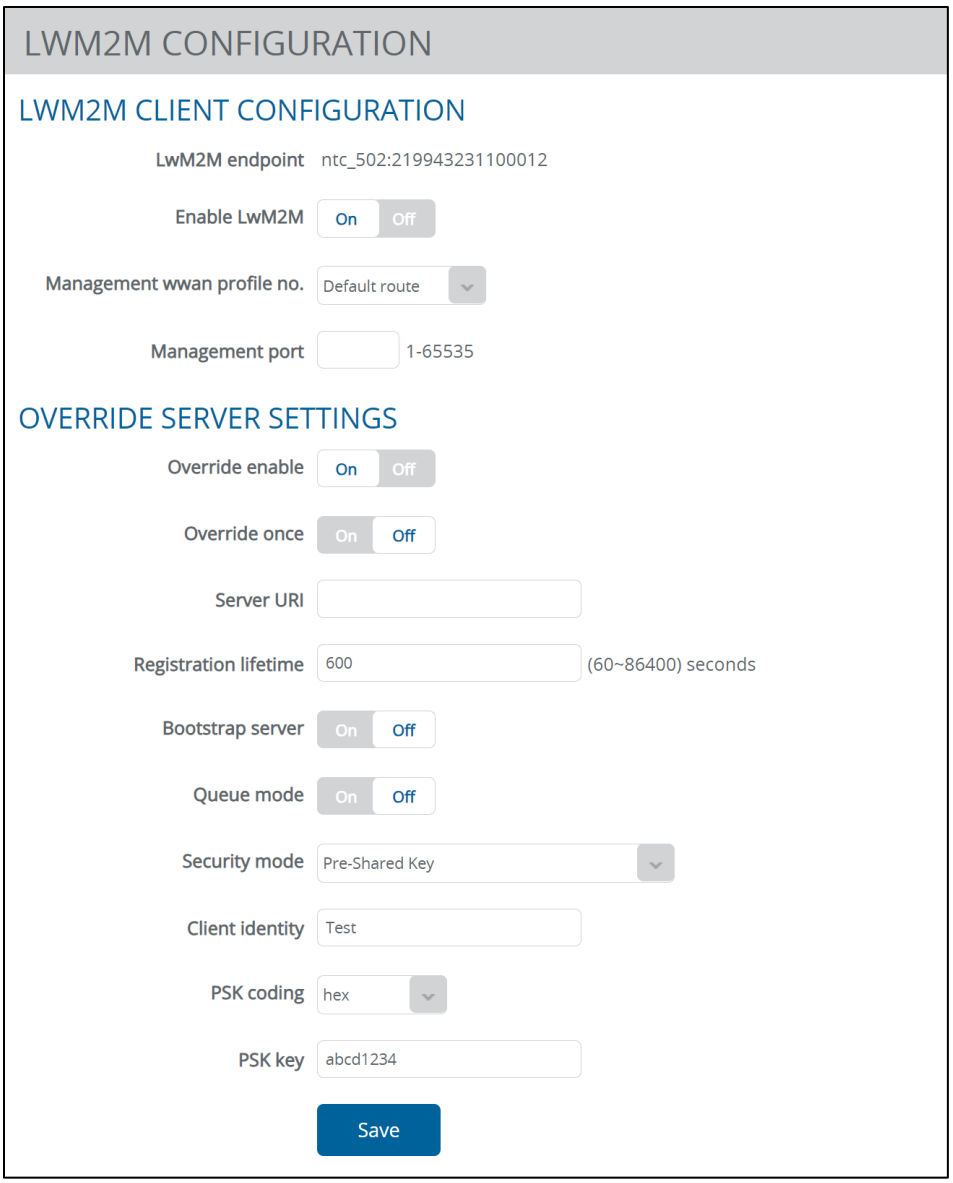
The OMA Lightweight M2M (OMA-LWM2M) protocol was designed by the Open Mobile Alliance to provide remote device management specifically for M2M devices. It is less taxing on the system and network than OMA-DM and TRS-069. OMA-LWM2M runs over UDP and supports asynchronous notifications when a resource changes.

It provides:

- Firmware upgrades
- Device monitoring and configuration
- Server provisioning

To configure the Lightweight M2M client, set the Enable LwM2M toggle key to **On** position.

Figure 9-15 OMA-LWM2M configuration



The table below lists the LWM2M Configuration details.

Table 9-16 LWM2M Configuration items

Item	Description
LWM2M Client Configuration	
LwM2M Endpoint Name	This is the unique ID the device will use to identify itself with LwM2M servers.
Enable LwM2M	Set to **On** to enable LwM2M. The configuration settings display.
Management wwan profile no.	Select the wwan profile to use with LwM2M client. Any profile, except default route, will require VLAN mapping. Refer to VLAN settings section for VLAN setup.
Management port	Enter the port used for client management. UDP port 5683 is the default port for unencrypted communication. UDP port 5684 is the default port for secure communication.
Override Server Settings	
Override Enable	Set to **On** to enable Override settings. The configuration settings display. The LwM2M client maintains the list of servers that it will connect to as part of its internal state. Enabling this setting will allow a user to specify new server details that will override whatever current settings the client has.
Override Once	Enable this option to apply the new server details only once, when the client is restarted (normal flow for configuring/reconfiguring the client) and disable this option to apply the new server details every time the client restarts (used for debugging/troubleshooting.)
Server URI	Enter the URI of the LwM2M server to connect to. It must be a fully specified CoAP or CoAPS URI, including port number, e.g. coap://server.com:5683 or coaps://server.com:5864.
Registration Lifetime	Specify the interval (in seconds) at which the LwM2M client will send registration updates (i.e. heartbeat messages) to the server.
Bootstrap server	Set to **On**, if the new server is an LwM2M bootstrap server
Queue mode	When set to **On**, the UDP binding mode is reported to the server as queued (UQ binding mode). When set to **Off**, it is reported as not queued (U binding mode)
Security mode	Select the security mode to be used to connect to the server. The options are **No Security** and **Pre-shared Key**. If Pre-shared key is selected the below fields display.
Client Identity	Enter the identity key associated with your pre-shared key.
PSK coding	Select the type of coding for the for the key. The options are **hex** and **text**
PSK key	Enter the key. The key can be a hexadecimal string or a plain text string depending on the **PSK coding** type selected

Supported LWM2M objects

The table below lists the supported object IDs on the NTC-550 Series router. For further information on the objects, refer to the Open Mobile Alliance LWM2M registry.

Table 9-17 LWM2M supported objects

Object	Object ID	Note
LWM2M Server	1	
LWM2M Access Control	2	
Device	3	
Connectivity Monitoring	4	
Firmware Update	5	
Location	6	
APN Connection Profile	11	
System Log	10259	Custom object
Runtime Database Access	10260	Custom object
Phone Module Info	33040	Custom object

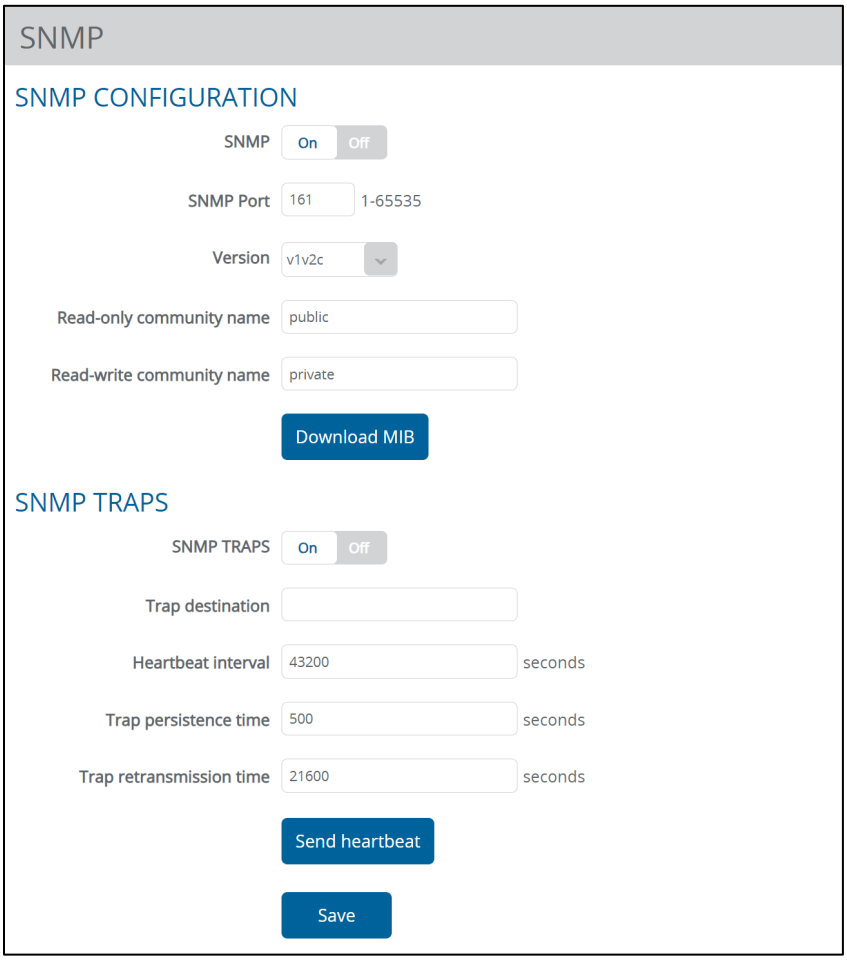
Timeouts

Most mobile networks use stateful firewalls or NAT where the timeout for UDP is approximately 1-2 minutes. If this applies to you, we suggest either configuring the LwM2M client with a registration lifetime that falls within this period (e.g. 60 seconds) or using the queued ("UQ") UDP binding mode.

SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NTC-550 Series router (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

Figure 9-16 SNMP Configuration



Configuring SNMP

6. Set the **SNMP** toggle to **On** to enable SNMP.
1. In the **SNMP Port** field, enter the SNMP port to be used.
2. Use the **Version** dropdown to set the SNMP version to be used. Available options are **v1v2c** and **v3**.
3. In the **Read-only community name** enter the read community name of the network.
4. In the **Read-write community name** enter the write community name of the network.
5. Select the **Save** button below the **SNMP Traps** section to apply the configuration.

Configuring SNMP traps

The NTC-550 Series router can be configured to send SNMP traps to a central SNMP Network Management System (NMS) when certain events occur. To configure the SNMP traps:

1. Set the **SNMP Traps** toggle to **On**.

2. In the **Trap Destination** field, enter the address of the SNMP NMS.
3. In the **Heartbeat interval** field, enter the interval in seconds which the NTC-550 Series router should send a heartbeat.
4. In the **Trap persistence time** field, enter the interval in seconds that the NTC-550 Series router should attempt to send a specific trap after the initial occurrence that triggered the trap.
5. In the **Trap retransmission time** field, enter the interval in seconds that the NTC-550 Series router should wait before retransmitting the trap.
6. Use the **Send heartbeat** button to send a test heartbeat.
7. Select the **Save** button to save and apply the settings.

TR-069

The Technical Report 069 (TR-069) protocol is a technical specification also known as CPE WAN Management Protocol (CWMP). It is a framework for remote management and auto-configuration of end-user devices such as customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It is particularly efficient in applying configuration updates across networks to multiple CPEs.

TR-069 uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol and provides several benefits for the maintenance of a field of CPEs:

- Simplifies the initial configuration of a device during installation
- Enables easy restoration of service after a factory reset or replacement of a faulty device
- Firmware and software version management
- Diagnostics and monitoring

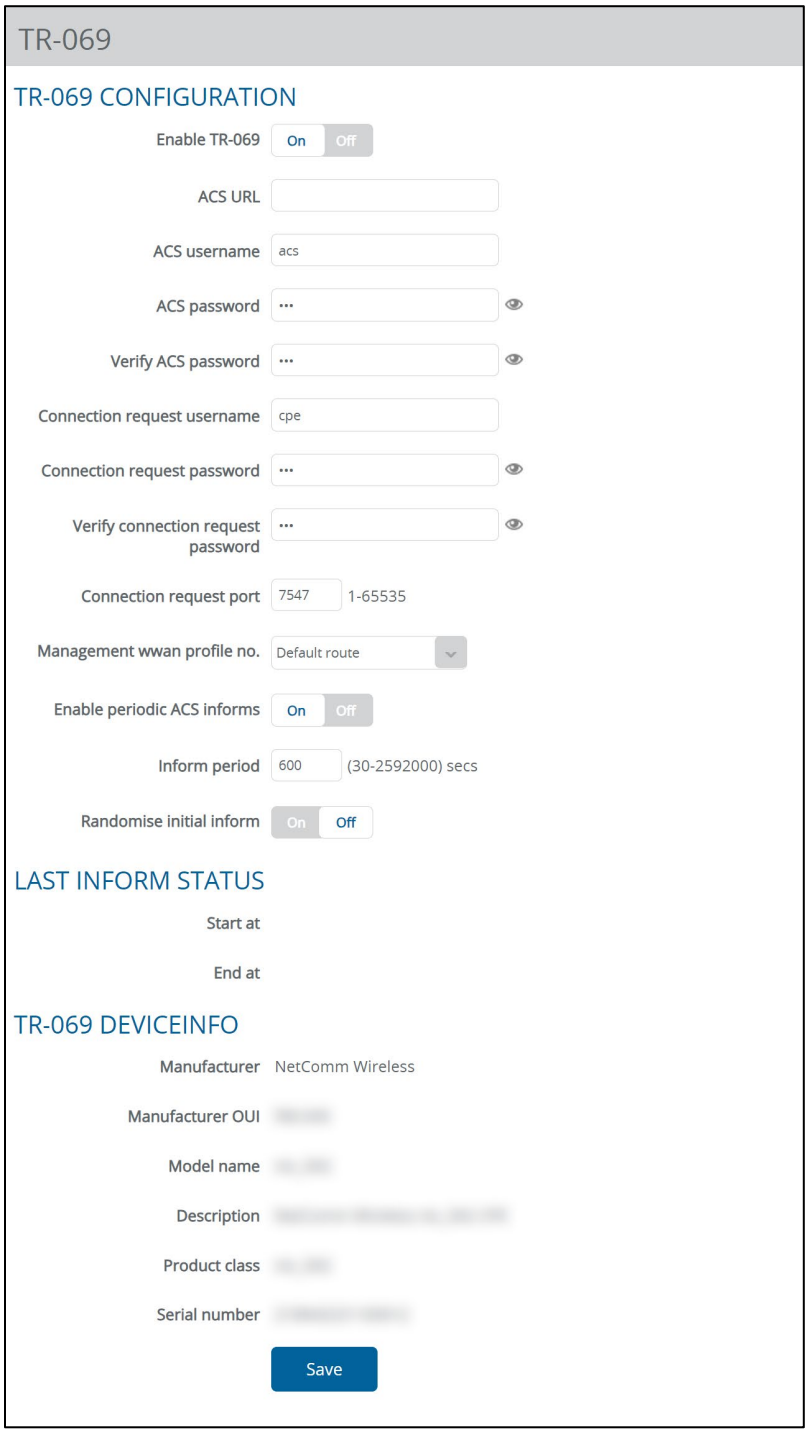
Note: *You must have your own compatible ACS infrastructure to use TR-069. To access and configure the TR-069 settings, you must be logged into the router with the root account.*

When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

The NTC-550 Series router sends “inform” messages periodically to alert the ACS server that it is ready. These inform messages can also be configured to accept a connection request from the ACS server. When a connection is established, any tasks queued on the ACS server are executed. These tasks may be value retrieval or changes and firmware upgrades.

To access the TR-069 configuration page, click the **Services** tab on the top menu bar, and in the **Remote management** section, click **TR-069.**

Figure 9-17 TR069 configuration



To configure TR-069:

1. Set **Enable TR-069** toggle key **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.
3. In the **ACS username** field to specify the username used by the server to authenticate the CPE when it sends an "inform" message.
4. In the **ACS password** and **Verify ACS password** fields, enter the password used by the server to authenticate the CPE when it sends an "inform" message.

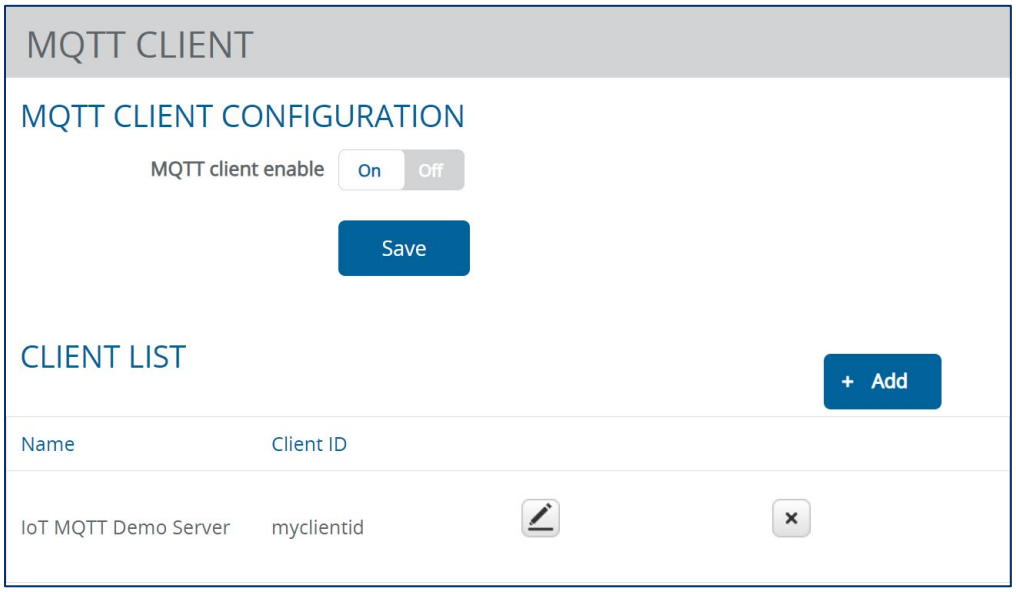
5. In the **Connection request** username field, enter the username that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
6. In the **Connection request password** and **Verify password** fields, enter the password that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
7. In the **Connection request port** field, enter the port that the request should connect to.
8. In the **Management wwan profile no.** field, enter the WAN profile that should handle the request.
9. The inform message acts as a beacon to inform the ACS of the existence of the router. Select **Enable periodic ACS informs** toggle key to **On** to turn on the periodic ACS inform messages.
10. In the **Inform Period** field, enter the number of seconds between the inform messages.
11. Select the **Save** button to save the settings.

Internet of Things

MQTT

The MQTT page is used to configure the NTC-550 Series router to use the MQTT protocol. MQTT is a standards-based messaging protocol used for machine-to-machine communication. Information is sent to clients in the form of a 'topic'. The NTC-550 Series router can be configured to send device information and neighbouring cells as a topic to common IoT monitoring applications, such as Microsoft Azure IoT Hub and Amazon IoT, using MQTT.

Figure 9-18 MQTT Client



Configuring MQTT

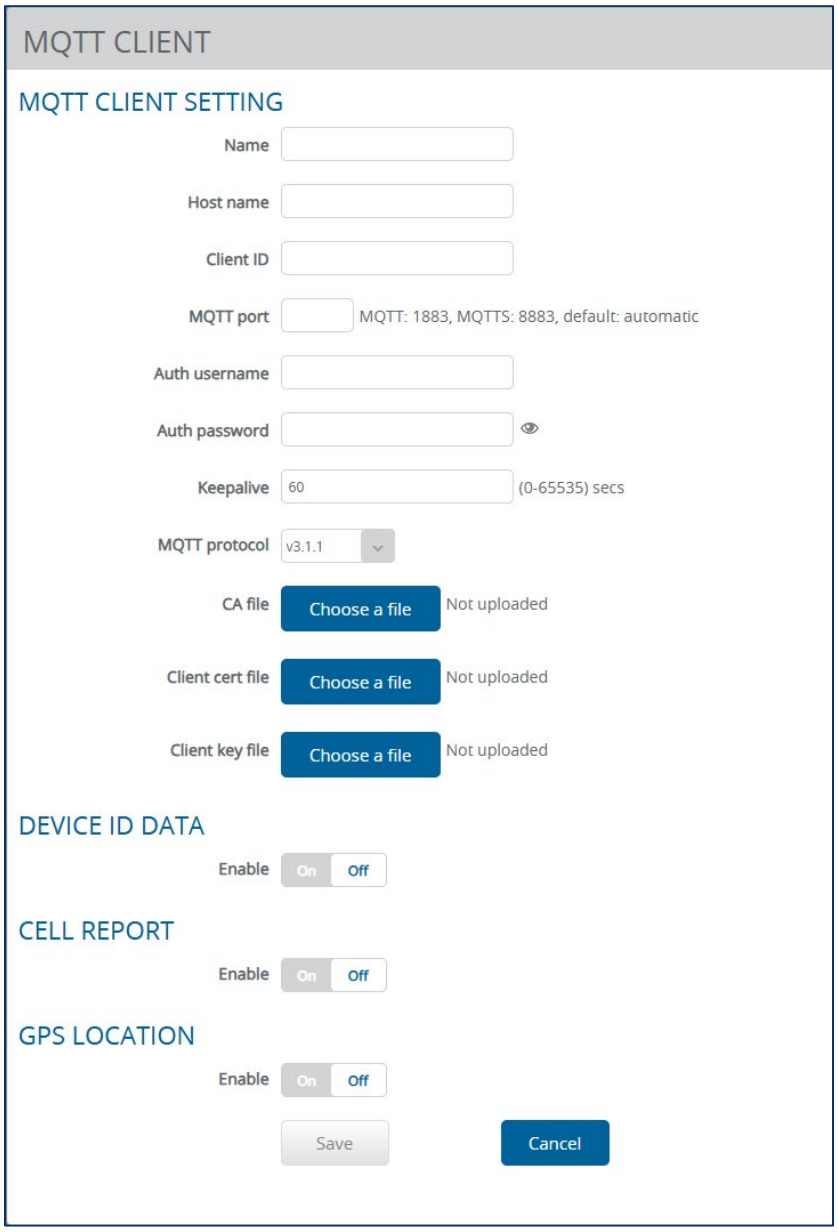
Prerequisites

To configure MQTT on the NTC-550 Series router, you need to create the device on your external MQTT client provider, and generate certificates and keys as required for secure authentication. Refer to your external MQTT provider's documentation for the required authentication configuration.

To configure MQTT:

1. Set the **MQTT client enable** toggle to **On**.
2. Click **+Add** button to add a new client. The **MQTT Client Setting** page displays.

Figure 9-19 MQTT – MQTT Client configuration



The table below lists the MQTT Client Setting configuration details.

Table 9-18 MQTT Client Settings configuration items

Item	Description
Name	Enter the name of the client to identify the client on the NTC-550 Series router
Host name	Enter the Hostname of your client
Client ID	Enter Client Id of the client. The Client Id may match the name of your client provider, for example, the name of your AWS IoT 'Thing'.

Item	Description
MQTT port	Enter the port MQTT should be initiated over.
Auth username	Enter the username of the connection.
Auth password	Enter the password of the connection.
Keepalive	Enter the number of seconds that the connection should be kept alive.
MQTT protocol	Enter the version of MQTT that should be used.
CA file	Upload the Certificate Authority file.
Client cert file	Upload the client certificate file generated as part of your client's configuration.
Client key file	Upload the client key file generated as part of your client's configuration.

3. Click **Save** to save the settings.
4. Configure MQTT topics. You can configure any one or all the available clients.

Figure 9-20 MQTT – MQTT Client Configuration – MQTT topics

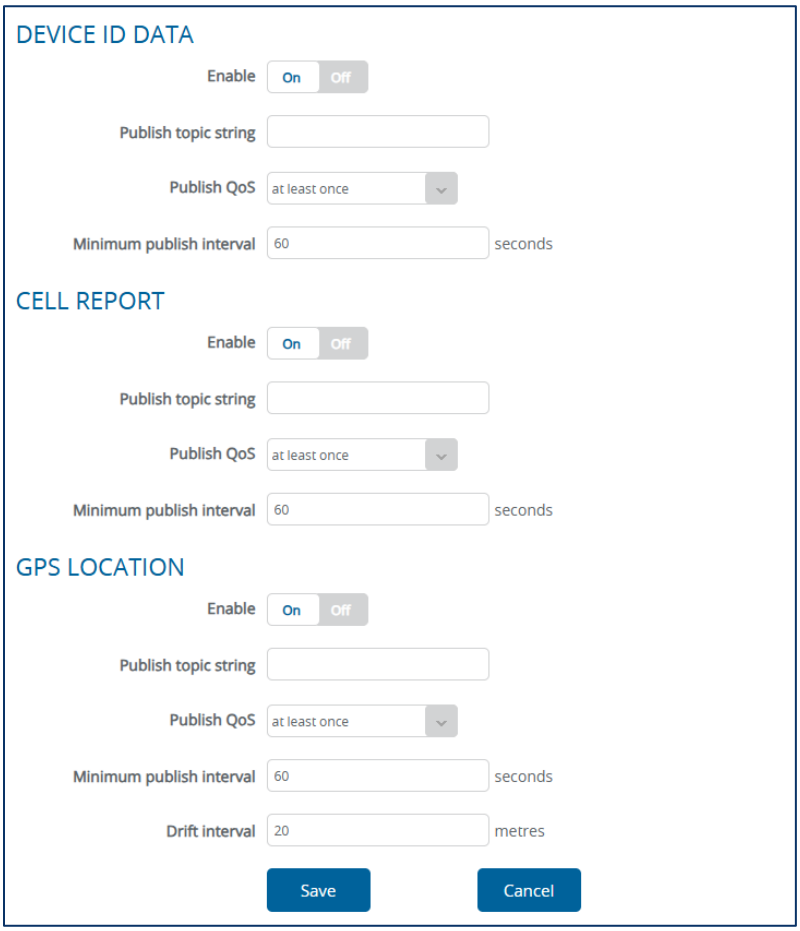


Table 9-19 MQTT Client Topic Items

Item	Description
Device ID Data	
Enable	Set to **On** to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • **At most once** • **At least once** • **Exactly once** At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish level in seconds. This is the amount of time the NTC-550 Series router will wait before attempting to publish a message.
Cell Report	
Enable	Set to **On** to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • **At most once** • **At least once** • **Exactly once** At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish level in seconds. This is the amount of time the NTC-550 Series router will wait before attempting to publish a message.
GPS Location	
Enable	Set to **On** to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.

