LANTRONIX®

NTC-220 Series User Guide

NTC-221, NTC-222, NTC-223, NTC-224, NTC-225, & NTC-227

Part Number PMD-00323
Revision A September 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 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 common identifier and device name 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
September 2025	A	Reformatted to Lantronix For prior document history, see *Appendix I. NetComm Revision History*

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

Contents

List of Tables

1. Overview

Introduction

This document provides you all the information you need to set up, configure, and use the Lantronix NTC-220 Series routers, specifically NTC-221, NTC-222, NTC-223, NTC-224, NTC-225, and NTC-227 routers.

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 common identifier and device name router, please confirm that you have the following:

An electronic computing device with a working Ethernet network adapter and a web browser such as Internet Explorer®, 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

- Ruggedized industrial cellular router supporting 4G LTE Cat 1 with failover to 3G/2G.
- An Ethernet port, a configurable RS232/RS422/RS485 Serial port and three multi-purpose I/O ports for flexible local connectivity.
- Integrated GPS support with an active GPS Antenna via an external SMA connector. (not available on NTC-223)
- Industrial features, including a rugged enclosure, a wide operating temperature range, a wide input voltage range and multiple wall mounting options.
- Intelligent, Tri-Color LED display for clear, easy to read modem status information
- Ignition sensing port for graceful shutdown and startup in vehicle applications.
- Configurable power save mode with minimum current draw when not operational.
- VPN support for establishing a secure connection over public cellular network using OpenVPN.
- Embedded Linux based OS with a 1GHz processor and 512MB of flash memory storage allowing for the installation of custom, edge processing applications. Software Development Kit (SDK) is available.
- Web interface for easy centralized configuration and management from any PC and full feature management via secure SMS.
- Support for firmware upgrades over the air.
- Extensive device fleet management capabilities with support for TR-069, SNMP, LWM2M.
- Roaming algorithm with prioritization for cost effective, flawless network connection across the globe.

Product features

The Lantronix NTC-220 Series router is a feature-packed Industrial IoT device designed to provide real-time wireless connectivity even in harsh environments at an affordable price. The Software Development Kit (SDK) allows you to develop your own software applications for large scale compatibility and an easy path to large deployments across a broad range of industries. The Lantronix NTC-220 Series router meets the global demand for a reliable and cost-effective Industrial IoT device that successfully caters to mass deployment across businesses.

Package contents

The Lantronix common identifier and device name Series router package consists of:

- 1 x Lantronix common identifier and device name Series router
- 2 x Cellular antennas
- 1 x 1.5 m Yellow Ethernet cable
- 1 x DIN rail mounting bracket

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-221	NTC-221-01-01	4G LTE IIoT Router for Australia and New Zealand

NTC-222	NTC-222-01-01	4G LTE IIoT Router for Europe
NTC-224	NTC-224-01-01	4G LTE IIoT Router for AT&T (US)
NTC-225	NTC-225-01-01	4G LTE IIoT Router for Verizon Wireless (US)
NTC-227	NTC-227-01-01	4G LTE IIoT Router

3. Physical dimensions and indicators

Physical dimensions

Below is a list of the physical dimensions of the Lantronix common identifier and device name Series router.

Figure 3-1 NTC-220 Series router top view

Table 3-1 NTC-220 Series dimensions

NTC-220 SERIES dimensions	
Length	148 mm
Depth	107 mm
Height	34 mm
Weight	221 grams

Interfaces

The following interfaces are available on the NTC-220 Series router:

Figure 3-2 Left end interfaces

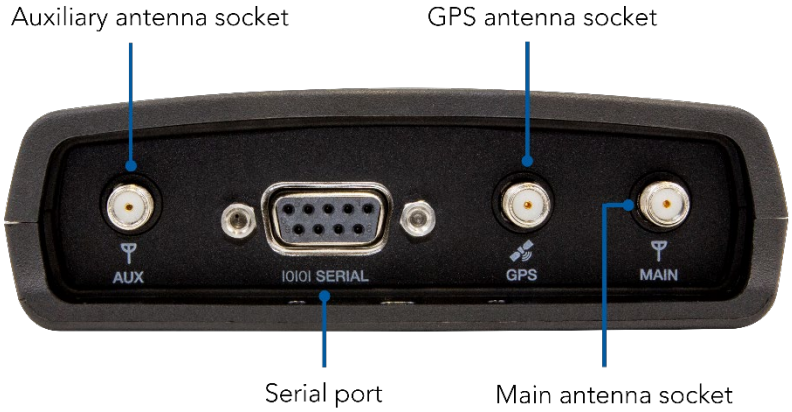
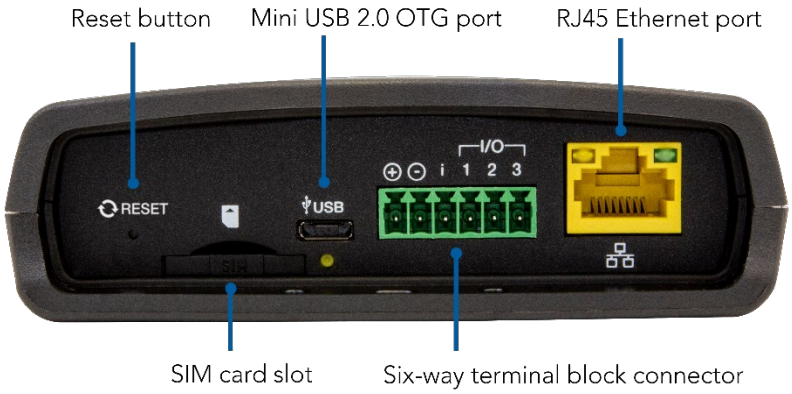


Figure 3-3 Right end interfaces



***Note:** The **NTC-223** does not support GPS and does not have a GPS antenna socket.*

Table 3-2 Interfaces

Item	Description
Main antenna socket	SMA female connector for main antenna.
Aux antenna socket	SMA female connector for auxiliary antenna (receive diversity).
GPS antenna socket	SMA female connector for an active GPS antenna.
Six-way terminal block connector	Connect power source, ignition and I/O wires here. Power, ignition and I/O wires may be terminated on optional terminal block and connected to DC input jack. Refer to the diagram and table under the Installation section for correct wiring of the terminal block. Operates in the 8-40V DC range.
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 15 seconds to reboot to recovery mode. The LEDs are amber and extinguish in sequence to indicate that the router will reboot to recovery mode if the button is released during this period. Press and hold for 15 to 20 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.
SIM card slot	Insert SIM card here.
RJ45 Ethernet port	Connect one or several devices via a network switch here.
Mini USB 2.0 OTG port	Provides connectivity for optional external storage or a USB Ethernet dongle. Supplies up to 0.5A to connected device.
Serial port	Female DB9 port supporting 9-wire RS-232, RS-485 or RS-422 (software selectable).

LED indicators

The NTC-220 Series router uses 8 LEDs to display the current system and connection status.

Figure 3-4 NTC-220 Series router LED indicators

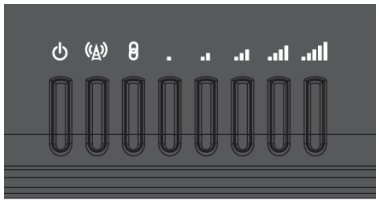


Table 3-3 LED indicators

LED	Name	Colour	State	Description
⏻	Power	⊘	Off	Power off
		■	Double flash	Powering up
		■	On	Power on
		■	On	Power on in recovery mode
		■	Slow flashing	Hardware error

	Network		On	Connected via WWAN
			Blinking	Traffic via WWAN
			Slow flashing	Connecting PDP
			On	Registered network
			Slow flashing	Registering network
			Slow flashing	SIM PIN locked
			Fast flashing	SIM PUK locked
			On	Cannot connect or device is in Configuration mode, see the *Initialization* section for more information.
	GPS* / Customizable LED Indicator		Off	GPS function disabled
			On	GPS function is enabled but no satellite is detected.
			Slow flashing	Satellite detected, acquiring location.
			On	Satellite detected, location acquired.
	Signal strength		On	LTE
			On	WCDMA signal
			On	GSM/GPRS signal

Note: *The term "blinking" means that the LED may pulse, with the intervals that the LED is on and off not being equal. The term "flashing" means that the LED turns on and off at equal intervals.*

Note: *The NTC-223 does not support GPS.*

Signal strength LEDs

The following tables list the signal strength range corresponding with the number of lit signal strength LEDs.

LTE signal mapping (Green)

Table 3-4 Signal strength LED descriptions

Number of lit LEDs	Signal Strength
All LEDs unlit	No signal
1	−115 dBm to −119 dBm
2	−105 dBm to −114 dBm
3	−100 dBm to −104 dBm
4	−90 dBm to −99 dBm
5	> −90 dBm

WCDMA signal mapping (Amber)

Table 3-5 Signal strength LED descriptions

Number of lit LEDs	Signal strength
All LEDs unlit	< –109 dBm
1	–109 dBm to –102dBm
2	–101 dBm to –92 dBm
3	–91 dBm to –86 dBm
4	–85 dBm to –78 dBm
5	≥ –77 dBm

GSM/GPRS signal mapping (Red)

Table 3-6 Signal strength LED descriptions

Number of lit LEDs	Signal Strength
All LEDs unlit	≤ −109 dBm
1	−102 dBm to −108 dBm
2	−93 dBm to −101 dBm
3	−87 dBm to −92 dBm
4	−86dBm to −78 dBm
5	> −78 dBm

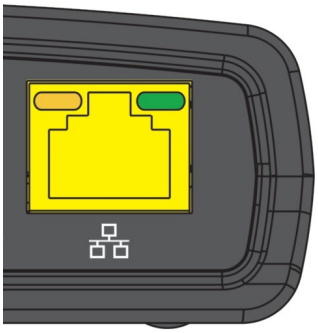
LED update interval

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

Ethernet port LED indicators

The Ethernet port of the NTC-220 Series router has two LED indicators on it.

Figure 3-5 NTC-220 Series Ethernet port LED indicators



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

Table 3-7 Ethernet port LED indicators description

LED	Status	Description
Green	On	There is a valid network link.
	Blinking	There is activity on the network link.
	Off	No valid network link detected.
Amber	On	The Ethernet port is operating at a speed of 100Mbps.
	Off	The Ethernet port is operating at a speed of 10 Mbps or no Ethernet cable is connected.

4. Placement of the router

The external high-performance antennas supplied with the router are designed to provide optimum cellular and Wi-Fi signal strength in a wide range of environments. 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.*

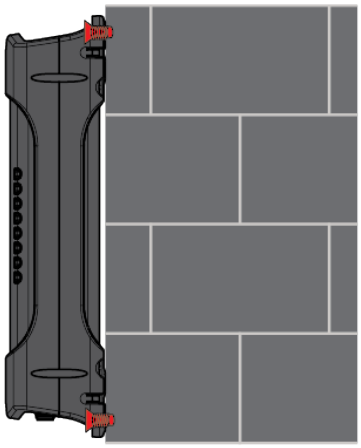
Mounting options

The NTC-220 Series router can be quickly and easily mounted in a variety of locations.

Mounted flat against the wall

When mounted flat against the wall, the NTC-220 Series router has a slimline form factor. Use appropriately sized screws in the mounting holes provided on the base of the unit.

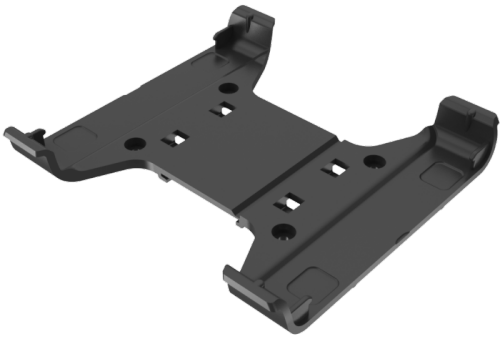
Figure 4-1 Wall mount – Flat against the wall



DIN rail mounting bracket

V Bend allows you to snap the DIN bracket onto the middle of a DIN rail rather than sliding it onto the end.

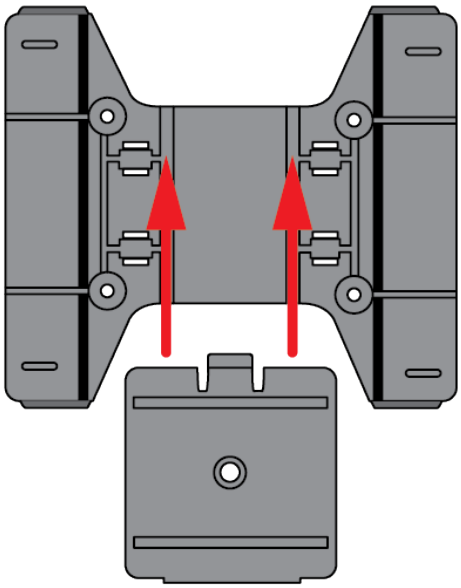
Figure 4-2 DIN rail mounting bracket



Horizontal DIN rail mounting adapter

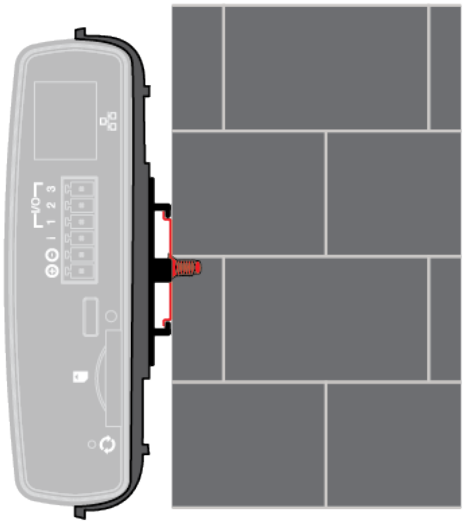
Used in conjunction with the DIN rail mounting bracket, this adapter lets you mount the NTC-220 Series in a horizontal orientation. With the DIN rail mounting bracket attached to the router, slide the adapter on to the bracket as shown in the image below. You can then mount the device horizontally on a DIN rail. Optionally, you may place a screw (max. 4.5mm diameter) through the centre hole of the adapter so that it doesn't move along the DIN rail.