Item	Description
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • **At most once** • **At least once** • **Exactly once** At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish level in seconds. This is the amount of time the NTC-550 Series router will wait before attempting to publish a message.
Drift interval	Enter the radius. If the device drifts beyond this radius, the message is sent.

5. Click **Save** to create the client. The client displays in the MQTT client list.

Figure 9-21 MQTT – MQTT Client Configuration – MQTT client list

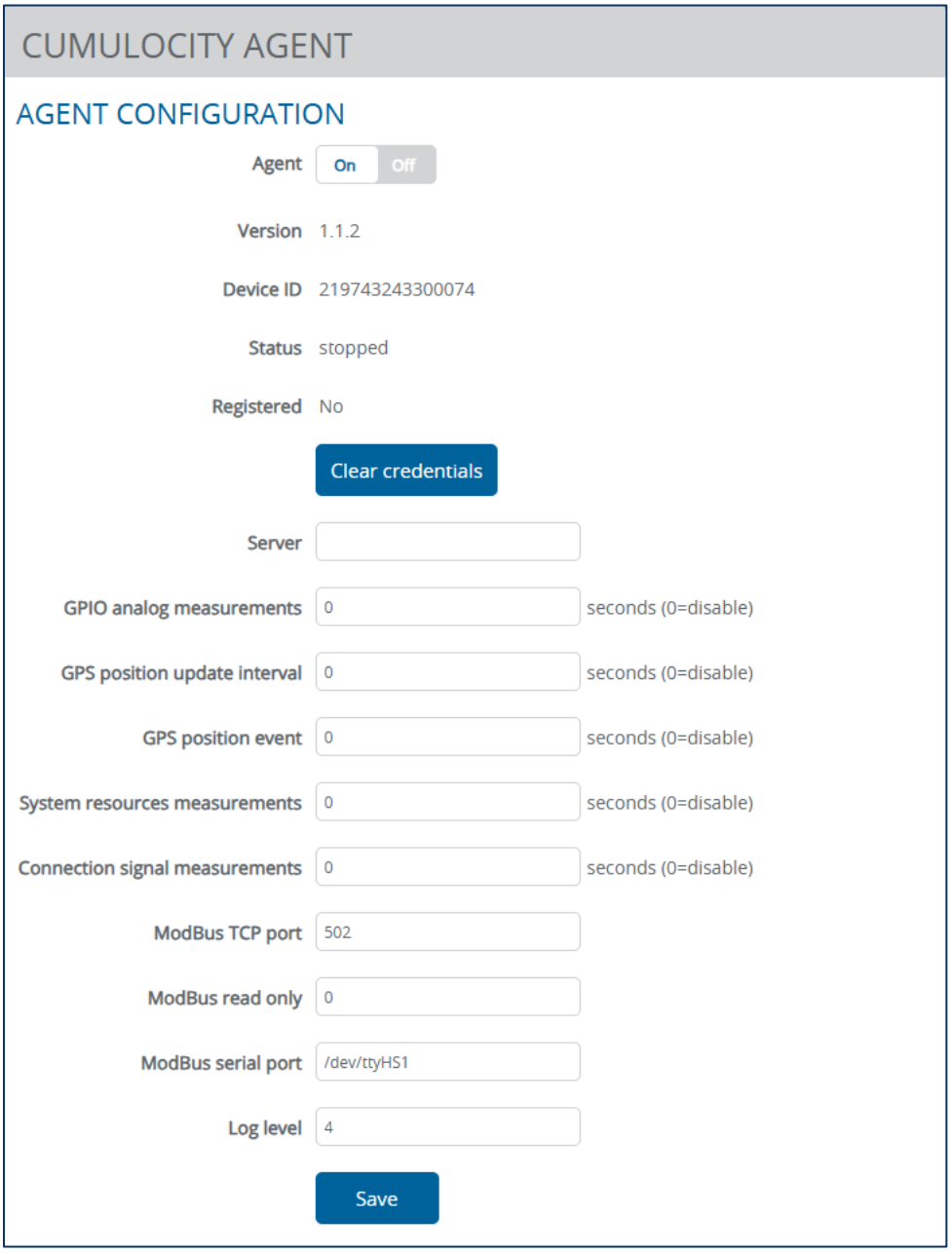
6. Click to edit the client.
7. click to delete the client.

Cumulocity agent

The Cumulocity agent page allows you to configure a cumulocity agent on the NTC-550 Series router which facilitates communication and data exchange between the router and the Cumulocity IoT platform. It enables centralized management and monitoring of devices.

To access the Cumulocity agent page navigate to **Services > Internet of Things > Cumulocity agent**.

Figure 9-22 Cumulocity Agent



The table below lists the Cumulocity Agent configuration details.

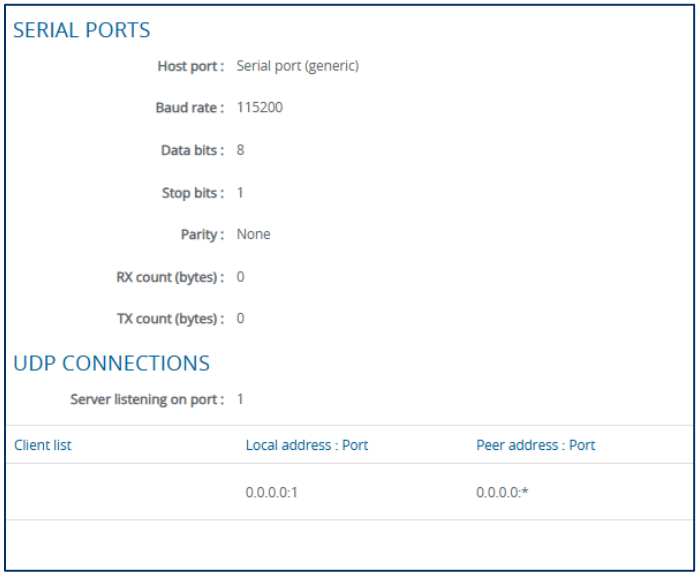
Item	Description
Agent	Set toggle to **On** to enable the agent.

Item	Description
Version	Version of the Cumulocity platform.
Device ID	Router's serial number. A unique identifier for the router in Cumulocity.
Status	Status of the agent.
Registered	Displays if the device is registered with the Cumulocity platform.
Clear credentials button	Click to clear credentials related to an existing cumulocity configuration.
Server	Enter the URL of the Cumulocity platform.
GPIO analog measurements	Enter the time interval at which the General Purpose Input/Output GPIO measurements are communicated.
GPS position update interval	Enter the time interval at which the GPS position is communicated.
GPS position event	Enter the time interval to generate a GPS position event. A GPS position event is generated by the device to report its current geographic location, using the c8y_Position fragment.
System resources measurements	Enter the time interval at which system resource measurements such as CPU usage, memory consumption, disk, and network I/Oare communicated.
Connection signal measurements	Enter the interval at which the cellular signal measurements are communicated.
ModBus TCP port	Enter the sever port for ModBus TCP connection. Default port is 502.
ModBus read only	Enter 0 to disable, 1 to enable.
ModBus serial port	Enter the device serial port for ModBus connection. Default port is /dev/ttyHS1
Log level	Enter the log level to be communicated. The available log levels are: • **1 – dmesg** • **2 – ipsec** • **3 – logread** • **4 – ntcagent**

Serial data status

It shows the details of configured and running data streams.

Figure 9-23 Serial Data Status



Data stream manager

The data stream manager allows you to create mappings between two endpoints on the router. These endpoints may be physical or virtual, for example, a serial port connected to the router's USB port could be configured as an endpoint or you could configure a TCP Server as an endpoint. You can then configure a virtual data tunnel or "stream" between the endpoints.

The data stream manager provides a wide range of possibilities including the forwarding and translation of data between any of the endpoints. For example, you could send the GPS data from the built-in module to a TCP server running on the router. In each case, the logical flow of the stream is from Endpoint A to Endpoint B.

Customers interested in developing their own applications to create custom endpoints and streams can contact Lantronix about our Software Development Kit.

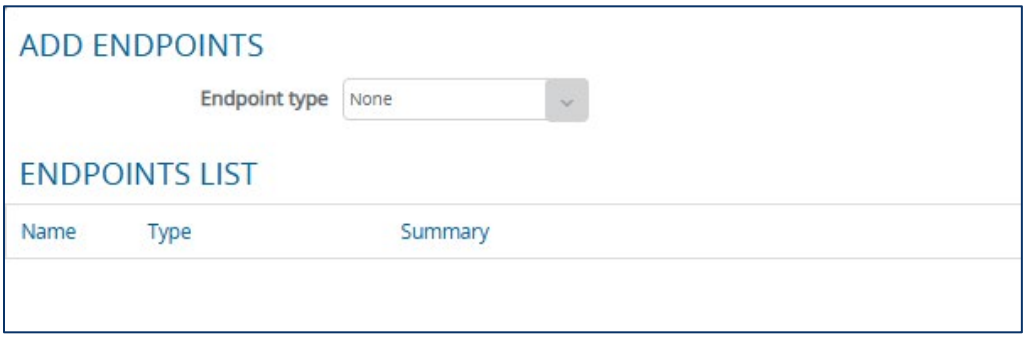
Endpoints

To create a data stream, you must first define endpoints. The NTC-550 Series router allows you to define the following types of endpoints:

- Serial port (generic)
- TCP server
- TCP client
- UDP server
- UDP client
- GPS data (for devices with GPS receiver)
- User defined executable
- RS232 port
- RS485 port
- RS422 port

- Modem emulator
- PPP server
- IP modem
- TCP connect-on-demand
- DNP3 master

To access the Endpoint page, navigate to **Services > Data Stream Manager > Endpoints**.

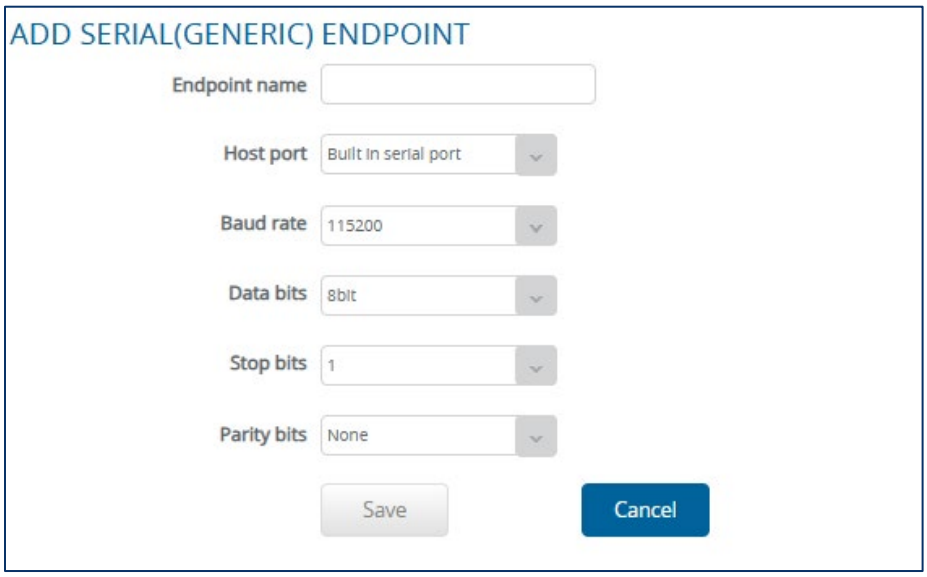


To add an endpoint, select the required **Endpoint type**, the configuration settings for the endpoint display. Once you set the values for all the configuration fields for an endpoint and click Save, the endpoint displays in the Endpoints List.

Serial Port (generic) Endpoint

When a USB to Serial cable is used, this creates a generic serial port as an endpoint defaulting to the commonly used settings as shown below.

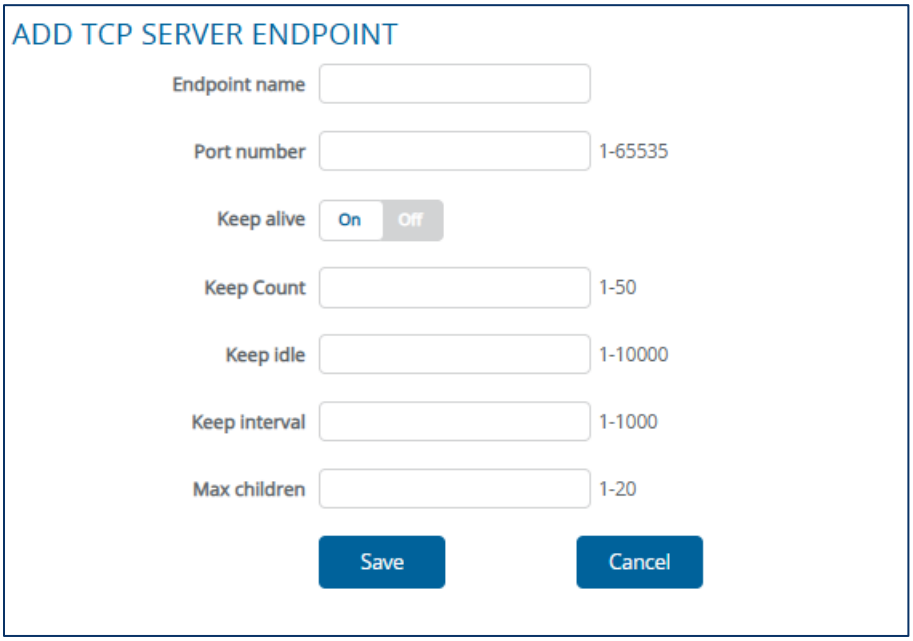
Figure 9-24 Serial Port endpoint Configuration



TCP Server Endpoint

This creates a TCP server endpoint with the following options available.

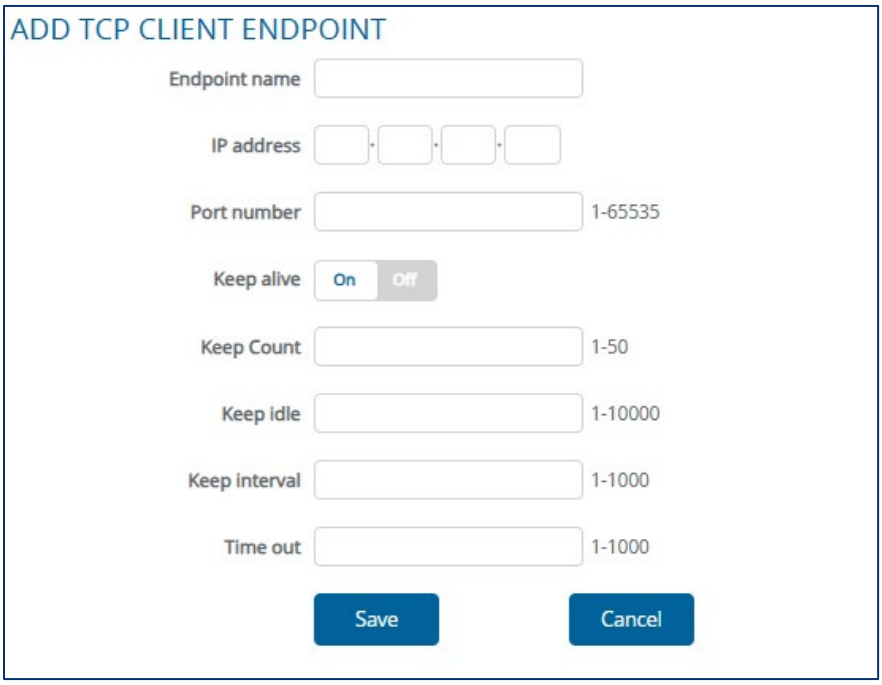
Figure 9-25 TCP Server Endpoint Configuration



TCP Client Endpoint

This creates a TCP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.

Figure 9-26 TCP Client Endpoint Configuration



UDP Server Endpoint

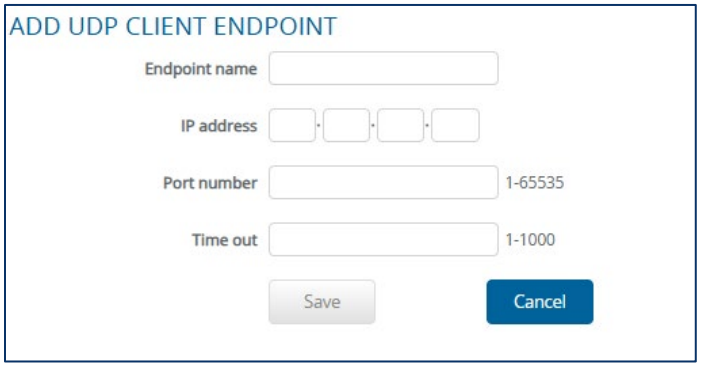
This creates a UDP server endpoint with the following options available.

Figure 9-27 UDP Server Endpoint Configuration

UDP Client Endpoint

This creates a UDP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.

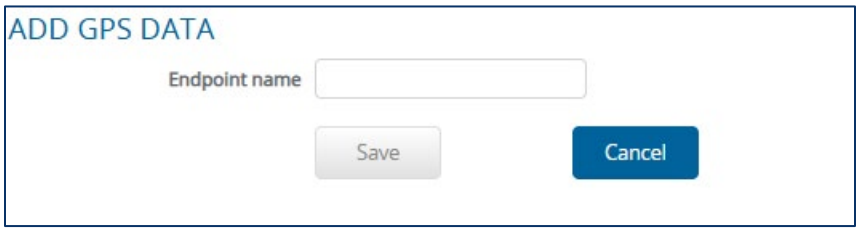
Figure 9-28 UDP Client Endpoint Configuration



GPS Data Endpoint

This creates a GPS data endpoint.

Figure 9-29 GPS Data Endpoint Configuration



User Defined Executable Endpoint

Allows you to specify an executable and parameters to be used as an endpoint. For example, the following executable reads the phone module temperature every second.

```
while true; do rdb_get wwan.0.radio.temperature; sleep 1; done
```

The temperature can then be sent to another endpoint.

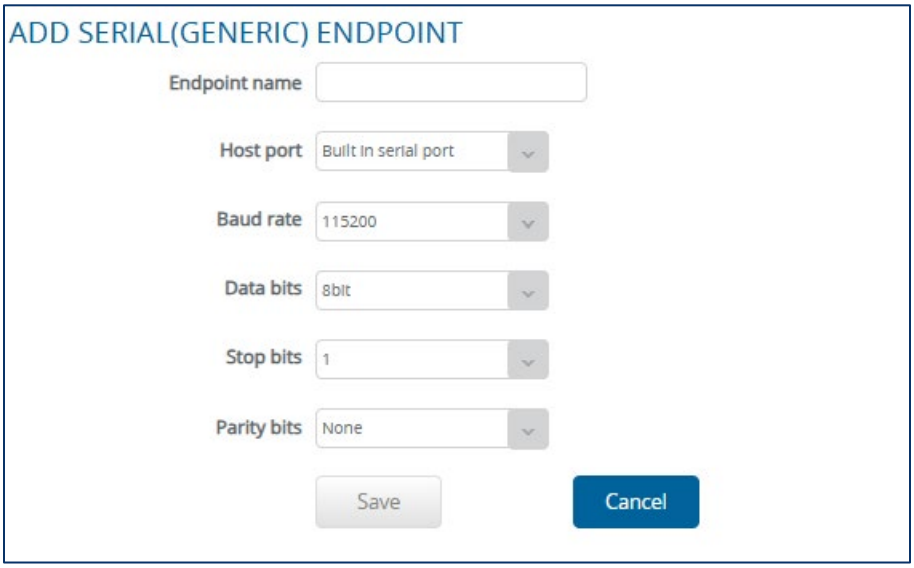
Figure 9-30 User Defined Executable Endpoint Configuration

RS232/RS485/RS422 Port Endpoints

These endpoint types all use the built-in serial port.

When one of these endpoints is used to create a stream, the hardware switches to accommodate the chosen serial communication interface.

Figure 9-31 RS232/RS485/RS422 Port Endpoints Configuration



Modem Emulator Endpoint

Modem emulator allows you to connect legacy equipment such as an RTU or PLC to the serial port of the router in place of a traditional dial-up modem. The NTC-550 Series router emulates the dial-up modem's behaviour and passes the serial data over the IP network.

Figure 9-32 Modem Emulator Endpoint Configuration

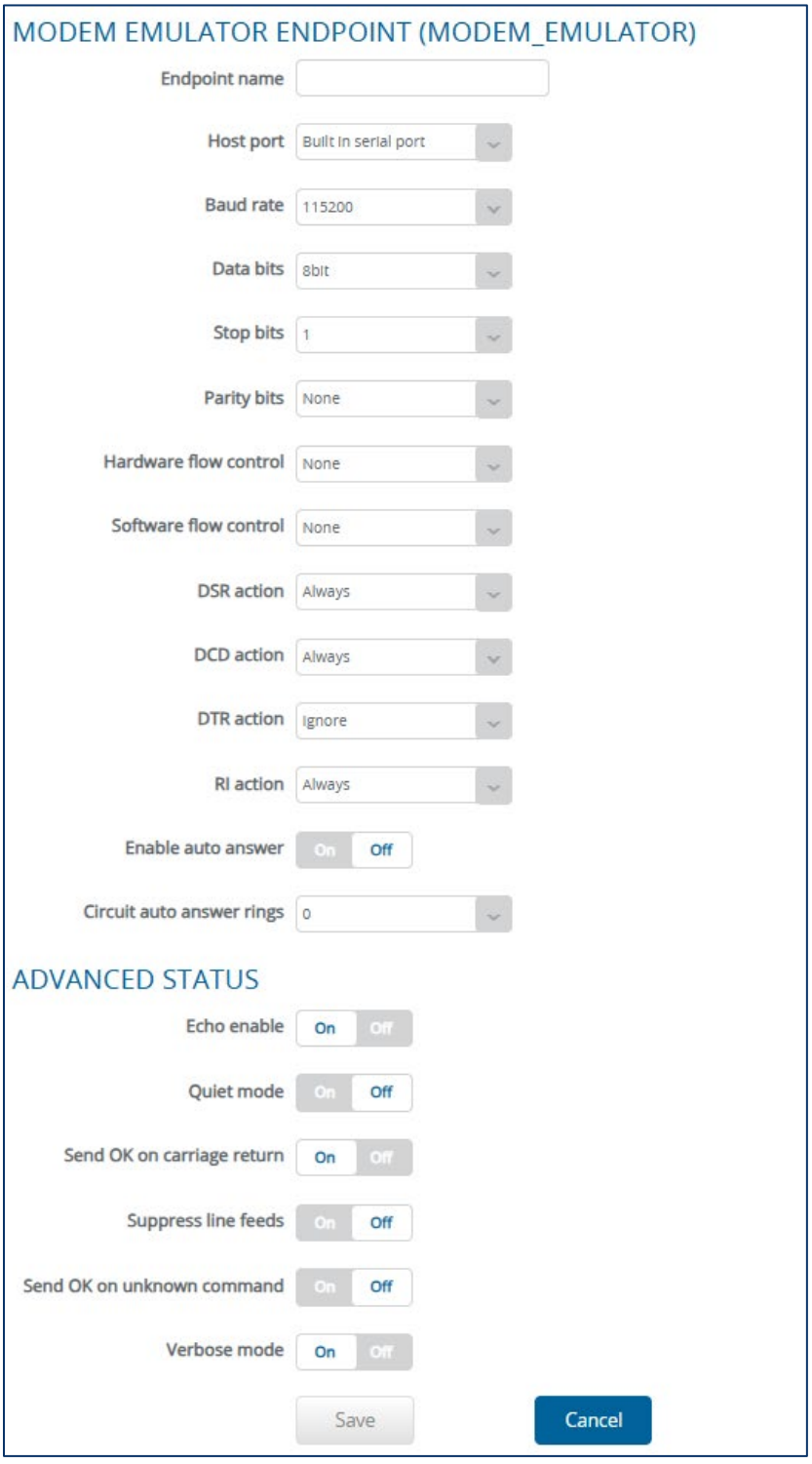


Table 9-20 Modem Emulator Endpoint Configuration Items

Item	Description
Modem Emulator endpoint	
Endpoint name	Enter a name for the endpoint
Host port	Select the serial port to use. If no USB-to-Ethernet adapter is connected, the only available selection is the Built-in serial port.
Baud rate	Select baud rate. The serial (V.24) port baud rate. By default the serial line format is 8 data bits, No parity, 1 Stop bit. Refer to the AT (V.250) AT Command Manual if you need to change the serial line format.
Data bits	Select data bits. The default serial line data bits setting used is 8. Options include 5 – 8 bits.
Stop bits	Select stop bits.The default stop bit setting is set to 1. However, the stop bit setting can be set to 2 bits if required.
Parity bits	Select parity bits. Parity is the means to detect transmission errors. An extra data bit is transmitted with each data character and is arranged in a fashion such that the number of 1 bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then this shows the data must be corrupt. Options include none, odd or even. The default setting is none for no parity checks.
Hardware flow control	Select hardware flow control • **None** – Serial port flow control off • **RTS/CTS** - Serial port uses RTS/CTS flow control
Software flow control	Select software flow control • **None** • **Xon/Xoff**
DSR action	Select the Data Set Ready action. This is an output from the modem and this configuration determines the pin's behaviour. • **Always** – DSR is always on. • **Registered** – When connected to a remote CSD endpoint, sets pin to "on" when modem is in data mode. • **Session established** – When connected to PPP endpoint, sets pin on when PDP is connected, when connected to IP modem endpoint, sets pin to on when modem is in online state (e.g. data connection is established). • **Never** – DSR is always off. • **Mimic DTR** – mimics the DTR pin.
DCD action	Select DCD action. Determines how the router controls the state of the serial port Data Carrier Detect (DCD) line. • **Always On** – DCD is always on.

Item	Description
	• **Connect** – DCD is on when a connection is established in response to an ATD command or DTR dial. • **Session established** – Pin is on when PPP session is in progress or modem is in an online state (e.g. data connection is established). • **Always Off** – DCD is always off.
DTR action	Select DTR action. Determines how the router responds to change of state of the serial port DTR line • **Ignore** – Take no action • **Enter Command State** – when connected to PPP endpoint, this is equivalent to disconnect. When connected to IP modem endpoint, this enters online command state (e.g. process AT commands without dropping the connection). • **Disconnect** – terminates connection.
RI action	Select RI action. Determines how the router controls the state of the serial port RI (Ring Indicator) line. • **Always On**: RI is always on. • **Incoming Ring**: RI is on when an incoming connection request is received. • **Always Off**: RI is always off
Enable auto answer	When enabled, the router accepts incoming connections.
Circuit auto answer rings	Select a value. Sets the number of incoming rings after which the router will answer incoming circuit switched data calls. The default value is Off. The other available options are from 1 to 12.
Advanced Status	
Echo enable	Enables echo on the serial side. All commands are echoes. This can be turned on/off via ATE1 and ATE0 commands. Recommended setting for this option is **On**.
Quiet mode	When **On**, there is no output from the modem on the serial side, i.e. you do not see OK, Connect etc. Recommended setting for this option is **Off**.
Send OK on carriage return	If enabled, will print OK every time CR is received on the serial side. Recommended setting for this option is **On**.
Suppress line feeds	If enabled, line termination is using CR (13). If disabled, line termination is CR LF (13 10). Recommended setting for this option is **Off**.
Send OK on unknown command	Will send OK when an unknown/invalid AT command is received. Recommended setting for this option is **On**.
Verbose mode	The modem returns messages to the computer to indicate the return status of commands and interrupts such as incoming call and call progress. Recommended setting for this option is **On**.

PPP Server Endpoint

Figure 9-33 PPP Server Endpoint Configuration

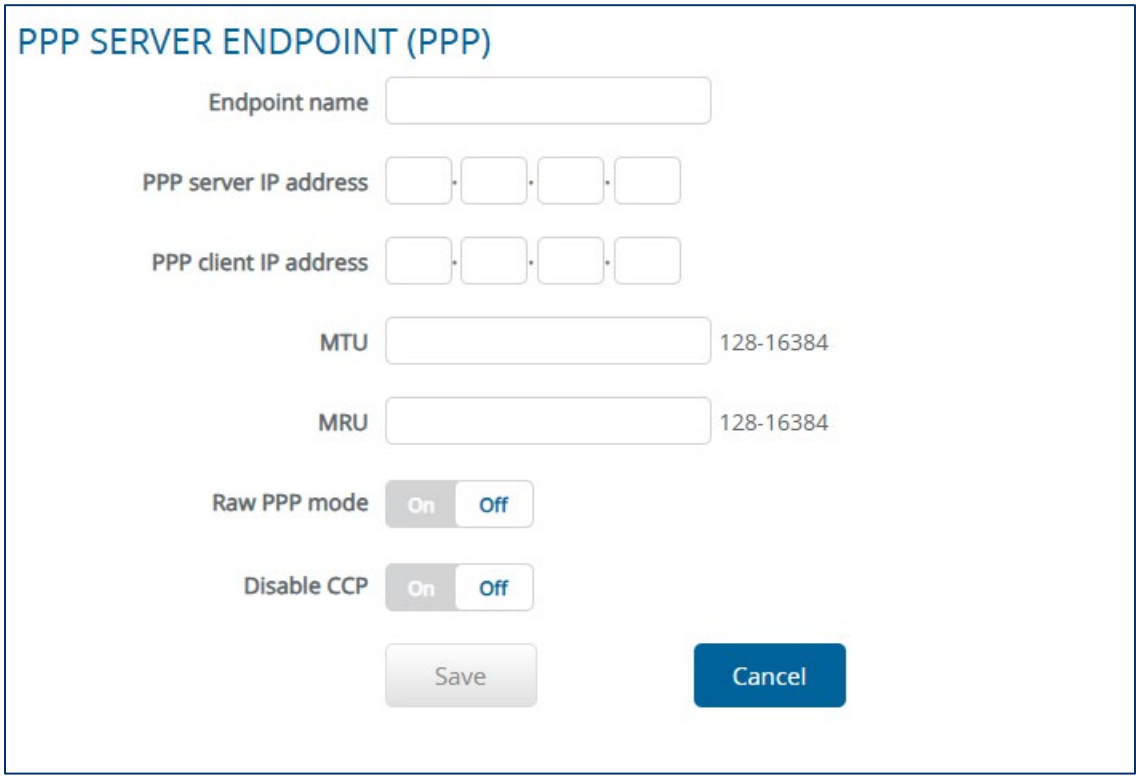


Table 9-21 PPP Server Endpoint Configuration Items

Item	Description
PPP server IP address	Enter IP address of the PPP server. This defaults to the router's current IP address.
PPP client IP address	Enter IP address of the PPP client. This defaults to the next IP address in the DHCP range after the router's address.
MTU	Enter maximum transmission unit size of packets sent by the PPP server.
MRU	Enter the maximum receive unit size of packets received by the PPP server.
Raw PPP mode	This option is provided for compatibility with legacy devices that assume there is a line available and do not require dial commands to be issued first. Raw PPP mode is turned **Off** by default.
Disable CCP	This option is provided for use with devices that do not support the compression control protocol. The router uses the compression control protocol and the toggle key is in the **Off** position by default.

IP Modem Endpoint

This endpoint can be used to connect to the modem emulator endpoint to achieve similar functionality to PAD Daemon. It allows a data stream from the serial port to a TCP/UDP server/client and provides modem control lines and AT interpreter on the serial side.

Figure 9-34 IP Modem Endpoint Configuration

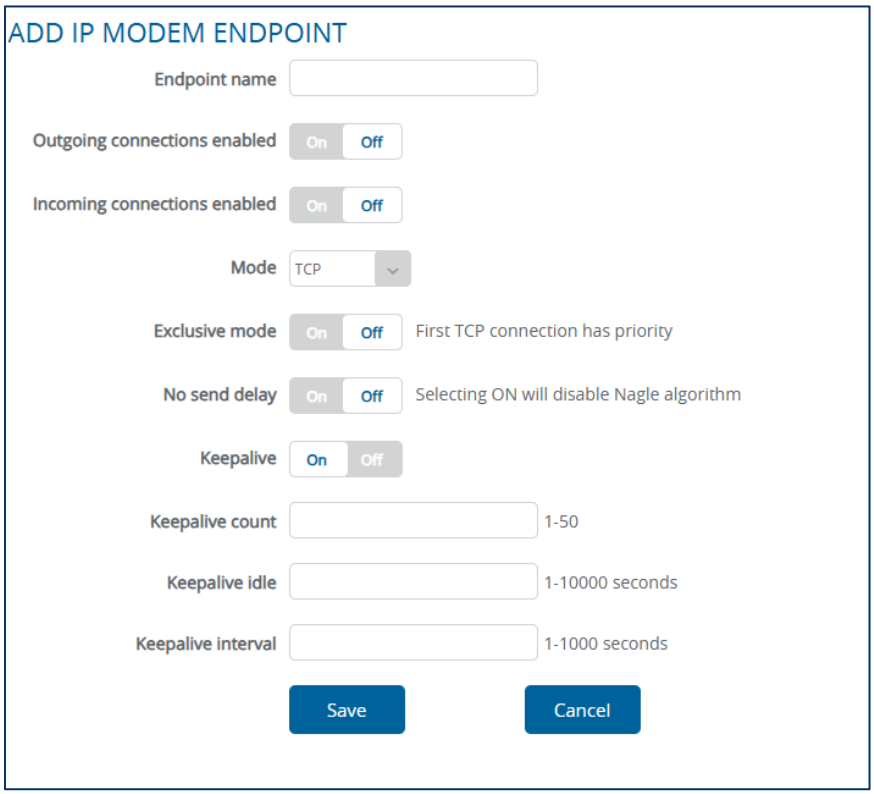


Table 9-22 IP Modem Endpoint Configuration Items

Item	Description
Outgoing connections enabled	Enables or disables the ability of the router to initiate outbound network connections i.e. act as a networking client. It will attempt to connect to the remote server when relevant activity is detected on the serial side e.g. ATD dial command.
Incoming connections enabled	Enables or disables the ability of the router to accept incoming network connections i.e. act as a networking server. When an incoming connection from a remote client is detected, the router simulates a dial-in call on the serial line.
Mode	Sets the IP modem to either TCP or UDP mode.
Exclusive mode (TCP mode only)	When this is **Off**, any new client connection disconnects the previous client connection and uses a new client instead.
No send delay	Disables Nagle algorithm. Disabling this is sometimes important so that serial data is sent as soon as possible instead of waiting for a more optimal block

Item	Description
	of data for Ethernet. Enabling this effectively reduces latency but increases the amount of network traffic.
Keepalive	Keepalive sends a message to check that the link is still active or to keep it active. When enabled the below fields display.
Keepalive count	Enter the number of keepalive messages to send.
Keepalive idle	Enter the duration between two keepalive transmissions when in idle condition.
Keepalive interval	Enter the duration between two successive keepalive retransmissions.

TCP Connect-on-demand Endpoint

The TCP connect-on-demand endpoint allows data to be buffered and then sent to a TCP server when the buffer has been filled. It is primarily useful in situations where you do not want 'keep alive' packets to keep the socket open and create an overhead when the TCP data connection is not in use.

Figure 9-35 TCP Connect-on-demand Endpoint Configuration

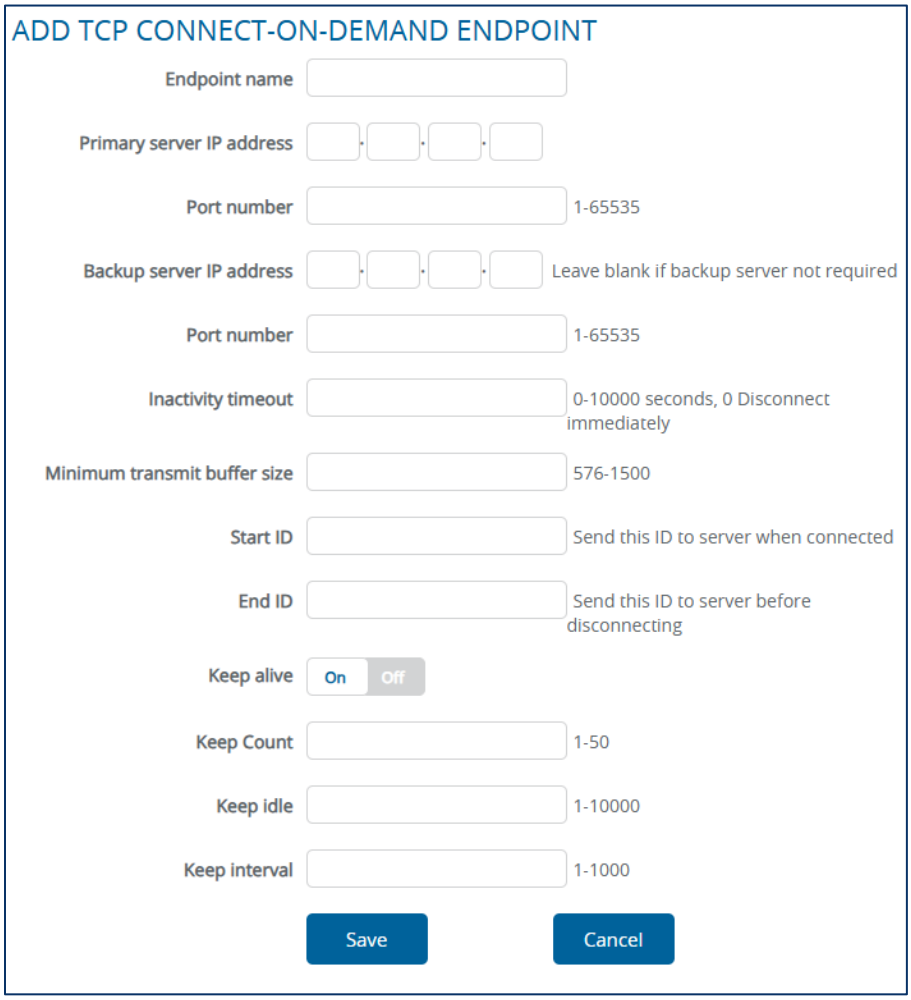
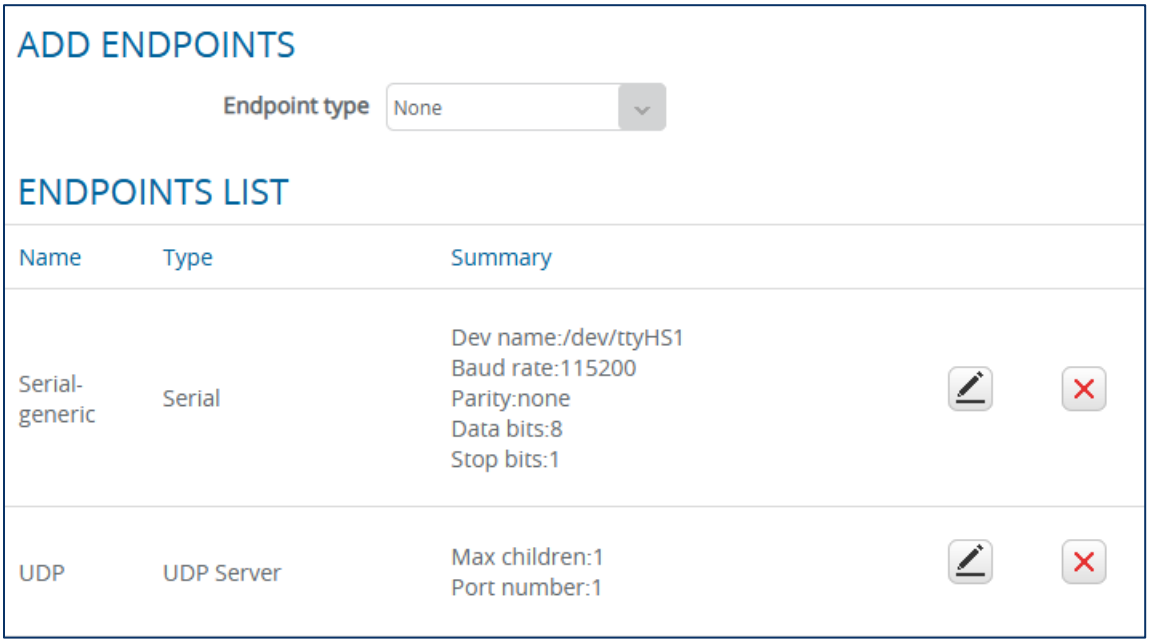


Table 9-23 TCP Connect-on-demand Endpoint Configuration Items

Item	Description
Primary server IP address	Enter IP address of the TCP server to which the router should attempt the initial connection.
Port number	Enter the port number that the TCP server operates on.
Backup server IP address	Enter IP address. If connection to the primary server fails, the router will attempt to connect to this address.
Port number	Enter the port number that the backup TCP server operates on.
Inactivity timeout	Enter the period, in seconds, that the socket is considered idle/inactive if no packets are sent. The timer begins at the end of the last sent packet. The valid range is 0-10000 seconds. If this field is set to 0, the client disconnects immediately after sending a packet.
Minimum transmit buffer size	Entre the number of bytes that must be reached before the client decides to transmit.
Start ID	This is a string which, if configured, is sent before any serial data is sent, every time the client connects <START ID><SERIAL DATA>
End ID	This is a string which, if configured, is sent after all serial data, just before the client disconnects <START ID><SERIAL DATA><END ID>
Keepalive	Keepalive sends a message to check that the link is still active or to keep it active. When enabled the below fields display.
Keepalive count	Enter the number of keepalive messages to send.
Keepalive idle	Enter the duration between two keepalive transmissions when in idle condition.
Keepalive interval	Enter he duration between two successive keepalive retransmissions.

The configured endpoints display in the Endpoints List.

Figure 9-36 Endpoints List



Click to edit that endpoint and click to delete that endpoint

Data stream

When you have created the required endpoints, you can then proceed to set up a data stream. A data stream sends data from one endpoint to another, performing any transformation of the data as required. When a stream is added, an underlying process on the router checks the validity of the stream, checking for conflicts and illogical configurations.

Important:

- *When any changes to the Data stream manager configuration are detected, all data streams are stopped and restarted as per the new configuration.*
- *Multiple Modbus clients cannot connect simultaneously to Modbus serial slaves connected to the router.*

To access the Data stream page, navigate to **Services > Data Stream Manager > Data Stream**

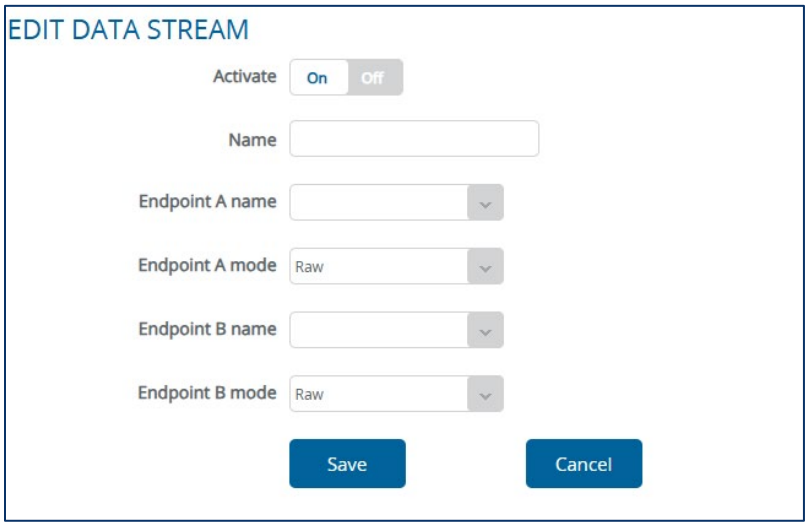
Figure 9-37 Data Stream List

Every Data stream requires two endpoints, Endpoint A and Endpoint B. In all cases, the flow of data is from Endpoint A to Endpoint B.

To create a new Data stream:

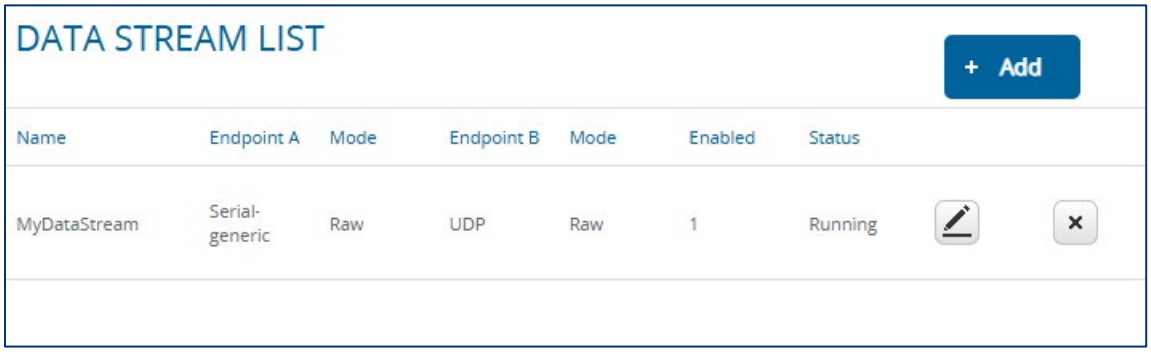
1. Click **+Add** in the Data Stream List, the Edit Data Stream page displays.

Figure 9-38 Edit Data Stream Configuration



2. Set **Activate** toggle to **On** to activate the Data stream.
3. In the **Data stream name** field, enter a name for the Data stream.
4. For **Endpoint A name** field, select one of the endpoints you created previously. This endpoint should be the starting point of the stream.
5. For **Endpoint A mode** field, select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it leaves this endpoint. For example, if Endpoint A type is Serial port (generic), the Mode can be set to various Modbus server and client types. This means that upon arrival at Endpoint A, the data will be transformed into the chosen Modbus format, ready to be sent to Endpoint B.
6. For **Endpoint B name** field, select one of the endpoints you created previously. This endpoint should be the destination of the stream.
7. For **Endpoint B mode** field, select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it arrives at this endpoint.
8. Click **Save**, the new Data stream displays in the Data Stream List.

Figure 9-39 Data Stream List with created Data Stream

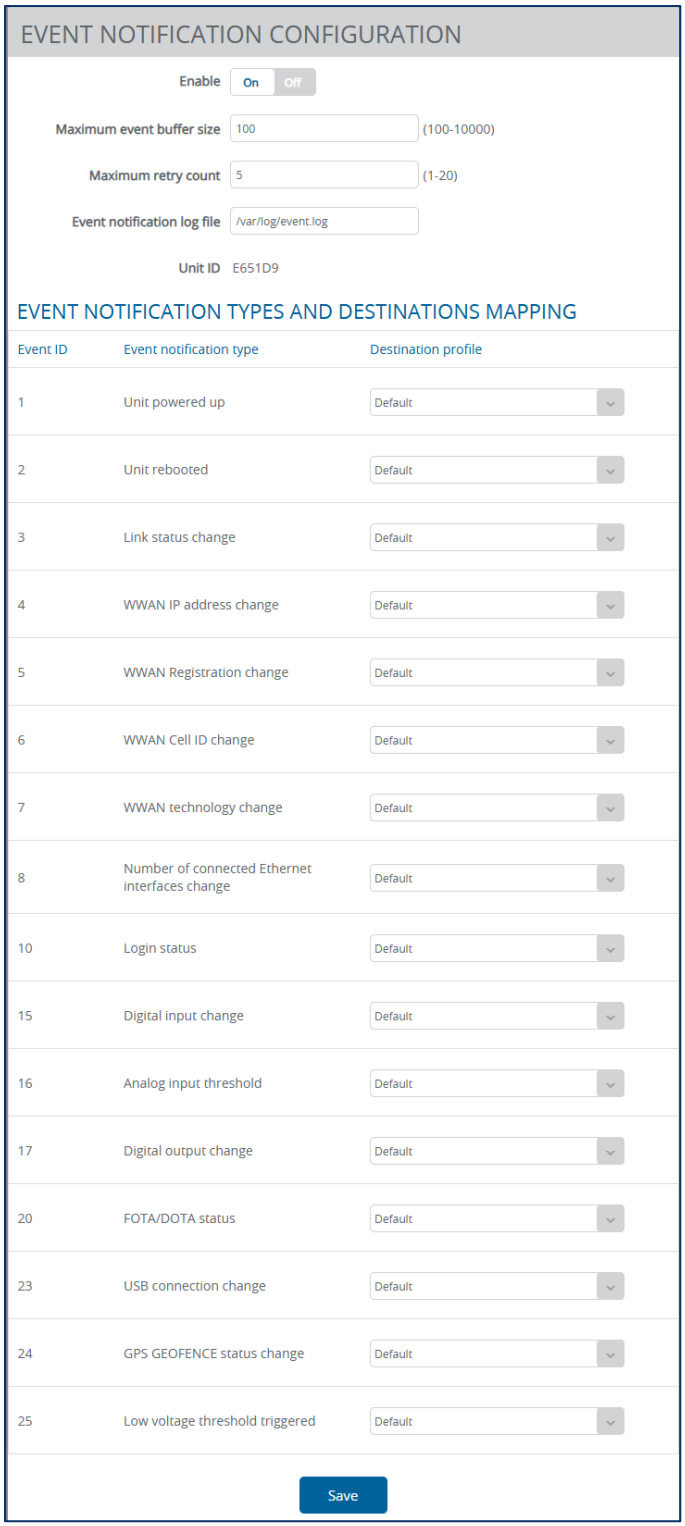


Click to edit that Data stream, Click to delete that Data stream.

Event Configuration

The NTC-550 Series router can be configured to send notifications when certain events occur on the router. These notifications can be used for proactive monitoring of events such as unit reboots and Ethernet link changes.

Figure 9-40 Event Notification – Configuration



Event Notification Configuration

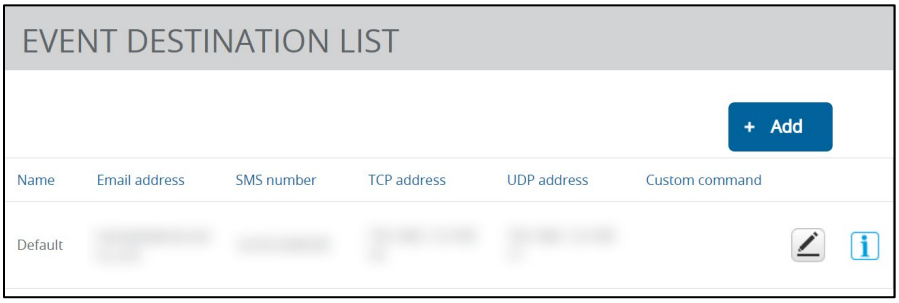
To configure Event Notifications:

1. Enable event notifications by setting the **Enable** toggle to **On.**
2. In the **Maximum buffer event size** field, specify the buffer size for event notifications which failed to be delivered or are yet to be sent.
3. In the **Maximum retry count** field, enter the number of times the NTC-550 Series router should attempt to deliver the notification in the event of a delivery failure.
4. If required, adjust the output location of the **Event notification log file.**
5. For each of the **Event Notification Types** select the **Destination Profile** which should send the notification when the notification is triggered. For details on how to configure the Destination Profiles, view the **Destination Configuration** section.
6. Click **Save** to apply the configuration.

Destination configuration

The **Destination Configuration** page allows for the configuration of the Event Destination List, which specifies where notifications should be sent when they are triggered.

Figure 9-41 Log – Event destination list

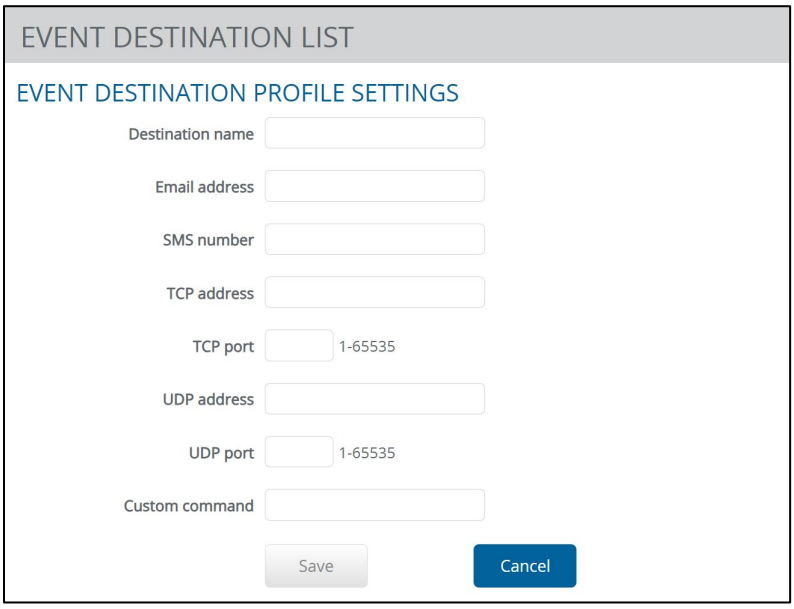


Multiple destinations can be configured and assigned to different event types, depending on what notifications need to be sent.