Figure 4-3 Horizontal DIN rail mounting adapter



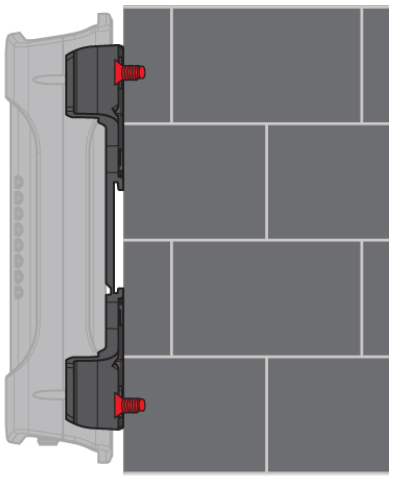
Wall mount with DIN rail mount adapter

Figure 4-4 Wall mount with DIN rail mount adapter



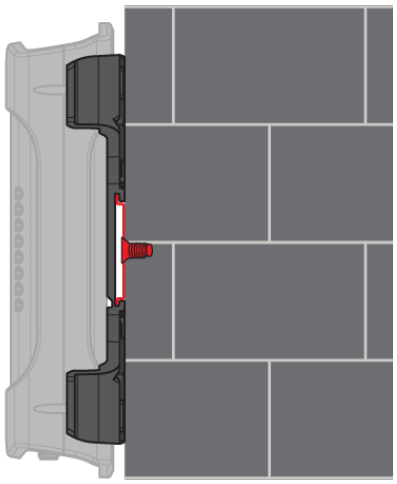
Wall mounted via DIN rail bracket

Figure 4-5 Wall mounted via DIN rail bracket



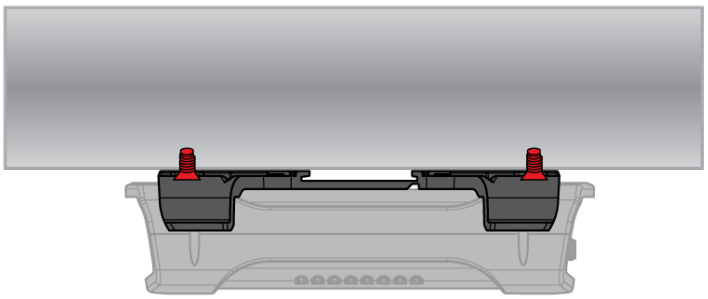
DIN rail mount

Figure 4-6 DIN rail mount



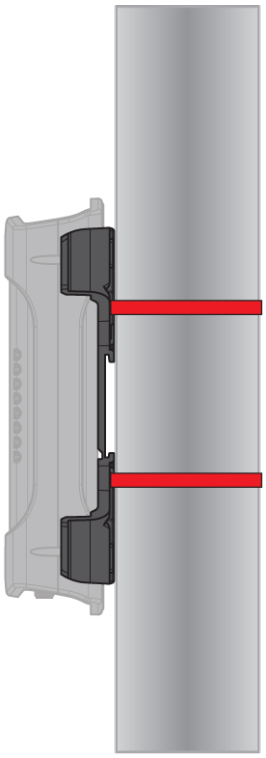
Ceiling mount via DIN rail bracket

Figure 4-7 Ceiling mount via DIN rail bracket



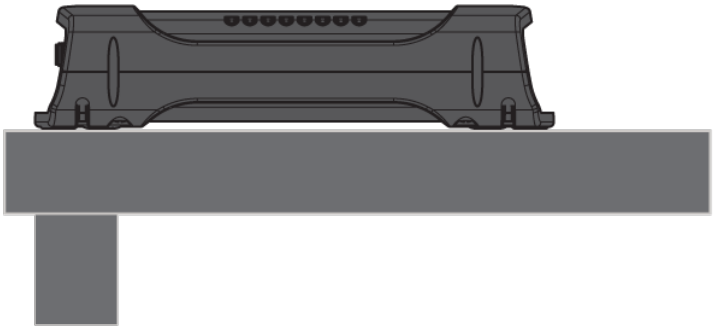
Pole mount using DIN rail bracket

Figure 4-8 Pole mount using DIN rail bracket



Desk mount

Figure 4-9 Desk mount



5. Installation and configuration of the NTC-220 Series router

Powering the router

The NTC-220 Series router can be powered in one of two ways:

- DC power input via 4-pin connector (8-40 V DC)
- DC power input via field terminated power source (8-40 V DC)

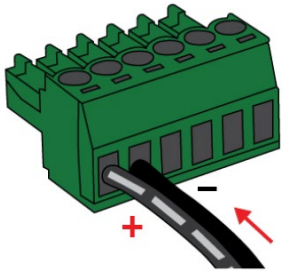
The green power LED on the router lights up when a power source is connected. Nominal power input is (12 V DC/1.5 A).

DC power via 6-pin 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

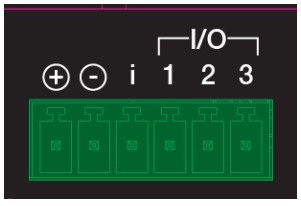


Table 5-1 Locking power block pin outs

Terminal	Description
+	Positive wire for power.
–	Ground wire.
i	Dedicated terminal for ignition detection.
I/O 1, 2, 3	Used for general purpose input/output (refer to the IO configuration section for more information).

Power consumption

To assist with power consumption planning, the following table summarises average power consumption during the various states of the NTC-220 Series router under normal usage conditions. It is important to note that this table serves as an indication only as the power consumed by the device is affected by many variables including signal strength, network type, and network activity.

Average power consumption figures

Table 5-2 Average power consumption figures

Power input	State	Power consumption
12V	Powered on, all functions disabled	1.38 W
12V	Powered on, connected to LTE and idle	1.92 W
12V	Powered on, connected to packet data with heavy traffic	4.86 W
12V	Peak power draw at maximum 4G module transmission power	5.88 W

Viewing power source information

You can view the current power input mode in the Advanced status section of the device's web user interface. This is useful for remotely monitoring the device. You can also use the Software Development Kit to access this information for advanced purposes (e.g. configuring SMS alerts to inform you of the power status of the router).

To view the router's power source information, log in to the router and expand the Advanced status box on the status page. See the Status section of this manual for more information on the status page.

Installing the router

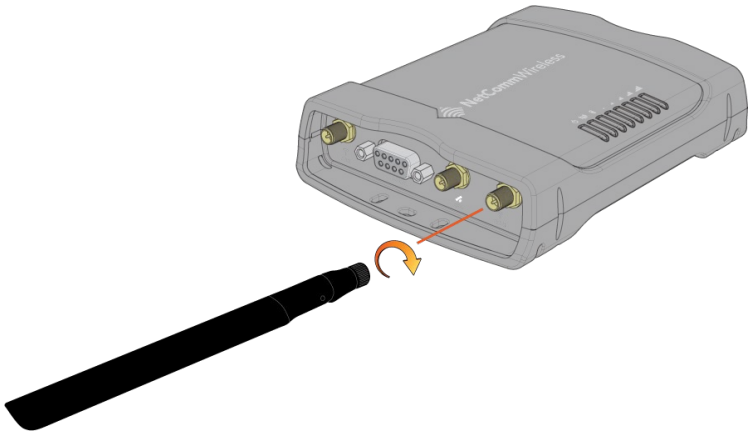
After you have mounted the router and connected a power source, follow these steps to complete the installation process.

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-220 series router. You can connect one device directly, or several devices using a network switch.

2. The NTC-220 Series router is shipped with caps on the Main, Auxiliary and GPS antenna sockets. To attach the supplied antennas, first remove the antenna socket caps from the Main and Auxiliary antenna sockets by turning them in an anticlockwise direction, then screw the antennas onto the sockets by turning them in a clockwise direction. Please refer to the Interfaces section for the antenna socket layout. If you have purchased a GPS antenna, remove the socket cap from the GPS antenna socket and attach the antenna to the socket in the same manner.

Note: *The NTC-223 router does not support GPS.*

Figure 5-3 Attaching the antennas



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, as shown below.

Figure 5-4 Inserting the SIM card

4. Ensure the external power source is switched on and wait 2 minutes for your NTC-220 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.

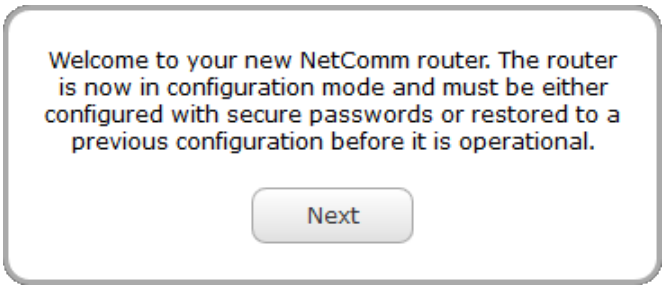
Important: *The HTTP protocol is disabled by default, secure HTTP (HTTPS) is the default protocol. HTTP access is available but must be manually enabled.*

Initialization

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

To complete the setup:

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

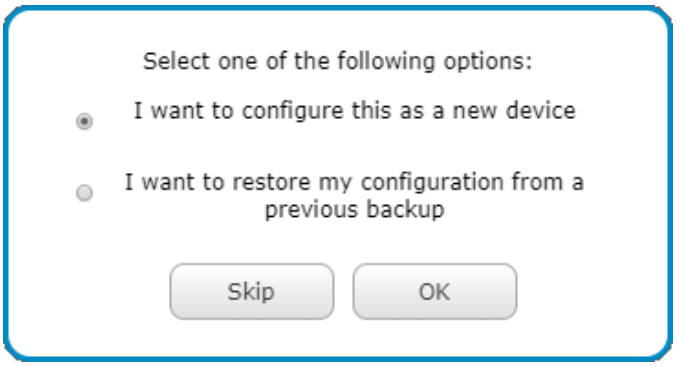


2. Enter the factory default password which is printed on the device label then click the **Next** button.

3. Select whether to configure the router as a new device or to 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 the **OK** button.



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 security criteria set out below:

- 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 and US television and 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 Passwords dialog page

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

Skip (use factory default password)

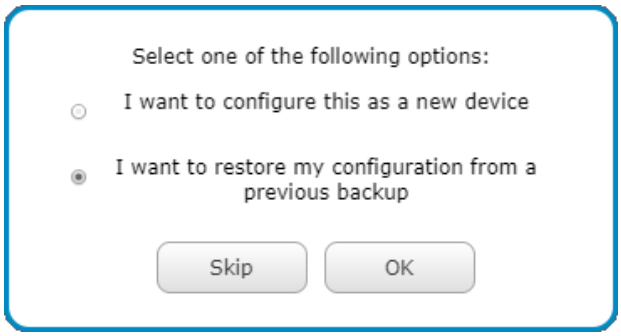
If you are satisfied with the level of security provided by the factory default password printed on your router's label, click the **Skip** button.

You will be logged out and asked to log back in using the factory default password.

Restore backed up configuration settings (use previous password)

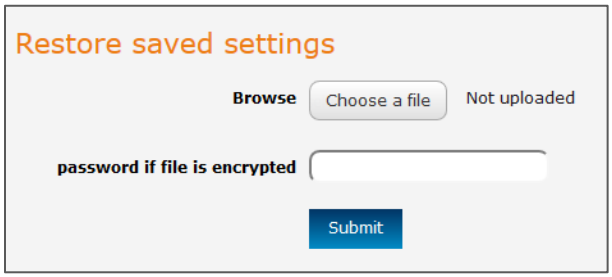
If you have made a backup of your configuration settings and would like to use the password(s) that you had previously created, select the ⊙ **I want to restore my configuration from a previous backup** and then upload and reapply all the settings in your backup file including your previous password(s).

1. Select ⊙ I want to restore my configuration from a previous backup then click the OK button.



2. Click the **Choose a file** button and locate the backup file on your computer. If the backup file is encrypted, enter the password, then click the **Submit** button to reapply all the previous configuration settings and passwords.

Figure 6-2 Configuration mode landing page



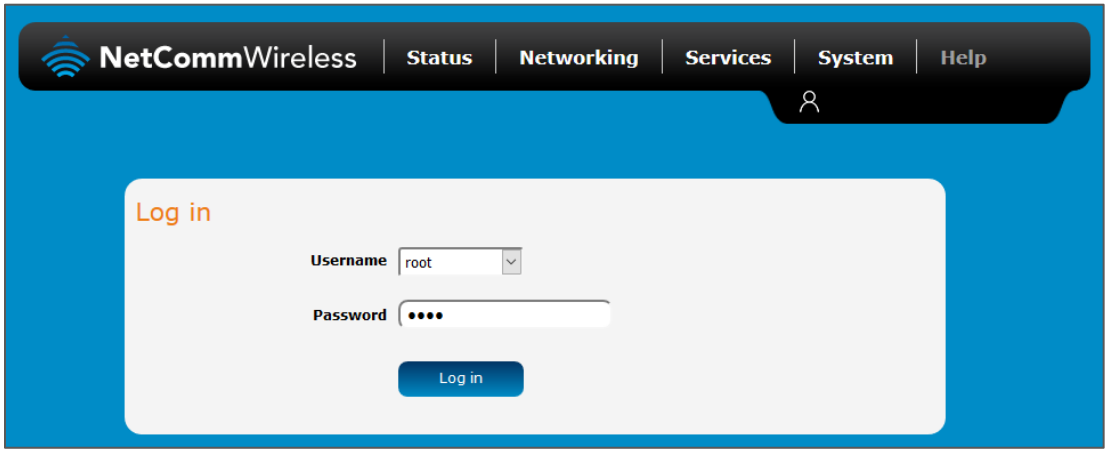
3. The router restores the previous configuration and then reboots.

Logging in

To login into the router:

1. Select the **Username** (root or user) and enter the **Password** that you configured during the initialization process.
2. Click **Log in**, the Status page is displayed.