To configure or edit an event destination:

1. Click **+Add** button to add a destination or the button to edit an existing destination. The Event Destination Profile Settings page opens.

Figure 9-42 Services – Event configuration – Destination Configuration – Event Destination Profile settings

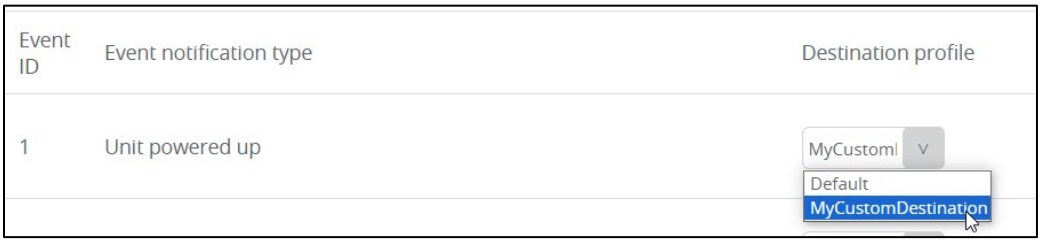


2. In the Destination name field enter a name to identify the destination profile. This name will appear on the Event Notification Configuration page, in the Destination Profile column.

Note: *The Email address, SMS number, TCP address, UDP address and Custom command fields listed below are all optional. Complete the fields which should be included when a notification is sent. The TCP port and UDP port fields are required if using a TCP address or UDP address.*

3. In the **Email address** field, enter an email address to receive the notification.
4. In the **SMS number** field, enter a phone number to receive the notification as an SMS.
5. In the **TCP address** and **TCP port** fields, enter a TCP address and TCP port to receive the notification over TCP.
6. In the **UDP address** and **UDP port** fields, enter a UDP address and UDP port to receive the notification over UDP.
7. In the **Custom command** field, enter a custom command to execute when the notification is triggered. The command should be a bash compatible command.
8. Select the **Save** button to save the destination profile.
9. Apply the destination profile by returning to the **Event Configuration > Event Notification Configuration** page.
10. Set the **Destination profile** dropdown on the appropriate Event Notification and Destination Mapping item to the new destination.

Figure 9-43 Services – Event Configuration – Destination profile mapping

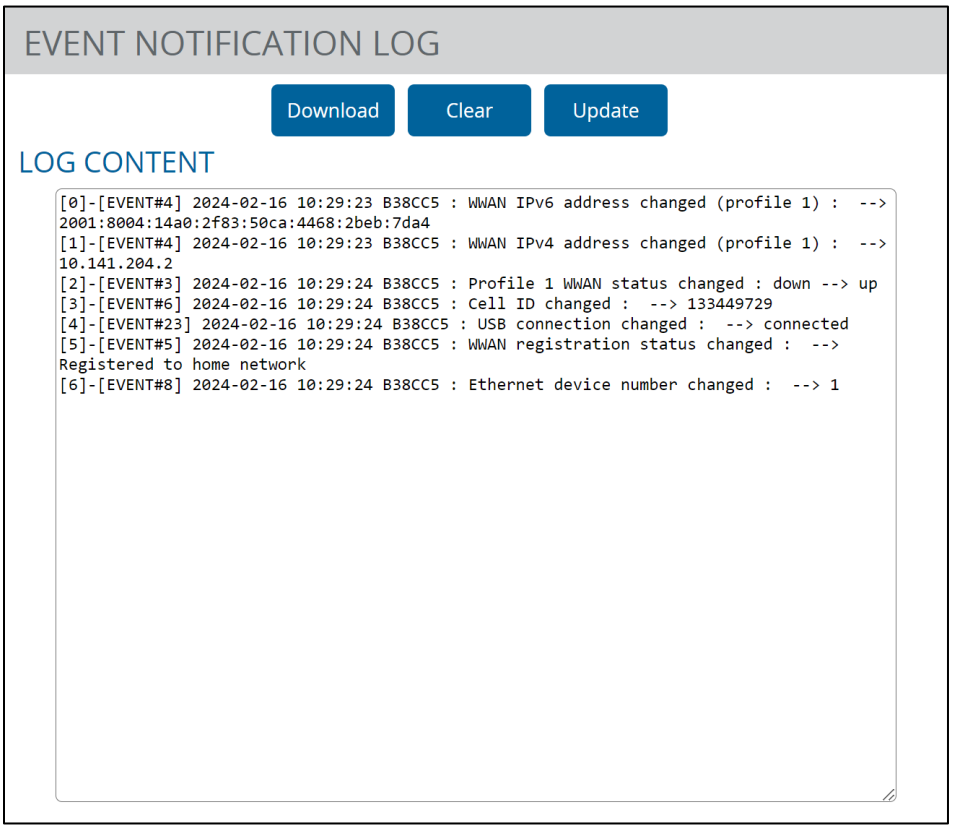


11. Click **Save** button at the bottom of the **Event Notification Configuration** page.

Event notification log

The **Event Notification Log** displays a log of Events which have been triggered. Click **Update** button to refresh the content in the Log Content window. Click **Download** button to download a log file for review in an external application. Click **Clear** button to clear the log.

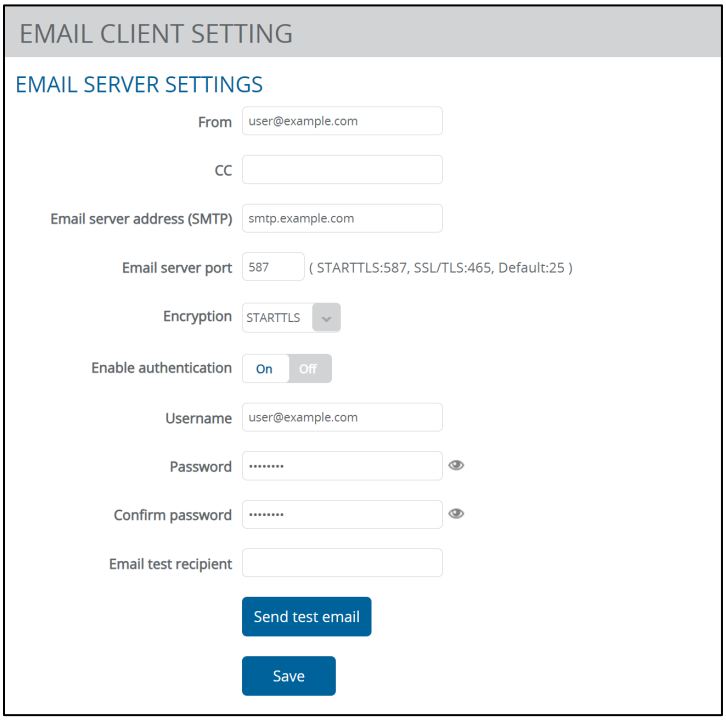
Figure 9-44 Services – Event Configuration – Event notification log



Email Settings

The email settings page is used to configure the SMTP server to be used to deliver Event Notifications (configured in the Event notification configuration section).

Figure 9-45 Email Client Setting



The table below lists the Email Server Settings Configuration Details

Table 9-24 Email Server Settings Configuration Items

Item	Description
From	Enter Email address that should represent sender of the email notification.
CC	Enter Email address or addresses that the notification should be sent to.
Email server address (SMTP)	Enter Domain name of the SMTP server that the email should be sent through.
Email server port	Enter the port that the SMTP server is expecting email on. The port varies depending on the encryption type used, refer to your email provider's SMTP instructions on which port is correct. The available encryption types are **STARTTLS (Port 587), SSL/TLS (Port 465),** or **Default (Port 25).**
Encryption	Select the encryption type from the drop-down. Available types are **STARTTLS, SSL/TLS, None.**
Enable authentication	Set toggle to **On** if the SMTP server is expecting authentication.
Username	Enter Username to authenticate with the SMTP server.
Password	Enter Password to authenticate with the SMTP server.

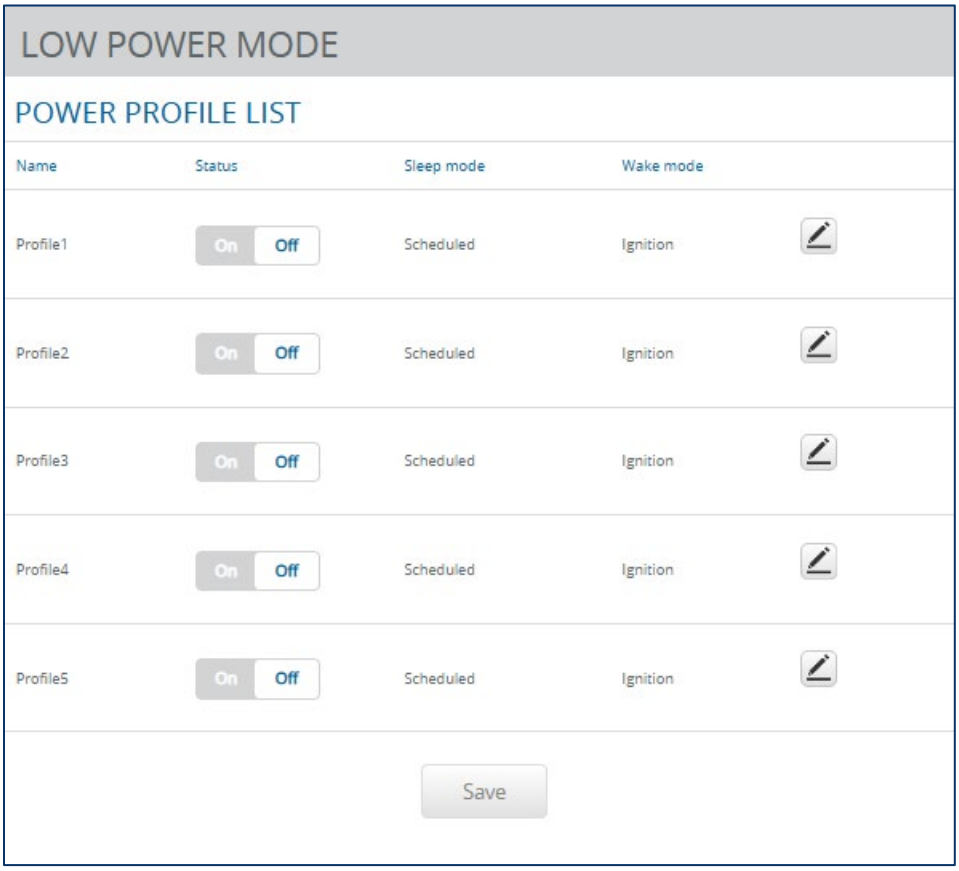
Item	Description
Confirm password	Re-enter the password to authenticate with the SMTP server.
Email test recipient	Enter recipient email address here after completing the previous details to test the SMTP configuration.
Send test email button	Click to send the test email to the address configured in the **Email test recipient** field.

Click **Save** to save and apply the settings.

Low power mode

The Low power mode page provides an overview of the power profiles and allows you configure them. Up to five power profiles can be configured and all of them can be active simultaneously.

To access the Low power mode page, navigate to **Services > Low power mode**.

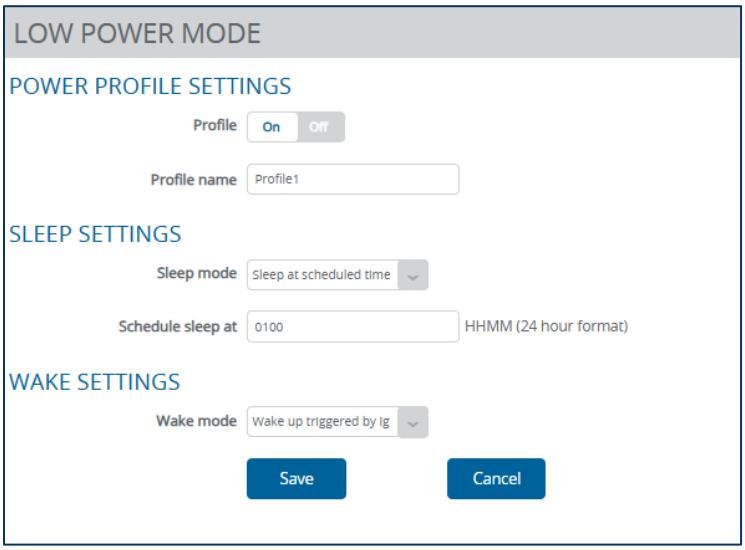


The **Status** column indicates whether the profile is active, while the **Sleep mode** and **Wake mode** columns display the method set for router sleep and wake functions.

Important: *When configuring multiple power profiles, be careful so that they do not overlap or conflict with one another, for example, configuring a schedule which wakes up the unit when another profile has it scheduled to be in low power mode.*

Click to edit that profile.

Figure 9-46 Low Power Mode Configuration



The table below lists the Low Power Mode configuration details.

Table 9-25 Low Power Mode Configuration Items

Item	Description
Power Profile Settings	
Profile	Set to **On** to activate the profile
Profile name	Enter a name for the profile.
Sleep Settings	
Sleep mode	Select Sleep mode from the following options: • **Sleep triggered by Ignition pin** • **Sleep after timer** • **Sleep at scheduled time** The Sleep mode selects the condition for the router to enter sleep mode.
Remain awake after ignition off	Enter the duration for which the router should remain awake after ignition is off, when Sleep mode is selected as **Sleep triggered by Ignition pin**.
Sleep after timer	Enter the duration after which the router should go to sleep mode, when Sleep mode is selected as **Sleep after timer**.
Schedule sleep time	Enter the time when the router should go to sleep mode, when Sleep mode is selected as **Sleep at schedule time**.
Wake mode	Select Wake mode from the following options: • **Wake up triggered by Ignition pin** • **Wake up triggered by bt button** • **Wake at scheduled time** The Wake mode selects the condition for the router to wake up.

Item	Description
Schedule wake up at	Enter the time when the router should wake up, when the Wake mode is selected as **Wake at scheduled time**.

Click **Save** to save the settings, the configured profile displays in the Power Profile List.

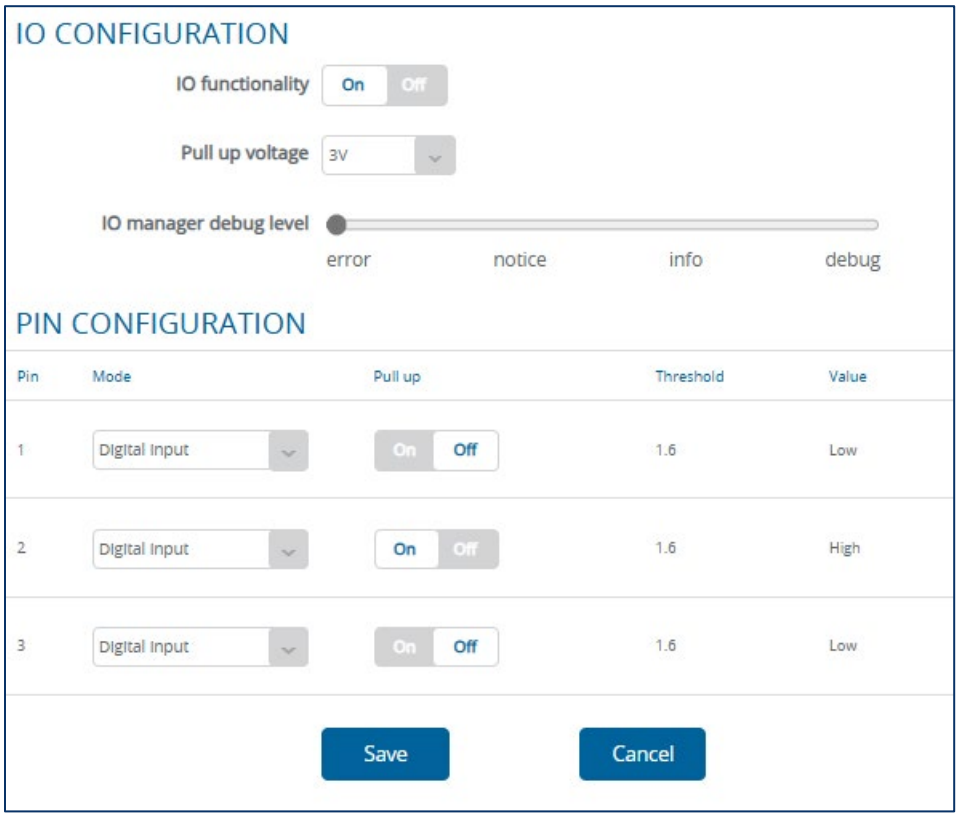
IO configuration

The NTC-550 Series router is equipped with a 6-way terminal block connector providing three identical multipurpose inputs and outputs as well as a dedicated ignition input. These inputs and outputs may be independently configured for various functions, including:

- NAMUR (EN 60947-5-6 / IEC 60947-5-6) compatible proximity sensor input
- Proximity sensor input for use with contact closure (open/closed) type of sensors (PIR sensors, door/window sensors for security applications) with the input tamper detection possible (four states detected: open, closed, short and break) using external resistors
- Analogue 0V to 30V input
- Digital input (the I/O voltage measured by the iMX283 LRADC and the software making decision about the input state) with the threshold levels configurable in software
- Open collector output.

To access the IO configuration page, navigate to **Services > IO configuration**.

Figure 9-47 IO Configuration



Use the pull up voltage options to select the desired output voltage of the I/O pins. The pull up voltage you select will be the same for each pin when pull up is enabled for that pin. Each pin is capable of outputting either 3 V or 8.2 V.

The table below lists the IO configuration details.

Table 9-26 IO Configuration Items

Item	Description
IO Configuration	
IO Functionality	Enables the configuration of the input and output pins on the four-way terminal block connector.
Pull up voltage	Specifies the output voltage of the I/O pins.
IO Manager Debug level	Use the slide bar to adjust the level of detail you would like to see in the log for IO messages. A higher debug level displays more detailed messages in the log file.
Pin Configuration	
Pin	The I/O pin number corresponding to the pin on the 6-way terminal block connector that you wish to configure.
Mode	The mode of operation for the corresponding pin. Available options are: • **Digital Input** – The corresponding pin accepts digital input. Pull up may be on or off and both 3 V and 8.2 V are available as pull up voltages. The value column displays whether the signal received on the pin is High or Low. The default value is High. When the I/O pin is shorted to ground the value changes to Low. • **Digital Output** – The corresponding pin outputs a digital signal. Pull up may be on or off and both 3 V and 8.2 V are available as pull up voltages. The value column contains a toggle key allowing you to set whether the output signal is High or Low. When set to Low, the output of the I/O pin is 0 V. When set to High, the output of the I/O pin is 5 V. • **Analogue input** – The corresponding pin accepts an analogue signal. Pull up may be on or off and both 3 V and 8.2 V are available as pull up voltages. The value column displays the current voltage detected on the pin. • **Namur input** – NAMUR is a sensor standard using low-level current signals. It can supply two different signal levels depending on the state of the switch and is commonly used in hazardous or explosive locations where compact sensors are required. When a pin is set to NAMUR mode, Pull up is turned on and the global Pull up voltage is set to 8.2 V. These settings may not be changed for as long as a pin is set to NAMUR mode as they are required settings according to the NAMUR IEC 60947-5-6 standard.

Item	Description
	The value column displays whether the signal received on the pin is High or Low. • **Contact closure input** –A common type of digital input where a sensor or switch opens or closes a set of contacts as a result of a process change. An electrical signal is then used to determine whether the circuit is open or closed. When a pin is set to Contact closure input, Pull up is enabled for that pin and may not be turned off as long as the pin remains configured as a Contact closure input. Global pull up voltage may be either 3 V or 8.2 V.
Pull up	Use the pull up toggle keys to turn the pull up **On** or **Off** for the corresponding pin. When turned **On**, the pull up voltage output is the value specified in the "Pull up voltage" option in the IO configuration section of this dialog box.
Threshold	Displays the current voltage threshold configured for the I/O pin.
Value	The value column displays whether the voltage detected on the line is low or high or allows you to set the output value to high or low. This can be useful for applications where monitoring of the transition between low and high is used to trigger an action.

Click **Save** to save the settings.

⚠ ***Important:*** *Please refer to the SDK Developer Guide for hardware information about the Input/Output pins, wiring examples and configuration of the pins via the command line interface. There are also wiring examples in Appendix J of this User Guide.*

10. System

Log

The Log section allows you to download the System logs, Diagnostic logs and IPSec logs on the router.

System log

The System Log enables you to troubleshoot any issues you may be experiencing with your NTC-550 Series router. To access the System Log page, navigate to **System > Log > System log**

The Log Filter Level allows you to select the type of logs you want to download

Table 10-1 Log – System Log Filter Level

ITEM	DEFINITION
Debug	Shows extended system log messages with full debugging level details.
Info	Shows informational messages only.
Notice	Shows normal system logging information.
Warning	Shows warning messages only.
Error	Shows error condition messages only.

Once you have selected the Log Filter Level, click **Download** to download the log file.

The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

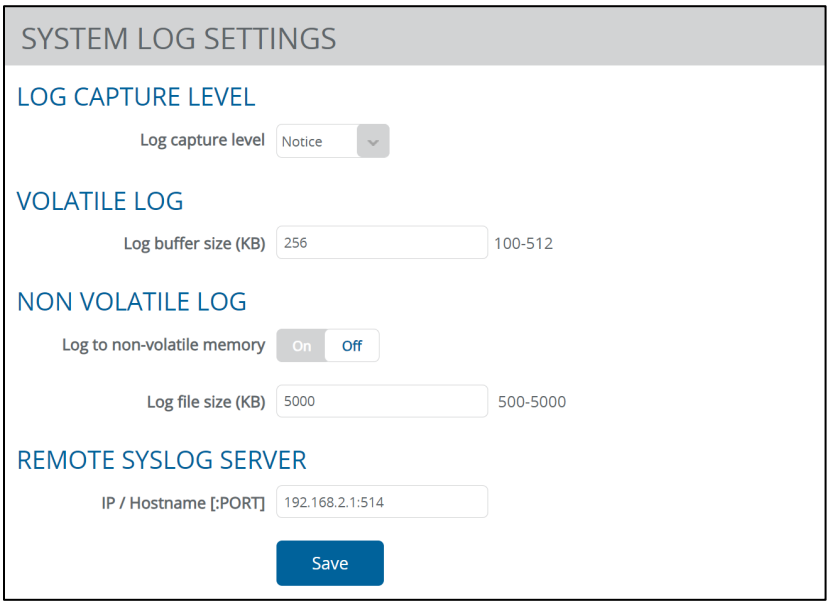
System log settings

To access the System log settings, navigate to **System > Log > System log settings**.

Log data is stored in RAM and therefore when the unit loses power or is rebooted the RAM will lose any log information stored in the RAM. To ensure that log information is accessible between reboots of the router there are two options:

- Enable the Log to non-volatile memory option.
- Use a Remote syslog server.

Figure 10-1 Log – System log settings



Log capture level

The log capture level defines the amount of detail that the system log stores. This setting also affects the Display level setting on the System log page, for example, if this is set to a low level, such as “Error”, the System log will not be able to display higher log levels.

Table 10-2 Log - System Log Settings – Log Capture Level

Item	Definition
Debug	Shows extended system log messages with full debugging level details.
Info	Shows informational messages only.
Notice	Shows normal system logging information.
Warning	Shows warning messages only.
Error	Shows error condition messages only.

Volatile Log

The size of the volatile log buffer can be configured to store larger logs if required. The default is 256KB.

Non-volatile Log

When the router is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the router. Up to 512kb of log data will be stored before it is overwritten by new log data. Flash memory has a finite number of program-erase operations that it may perform to the blocks of memory.

While this number of program-erase operations is quite large, we recommend that you do not enable this option for anything other than debugging to avoid excessive wear on the memory.

Remote syslog server

The router can be configured to output log data to a remote syslog server. This is an application running on a remote computer which accepts and displays the log data. Most syslog servers can also save the log data to a file on the computer on which it is running allowing you to ensure that no log data is lost between reboots.

To configure the NTC-550 Series router to output log data to a remote syslog server enter IP address or hostname of the syslog server in the **IP / Hostname [:PORT] field** in Remote Syslog Server section. You can also specify the port number after the IP or hostname by entering a semi-colon and then the port number e.g. 192.168.1.102:514. If you do not specify a port number, the router will use the default UDP port 514.
Click **Save** to save the setting.

Figure 10-2 Log – System log settings – Remote syslog server

Diagnostic log

The router may be configured to enable the collection of diagnostic logs for the purpose of troubleshooting problems. These log files are intended for use by Lantronix technicians. By default, this feature is disabled and should only be enabled if you are trying to find out the cause of a problem and are instructed to enable this by Lantronix technical support staff.