Figure 6-3 Log in prompt for the web-based user interface



Note: *The user 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 of the web interface provides system related information and is displayed when you log in to the NTC-220 Series router management console. The status page shows System information, LAN details, Cellular connection status, Packet data connection status, Wireless LAN status and Advanced status details. You can toggle the sections from view by clicking the ▽ or △ buttons to show or hide them. Extra status boxes will appear as additional software features are enabled (e.g. VPN connectivity).

Figure 7-1 NTC-220 status page

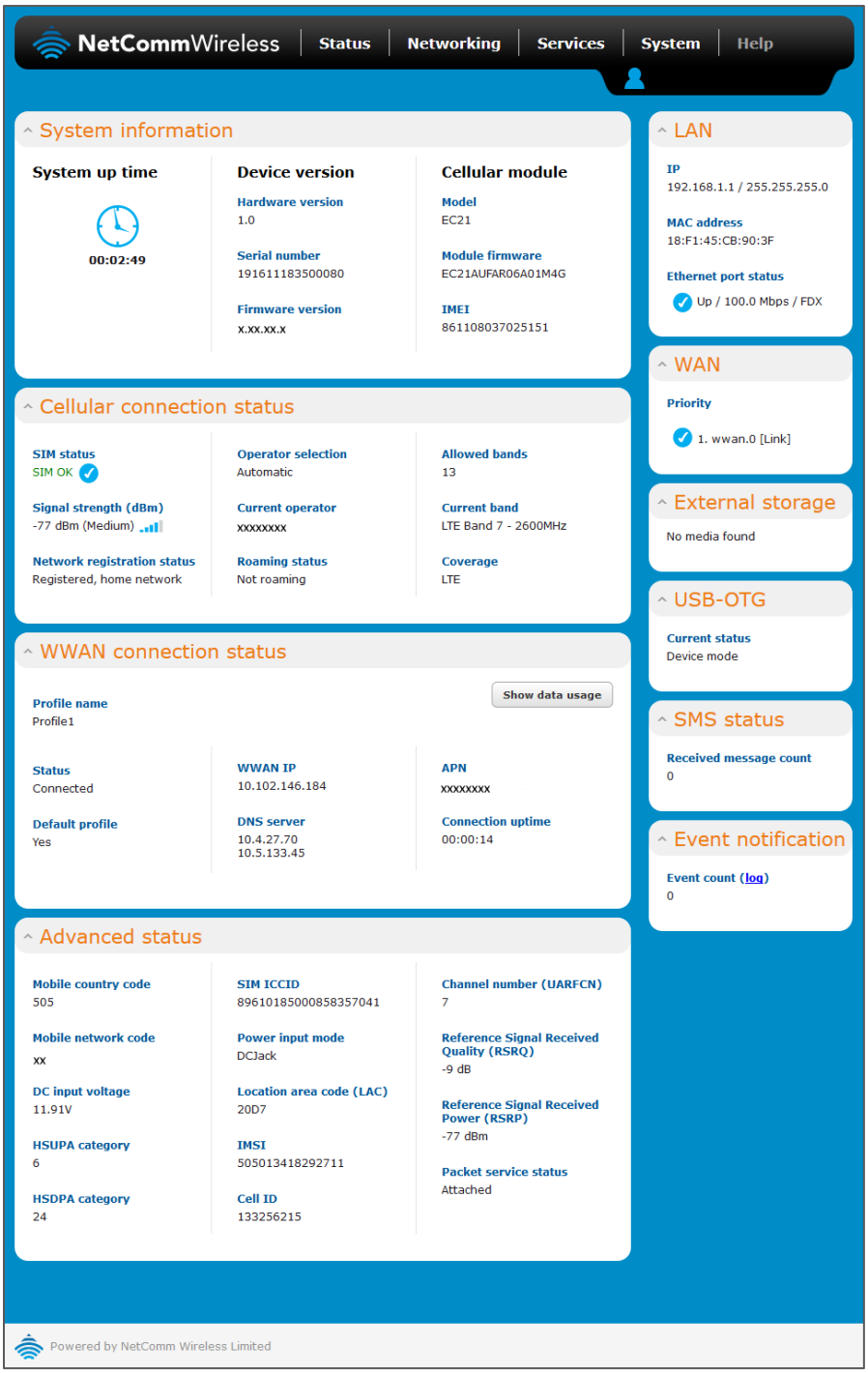


Table 7-1 Status page item details

Item	Definition
System information	
System up time	The current up time (the time since the router was last turned on) of the router.
Board version	The hardware version of the router.
Serial number	The serial number of the router.
Firmware version	The firmware version of the router
Hardware version	The commercial product name which helps to identify the available features of the router.
Model	The type of phone module and the firmware version of the module.
Module firmware	The firmware revision of the phone module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
LAN	
IP	The IP address and subnet mask of the router.
MAC address	The MAC address of the router.
LAN Port Status	Displays the current status of the LAN port and its operating speed.
WAN	
WAN/LAN port status	Displays the current status of the WAN/LAN port and its operating speed.
Priority	Displays the priority of the available WAN connections with the interface at the top having the highest priority.
External Storage	
External Storage	Lists the type and size of external storage (onboard/USB), if connected.
USB-OTG	
Current status	Displays the current status of the USB-OTG port (Device mode or Host mode)
SMS status	

Received message count	Number of SMS messages received.
Event notification	
Event count	Displays the number of notifications sent using the Event notification feature.
Cellular connection status	
Network registration status	The status of the router's registration for the current network.
SIM Status	Displays the activation status of the SIM in the router.
Provider	The current operator network in use.
Signal strength (dBm)	The current signal strength measured in dBm
Frequency	Displays the band and frequency currently in use.
Coverage	The type of mobile coverage being received by the router.
Roaming status	The roaming status of the router.
WWAN connection status	
Profile name	The name of the active profile.
Status	The connection status of the active profile.
Default profile	Indicates whether the current profile in use is the default profile.
WWAN IP	The IP address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary DNS servers for the WWAN connection.
APN	The Access Point Name currently in use.
Connection uptime	The length of time of the current mobile connection session.
Show data usage button	Click to enlarge the status box to display the amount in bytes of Data received, Data sent and Total data usage. For each session you can also Show duration or Show end time.
Ethernet WAN connection status	
No.	The index number of the WAN interface.

Name	The device name as it is known on the system.
Status	Displays whether the interface is up or down.
IP address	The IP address assigned to the Ethernet interface.
Netmask	The Netmask address assigned to the Ethernet interface.
Gateway	The Gateway address assigned to the Ethernet interface.
WLAN AP status	
No.	The index number of the SSID profile.
Status	Displays whether the profile is enabled or disabled.
Network Name (SSID)	The network name (SSID) that clients use to identify the access point.
Channel	The wireless channel that the access point operates on.
Network authentication	The type of security on the wireless network.
Station info	Click the Station info link to display information about connected clients.
WLAN client connection status	
Remote SSID	Shows the network name (SSID) of the wireless network.
BSSID	Shows the MAC address of the WLAN interface of the MachineLink 4G.
Security	The type of security/encryption in use on the wireless network.
IP address	The IP address assigned to the WLAN interface by the AP to which it is connected.
DNS server	The primary DNS server for the WLAN connection.
Status	Shows the current status of the wireless LAN network.
Advanced status	
Country code	The Mobile Country Code (MCC) of the router.
Network code	The Mobile Network Code (MNC) of the router.
DC input voltage	Displays the current voltage of the power input source provided via the DC Input jack

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.
Reference Signal Received Power (RSRP)	A cell-specific reference signal used to determine RSRP.
HSUPA category	Displays the HSUPA category which is category 6 for the NTC-220 router. This allows uplink speeds of up to 5.76Mbps.
HSDPA category	Displays the HSDPA category which is category 24 for the NTC-220 router. This allows downlink speeds of up to 42Mbps.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the router, a unique number up to 19 digits in length.
Power input mode	Displays the power source being used.
Location area code (LAC)	The ID of the cell tower grouping the current signal is broadcasting from.
IMSI	The International mobile subscriber identity is a unique identifier of the user of a cellular network.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile network signal.
Channel number (UARFCN)	The channel number of the current cellular connection.
Module PRIID Revision	Module version used for customization.
Module PRIID PRI part number	The part number of the Module PRIID.
PRI carrier	The carrier network.
PRI config	Configuration file for the current carrier network.

8. Networking

The Networking section provides configuration options for Wireless WAN, LAN, Wireless settings, Ethernet WAN/LAN interface assignment, PPPoE, WAN failover priorities, Routing and VPN connectivity.

Wireless WAN

Data connection

The data connection page allows you to configure and enable/disable connection profiles. To access this page, click on the **Networking** menu, and under the **Wireless WAN** menu, select the **Data connection** item.

Each profile refers to a set of configuration items which are used by the router to activate a Packet Data (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 for advanced networking configuration where multiple simultaneous PDP contexts may be required.

Figure 8-1 Data connection settings

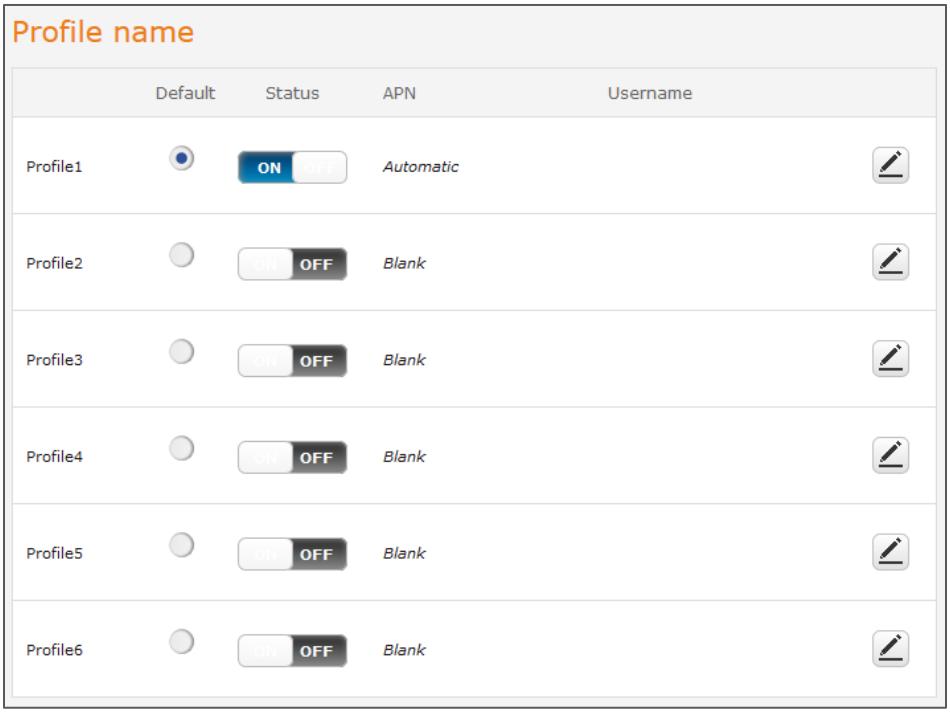


Table 8-1 Data connection item details

Item	Definition
Profile name	
Default	Sets the corresponding profile to be the default gateway for all outbound traffic except traffic for which there are configured static route rules or profile routing settings.
Status	Toggles the corresponding profile on and off. Only one profile may be turned on at any time.

APN	The APN configured for the corresponding profile.
Username	The username used to log on to the corresponding APN.

Connecting to the mobile broadband network

The 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 4G/3G network and switch easily between different connection settings.

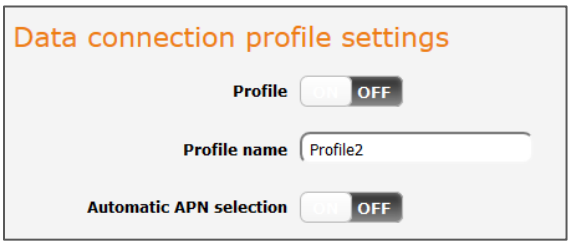
For advanced networking purposes, you may activate a maximum of two profiles simultaneously (dependent on network support). When activating two connection profiles, you should avoid selecting two profiles with the same APN as this can cause only one profile to connect. Similarly, activating two profiles which are both configured to automatically determine an APN can cause a conflict and result in neither profile establishing a connection. We recommend 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:

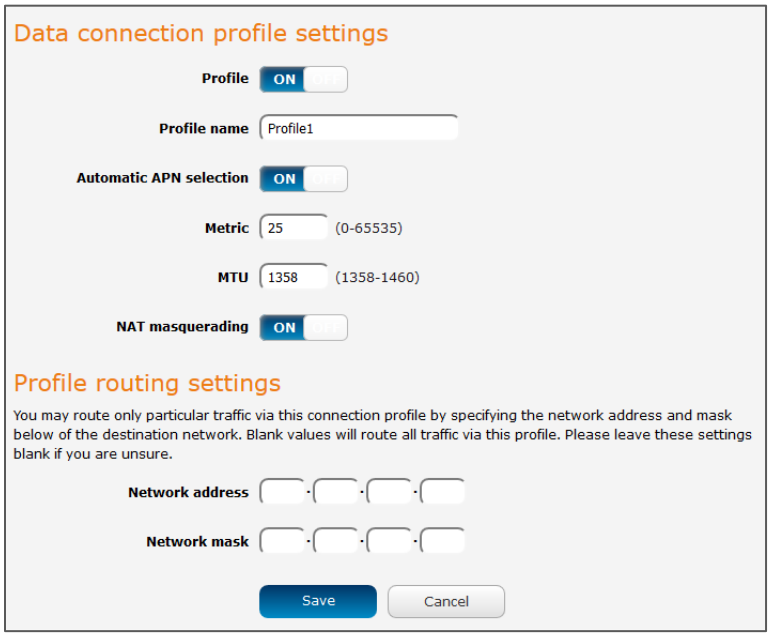
1. Click the edit button corresponding to the **Profile** that you wish to modify. The **Data connection profile settings** page is displayed.