Figure 10-3 Log – Diagnostic log configuration and download

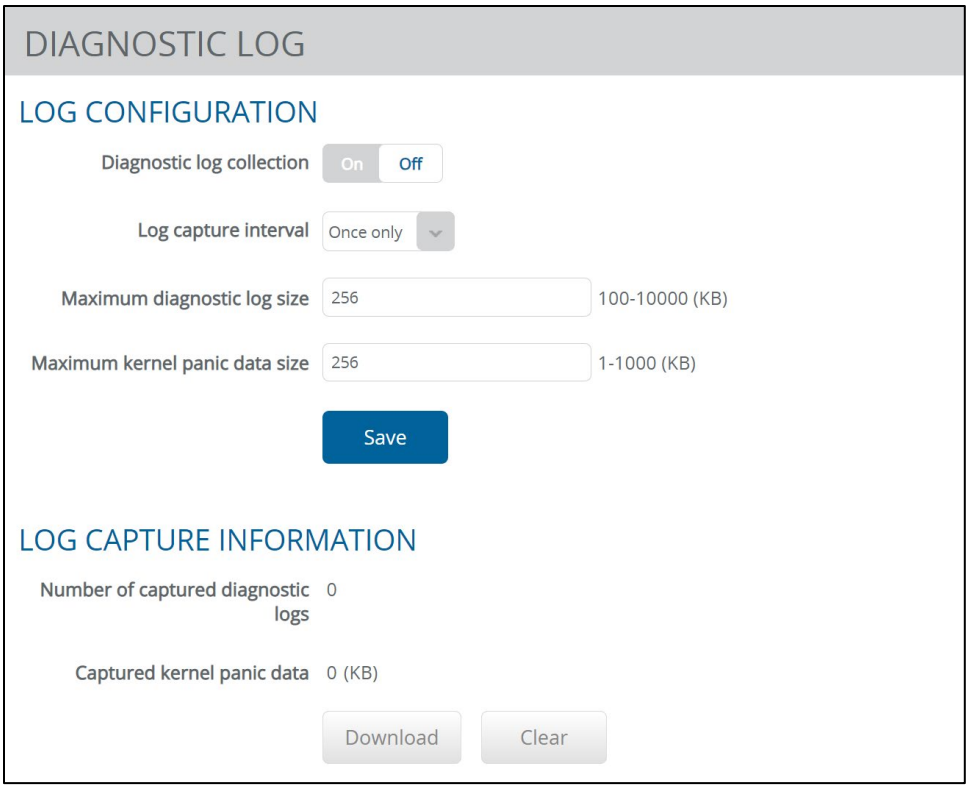


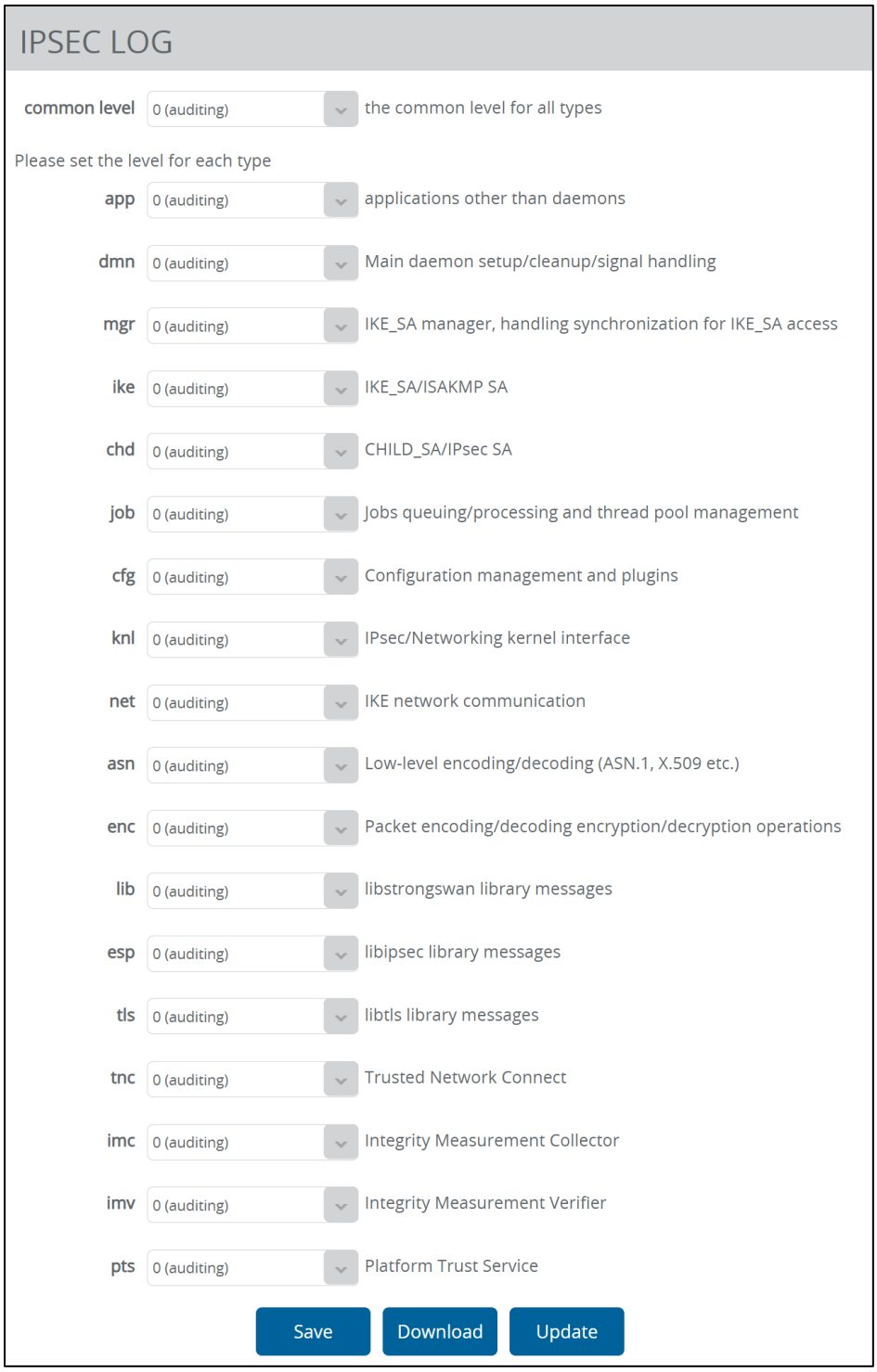
Table 10-3 Diagnostic log descriptions

Item	Description
Diagnostic log configuration	
Periodic log collection	Turn on this toggle key to enable diagnostic log collection.
Log capture interval	Select the interval at which the router should collect diagnostic log data.
Maximum periodic log size (KB)	Enter the maximum size of the log file in kilobytes.
Maximum kernel panic data size (KB)	Enter the maximum size of the kernel panic data file in kilobytes.
Save button	Click to save Log Configuration.
Log capture information	
Number of captured periodic logs	Displays the number of captured periodic logs.
Captured kernel panic data (KB)	Displays the total size of captured kernel panic data in kilobytes.
Download button	Click to download all captured logs.
Clear button	Click clear all captured periodic logs.

IPSec log

The IPsec Log allows you to identify and troubleshoot issues with the IPsec VPN connection. To access the IPsec Log page, navigate to **System > Log > IPSec log**.

Figure 10-4 Log - IPSec Log



To use the IPsec log, set the log level for each type of log that should be captured. The following log levels are available:

Table 10-4 IPSec log descriptions

ITEM	DEFINITION
Off	No logs collected.
0 Auditing	Auditing is the lowest log level, providing minimal information. This level is typically used for logging only critical security events or administrative actions that have a significant impact on the VPN.
1 Control Flow	Control Flow logging provides information about the establishment and termination of IPsec VPN connections and security associations (SAs). Control Flow includes details about the negotiation of encryption and authentication parameters, as well as key exchange protocols like IKE (Internet Key Exchange).
2 Debug Control Flow	Debug Control Flow logging provides more detailed information than the standard Control Flow level. Debug Control Flow includes additional debugging information related to the establishment and management of IPsec SAs.
3 Raw Data Dumps	Raw Data Dumps logging is a very verbose level that includes detailed packet-level information. Raw Data Dumps logs raw data, such as the contents of IPsec packets and payloads.
5 Private Data Dumps	Private Data Dumps logging is the highest log level and provides the most detailed information. Private Data Dumps logs sensitive and private data, such as encryption keys and other security-related information. This level should only be used in a secure environment for advanced debugging or security analysis.

Once the log level has been set, click **Save** button to apply the log configuration.

As logs are collected, they are visible in the Log Content section at the bottom of the page. Click **Update** button to refresh the Log Content window.

Click **Download** button to download and view the logs in an external tool

Watchdog

Periodic ping

The Periodic ping page is used to configure the behaviour of the Periodic Ping monitor function.

When configured, the Ping watchdog feature transmits controlled ping packets to 1 or 2 user specific IP addresses. Should the watchdog not receive responses to the pings, it will reboot the device in a last resort attempt to restore connectivity.

Caution should be exercised when using this feature in situations where the device is intentionally offline for a particular reason (e.g. user configured PDP session disconnect, or the Connect on demand feature enabled). The ping watchdog feature expects to be able to always access the internet and will always eventually reboot the router if access isn't restored by the time the various timers and retries expire.

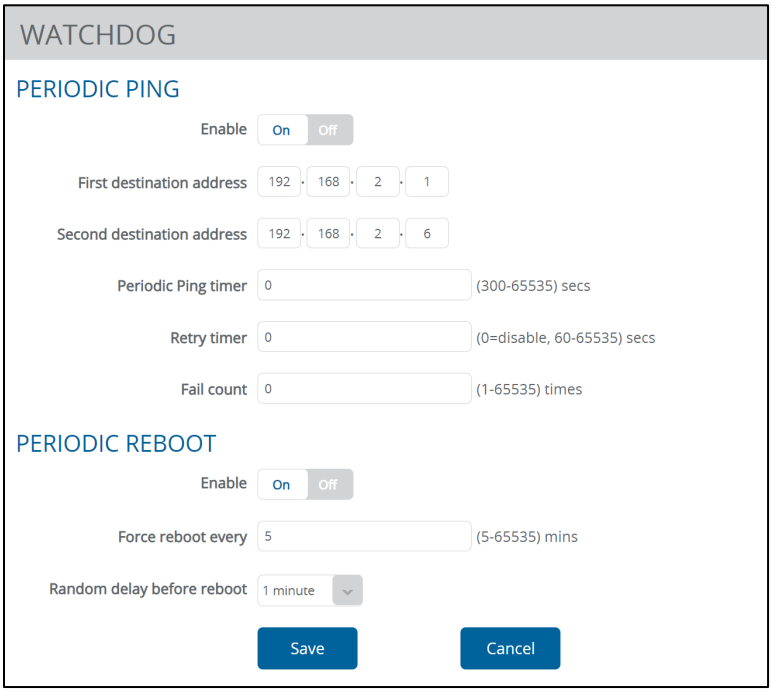
The ping watchdog being a last resort standalone backup mechanism, it will continue to do its job and reboot the device even when the Connect on demand session is idle, or the PDP context is disabled by the user. It is

recommended to disable this feature if Connect on demand is configured, or if the PDP context will be intentionally disconnected on the occasion.

The feature operates as follows:

1. After every “Periodic Ping timer” configured interval, the router sends 3 consecutive pings to the “First destination address”.
2. If all 3 pings fail the router sends 3 consecutive pings to the “Second address”.
3. The router then sends 3 consecutive pings to the “Destination address” and 3 consecutive pings to the “Second address” every “Retry timer” configured interval.
4. If all retry pings in step 3 above fail the number of times configured in “Fail count”, the router reboots.
5. If any ping succeeds, the router returns to step 1 and does not reboot.

Figure 10-5 Watchdog – Periodic ping and reboot configuration



To configure the ping watchdog:

1. Enable the ping watchdog by setting the **Enable** toggle to **On.**
2. In the **First destination address** field, enter a website address or IP address to which the router will send the first round of ping requests.
3. In the **Second destination address** field, enter a website address or IP address to which the router will send the second round of ping requests.
4. In the **Periodic Ping timer** field, enter a number between 300 and 65535 for the number of seconds the router should wait between ping attempts. Setting this to 0 disables the ping watchdog function.
5. In the **Retry timer** field, enter a number between 60 and 65535 for the number of seconds the router should wait between retry ping attempts, i.e. pings to the second destination address.
6. In the **Fail count** field, enter an integer between 1 and 65535 for the number of times an accelerated ping should fail before the router reboots. Setting this to 0 disables the ping watchdog function.
7. Click **Save** button to save the configuration.

Periodic reboot

The router can be configured to automatically reboot after a period of time specified in minutes. While this is not necessary, it does ensure that in the case of remote installations, the router will reboot if some anomaly occurs.

To configure Periodic reboot:

1. Set the **Enable** toggle to **On**.
2. In the **Force reboot every** field, enter the time in minutes between forced reboots. The default value is 0 which disables the Periodic reboot function. The minimum period between reboots is 5 minutes while the maximum value is 65535 minutes.
3. If you have configured a forced reboot time, select a tine for **Random delay before reboot** from the drop-down list. Randomly delaying the reboot time is useful for preventing a large number of devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured Force reboot every time and then randomly selects a time that is less than or equal to the **Random delay before reboot** time setting. After that time has elapsed, the router reboots.

Important: *The Random delay before reboot time is not persistent across reboots; each time the router is due to reboot, it randomly selects a time less than or equal to the time set for Random delay for reboot.*

4. Click **Save** button to save the settings.

System configuration

LDAP Settings

The LDAP Settings allows you to configure a Lightweight Directory Access Protocol (LDAP) on the NTC-550 Series router. The LDAP allows the router to use a centralized directory service for user authentication and authorization.

Figure 10-6 LDAP Settings

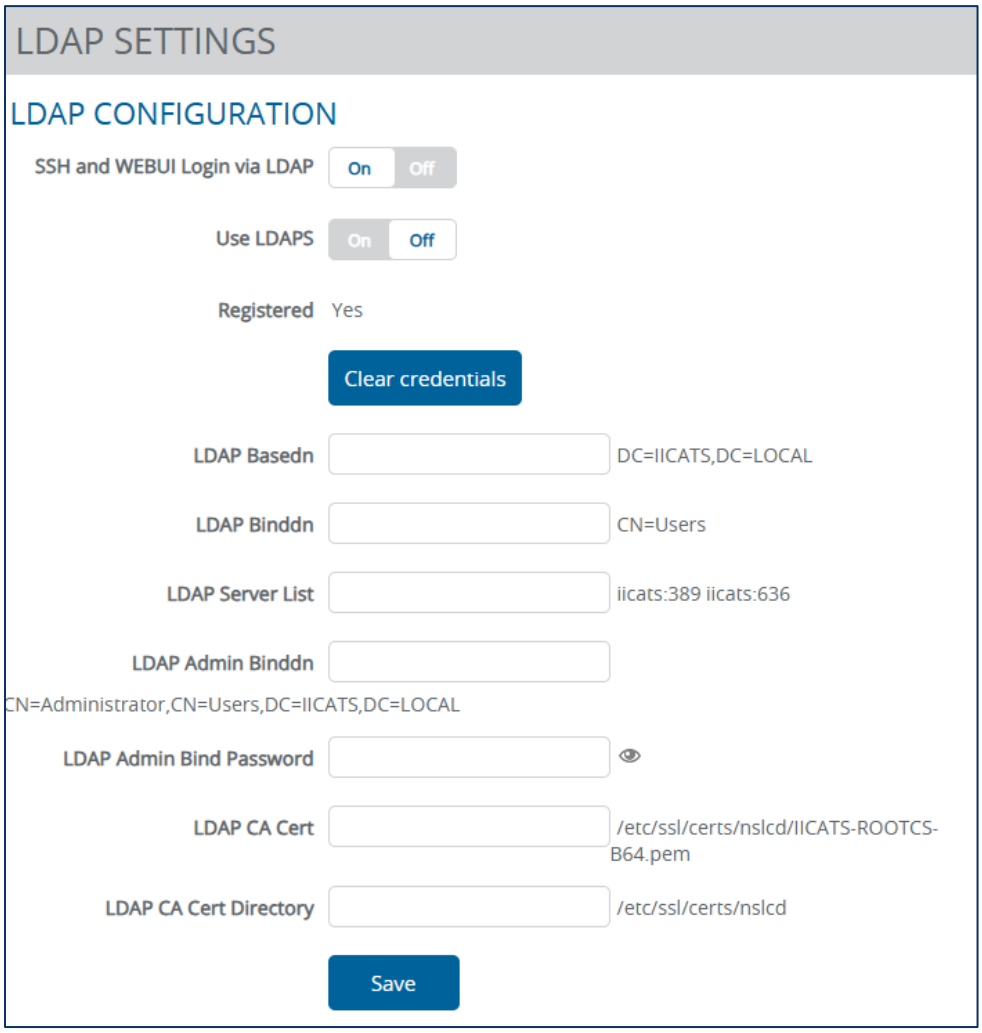


Table 10-5 LDAP Configuration

ITEM	DEFINITION
SSH and WEBUI Login via LDAP	Set to **On** to enable SSH and WEBUI login via LDAP.
Use LDAPS	Set to **On** to enable use of LDAP over SSL/TLS, a secure version of LDAP.
Registered	Displays whether the LDAP server in registered on the router.
Clear Credentials button	Click to clear credentials related to an existing LDAP configuration.

ITEM	DEFINITION
LDAP Basedn	Enter the LDAP Base Distinguished Name. It specifies the starting point within the LDAP directory tree from which searches will be performed.
LDAP Binddn	Enter the LDAP Bind Distinguished Name of the LDAP entry used to authenticate (bind) to the LDAP server.
LDAP Server List	Enter the IP address or Hostname of the LDAP server and port number. (IP address/Hostname:Port)
LDAP Admin Binddn	Enter the LDAP Admin Bind Distinguished Name, which refers to a special Bind DN with administrative privileges in the LDAP directory.
LDAP Admin Bind Password	Enter the password for the LDAP Admin Bind DN used.
LDAP CA Cert	Enter the complete path of the Certificate Authority (CA) certificate that is used to validate the SSL/TLS certificate presented by an LDAP server when connecting over LDAPS (LDAP over SSL/TLS).
LDAP CA Cert Directory	Enter the path for the directory where the LDAP CA certificate is located.
Save button	Click to save the settings.

Restore factory defaults

Restoring factory defaults will reset the NTC-550 Series router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-550 Series router. There are three levels of factory reset:

- Installer reset
- Carrier reset
- Full factory reset

The availability of the above levels depends on your Runtime Configuration settings.

Installer reset

The installer reset only resets settings that have changed after the NTC-550 Series was installed. The settings that are included are those that were likely changed through the web interface. This reset level is generally the first one that should be attempted, as it will reset less important configurations.

Carrier reset

The carrier reset will reset the device with the carrier-defined default settings to operate on the network. This also resets the user-configured options to their default settings. This reset should be attempted after trying the installer reset.

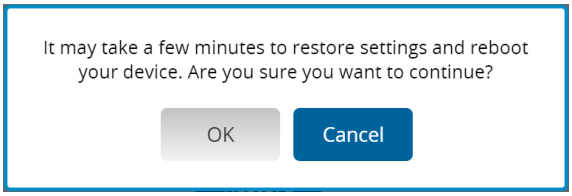
Full factory reset

The full factory reset is generally used for refurbishment or to remove an erroneous configuration. This will remove all settings including the carrier settings that are required for the device to operate on the network. All configurations and settings are completely removed.

⚠ ***Important:*** *The full factory reset will require the NTC-550 Series to be completely reconfigured.*

To complete a reset at any level

1. In the **Restore Factory Defaults** page, select the **Clear HTTPS certificate** checkbox if you want to clear the HTTPS certificate.
2. Select the appropriate reset level.
3. You will be prompted to confirm. Select the **Ok** button to proceed with the reset.

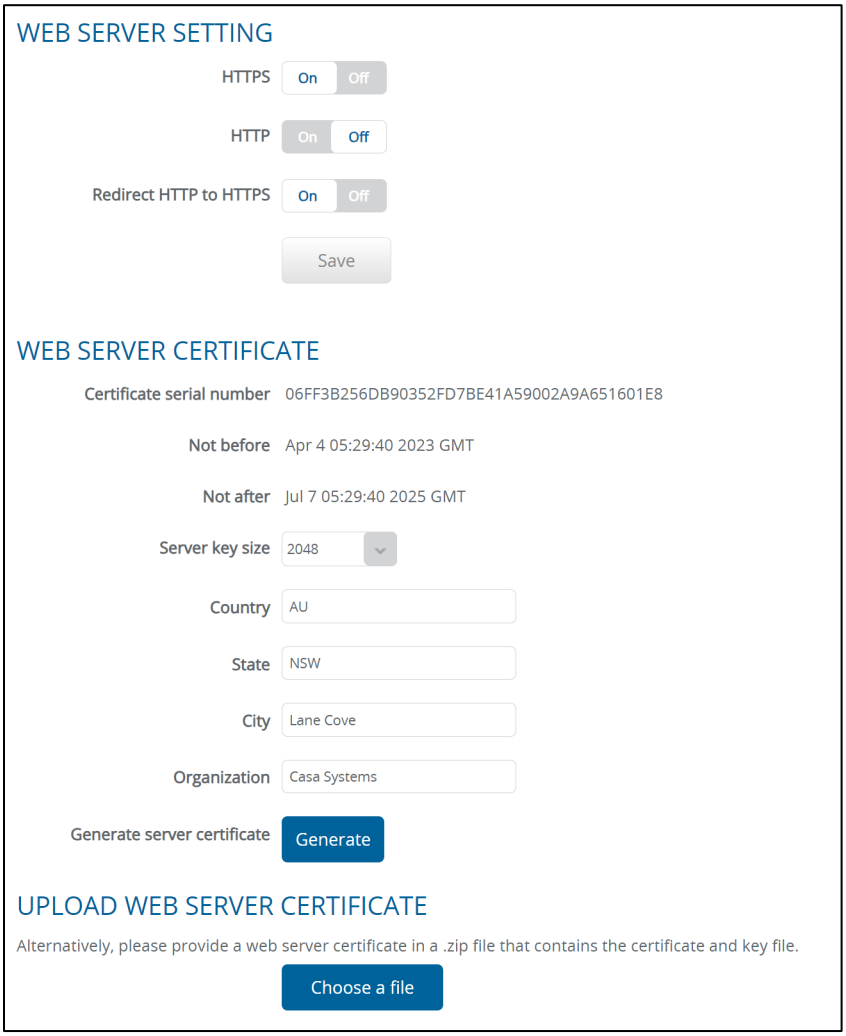


4. Wait for the router to reset and reboot, then access the device through the web interface at **https://192.168.1.1**

Web server setting

Allows you configure whether the NTC-550 Series router web server uses HTTP or HTTPS and the server port. Additionally, you can generate a web server certificate by entering data in all the fields in the **Web Server Certificate** section.

Figure 10-7 Web server setting configuration



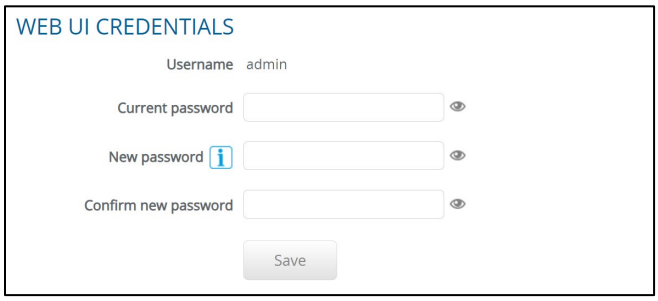
Administration settings

The Administration settings page allows you to update administration credentials and Web UI login limits.

Web UI credentials

Use this section to update the password for the different users that have access to the NTC-550 Series router via the web interface. Select the **Username**, enter the current password for the that user and then enter a new password. Click **Save** button to confirm the changes.

Figure 10-8 Administration settings – Web UI credentials configuration



Web UI login limits

The Web UI login limits section allows you to configure the timeout and lock setting for access to the web interface. It is designed to improve security by reducing the risk of brute force attacks on the web interface.

Figure 10-9 Administration settings – Web UI login limit configuration

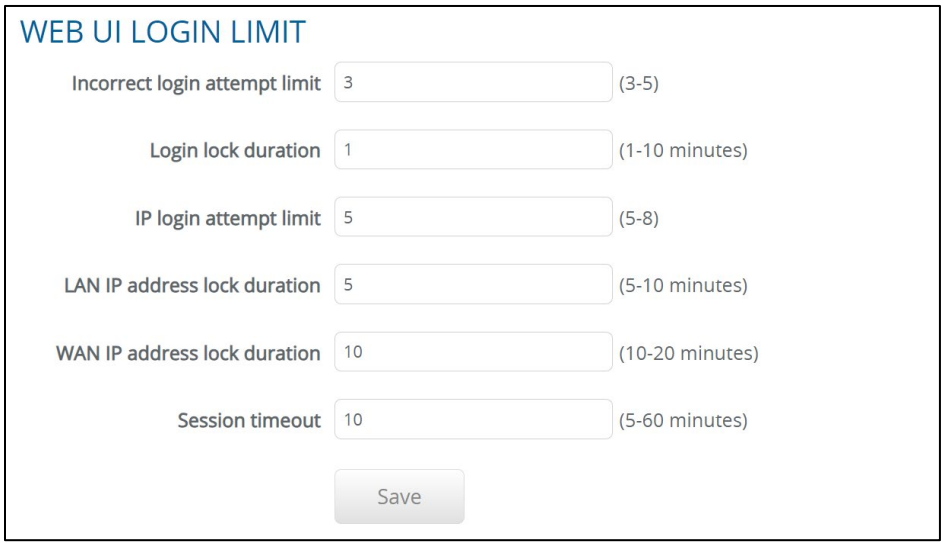


Table 10-6 WebUI login limits configuration items

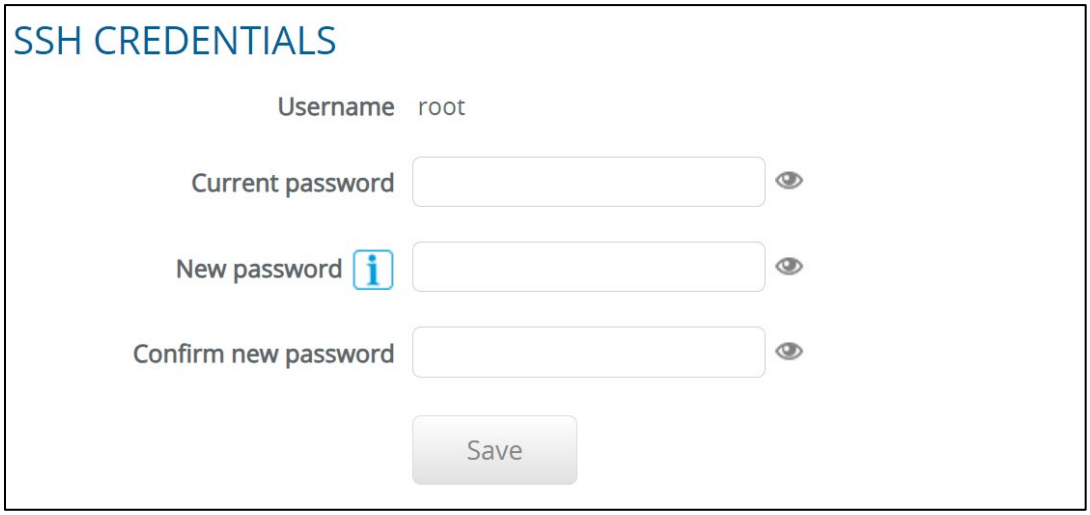
Item	Description
Incorrect login attempt limit	Enter the number of times an incorrect password can be entered into the web interface before it locks access and does not allow any further attempts.
Login lock duration	Enter the amount of time the login lock lasts.

Item	Description
IP login attempt limit	Enter the number of logins that can be attempted from one IP before any further attempts are locked out.
LAN IP address lock duration	Enter the amount of time an IP attempting to log in from the LAN is forbidden from trying to login.
WAN IP address lock duration	Enter the amount of time an IP attempting to log in from the WAN is forbidden from trying to login.
Session timeout	The amount of time in minutes that a logged in session lasts on the web interface without any activity. The web interface will log out the current user after the configured time.

SSH credentials

Use this section to update the root user password for SSH access to the NTC-550 Series router.

Figure 10-10 Administration – Administrator credentials configuration

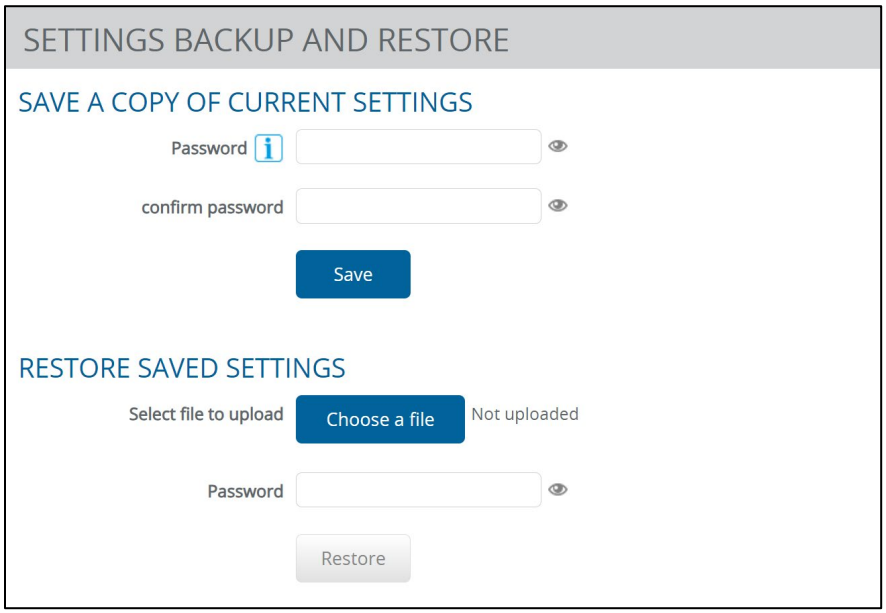


Settings backup/restore

The Settings Backup and Restore page allows you to backup or restore the router's configuration or to reset it to factory defaults. To view the settings page, you must be logged into the web user interface as root using the password admin. The backup / restore functions can be used to easily configure many NTC-550 Series routers by configuring one router with your desired settings, backing them up to a file and then uploading that file to multiple NTC-550 Series routers.

To access the Settings Backup and Restore page, navigate to **System > System configuration > Settings backup/restore**.

Figure 10-11 System configuration - Backup and restore



Creating a settings backup

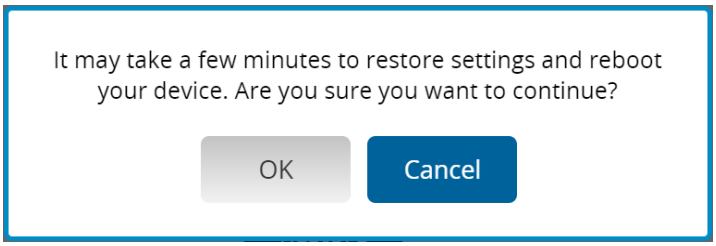
To create a settings backup, in the Save a Copy of Current Settings section, Click the **Save** button. The configuration will download. If you wish to protect the configuration with a password, enter a password into the **Password** and **Confirm password** fields, then click **Save.**

Restoring a settings backup

To restore a settings backup:

1. in the Restore **Settings** section, click **Choose a file** for the **Select file to upload** field.
2. Locate and upload the saved configuration.
3. If the file was saved with a password, enter the password, then click **Restore.** You will be prompted to confirm, select **Ok** to proceed. The device will reboot with the saved settings.

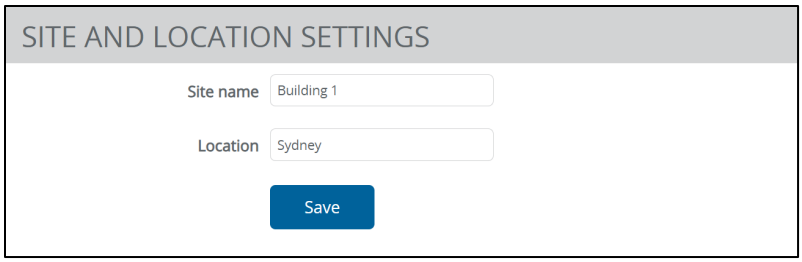
Figure 10-12 Systems configuration – Restoring a settings backup confirmation



Site and location settings

The Site and location settings allows you to add a name that displays in the System information section of the Status page. This can be useful for identifying the particular device you are using when you have a fleet of them in various locations.

Figure 10-13 System configuration – Site and location settings

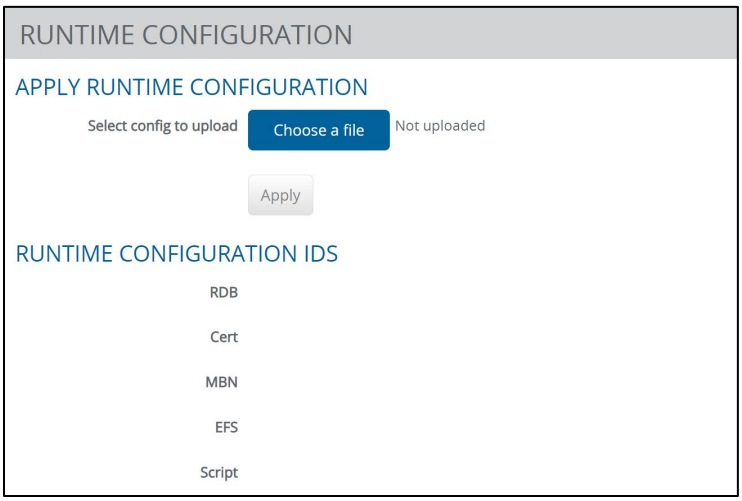


Enter the vales for **Site name** and **Location** fields. Click **Save** to save the settings

Runtime configuration

Runtime Configuration allows you to to load a configuration file containing carrier-specific settings such as default settings, MBN changes which is not possible via the web user interface. It is used for late binding of carrier configurations at the time of installation.

Figure 10-14 System configuration – Runtime configuration upload



To apply runtime configuration:

1. Click the **Choose a file** button, locate the configuration file and select it.
2. **Uploaded** displays next to the button.
3. Click the **Apply** button to install the configuration file.
4. The device automatically reboots after successful upload of the configuration file.

SSH key management

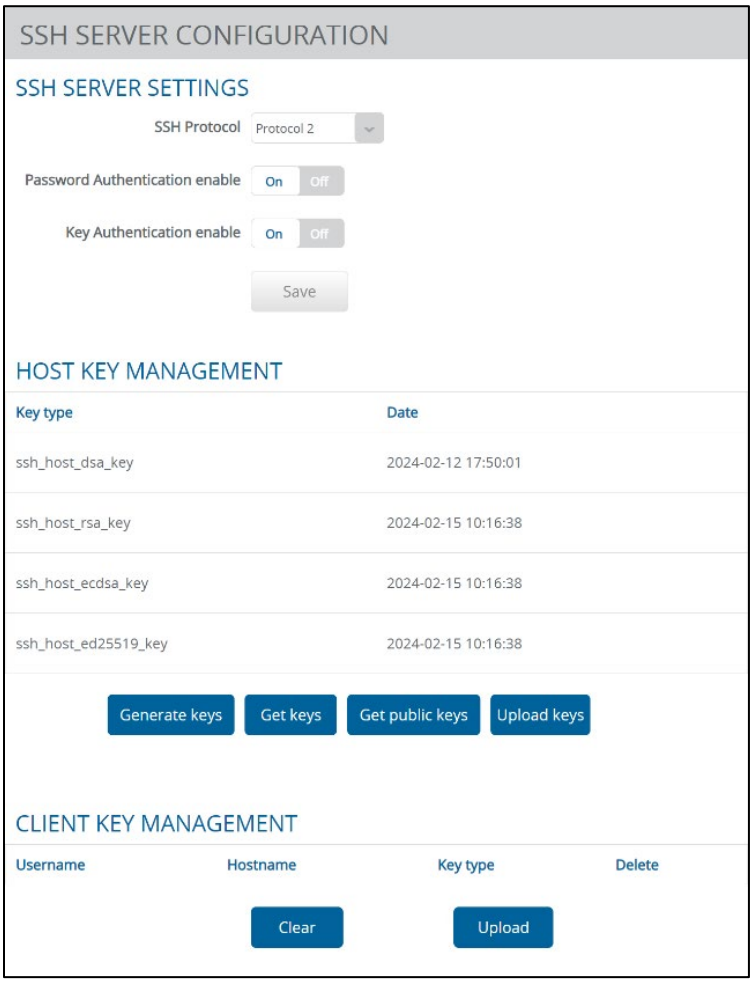
Secure Shell (SSH) is UNIX-based command interface and network protocol used to gain secure access to a remote machine, execute commands on the remote machine, andtransfer files between machines.

SSH uses RSA public key cryptography for both connection and authentication. Two common ways of using SSH are:

- Use automatically generated public-private key pairs to encrypt the network connection and then use password authentication to log on.
- Use a manually generated public-private key pair to perform the authentication and allow users or programs to log in without using a password.

To access the SSH key management page, navigate to **System > System configuration > SSH Key Management**.

Figure 10-15 System configuration – SSH server configuration



SSH Server Configuration

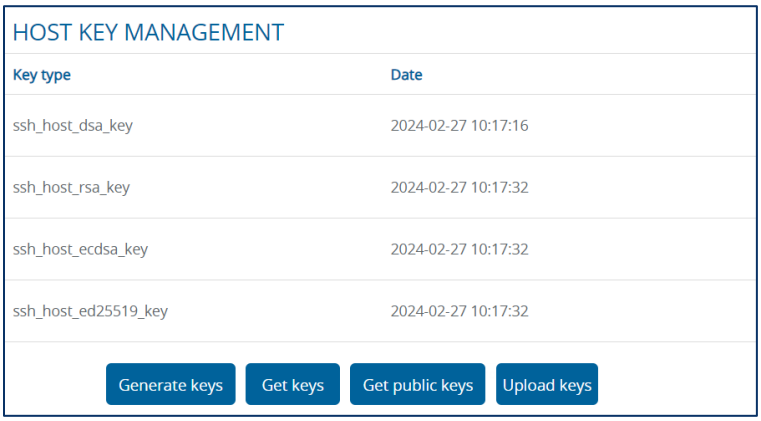
To configure the SSH server settings:

1. Select the **SSH Protocol** to use. Protocol 2 is more recent and is considered more secure.
2. Select the type of authentication you want to use by setting the **Password Authentication enable** and **Key Authentication enable** toggle keys to **On** or **Off**. Note that you may have both authentication methods on, but you cannot turn them both off.
3. Click the **Save** button to confirm your settings.

Host key management

The Host key management section allows you to manage the SSH keys on the NTC-550 Series router.

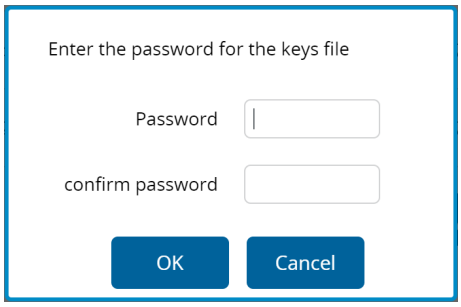
Figure 10-16 System configuration – SSH server configuration – Host key management



Click the **Generate Keys** button to generate new keys. Use caution when selecting the **Generate Keys** button, as this invalidates any previously generated keys.

Click the **Get Keys** button to download the generated private and public keys. You will be asked to enter a password for the keys file.

Figure 10-17 System configuration – SSH server configuration – Host key management – Password



In the **Password** field enter a password and in the **confirm password** filed, re-enter the password. Click the **OK** button to download the keys file.

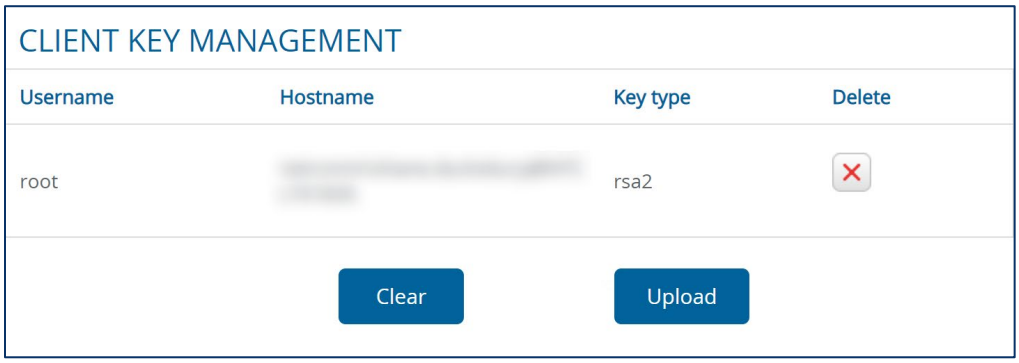
Click the **Get Public Keys** button to download just the public keys.

Click the **Upload keys** button to upload a keys file. You will be prompted to enter the password created in the **Get Keys** step to upload the file. The keys will replace the previously generated keys.

Client key management

The Client key management page allows you to upload client keys to the NTC-550 Series router and enables key based SSH access to the NTC-550 Series router. Click the **Upload** button to upload the public key of your SSH client. The key displays in **Client key management** window. Click ✕ in the **Delete** column to remove that key. Click **Clear** to clear all the uploaded keys.

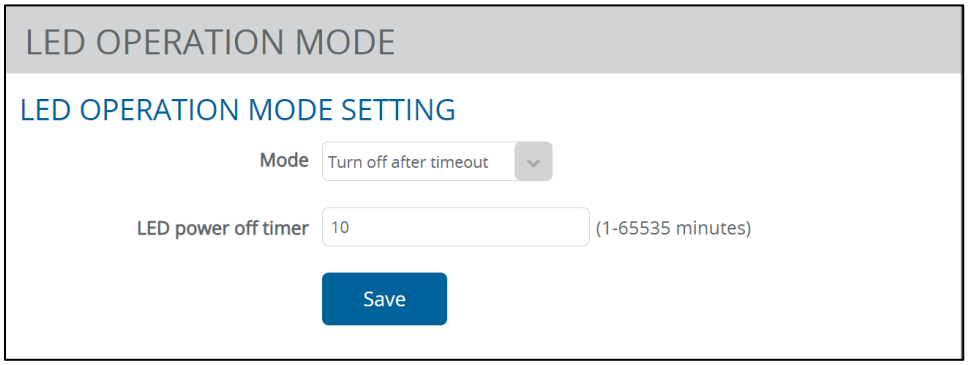
Figure 10-18 System configuration – SSH server configuration – Host key management – Password



LED operation mode

The LED operation mode page allows you to control the operation of the LED indicator lights on the NTC-550 Series router. There are two modes available, **Always on** and **Turn off after timeout.** Setting the mode to **Always on** sets the indicator LEDs to be lit when the device is on. Setting the mode to **Turn off after timeout** sets the indicator LEDs to turn off after the timer has expired.

Figure 10-19 LED operation mode



Setting the LED operation mode

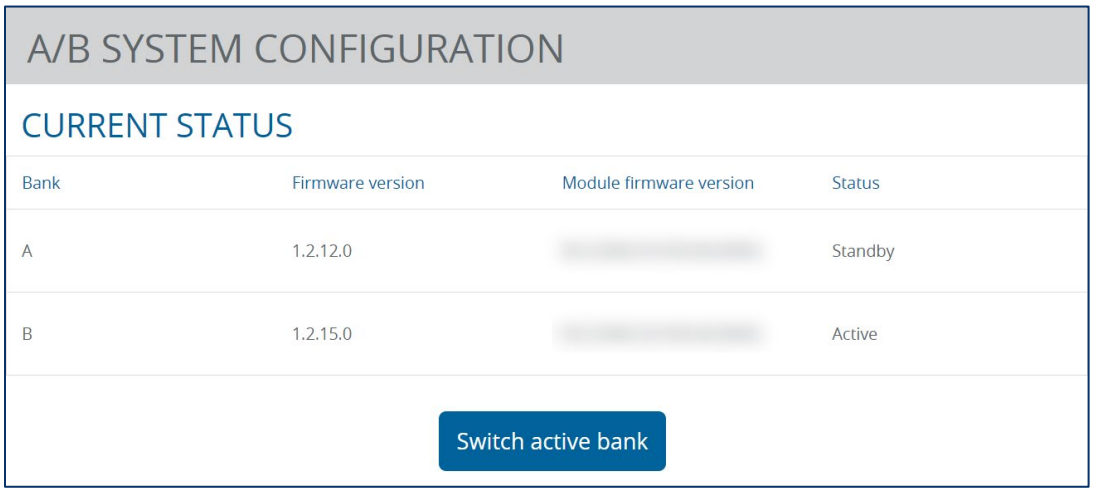
To set the LED operation mode:

1. Select the **Mode** to use. Options are **Always on** and **Turn off after timeout**.
2. If using the **Turn off after timeout** mode, set the LED power off timer to the number of **minutes** that the indicator LEDs should be lit after the device has started.
3. Click the **Save** button to save and apply the configuration.

A/B system configuration

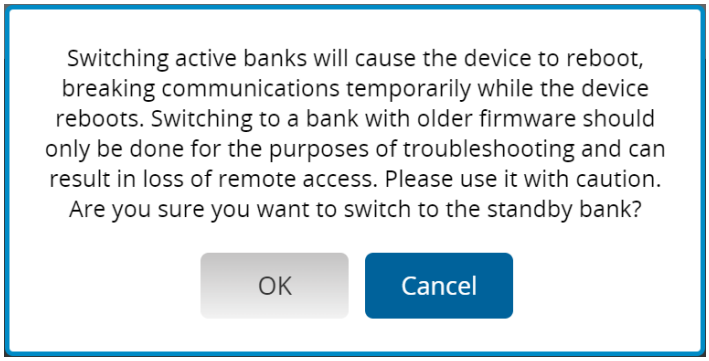
The A/B system configuration page allows you to switch between an active and previous firmware. Switching between firmware allows you to restore a previous firmware for troubleshooting in the event of an issue with the current firmware. Restoring a previous firmware should only be used for troubleshooting.

Figure 10-20 A/B System configuration



To switch the active bank, Click the **Switch active bank** button. You will be prompted with the following message:

Figure 10-21 A/B System configuration - Confirmation

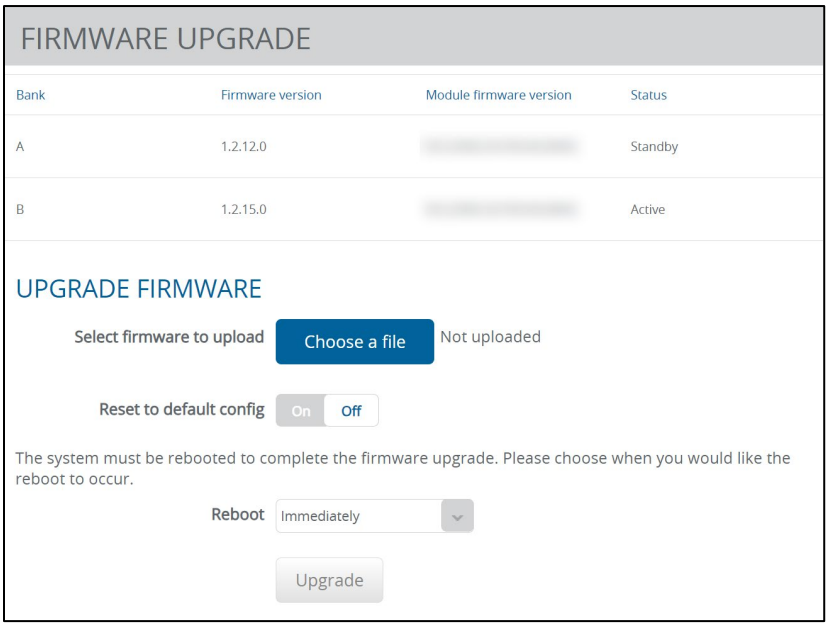


To proceed click the **OK** button. Once the reboot is complete, the previous firmware will be restored. To switch active banks again, return to this screen and select the **Switch active bank** button.

Firmware upgrade

The Firmware upgrade page allows you to upload firmware files to update the NTC-550 Series router. The firmware upgrade will be applied to the Standby bank, to ensure the current firmware can be restored in the event of an issue.

Figure 10-22 File uploads

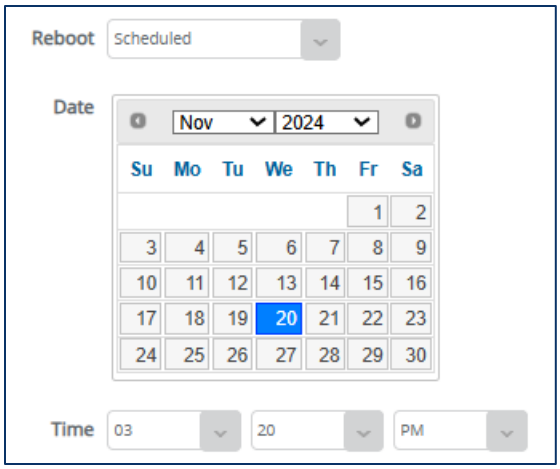


Updating the router firmware

The firmware update process involves first uploading the recovery image firmware and then updating the main firmware image.

To update the NTC-550 Series router's firmware:

1. Power on the router as described in the Installing the router section.
2. Log in to the router with the root user account (See the Advanced configuration section for details)
3. Click the **System** tab from the top menu bar, then click the **Firmware upgrade** menu item.
4. In the Upgrade Firmware section click section, click **Choose a file** button. Locate the firmware image file on your computer and select **Open**.
5. If required set the **Reset to default config** toggle to **On** to reset the NTC-550 Series router to the default configuration.
6. Select an option for Reboot filed. The options are **Immediately** and **Scheduled**. If you select **Scheduled** option, the **Date** and Time **settings** display.

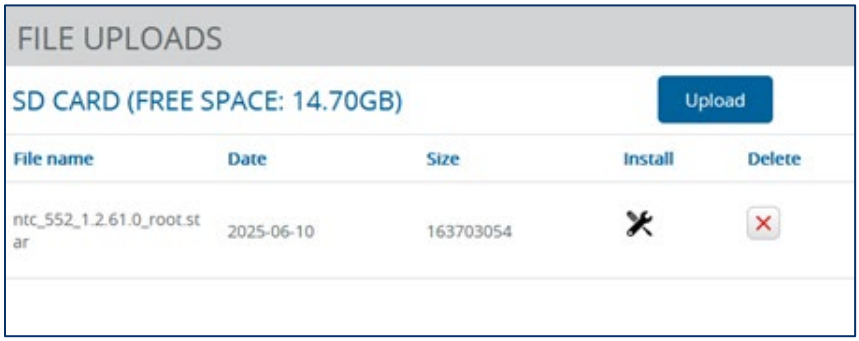


7. Set the required **Date** and **Time**.
8. Click **Upgrade** button to upgrade the firmware.

SD Card

The SD card page displays available space and contents of micro-SD card. You can click **Upload** to add a file to the SD Card. In the below example the SD card contains a firmware file. Click to install the firmware and click to remove the file.

Figure 10-23 SD Card Display



Access control

The Access control pages are used to configure the remote and local access to the router.

Note: *All remote access to the router is disabled by default.*

Figure 10-24 Access control configuration

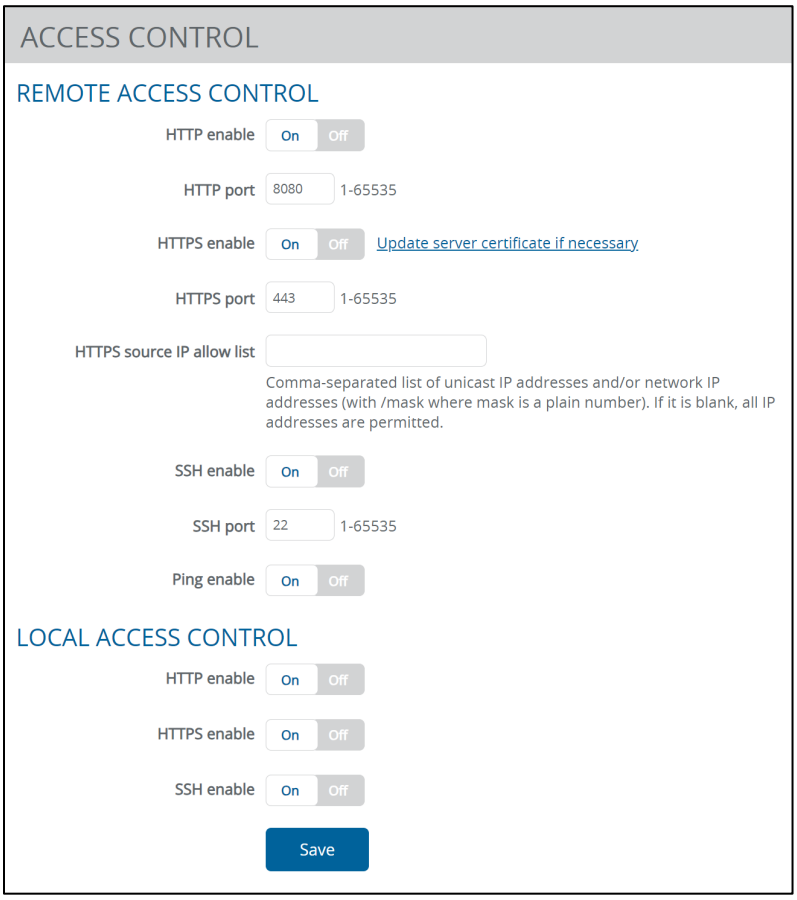


Table 10-7 Access control configuration items

Item	Description
Remote Access Control	
HTTP enable	Enable or disable remote HTTP access to the router.
HTTP port	When HTTP is enabled (see previous) you can set the HTTP management port. Enter a port number between 1 and 65534 to use when accessing the router remotely.
HTTPS enable	Enable or disable remote HTTPS access to the router using a secure connection.
HTTPS port	When HTTPS is enabled you can set the HTTPS remote access port. Enter a port number between 1 and 65534 to use when accessing the router remotely over a secure HTTPS connection.
HTTPS source IP allow list	When HTTPS is enabled (see Enable HTTPS above) you can enter a 'whitelist' of IP addresses that will be permitted to access the router. Enter a list of comma-separated unicast IP addresses. You may also enter IP addresses in CIDR notation, however, no spaces are permitted.