Figure 8-2 Data connection profile settings



2. Click the **Profile** toggle key to turn the profile **ON**.

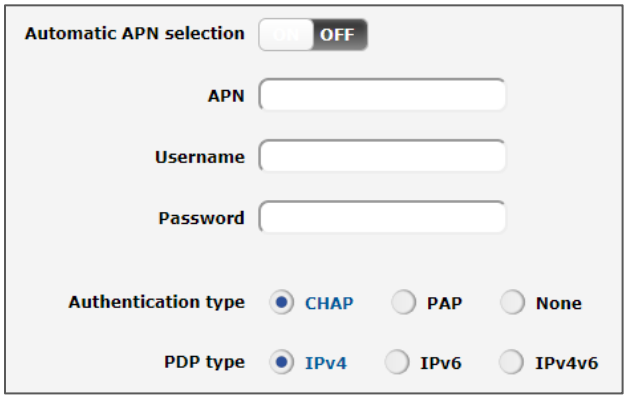
Figure 8-3 Data connection settings – Profile turned on



3. In the **Profile name** field, enter a name for the profile. This name is only used to identify the profile on the router.
4. If the **Automatic APN selection** is set to **ON**, the most appropriate APN will be chosen based on the MCC and MNC contained in your SIM card.

   If the **Automatic APN selection** is set to **OFF** the following additional fields will be displayed:

Figure 8-4 Manual APN settings

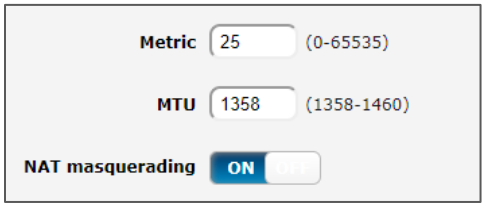


   a. Enter the APN name (Access Point Name).
   b. In the **Username** and **Password** fields to enter your login credentials (if required).
   c. Next to **Authentication type**, select the either **CHAP** or **PAP** or **None**, depending on the type of authentication used by your provider.
   d. Select the **PDP type**:
      - ⊙ **IPv4** – Sets a single stack IPV4 connection through which the router receives only IPV4 network and DNS addresses.
        This is the default **PDP type.**
      - ⊙ **IPv6** – Sets a single stack IPV6 connection through which the 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 router receives both IPv4 and IPV6 network and DNS addresses.

Figure 8-5 Metric, MTU and Nat masquerading settings



5. The **Metric** value is used by router to prioritize routes (if multiple are available) and is set to 25 by default. This value is sufficient in most cases, but you may modify it if you are aware of the effect your changes will have on the service.
6. The **MTU** size value is specific to your carrier and the value will be automatically displayed in this field once the carrier network registration is complete.
7. Use the **NAT masquerading** toggle key to turn NAT Masquerading **ON** or **OFF**. NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent

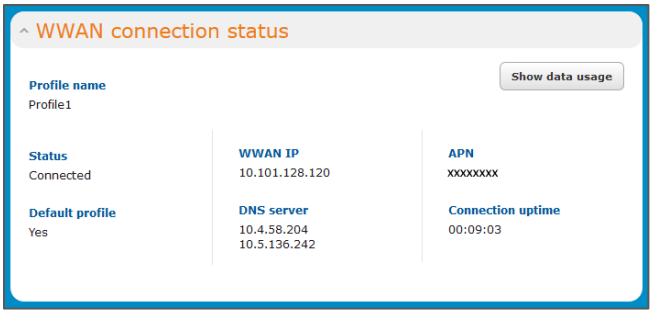
and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses.

8. For advanced networking such as using dual simultaneous PDP contexts, you may wish to configure a particular profile to route only certain traffic via that profile by configuring a custom address and mask of traffic to send via that profile. To do this, in the **Profile routing settings** section, enter the **Network address** and **Network mask** of the remote network. If you do not enter any profile routing settings, the profile will be active but no traffic will be routed through it. For more information on configuring Profile routing settings, see the Setting a default gateway with two active connection profiles example.
9. Click the **Save** button when you have finished entering the profile details.

Confirming a successful connection

After configuring the packet data session, and ensuring that it is enabled, click on the Status menu item at the top of the page to return to the Status page. When there is a mobile broadband connection, the WWAN connection status section is expanded showing the details of the connection and the Status field displays Connected.

Figure 8-6 WWAN connection status section

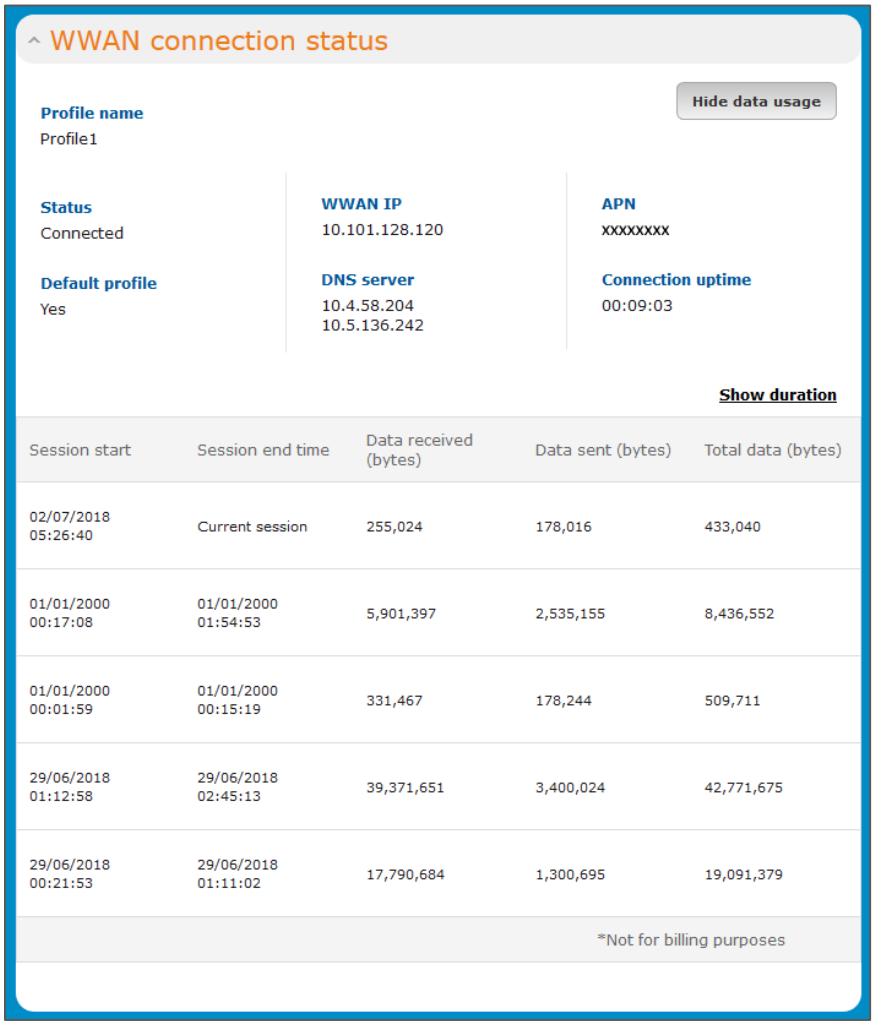


Checking data usage

On the **Status** page, each packet data connection profile has a **Show data usage** button which displays the amount of data received, sent and a total data usage figure.

To show the data use for a connected profile, click the **Show data usage** button. The data usage for the last 10 sessions is displayed in addition to the current session.

Figure 8-7 Data usage



Click the **Show duration** link to toggle the display to show the duration of each session rather than the start and end times.

Figure 8-8 Data usage with connection duration

Session start	Session duration	Data received (bytes)	Data sent (bytes)	Total data (bytes)
02/07/2018 05:26:40	00:09:03	307,809	246,955	554,764
01/01/2000 00:17:08	01:37:45	5,901,397	2,535,155	8,436,552

Connect on demand

The connect on demand feature keeps the Packet Data Protocol (PDP) context deactivated by default while making it appear to locally connected devices that the router has a permanent connection to the mobile broadband network. When a packet of interest arrives or an SMS wake-up command is received, the router attempts to establish a mobile broadband data connection. When the data connection is established, the router monitors traffic and terminates the link when it is idle.

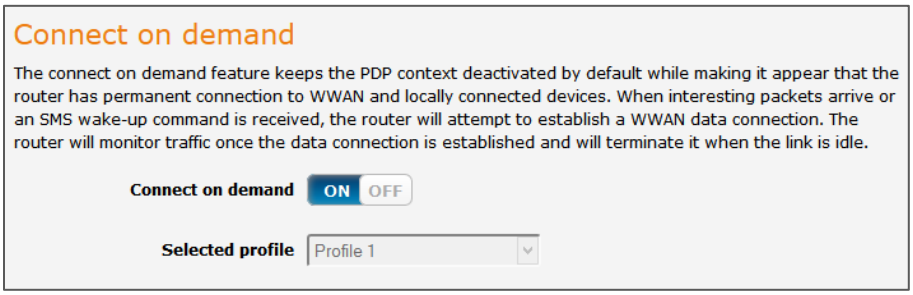
Note: *When interesting packets arrive, the recovery time for the wireless WAN connection is approximately 20-30 seconds.*

Configuring Connect on demand

To configure Connect on demand:

1. Click the **Networking** menu item from the top menu bar.
2. On the **Connect on demand** page, click the **Connect on demand** toggle key so that it is **ON**. Extra options appear. Note that the **Selected profile** drop-down list is greyed out and is used to display the currently selected default profile for which the Connect on demand configuration will apply. See the following sub-sections for further instructions.

Figure 8-9 Connect on demand configuration options



Setting the router to dial a connection when traffic is detected on specific ports

In some situations, you may wish to have the internet connection disabled except at times when outbound traffic to a particular external host's port or group of ports is sent to the router. To use this feature, click **Enable dial port filter** and enter the port number or list of port numbers separated by commas. When you select this option, all outbound TCP/UDP packets to any remote host on the specified port(s) will trigger the connection to dial. Note that when this feature is enabled, the options to ignore specific packet types are not available.

Figure 8-10 Connect on demand – Data activity triggered connection

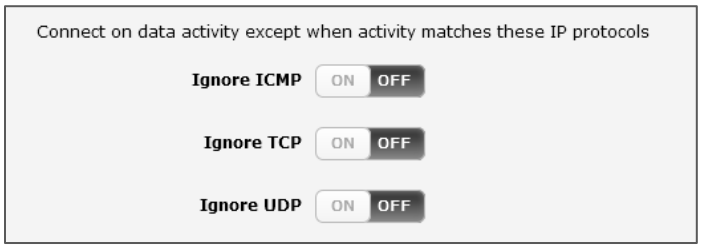
You can allow Microsoft network awareness (NCSI) traffic through but if you prefer that they do not trigger the connection, click the Ignore Microsoft network awareness (NCSI) traffic toggle key to set it to ON.

Figure 8-11 Connect on demand – Ignore NCSI traffic

Excluding certain packet types from triggering the connection to dial

Depending on your environment, you might prefer to exclude certain types of traffic passing through the router from triggering the data connection. You can tell the router to ignore outbound TCP, UDP or ICMP packets. When any of these options are checked the router will not dial a connection when that type of outbound destined data packet reaches the router from a locally connected device.

Figure 8-12 Connect on demand – Excluding IP protocols



Excluding certain application types from triggering the connection to dial

Some devices may generate general traffic as a part of normal operation which you may not want to trigger the data connection. You can set the router to ignore Domain Name System (DNS), Network Time Protocol (NTP) or Microsoft network awareness (NCSI) traffic from devices behind the router. When you check the box for these options, it tells the router to ignore the request from that application type and will not dial a connection when this data type is received. Note that enabling Ignore Microsoft network awareness (NCSI) traffic also enables Ignore DNS and Ignore NTP.

Figure 8-13 Connect on demand – Excluding application types

Setting timers for connection and disconnection

The router has a number of timer settings which let you determine when a connection is dialled and when it is disconnected.

Figure 8-14 Connect on demand – Connect and disconnect timers

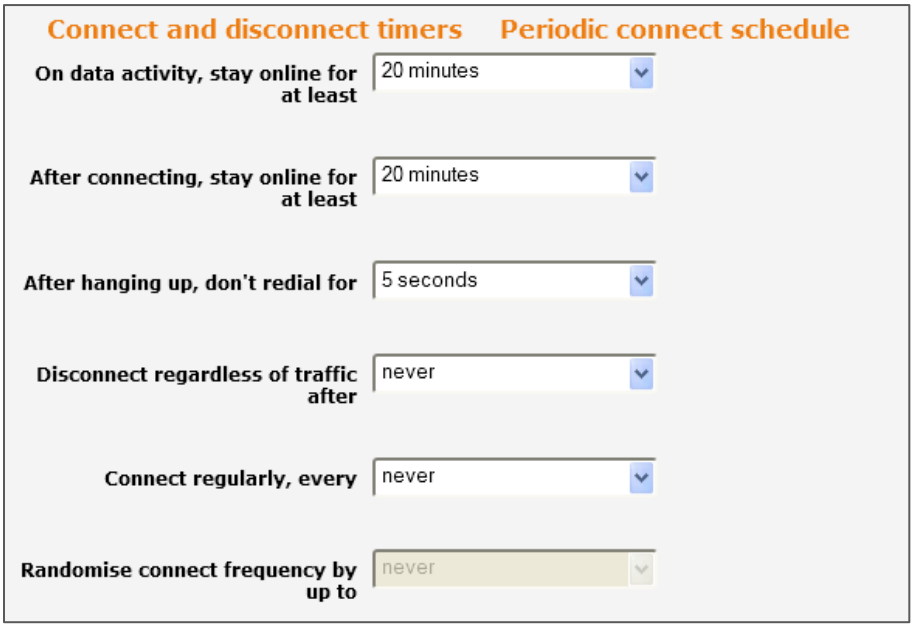


Table 8-2 Connect on demand – Connect and disconnect timers' descriptions

Option	Description
On data activity, stay online for at least	When traffic as per the configured settings above appear, the router will either continue to stay online or dial a connection and will not disconnect it for the specified time period (min. 1 minute, max. 1 hour). This timer is continuously reset throughout the duration of a dial-up session, whenever data activity is detected matching the rules above.
After connecting, stay online for at least	This timer configures the router to not hang-up the connection for the specified time period after initially dialing the connection. This setting cannot be less than the keep online period above. This timer affects the connection only once per dial up session, at the beginning of the session.
After hanging up, don't redial for	After a connection has been disconnected, you can tell the router to rest for a period of time before re-dialing.
Disconnect regardless of traffic after	Forces the router to disconnect the connection regardless of the traffic passing through it. The default setting is never.
Connect regularly, every / Randomise connect frequency by up to	If you want to have the router dial a connection at regular intervals, use Connect regularly, every to specify the interval between dials. Setting this to never effectively disables this option. The router also features the ability to randomise the time at which the first dial action is performed. This is useful in situations such as where you have numerous routers in an area where a power outage has occurred. Setting a random dial time helps to reduce network congestion when all the routers are powered on so they do not all try to connect simultaneously. When **Connect regularly, every** is set to at least 2 minutes, you are able to configure the router to randomise the time it begins to dial. The randomised dial timer only affects the initial dial after the unit powers on or after the settings are saved. For example, if you configure the router to dial every 2 minutes with a randomised dial starting time of 1 minute, the router waits for the Connect regularly, every time (2 minutes) and then randomly selects a time less than or equal to the Randomise connect frequency by up to time (1 minute). After the randomly selected time has elapsed, the router dials the connection. After the first dial, the router dials the connection every 2 minutes, ignoring the Randomise connect frequency by up to time.

Verbose mode

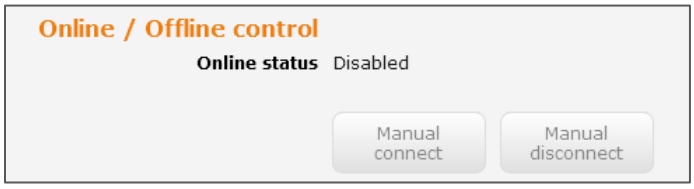
The router provides the option of logging all the data activity which matches the settings for the Connect on demand feature for advanced troubleshooting purposes. To enable the recording of detailed logs, click the Enable verbose mode toggle key to switch it **ON**. See the **System log** section for more information.

Figure 8-15 Connect on demand – Verbose logging configuration

Manually connecting/disconnecting

There may be times when you need to either force a connection to be made or force a disconnection manually. You can use the **Manual connect** and **Manual disconnect** buttons to do this whenever necessary. The online status of the connection is displayed above the buttons.

Figure 8-16 Connect on demand – Online/Offline control



When you have finished configuring the options for the Connect on demand feature, click the **Save** button at the bottom to save your changes.

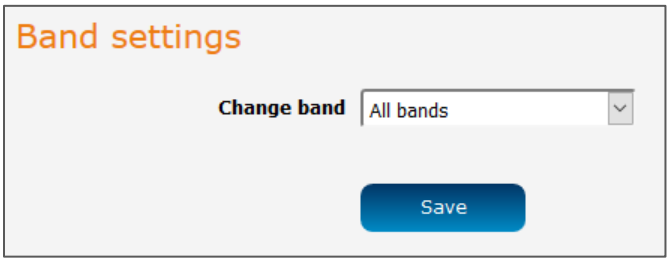
SMS Wake up

The router can also be woken up by means of an SMS message using the SMS diagnostics feature by sending a zero-byte class 1 flash SMS. See the Diagnostics section for details on using the SMS Wake up function.

Operator settings

The **Operator settings** page enables you to select which frequency band you will use for your connection and enables you to scan for available network operators in your area.

Figure 8-17 Band settings



You may want to do this if you're using the router in a country with multiple frequency networks that may not all support LTE. You can select the router to only connect on the network frequencies that suit your requirements.

Use the **Change band** drop-down list to select the band you wish to use.

The following band settings options are available:

Figure 8-18 Available bands

NTC-221	NTC-222	NTC-224	NTC-225	NTC-227
LTE FDD Bands: -Band 1 (2100 MHz) -Band 2 (1900 MHz) -Band 3 (1800 MHz) -Band 4 (1700 MHz) -Band 5 (850 MHz) -Band 7 (2600 MHz) -Band 8 (900 MHz) -Band 28 (700 MHz) LTE TDD Bands: -Band 40 (2300 MHz) WCDMA Bands: -Band 1 (2100 MHz) -Band 2 (1900 MHz) -Band 5 (850 MHz) -Band 8 (900 MHz) GSM Bands: -Band 2 (1900 MHz) -Band 3 (1800 MHz) -Band 5 (850 MHz) -Band 8 (900 MHz	LTE FDD Bands: -Band 1 (2100 MHz) -Band 3 (1800 MHz) -Band 5 (850 MHz) -Band 7 (2600 MHz) -Band 8 (900 MHz) -Band 20 (800 MHz) WCDMA Bands: -Band 1 (2100 MHz) -Band 5 (850 MHz) -Band 8 (900 MHz) GSM Bands: -Band 3 (1800 MHz) -Band 8 (900 MHz)	LTE FDD Bands: -Band 2 (1900 MHz) -Band 4 (1700 MHz) -Band 12 (700 MHz) WCDMA Bands: -Band 2 (1900 MHz) -Band 4 (1700 MHz) -Band 5 (850 MHz)	LTE FDD Bands: -Band 4 (1700 MHz) -Band 13 (700 MHz)	LTE FDD Bands: -Band 1 (2100 MHz) -Band 2 (1900 MHz) -Band 3 (1800 MHz) -Band 4 (1700 MHz) -Band 5 (850 MHz) -Band 7 (2600 MHz) -Band 8 (900 MHz) -Band 12 (700 MHz) -Band 13 (700 MHz) -Band 18 (850 MHz) -Band 19 (850 MHz) -Band 20 (800 MHz) -Band 25 (1900 MHz) -Band 26 (850 MHz) -Band 28 (700 MHz) LTE TDD Bands: -Band 38 (2600 MHz) -Band 39 (1900 MHz) -Band 40 (2300 MHz) -Band 41 (2500 MHz) WCDMA Bands: -Band 1 (2100 MHz) -Band 2 (1900 MHz) -Band 4 (1700 MHz)

				-Band 5 (850 MHz) -Band 6 (800 MHz) -Band 8 (900 MHz) -Band 19 (800 MHz) GSM Bands: -Band 2 (1900 MHz) -Band 3 (1800 MHz) -Band 5 (850 MHz) -Band 8 (900 MHz)

It is not necessary to change the default setting of All bands in most cases. In fact, locking to a particular band can cause connection difficulties if the device is moved to a location where the forced band selection is no longer available.

When **All bands** is selected, the router attempts to find the most suitable band based on the available networks for the inserted SIM card.

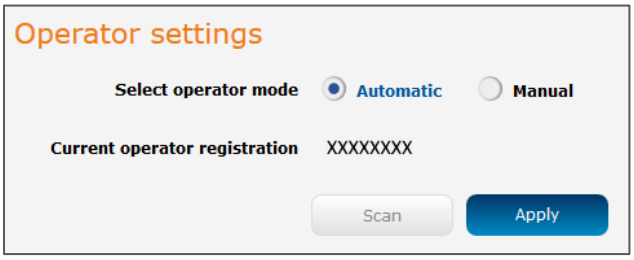
The **GSM all**, **WCDMA all** and **LTE all** options allow you to force the device to lock to those particular network technologies only.

Click the **Save** button to save and apply your selection.

Operator settings

The operator settings feature allows you to select whether to allow the router to automatically select a network or to manually scan for a network to which the router is locked.

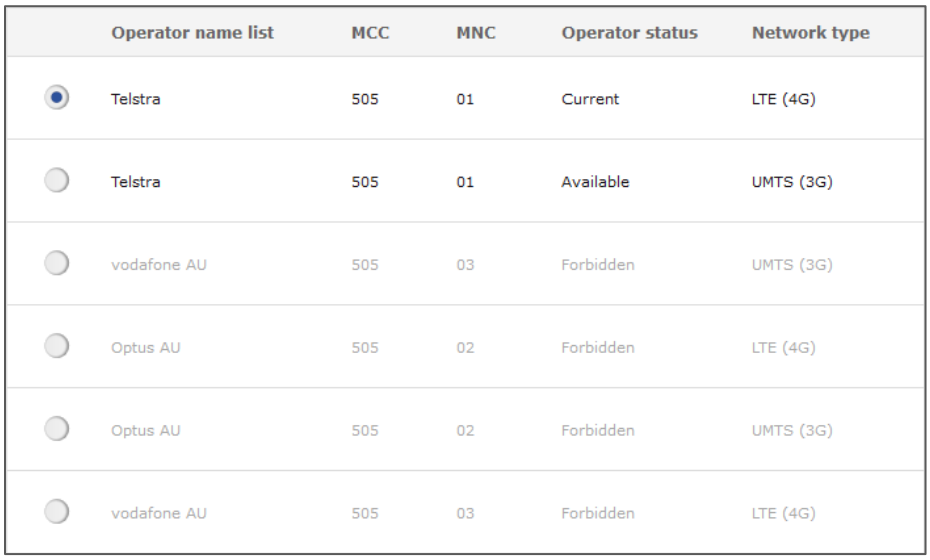
Figure 8-19 Operator settings



To scan for available networks, set the **Select operator** mode from ○ **Automatic** to ⊙ **Manual** then click the **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 8-20 Detected operator list



	Operator name list	MCC	MNC	Operator status	Network type
◉	Telstra	505	01	Current	LTE (4G)
○	Telstra	505	01	Available	UMTS (3G)
○	vodafone AU	505	03	Forbidden	UMTS (3G)
○	Optus AU	505	02	Forbidden	LTE (4G)
○	Optus AU	505	02	Forbidden	UMTS (3G)
○	vodafone AU	505	03	Forbidden	LTE (4G)

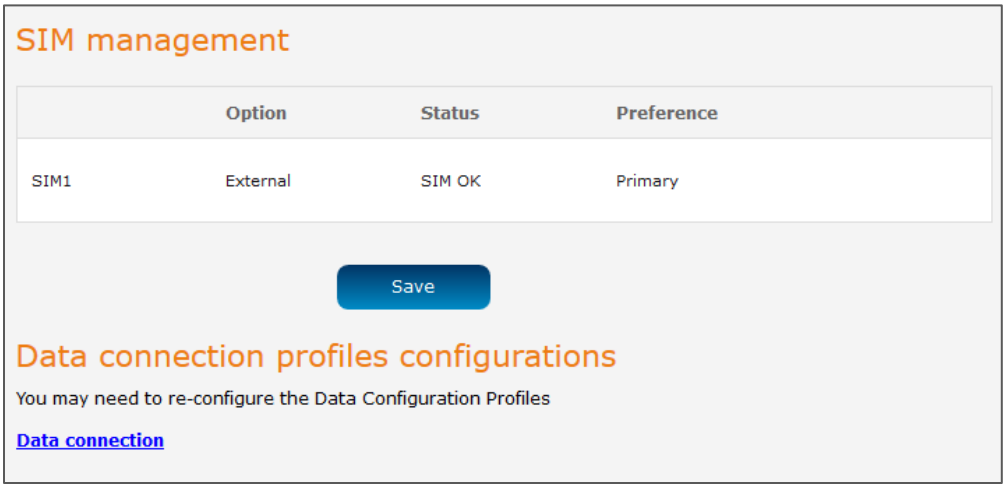
Select the most appropriate service from the list shown and click **Apply**.

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.

SIM management

The **SIM management** page displays the status of the SIM card.

Figure 8-21 SIM Management



SIM security settings

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

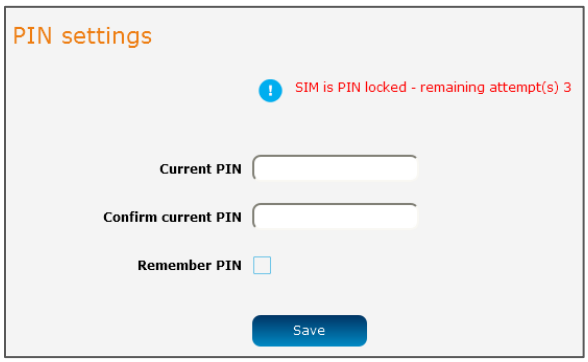
Unlocking a PIN locked SIM

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 on the **Networking** menu from the top menu bar, and then click **SIM security settings**.

Figure 8-22 SIM security settings – SIM PIN locked



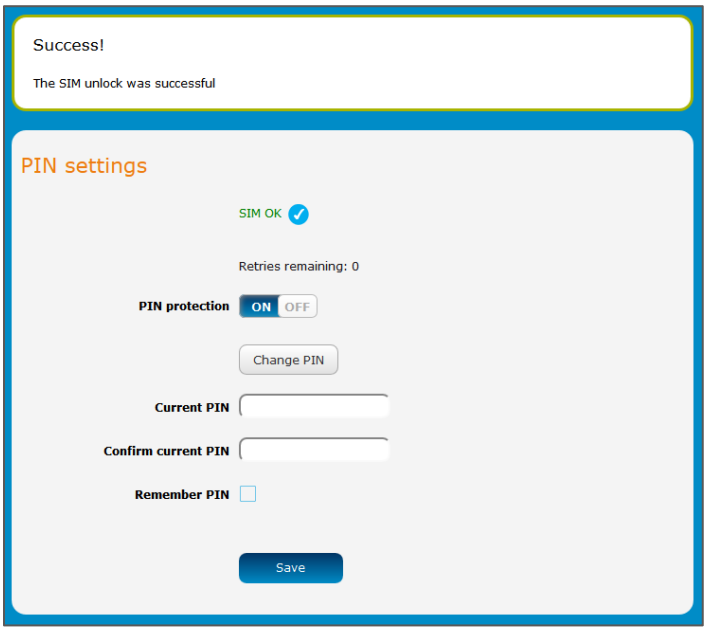
2. Enter the PIN in the **Current PIN** field (enter numbers only) and then enter it again in the **Confirm current PIN** field to confirm the PIN.
3. If you are placing the router in a remote, unattended location, you may wish to check the Remember PIN option. This feature allows the router to automatically send the PIN to the SIM each time the SIM asks for it (usually at power up). This enables the SIM to be PIN locked (to prevent unauthorized re-use of the SIM elsewhere), while still allowing the router to connect to the cellular service.
   When this feature is enabled, the PIN you enter when setting the **Remember PIN** ☑ feature is encrypted and stored locally on the router. The next time the SIM asks the router for the PIN, the router decrypts the PIN and automatically sends it to the SIM without user intervention.