Item	Description
	Note that if this field is left blank, all IP addresses will be permitted to access the router.
SSH enable	Enable or disable Secure Shell access to the router.
SSH port	When SSH is enabled you can set the SSH access port. Enter the port number for remote SSH access. The port number must be between 1 and 65534.
Ping enable	Enable or disable remote ping responses on the WWAN connection.
Local Access Control	
HTTP enable	Enable or disable local HTTP access to the router. The default setting is disabled.
HTTPS enable	Enable or disable local secure HTTP access (https). The default setting is enabled.
SSH enable	Enable or disable local Secure Shell on the router. The default setting is enabled.
Save button	Click to save the configuration.

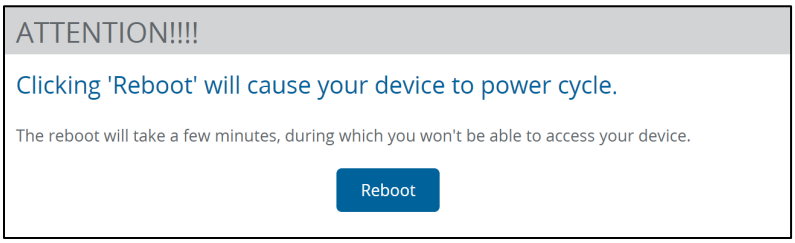
Reboot

The Reboot option in the System section performs a soft reboot of the device. This can be useful if you have made configuration changes you want to implement.

To reboot the NTC-550 Series:

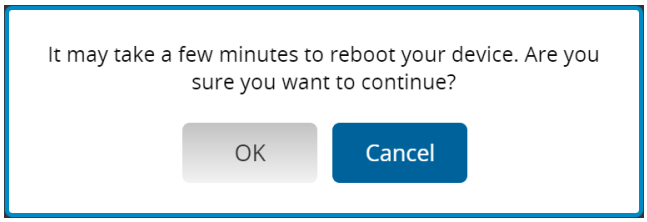
1. Click the **System** tab from the top menu bar.
2. Click the **Reboot** button from the menu on the left side of the screen.

Figure 10-25 Reboot



3. The NTC-550 Series router displays a warning that you are about to perform a reboot.
4. If you wish to proceed, select the Reboot button.

Figure 10-26 Reboot – Reboot confirmation



5. A warning popup will advise that “It may take a few minutes to reboot your device. Are you sure you want to continue?”
6. Click **OK** to continue with the reboot process.

Field test

The Field test page contains LTE, LTE SCELL and NR5G cell information which may be useful when troubleshooting signal strength issues. To access this page, navigate to **System > Field test**.

Figure 10-27 Field Test

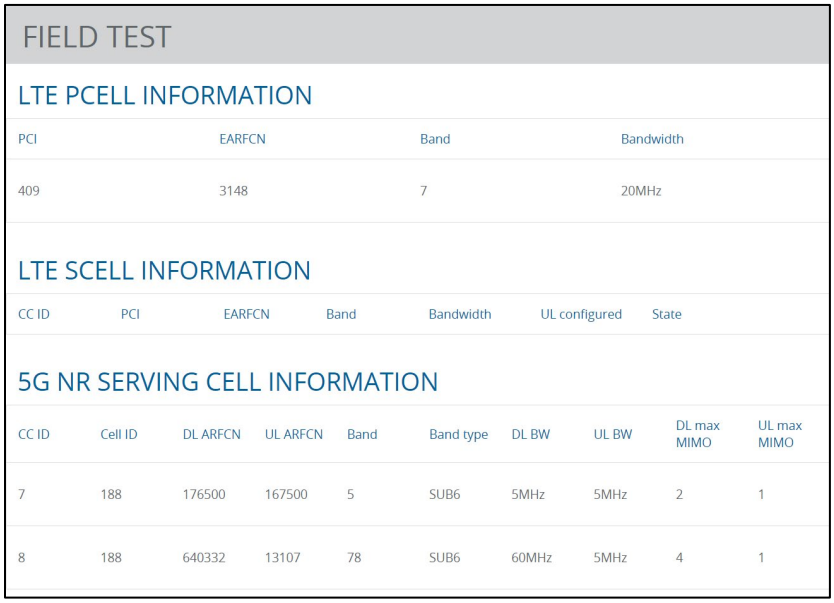


Table 10-8 LTE PCELL Information

LTE PCELL INFORMATION	
PCI	Physical Cell ID of the LTE Cell.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
Band	The current LTE band.
Bandwidth	The current LTE bandwidth.

Table 10-9 LTE SCELL Information

LTE SCELL INFORMATION	
CC ID	Component Carrier ID.
PCI	Physical Cell ID of the LTE Cell.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
Band	The current LTE band.
Bandwidth	The current LTE bandwidth.
UL Configured	If the Up Link is configured.
State	The current state of the LTE SCELL.

Table 10-10 NR5G Serving cell information

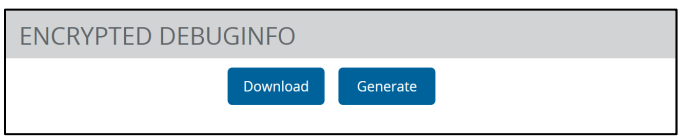
NR5G Serving Cell Information	
CC ID	Component Carrier ID.
Cell ID	The physical cell identifier.
DL ARFCN	Downlink Absolute Radio Frequency Channel Number.
UL ARFCN	Uplink Absolute Radio Frequency Channel Number.
Band	The NR5G band.
Band Type	The type of the NR5G band, e.g. Sub6 or mmWave.
DL BW	Downlink bandwidth.
UL BW	Uplink bandwidth.
DL max MIMO	Downlink maximum Multiple Input Multiple Output.
UL max MIMO	Uplink maximum Multiple Input Multiple Output.

Encrypted debuginfo

The Encrypted debuginfo page contains NR5G cell information which may be useful when troubleshooting signal strength issues.

Click the **Generate** button to force the NTC-550 Series router to create a debug file. A success message will appear when the debug file generation is complete. Click the **Download** button to download the generated file.

Figure 10-28 Encrypted debuginfo download

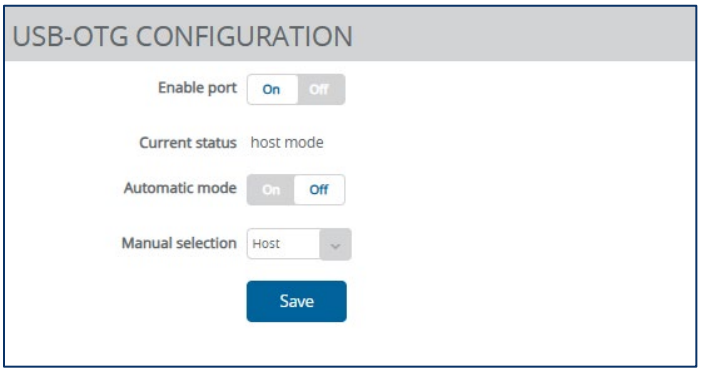


USB-OTG

The USB-OTG page allows you to enable or disable the USB port. By default, the port is enabled.

To access the USB-OTG page navigate to **System > USB-OTG**.

Figure 10-29 USB-OTG Configuration



When the port is enabled, the USB-OTG page displays the current status of the USB port, i.e. whether it is in **Device mode** or **Host mode**.

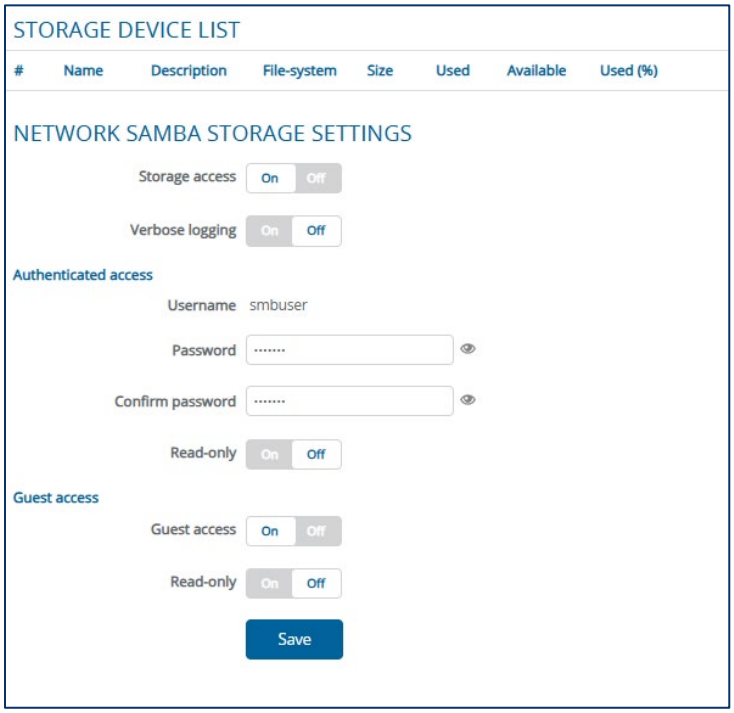
By default, **Automatic mode** is set to **On**, allowing the router to intelligently choose the correct mode. If you wish to manually override this selection, turn **Automatic mode** to **Off** and manually select either **Host** or **Device** mode.

Storage

The Storage page provides configuration options with relation to USB and SD storage devices.

To access the Storage page, navigate to **System > Storage**.

Figure 10-30 Storage Settings Configuration



The Storage Device List displays any connected storage devices and summarises the type, file system, size, used and available space on each device. Additionally, an eject button is provided to unmount the storage device so you can safely remove it.

Storage devices connected to the router can be shared using the Samba protocol. The table below lists the Network Samba Storage Settings Configuration details

Table 10-11 Network Samba Storage Settings Configuration Items

Item	Description
Storage access	Set to **On** to enable Samba sharing function
Verbose logging	Set to **On** to provide additional logging data in the system log. This should generally only be used when debugging to avoid generating excessively long logs.
Authenticated Access	
Username	The username to be used for authenticated access to the storage device. This is configured as **smbuser** and cannot be changed.
Password	Enter the password to be used for authenticated access to the storage device.
Verify password	Re-enter the password to be used for authenticated access to the storage device.
Read-only	Set to **On** to provide read-only access to the files on the connected storage device(s). When read-only access for authenticated accounts is turned on, the guest access read-only option is hidden and guests are permitted read-only access also.
Guest access	
Guest access	Set to **On** to enable guest access to the storage device.
Read-only	Set to **On**, to provide read-only access to the files on the connected storage device(s) for guest users. If the authenticated account has Read-only enabled then this option is not available and read-only access is automatically granted to guest users.

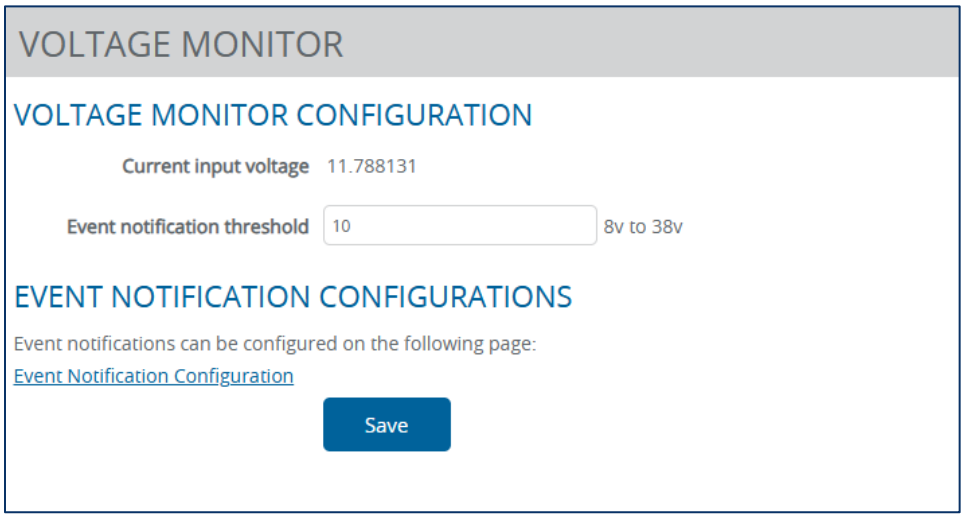
Click **Save** to save the settings.

Voltage Monitor

The Voltage Monitor page displays the Current Input Voltage and allows you to set a threshold voltage for event notification.

To access the Voltage Monitor page navigate to **System > Voltage Monitor**.

Figure 10-31 Voltage Monitor Configuration



In the **Event notification threshold field**, enter the value for threshold voltage. If the voltage drops below this value, notification is generated.

Click **Save** to save the settings

Click the **Event Notification Configuration** link to go to Event Notification Configuration page.

Appendix A. Configuring Radio Access Technologies

This device supports the following modes of operations in various combinations

- **LTE** (3GPP Core Network Option 1)
- **5G Non Standalone** (3GPP Core Network Option 3x)
- **5G Standalone** (3GPP Core Network Option 2)

Please refer to the following table to understand which modes of operation are possible and how to configure them.

Table A-1 RAT/Band Selection table

	Allowed RAT				How to Configure	
Mode	**LTE**	**5G NSA**	**5G SA**	**Supported**	**RAT Selection Menu**	**Band Selection Menu**
LTE Only	Yes	No	No	Yes	Select LTE only	Select LTE Frequency Bands
LTE + 5G NSA	Yes	Yes	No	Yes	Select LTE + 5G NR	Select LTE + NSA Frequency Bands
5G NSA Only	No	Yes	No	No	–	–
LTE + 5G NSA + 5G SA	Yes	Yes	Yes	Yes	Select LTE + 5G NR	Select LTE + NSA + SA Frequency Bands
LTE + 5G SA	Yes	No	Yes	No	–	–
5G NSA + 5G SA	No	Yes	Yes	No	–	–
5G SA Only	No	No	Yes	Yes	Select 5G NR	Select SA Frequency Bands

Use this table in conjunction with the settings described in sections ***6.2.1.3 RAT selection*** and ***6.2.1.2 Band selection*** of this guide.

Note: *5G Standalone Mode is not supported when utilising mmWave frequency bands.*

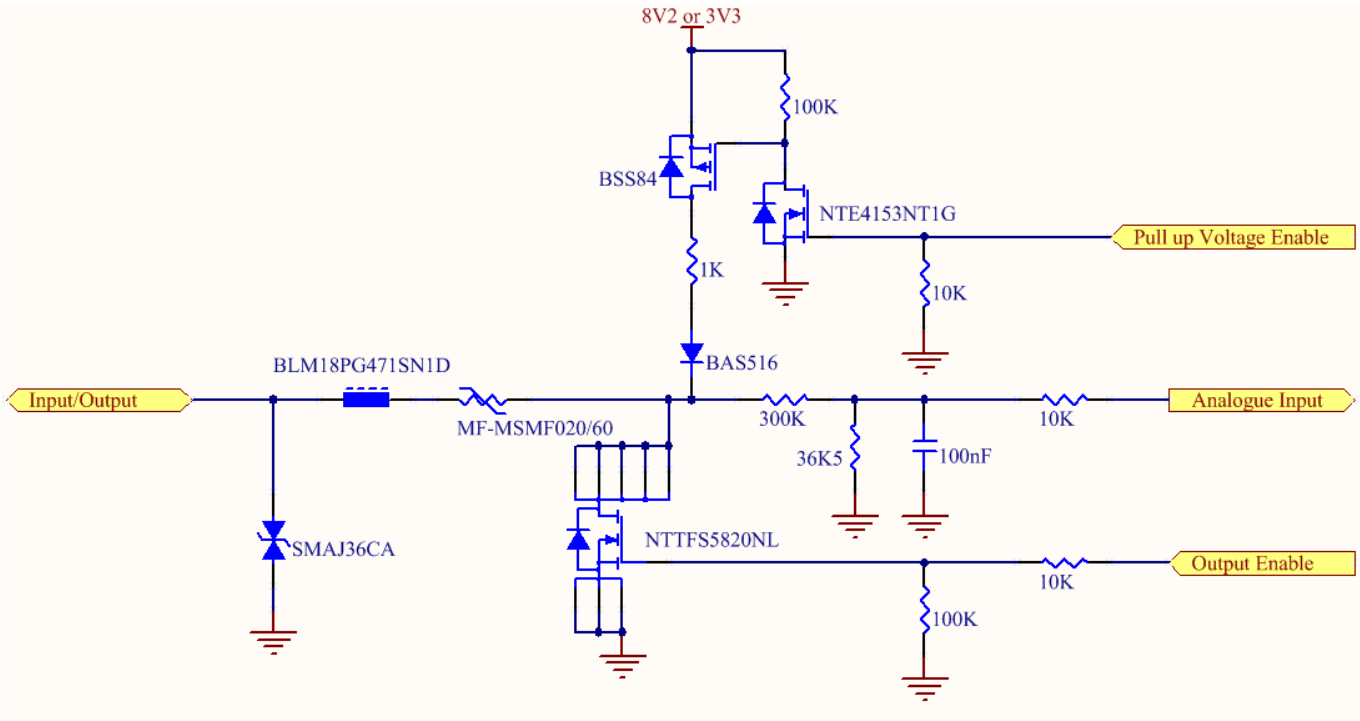
Appendix B. Inputs / Outputs

The NTC-550 Series router is equipped with a 6-way terminal block connector providing 3 identical multipurpose inputs and outputs as well as a dedicated ignition input. These inputs and outputs may be independently configured for various functions, including:

- NAMUR (EN 60947-5-6 / IEC 60947-5-6) compatible sensor input
- Proximity sensor input for use with contact closure (open/closed) type of sensors (PIR sensors, door/window sensors for security applications) with the input tamper detection possible (four states detected: open, closed, short and break) by the use of external resistors
- Analogue 2.7V to 30V input
- Digital input (the I/O voltage measured by the Analogue input and the software making a decision about the input state) with the threshold levels configurable in software
- Open collector output.

Hardware Interface

The interface of the 3 multipurpose inputs/outputs are based on the circuit diagram below



The Input/Output label is the physical connection to the outside world. There are protection devices and resistor dividers to condition the signal prior to it going into the processor. The three labels to the right are the interface to the processor. Output Enable activates the Transistor which provides an open collector (ground) output and can sink 200mA at 230C. It is protected by a resettable fuse and transient protection diode. If used with the pull up resistor, which can be activated by the Pull up Voltage Enable pin, then you can have a High or Low output rather than open drain. The resistor can be pulled up to 3V3 for Cmos compatible output or 8.2V by software. The Analogue Input pin can read values from 0V to 30V. It is divided by a resistor network to read appropriate levels in the processor. Depending on the sensor type used, the pull up resistor can be switched on or off. If using the NAMUR sensor configuration, the pull up will be activated to 8V2 by default.

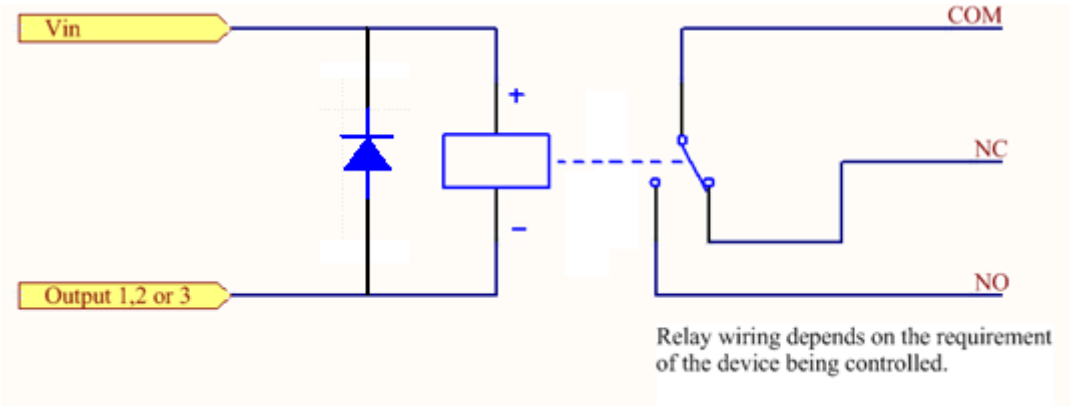
Wiring examples

The following examples are shown as a guide as to what can be achieved by the I/O features. It is up to the system integrator to have enough knowledge about the interface to be able to achieve the required results.

⚠ ***Important:*** *Lantronix does not offer any further advice on the external wiring requirements or wiring to particular sensors, and will not be responsible for any damage to the unit or any other device used in conjunction with it. Using outputs to control high voltage equipment can be dangerous. The integrator must be a qualified electrician if dealing with mains voltages controlled by this unit.*

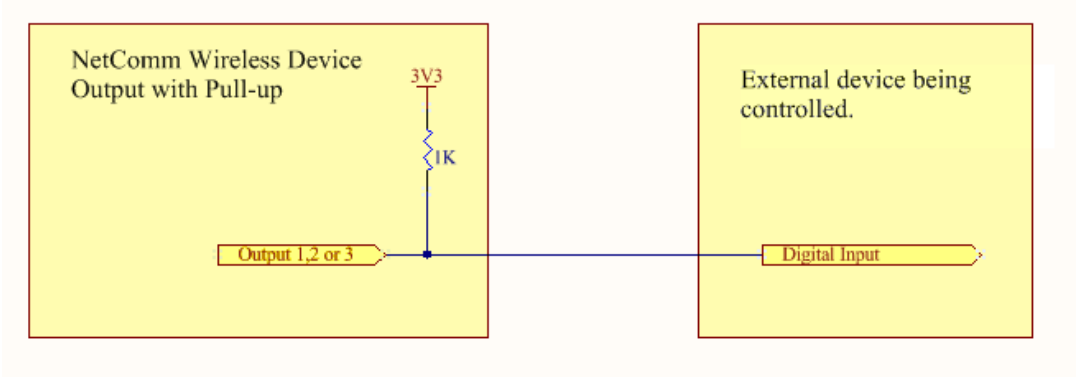
Open Collector Output driving a relay

Any output can be configured to control a relay. This is an example where the transistor will supply the ground terminal of the solenoid. External voltage is supplied to the other side of the solenoid.



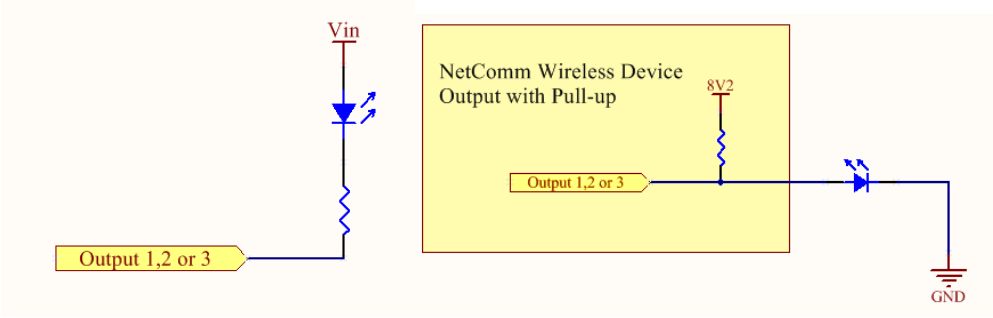
Logic level output

An output can be used with the pull up resistor to provide a logic level output which would be suitable to control an external digital device.



LED output

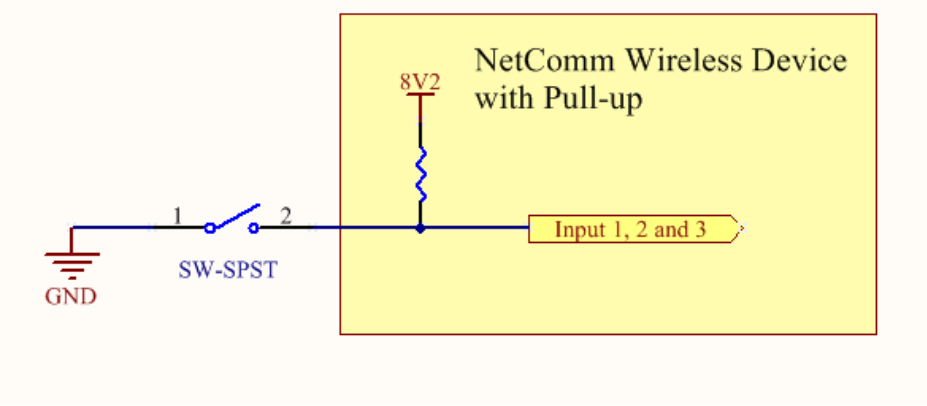
An LED can be controlled by simply providing an open collector ground to an externally powered LED Resistor value and Voltage will need to suit the LED type used. Alternatively, an LED can be powered using 8V2 via 1K resistor. The suitability of the LED will need to be investigated.



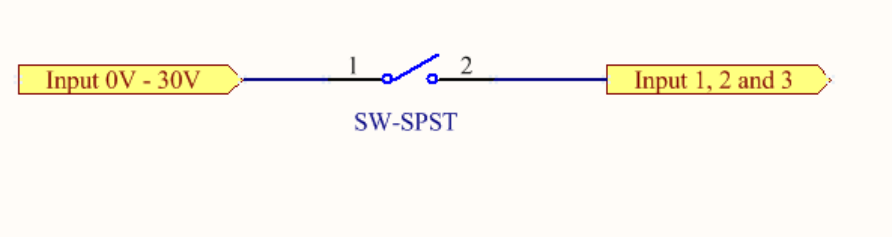
Digital inputs

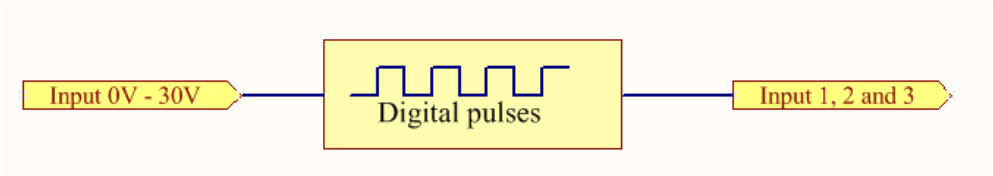
There are several ways to connect a digital input. A digital input can be anything from a simple switch to a digital waveform or pulses. The unit will read the voltage in as an analogue input and the software will decode it in a certain way depending on your configuration.