   When this feature is disabled and the SIM is PIN locked, the PIN must be manually entered via the router's configuration interface. In situations where the router will be unattended, this is not desirable.

Note: *Select Remember PIN if you do not want to enter the PIN code each time the SIM is inserted.*

4. Click the **Save** button. If successful, the router displays the following screen:

Figure 8-23 SIM security settings – SIM unlock successful



Enabling/Disabling SIM PIN protection

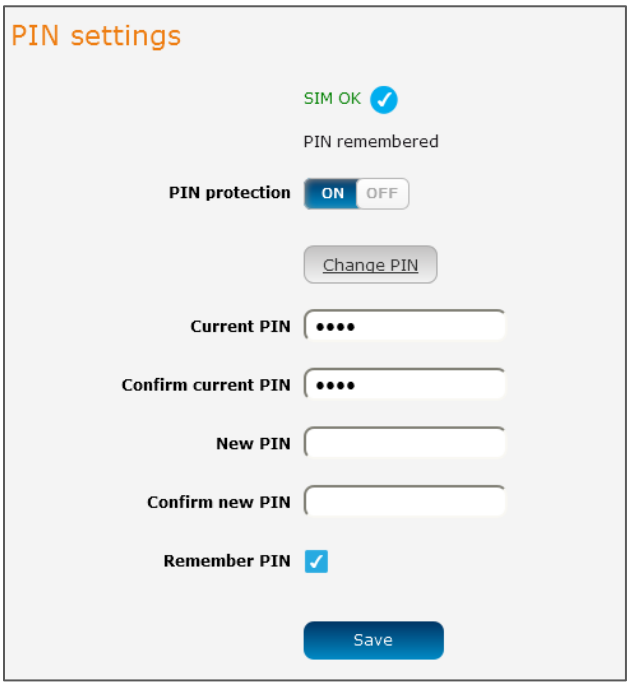
The security PIN protection can be turned on or off using the **PIN protection** toggle key.

Figure 8-24 PIN protection toggle key

Changing the SIM PIN

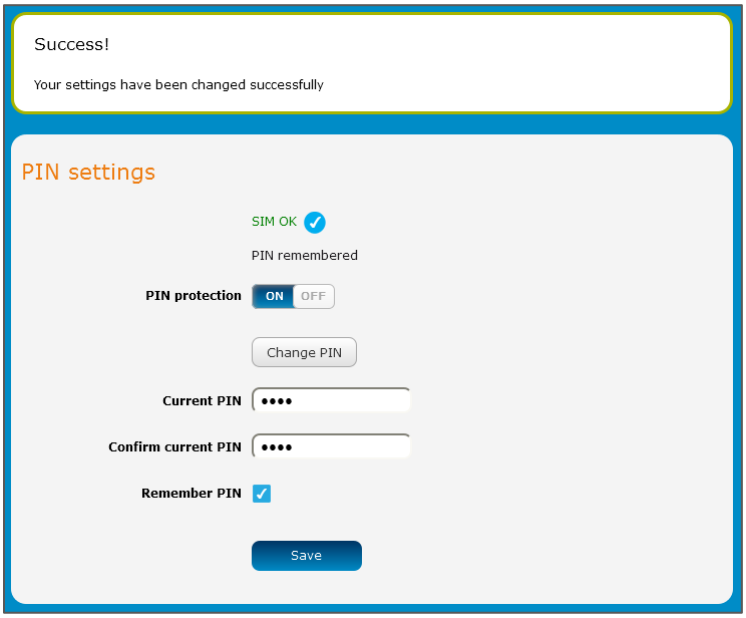
If you would like to change the PIN, click the Change PIN button and enter the current PIN into the **Current PIN** and **Confirm current PIN** fields, then enter the desired PIN into the **New PIN** and **Confirm new PIN** fields and click the **Save** button.

Figure 8-25 PIN settings – Change PIN



When the PIN has been changed successfully, the following screen is displayed:

Figure 8-26 SIM security settings – PIN change successful



Unlocking a PUK locked SIM

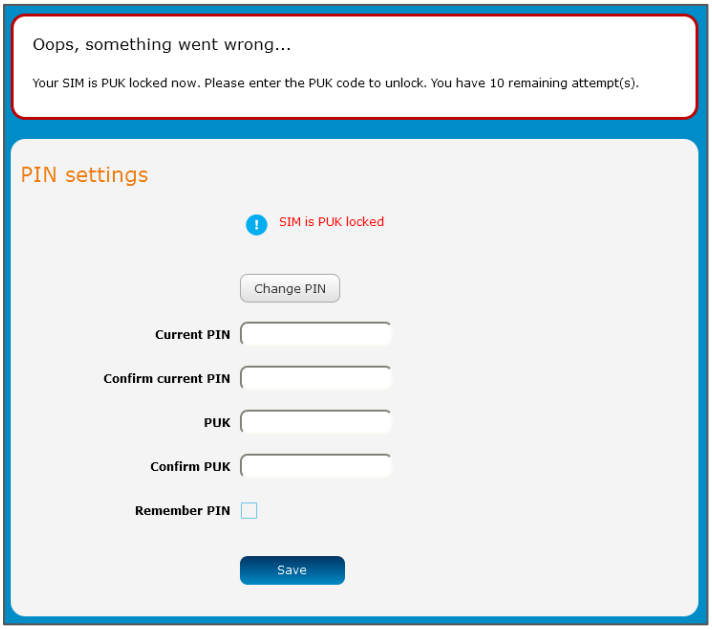
After three incorrect attempts at entering the PIN, the SIM card becomes PUK (Personal Unblocking Key) locked and you are requested to enter a PUK code to unlock it.

Note: *To obtain the PUK unlock code, you must contact your service provider.*

You will be issued a PUK to enable you to unlock the SIM and enter a new PIN. Enter the new PIN and PUK codes.

Click the **Save** button when you have finished entering the new PIN and PUK codes.

Figure 8-27 SIM security – SIM PUK locked

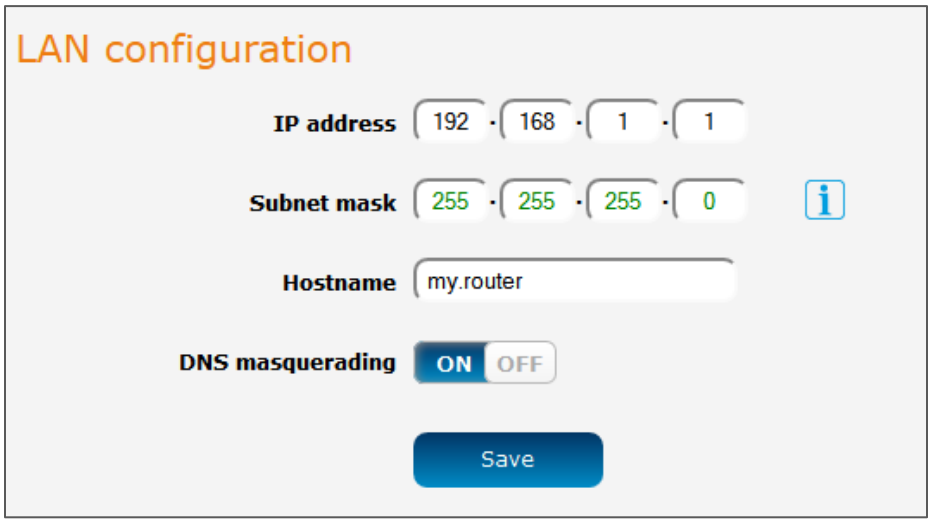


LAN

LAN

The **LAN configuration** page is used to configure the LAN settings of the router and to enable or disable **DNS Masquerading**. To access the LAN configuration page, click on the Networking menu at the top of the screen, then click on the LAN menu on the left.

Figure 8-28 LAN configuration settings



The default IP of the LAN port is 192.168.1.1 with subnet mask 255.255.255.0. To change the IP address or Subnet mask, enter the new IP Address and/or Subnet mask and click 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 router.*

DNS masquerading

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

With **DNS masquerading ON**, the DHCP server embedded in the NTC-220 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-220 Series router which proxies them to the upstream DNS servers.

With **DNS masquerading OFF**, the DHCP server hands out the upstream DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the NTC-220 Series router.

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

In most cases, it is not necessary to disable DNS masquerading but if you need to, click the DNS masquerading toggle key to turn it **OFF** and then click the **Save** button. DHCP

The DHCP page is used to adjust the settings used by the router's built in DHCP Server which assigns IP addresses to locally connected devices. To access the LAN configuration page, click on the Networking menu at the top of the screen, click on the **LAN** menu on the left then select the **DHCP** menu item.

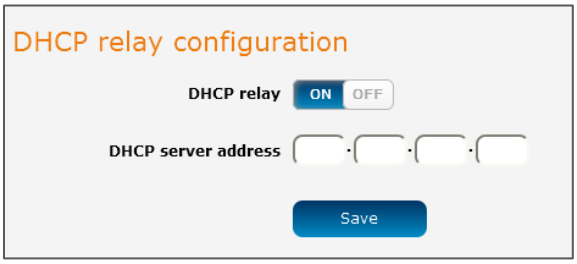
DHCP

DHCP relay configuration

In advanced networks configurations where the NTC-220 Series router should not be responsible for DHCP assignment, but instead an existing DHCP server is located on the Wireless WAN or LAN connections, the clients behind the NTC-220 Series router are able to communicate with the DHCP server when DHCP relay is enabled. This enables the NTC-220 Series router to accept client broadcast messages and to forward them onto another subnet.

To configure the router to act as a DHCP relay agent click the **DHCP relay** toggle key to turn it **ON** and enter the DHCP server address into the **DHCP server address** field. DHCP relay is disabled by default.

Figure 8-29 DHCP relay configuration



DHCP configuration

You can manually set the start and end address range to be used to automatically assign addresses within, 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 8-30 DHCP configuration

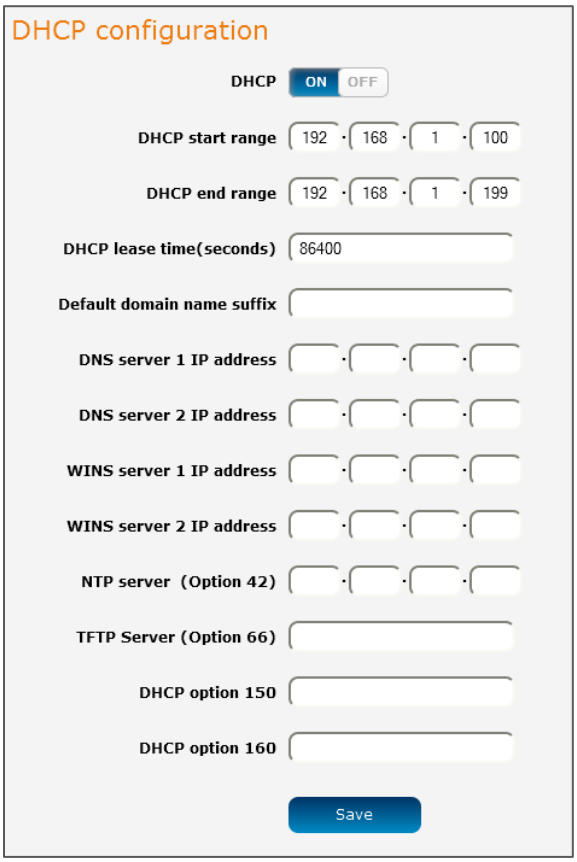


Table 8-3 DHCP configuration descriptions

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 length of time 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 IP address

WINS server 2 IP address	Specifies the secondary WINS (Windows Internet Name Service) server 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 the desired DHCP options and click the **Save** button.

Address reservation list

DHCP clients are dynamically assigned an IP address as they connect, but you can reserve an address for a particular device using the **Address reservation list**.

Figure 8-31 DHCP – Address reservation list

To add a device to the address reservation list:

1. Click the **+Add** button.
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** fields, enter the IP address that you wish to reserve for the device.
5. If the **Enable** toggle key is not set to **ON**, click it to switch it to the ON position.
6. Click the **Save** button to save the settings.

Dynamic DHCP client list

The **Dynamic DHCP client list** displays a list of the DHCP clients. If you want to reserve the current IP address for future use, click the **Clone** button and the details will be copied to the address reservation list fields. Remember to click the **Save** button under the Address reservation list section to confirm the configuration.

Figure 8-32 Dynamic DHCP client list

Ethernet WAN/LAN

The Ethernet WAN/LAN pages provide configuration options for the two built-in Ethernet ports and any USB-to-Ethernet ports you may connect.

Ethernet interface assignment

The Ethernet assignment page displays the Ethernet interfaces and allows you to configure whether they operate in LAN or WAN mode.

To access the Ethernet assignment page, click on the **Networking** menu at the top of the screen, click on the **Ethernet WAN/LAN** menu on the left then select the **Interface assignment** menu item.