Below is a contact closure type input, which is detecting an Earth. Pull up is activated for this to work.



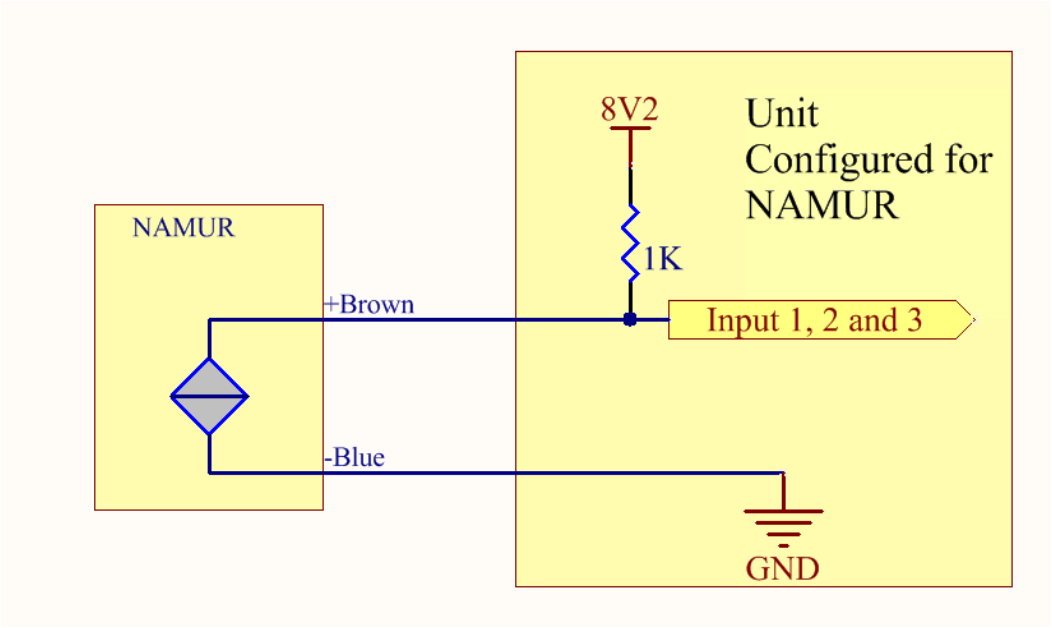
The following input detects an input going high. The turn on/off threshold can be set in the software.





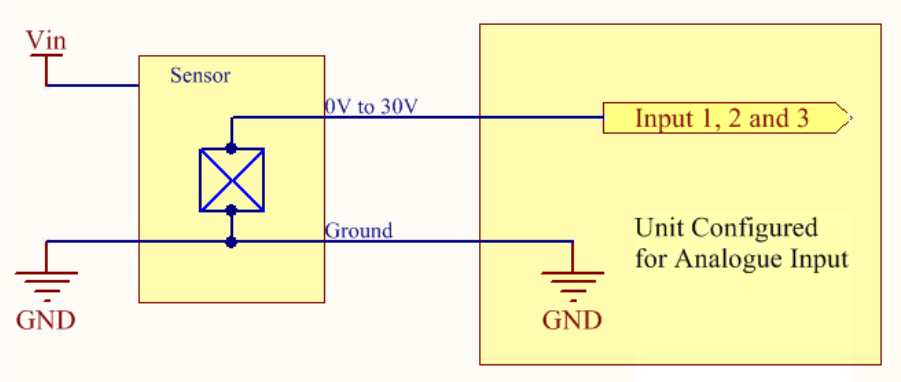
NAMUR sensor

A NAMUR sensor is a range of sensors which conform to the EN 60947-5-6 / IEC 60947-5-6 standards. They basically have two states which are reflected by the amount of current running through a sense resistor.



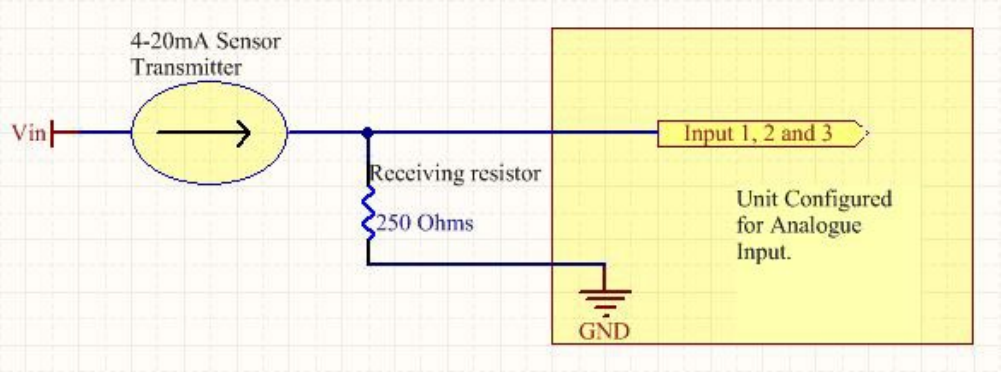
Analogue Sensor with Voltage output

There are various analogue sensors that connect directly to the unit which can provide a voltage output. These would require an external power source which may or may not be the same as the unit itself. The voltage range they provide can be between 2.7V and 30V. Some common sensor output ranges include 0V to 10V. These would work on the unit, The pull up resistor is not activated in this case.



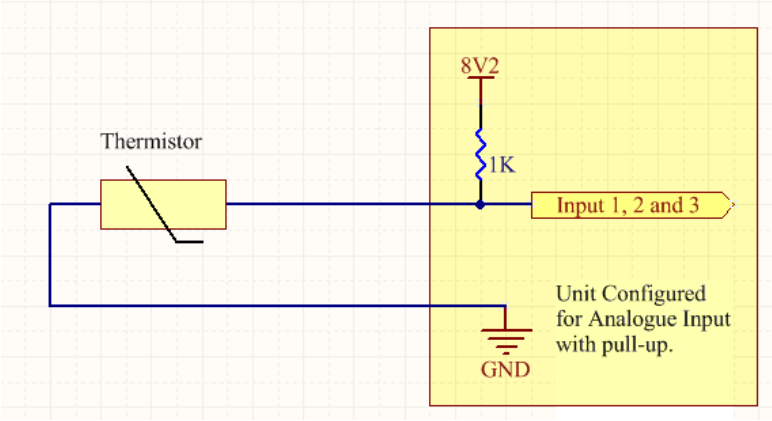
Analogue Sensor with 4 to 20mA output

Another common type of sensor type is the 4-20mA current loop sensor. It provides a known current through a fixed resistor, usually 750 ohms thus producing a voltage of 3v to 15V at the input. The sensor would require an external power source which may or may not be the same as the unit itself. It will also require an external resistor. The internal pull up resistor is not activated.



Analogue Sensor with Thermistor

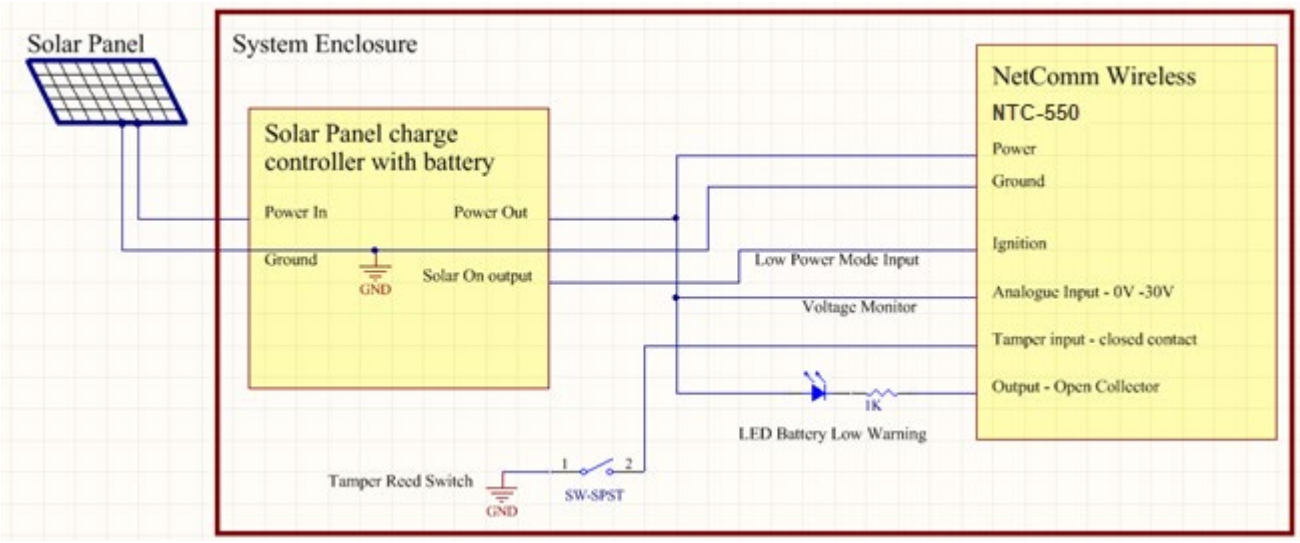
Some sensors work by changing resistance due to a change, such as temperature, light etc. These may be wired up to an external or internal power source and the resistance can be read into the analogue signal. This will require some software calibration like scaling or offset to map the voltage received to the sensor resistor value. An example below shows the internal pull-up voltage and 1K resistor activated. The voltage received depends on the combination of resistors and the value of the resistance of the sensor itself.



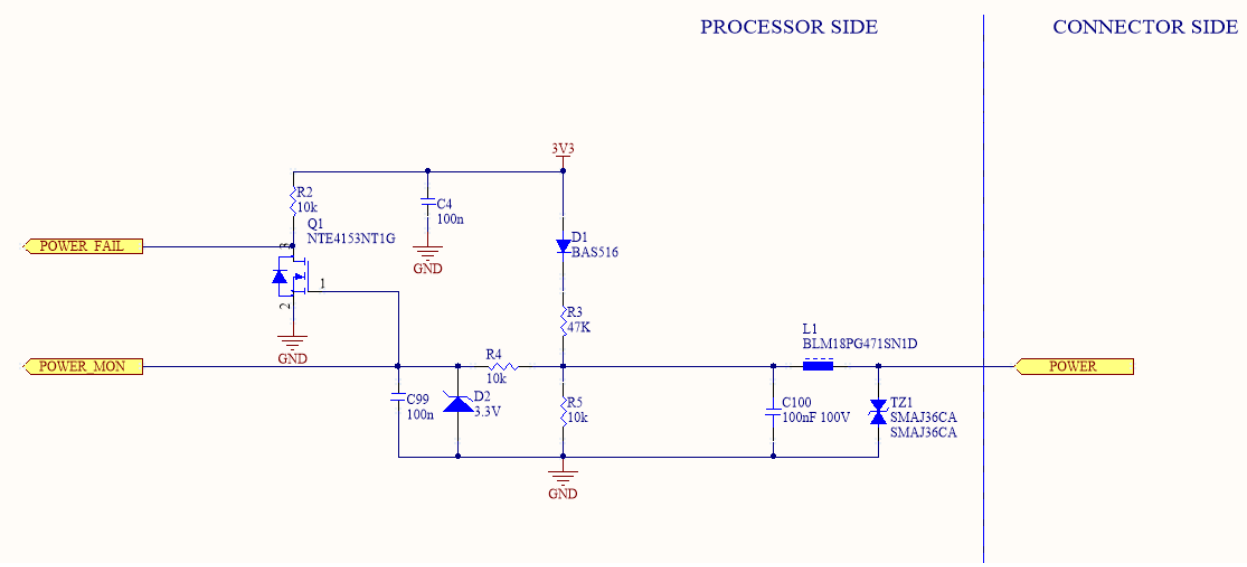
Note: *Need to choose NTC with maximum temperature to have impedance > 500 Ohms*

System Example – Solar powered router with battery backup

The previous examples of wiring can be used to come up with a system. The following test case is an example of how the I/O's can be used to enhance a simple router setup.



Power detection (ignition) input



The Power detection or Ignition input will detect the presence of three states from the connector side (outside world). It will detect three states, those being High, Low and Unconnected (floating).

The detection uses both analogue and digital inputs to the microprocessor.

- This is the “LOW” state:
  If input voltage at POWER port is less than 0.5V the transistor Q1 is shut, POWER FAIL is asserted high advising micro that no Backup Power is present on POWER port.
- This is the “Floating” state:
  If voltage at POWER port is 0.5-3V POWER FAIL signal de-asserts but POWER MON signal can be measured by ADC of micro and advise the system that there is little or no connection to the unit.
- This is the “HIGH” state:
  If voltage at POWER port is higher than 3.3V (which normally is an indication of presence of decent power source), the POWER FAIL is still de-asserted, the POWER MON will measure from 3.3V up to whatever voltage is detected. The maximum detection voltage is 30V and clamps to anything above 36V.

The states can be adjusted in software to fine tune the transition points between the states.

Appendix C. Compliance Information

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

Lantronix, Inc. 48 Discovery, Suite 250, Irvine, CA 92618 USA

Product Family:

NTC-550 Series
Conforms to the following standards or other normative documents:

Country	Specification
USA	In progress
Canada	In progress
EU	See EU Declaration of Conformity (figure C-1)
United Kingdom	See UK Declaration of Conformity (figure C-2)
Safety	EN IEC 62368-1 AS/NZS 62368-1

EU Declaration of Conformity

Figure C-1 EU Declaration of Conformity

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250 Irvine, CA 92618 USA
Model Name: NTC-552
Rated: 12Vdc, 3A
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)

- EN IEC 62368-1:2020/A11:2020

EMC Directive (2014/30/EU)

- EN 301 489-1 V2.2.3 (2019-11) Class B
- EN 301 489-17 V3.2.4 (2020-09)
- EN 301 489-19 V2.2.1 (2022-09)
- EN 301 489-52 V1.2.1 (2021-11)
- EN 55032:2015/A11:2020, Class B
- EN 55035:2017+A11:2020
- EN 61000-3-2:2014 Class A
- EN 61000-3-3:2013

RF Radio Directive (2014 / 53 / EU)

- EN 301 908-1 V15.2.1(2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.2.1 (2022-02)
- Draft EN 301-908-25 V15.1.1_15.0.9 (2021-06)
- EN 300 328 V2.2.2 (2019-07)
- EN 301 893 V2.1.1 (2017-05)
- EN 303 413 V1.2.1 (2021-04)

Health Directive (2014 / 53 / EU)

- EN IEC 62311:2020

RoHS 2011/65/EU(RoHS 2.0) & and its subsequent amendments Directive (EU) 2015/863

- EN 62321-2:2021

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: _____ Date: 26 Jun 2025
Name: Steve Burrington Title: Vice President RnD

CERT-00512 rev A

EU Statements

Table C-1 EU Statements

Code	Language	Statement
bg	Bulgarian	Lantronix, Inc., декларира, че този NTC-550 Series отговаря на основните изисквания и други приложими разпоредби на Директива 2014/53/EU. Пълният текст на декларацията на ЕС за съответствие е достъпен на следния интернет адрес: https://www.lantronix.com/products/ntc-550-series/ Известие на ЕС за ограничения при употреба: Това устройство е ограничено само за вътрешна употреба. Може да не се работи наоткрито.
cs	Česky [Czech]	Lantronix, Inc. tímto prohlašuje, že tento NTC-550 Series je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. Úplné znění ES prohlášení o shodě je k dispozici na této internetové adrese: https://www.lantronix.com/products/ntc-550-series/ Oznámení EU o omezení používání: Toto zařízení je omezeno pouze na použití uvnitř. Nesmí být provozován venku.
da	Dansk [Danish]	Undertegnede Lantronix, Inc. erklærer herved, at følgende udstyr NTC-550 Series overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. Den fulde tekst til EU-overensstemmelseserklæringen er tilgængelig på følgende internetadresse: https://www.lantronix.com/products/ntc-550-series/ EU-meddelelse om begrænsninger i brug: Denne enhed er kun begrænset til indendørs brug. Det betjenes måske ikke udendørs.
de	Deutsch [German]	Hiermit erklärt Lantronix, Inc., dass sich das Gerät NTC-550 Series in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EUbefindet. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse abrufbar: https://www.lantronix.com/products/ntc-550-series/ EU-Hinweis zu Nutzungsbeschränkungen: Dieses Gerät darf nur in Innenräumen verwendet werden. Es darf nicht im Freien betriebenwerden.
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix, Inc. seadme NTC-550 Series vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. EL-i vastavusdeklaratsiooni täielik tekst on saadaval järgmisel Interneti-aadressil: https://www.lantronix.com/products/ntc-550-series/ EL-i teade kasutuspiirangute kohta: seda seadet saab kasutada ainult siseruumides. Seda ei tohi õues kasutada.

Code	Language	Statement
en	English	Hereby, Lantronix, Inc., declares that this NTC-550 Series is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.lantronix.com/products/ntc-550-series/ EU Notice of Restrictions on Use: This device is limited to indoor use only. It may not be operated outdoors.
es	Español [Spanish]	Por medio de la presente Lantronix, Inc. declara que el NTC-550 Series module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: https://www.lantronix.com/products/ntc-550-series/ Aviso de restricciones de uso de la UE: este dispositivo está limitado solo para uso en interiores. No puede ser operado al aire libre.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix, Inc. ΔΗΛΩΝΕΙ ΟΤΙ NTC-550 Series ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ διατίθεται στην ακόλουθη διεύθυνση διαδικτύου: https://www.lantronix.com/products/ntc-550-series/ Ειδοποίηση της ΕΕ για περιορισμούς χρήσης: Η συσκευή αυτή περιορίζεται μόνο σε εσωτερικούς χώρους χρήσης. Μπορεί να μην λειτουργεί σε εξωτερικούς χώρους.
fr	Français [French]	Par la présente Lantronix, Inc. déclare que l'appareil NTC-550 Series est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante: https://www.lantronix.com/products/ntc-550-series/ Avis de restrictions d'utilisation de l'UE: Cet appareil est limité à une utilisation en intérieur uniquement. Il ne doit pas être utilisé àl'extérieur
is	Icelandic	Hér með lýsir Lantronix, Inc. því yfir að NTC-550 Series sé í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53 / ESB. Í heildartexta ESB-samræmisyfirlýsingarinnar er að finna á eftirfarandi internetfangi: https://www.lantronix.com/products/ntc-550-series/ Tilkynning ESB um takmarkanir á notkun: Þetta tæki er eingöngutakmarkað við notkun innanhúss. Það má ekki nota það úti.
it	Italiano [Italian]	Con la presente Lantronix, Inc. dichiara che questo NTC-550 Series è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.

Code	Language	Statement
		Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: https://www.lantronix.com/products/ntc-550-series/ Avviso di restrizioni d'uso dell'UE: questo dispositivo è limitato esclusivamente all'uso in interni. Potrebbe non essere utilizzatoall'aperto.
lv	Latviski [Latvian]	Ar šo Lantronix, Inc. deklarē, ka NTC-550 Series atbilst Direktīvas 2014/ 53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā tīmekļa vietnē: https://www.lantronix.com/products/ntc-550-series/ ES paziņojums par lietošanas ierobežojumiem: šo ierīci var izmantot tikai iekštelpās. To nedrīkst darbināt ārpus telpām.
lt	Lietuvių [Lithuanian]	Šiuo Lantronix, Inc. deklaruoja, kad šis NTC-550 Series atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. Visą ES atitikties deklaracijos tekstą galite rasti šiuo interneto adresu: https://www.lantronix.com/products/ntc-550-series/ ES pranešimas apie naudojimo apribojimus: Šis prietaisas skirtas naudoti tik patalpose. Jo negalima naudoti lauke.
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix, Inc. dat het toestel NTC-550 Series overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: https://www.lantronix.com/products/ntc-550-series/ EU kennisgeving van gebruiksbeperkingen: dit apparaat is beperkt tot gebruik binnenshuis. Het mag niet buitenshuis worden gebruikt.
mt	Malti [Maltese]	Hawnhekk, Lantronix, Inc., jiddikjara li dan NTC-550 Series jikkonforma malħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU. It-test sħiħ tad-dikjarazzjoni ta 'konformità tal-UE huwa disponibbli flindirizz tal-internet li ġej: https://www.lantronix.com/products/ntc-550-series/ Avviż tal-UE dwar Restrizzjonijiet fuq l-Użu: Dan l-apparat huwa limitat għal użu ġewwa biss. Ma jistax jitħaddem barra.
hu	Magyar [Hungarian]	Alulírott, Lantronix, Inc. nyilatkozom, hogy a NTC-550 Series megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. Az EU-megfelelőségi nyilatkozat teljes szövege a következő internetes címen érhető el: https://www.lantronix.com/products/ntc-550-series/ EU értesítés a korlátozásokról: Ez az eszköz csak beltéri használatra korlátozódik. Lehet, hogy szabadban nem üzemeltethető.
no	Norwegian	Lantronix, Inc. erklærer herved at denne NTC-550 Series er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53 / EU.

Code	Language	Statement
		Den fullstendige teksten til EU-samsvarserklæringen er tilgjengelig på følgende internettadresse: https://www.lantronix.com/products/ntc-550-series/ EUs merknad om bruksbegrensninger: Denne enheten er bare begrenset til innendørs bruk. Det kan hende at den ikke brukesutendørs.
pl	Polski [Polish]	Niniejszym Lantronix, Inc. oświadcza, że NTC-550 Series jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. Pełny tekst deklaracji zgodności EU jest dostępny pod następującym adresem internetowym: https://www.lantronix.com/products/ntc-550-series/ Zawiadomienie UE o ograniczeniach użytkowania: To urządzenie jest przeznaczone wyłącznie do użytku w pomieszczeniach. Nie można go obsługiwać na zewnątrz.
pt	Português [Portuguese]	Lantronix, Inc. declara que este NTC-550 Series está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. O texto completo da declaração UE de conformidade está disponível no seguinte endereço na Internet: https://www.lantronix.com/products/ntc-550-series/ Aviso da UE de restrições de uso: Este dispositivo está limitado apenas ao uso interno. Não pode ser operado ao ar livre.
ro	Romanian	Prin prezenta, Lantronix, Inc., declară că acest NTC-550 Series respect cerințele esențiale și alte dispoziții relevante din Directiva 2014/53 / UE. Textul complet al declarației de conformitate a UE este disponibil la următoarea adresă de internet: https://www.lantronix.com/products/ntc-550-series/ Notificarea UE privind restricțiile de utilizare: Acest dispozitiv este limitat numai la uz interior. Este posibil să nu funcționeze în aer liber.
sr	Serbian	Овиме, Лантроник, Инц., изјављује да је овај NTC-550 Series у складу са суштинским захтевима и осталим релевантним одредбама Директиве 2014/53 / ЕУ. Комплетан текст ЕУ изјаве о усаглашености доступан је на следећој Интернет адреси: https://www.lantronix.com/products/ntc-550-series/ Обавештење ЕУ о ограничењима употребе: Овај уређај је ограничен само на унутрашњу употребу. Можда се не користи на отвореном.
sl	Slovensko [Slovenian]	Lantronix, Inc. izjavlja, da je ta NTC-550 Series v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu: https://www.lantronix.com/products/ntc-550-series/ Obvestilo EU o omejitvah uporabe: Ta naprava je omejena samo na notranjo uporabo. Morda ga ne uporabljate na prostem.
sk	Slovensky [Slovak]	Lantronix, Inc. týmto vyhlasuje, že NTC-550 Series enterprise Wi-Fi IoT module spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.

Code	Language	Statement
		Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: https://www.lantronix.com/products/ntc-550-series/ Oznámenie EÚ o obmedzeniach pri používaní: Toto zariadenie je obmedzené iba na použitie v interiéri. Nesmie sa používať vonku.
fi	Suomi [Finnish]	Lantronix, Inc. vakuuttaa täten että NTC-550 Series tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavana seuraavassa Internet-osoitteessa: https://www.lantronix.com/products/ntc-550-series/ EU: n ilmoitus käyttörajoituksista: Tämä laite on rajoitettu vain sisäkäyttöön. Sitä ei saa käyttää ulkona.
sv	Svenska [Swedish]	Härmed intygar Lantronix, Inc. att denna NTC-550 Series står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: https://www.lantronix.com/products/ntc-550-series/ EU-meddelande om begränsningar för användning: Den här enheten är endast begränsad till inomhusbruk. Det får inte användas utomhus.

UK Declaration of Conformity

Figure C-2 –UK Declaration of Conformity

LANTRONIX®

UK CA

UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250 Irvine, CA 92618 USA
Model Name: NTC-552
Rated: 12Vdc, 3A
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

TÜVRheinland

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Electrical Equipment Regulations 2016

- EN IEC 62368-1:2020/A11:2020
- EN IEC 62311:2020

Electromagnetic Compatibility Regulations 2016

- EN 301 489-1 V2.2.3 (2019-11) Class B
- EN 301 489-17 V3.2.4 (2020-09)
- EN 301 489-19 V2.2.1 (2022-09)
- EN 301 489-52 V1.2.1 (2021-11)
- EN 55032:2015/A11:2020, Class B
- EN 55035:2017+A11:2020
- EN 61000-3-2:2014 Class A
- EN 61000-3-3:2013

Radio Equipment Regulations 2017

- EN 301 908-1 V15.2.1(2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.2.1 (2022-02)
- Draft EN 301-908-25 V15.1.1_15.0.9 (2021-06)
- EN 300 328 V2.2.2 (2019-07)
- EN 301 893 V2.1.1 (2017-05)
- EN 303 413 V1.2.1 (2021-04)

RoHS
UK SI 2012 No. 3032 for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and 6(c).
2011/65/EU(RoHS 2.0) & and its subsequent amendments Directive (EU) 2015/863

- BS EN 62321-2:2021

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: _____ Date: 26 Jun 2025
Name: Steve Burrington Title: Vice President RnD

CERT-00513 rev A