The default failover sequence is as follows:

1. Ethernet WAN
2. USB to Ethernet adapter (if configured)
3. WWAN

Figure 8-33 Ethernet group configuration

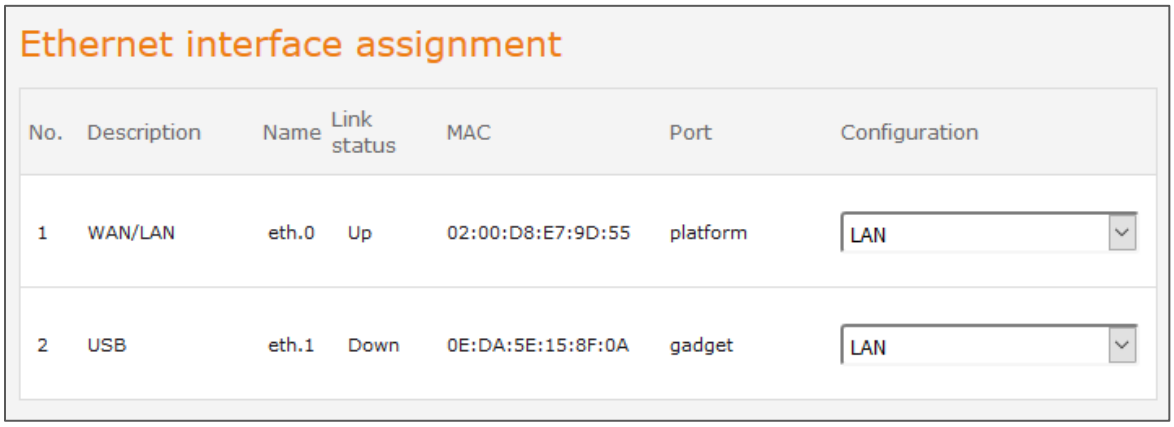


Table 8-4 Ethernet group configuration items

Option	Definition
No.	A number identifying the interface on the router.
Description	A description of the type of interface.

Name	The name used to identify the interface on the router.
Link status	Displays whether the interface is inserted
MAC	The MAC address of the interface.
Port	The type of port.
Configuration	Use the drop-down list to select whether the port operates in LAN mode, WAN mode or is disabled.

Ethernet WAN

The **Ethernet WAN configuration** page allows you to configure the connection type and metric of the available WAN connections. To access the Ethernet WAN page, click on the **Networking** menu at the top of the screen, click on the **Ethernet WAN/LAN** menu on the left then select the **WAN configuration** menu item.

Figure 8-34 Ethernet WAN configuration

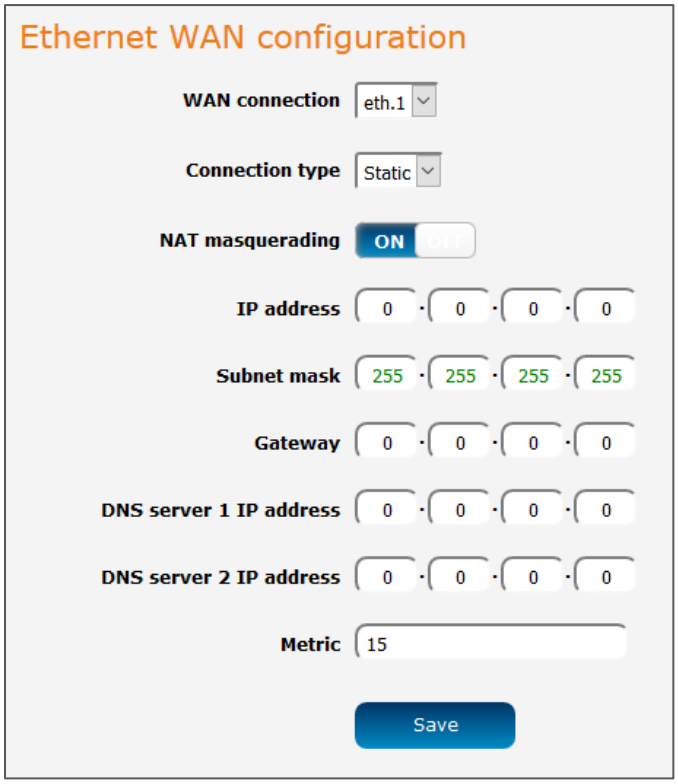


Table 8-5 Ethernet WAN configuration options

Option	Definition
WAN Ethernet	Use this field to select the WAN interface to configure.
Connection Type	Selects whether the WAN interface has static IP settings or DHCP.
IP address	The IP address to assign to the selected WAN interface.

Subnet mask	The Subnet mask of the IP address above.
Gateway	The gateway to assign this WAN interface.
DNS server 1 IP address	The first DNS server for the WAN interface.
DNS server 2 IP address	The second DNS server for the WAN interface.
Metric	The metric value is used to define the priority of the interface. Lower metric values indicate higher priority.

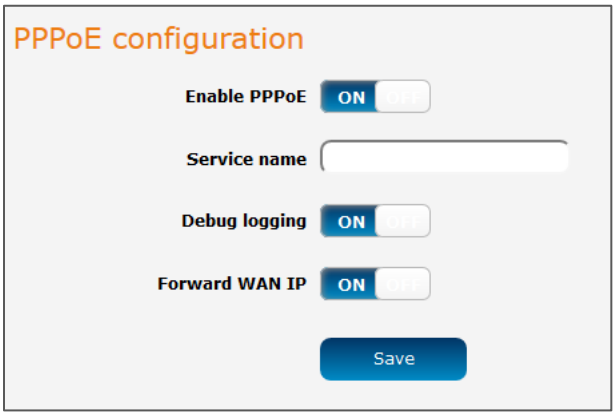
PPPoE

If desired, you can have a client device connected to the Ethernet port initiate the mobile broadband connection using a PPPoE session. This is particularly useful in situations where you wish to provide Wireless WAN data access to an existing router which you want to have full public WAN IP access and have control over routing functionality. The PPPoE connection is established over the highest priority interface.

To configure PPPoE:

1. Select the **Networking** menu item from the top menu bar, then select the **PPPoE** menu on the left side of the screen. The **PPPoE configuration** screen is displayed.

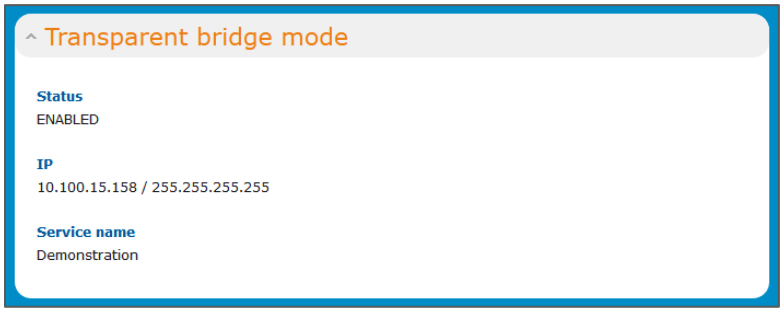
Figure 8-35 PPPoE configuration



2. Click the **Enable PPPoE** toggle key so that it is **ON**.
3. (Optional) In the **Service name** field, enter a name to use for the connection. This name is displayed on the Status page to identify the PPPoE connection. Any name you enter here must also be entered in the PPPoE connection profile in order for it to work.
4. If you require additional logging to be made available, click the **Debug logging** toggle key so that it is in the **ON** position. This displays PPPoE negotiation details in the System log.
5. The **Forward WAN IP** option determines whether the router passes the WAN IP address on to the PPPoE client. When this option is set to **ON** the first PPPoE client to connect will receive the WAN IP address and no further clients will be able to make a connection. In this mode, the router transparently bridges the connection and many of the router's features are disabled. When this option is set to **OFF**, the router retains the WAN IP address and performs Network Address Translation (NAT) for connected clients. In this mode, you are able to connect multiple PPPoE clients and all of the router's features are available.

6. Click the **Save** button to confirm the settings.
7. Click the **Status** menu item from the top menu bar. When **Forward WAN IP** is enabled, the status page shows a **Transparent bridge mode** section and displays the WAN IP.

Figure 8-36 Transparent bridge mode status



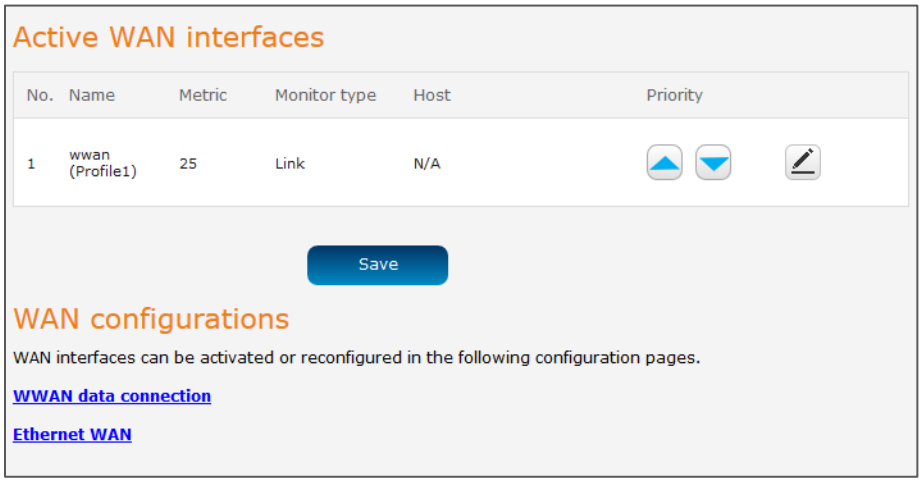
8. Configure the properties of the interface that the PPPoE connection will use (determined by WAN priority) in order to provide authentication credentials. Each interface uses the authentication credentials configured on the router for that particular interface, not those entered in the PPPoE client. For example, when using WWAN as the PPPoE interface, enter the username and password on the Data connection profile settings before connecting. See the Manually configuring a connection profile section for more detail.
9. Use your downstream device to initiate a network connection using a PPPoE client.

WAN failover

The WAN failover page displays a summary of the configured WAN interfaces and their priorities (Metric). Lower metric value determines higher priority. The priority of the interfaces can be adjusted using the up and down arrows in the Priority column. When the interface with the highest priority goes down, the router fails over to the next highest priority interface. The method used to determine whether an interface is "up" or "down" is defined by the Monitor setting. By default, an interface is monitored by its link status, but it may be configured to be monitored by pings instead.

To access the WAN failover page, click on the **Networking** menu at the top of the screen then click on the **WAN failover** menu item on the left.

Figure 8-37 WAN summary



To edit an interface, select the edit icon for the interface you wish to edit. The **Failover configuration** page is displayed.

Hardware link

When **Monitoring method** is set to Hardware 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 (metric).

Figure 8-38 Failover configuration – hardware link

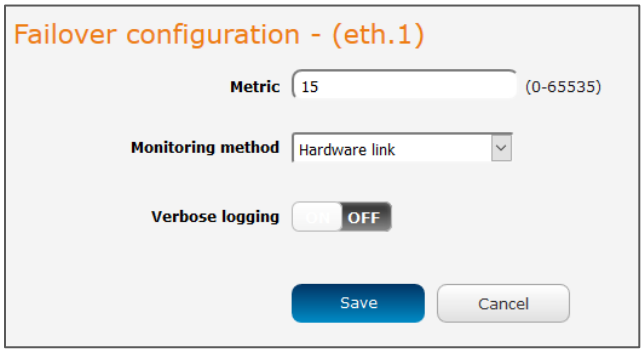


Table 8-6 Failover configuration – Hardware link monitoring

Option	Description
Priority	The priority (metric) is a numeric value which determines which interface has priority. Lower priority values mean higher priority.
Monitoring method	Specifies the means used to determine whether the link is up or down.
Verbose logging	When enabled, this logs verbose comments in the system log related to the failover monitoring.

Ping monitor

When **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, 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. The pings sent at each interval are from here on referred to as an “instance” of pings.

Ping timers

The Periodic ping timer setting sets a regular interval at which an instance of pings is sent to test the availability of an interface.

The Retry timer setting is activated only when all pings in an instance sent at the Periodic ping timer interval fail and is used to set a different, usually shorter, interval to speed up the router’s response to an interface failure.

Methods of evaluating ping responses

For simplicity, we recommend using only one of the two methods of evaluating the ping responses. The available methods are:

- **Consecutive errors** - 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.

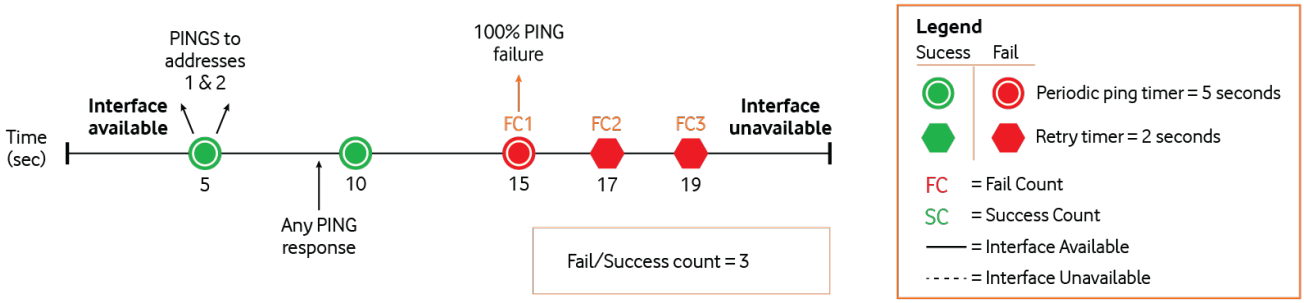
It should be noted that the Periodic ratio monitor evaluates an interface over a Series of ping instances (defined by the Total monitor count) and when the Series has completed, the success and fail counts are reset. For example, with the default Total monitor count value set to 10 and Failover fail 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.

Failing over to a lower priority interface

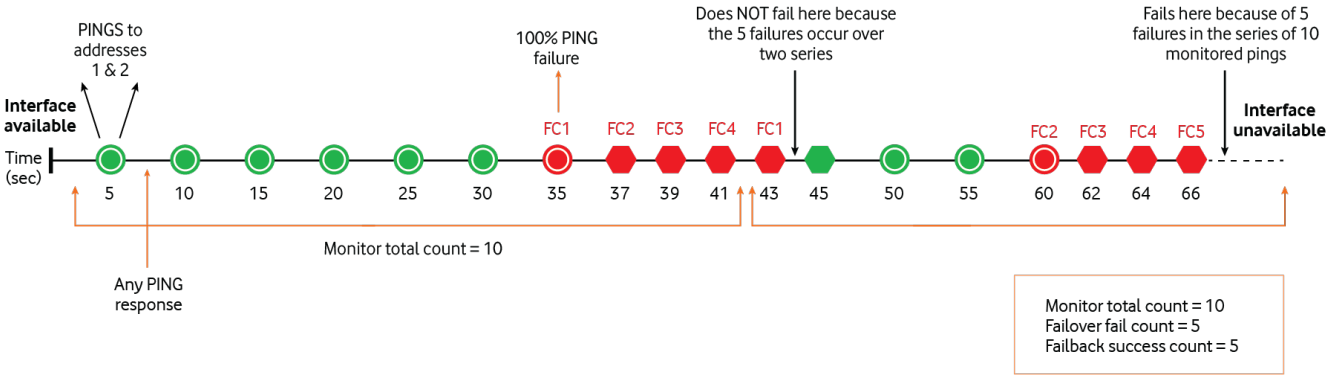
Each WAN interface is independently monitored according to its own distinct settings, following the processes outlined below.

1. At a regular interval stipulated by the Periodic ping timer setting, the router sends 3 ping requests via the interface to both the first and second destination addresses simultaneously. If it receives a reply to any of those pings on the interface, it is considered to be up and the router continues pinging on the interface at the Periodic ping timer interval.
2. If the router does not receive a response to all six pings on the interface by the start of the next Periodic ping timer interval, it registers this failure as a Fail count and continues to send pings to both destination addresses at the Retry timer interval (typically set at a shorter interval than the Periodic ping timer since there may be a problem). If a response is received to any of those pings, the router returns to sending pings according to the Periodic ping timer setting.
3. However, if after another period defined by the Retry timer setting the router again does not receive a response to any of the pings, it registers another Fail count.
4. The router repeats the retry process until one of the following conditions is met:
    - it receives a ping response and returns to testing the interface according to the Periodic ping timer;
    - the number configured in the Failover fail count field (under Consecutive error monitor) is reached, in which case the interface is marked as unavailable and the router automatically reroutes packets according to the configured priorities of the remaining interfaces;
    - the number of Failover fail count pings (under Periodic ratio monitor) is reached within a particular Series of the Monitor total count, in which case the interface is marked as unavailable and the router automatically reroutes packets according to the configured priorities of the remaining interfaces.

Consecutive error monitor failover example



Periodic ratio monitor failover example

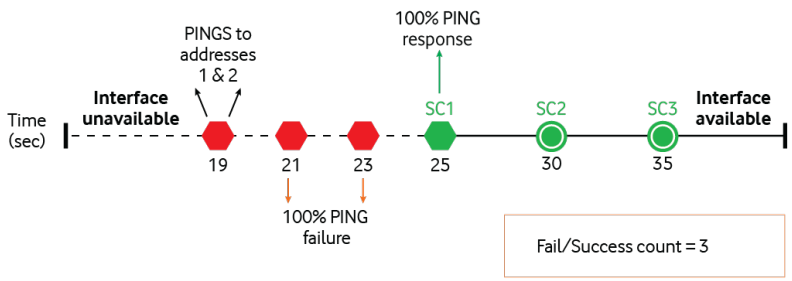


Failing back to a higher priority interface

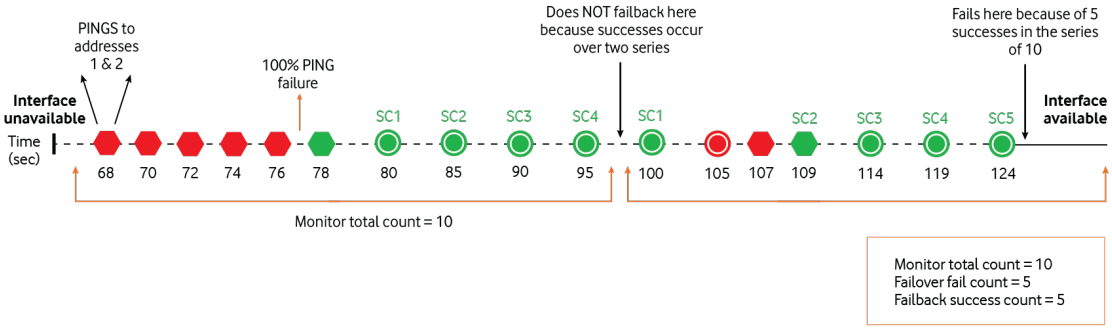
The process for returning an unavailable interface to an available state is similar to the above process. When an interface is marked unavailable by the ping monitor, the router continues to retry pings to the two destination addresses via that interface according to the Periodic ping timer setting until one of the following conditions is met:

- it receives a 100% successful response to the six pings for a number of consecutive periods that equal the configured Failback success count setting
- the number of Failback success count pings (under Periodic ratio monitor) is reached within a particular Series of the Monitor total count, in which case the router continues pinging at the Periodic ping timer interval and marks the interface as available. The router automatically reroutes packets according to the configured priorities of the available interfaces.

Consecutive error monitor failback example



Periodic ratio monitor failback example

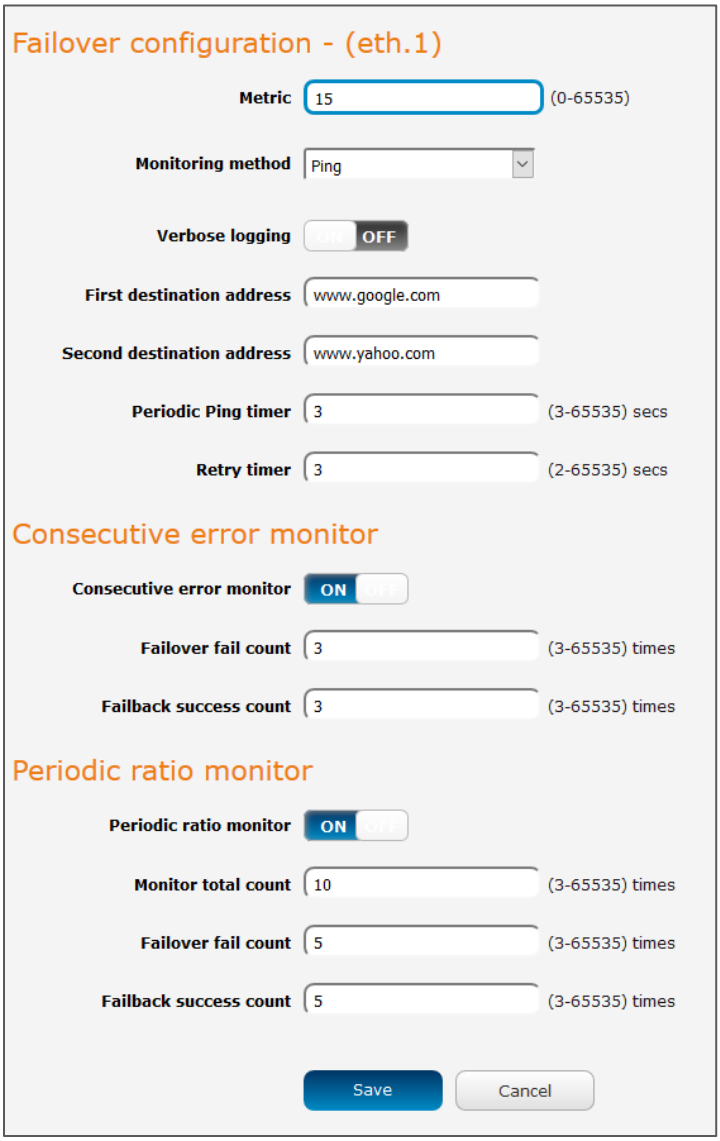


To configure the ping monitoring method:

1. Select the **Edit** button corresponding to the interface with the lowest metric (highest priority).

2. Use the **Monitoring method** drop-down list to select **Ping**.

Figure 8-39 Failover configuration –Ping monitoring method



3. 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.
4. 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.
5. 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.
6. 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.

7. 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**.

Consecutive error monitor

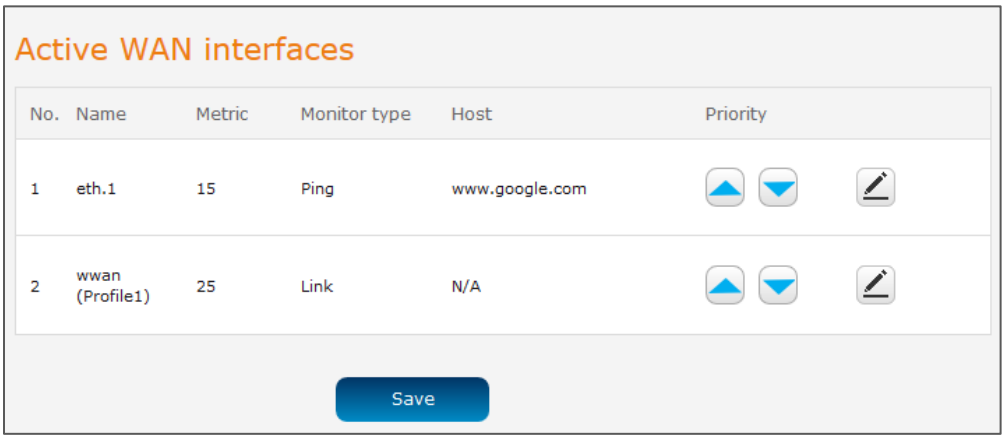
1. To use the Consecutive error monitor type, click the **Consecutive error monitor** toggle key so that it is in the **ON** position.
2. In the **Failover fail count** field, enter an integer between 3 and 65535 for the number of times a retry ping should fail before the router fails over to the next WAN interface.
3. 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.
4. Click the **Save** button when you have finished entering your settings.

Periodic ratio monitor

1. To use the Periodic ratio monitor, set the **Fail/success count** field to **0**.
2. In the **Monitor total count** field, enter an integer between **3** and **65535** for the number of previous pings to consider for failover and failback.
3. If you do not wish to use the periodic ratio monitor, set this to 0. 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.
4. 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.

The **Active WAN interfaces** are displayed once again, this time showing that the Ping monitor type is in use for the interface.

Figure 8-40 Active WAN interfaces



Click the **Save** button to save the settings. The WAN failover configuration is complete.

The table below describes each field on the **Failover configuration** screen.

Table 8-7 Failover configuration – Ping monitoring

Option	Description
Metric	The metric is a numeric value which determines which interface has priority. Lower priority values mean higher priority.
Monitoring method	Specifies the means used to determine whether the link is up or down.
Verbose logging	When enabled, this logs verbose comments 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	
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	
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 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.

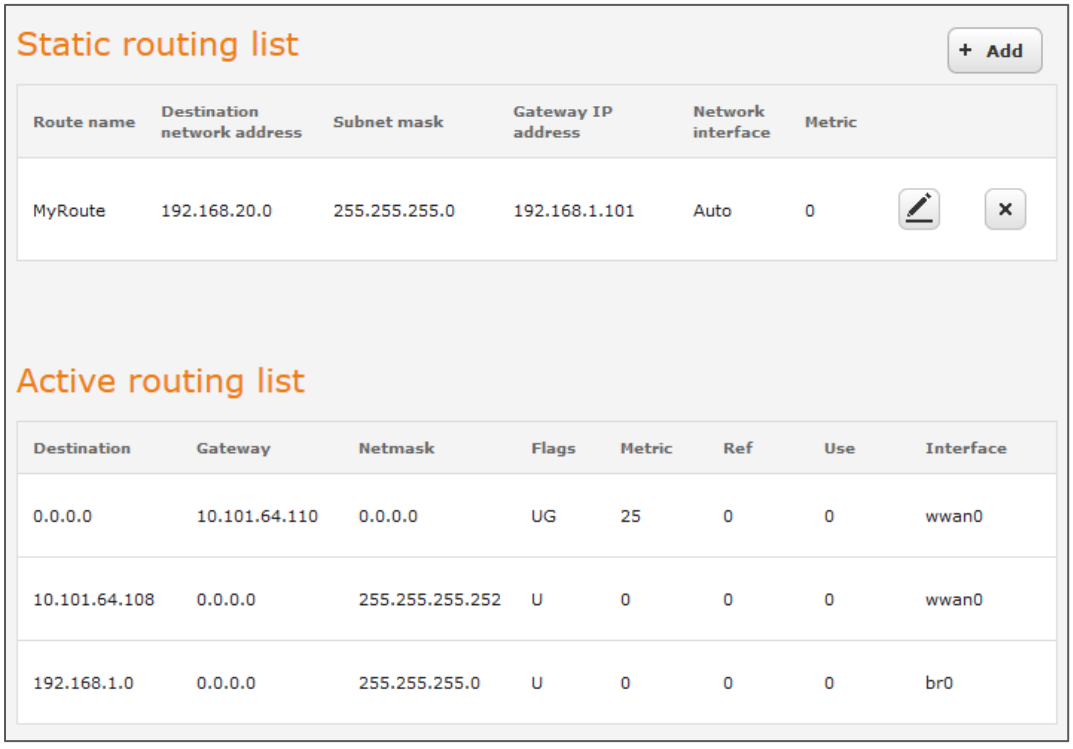
Routing

Static

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, click on the **Networking** menu at the top of the screen, click on the **Routing** menu on the left, then click on the **Static** menu item.

Figure 8-41 Static routing list



Some routes are added by default by the router on initialization such as the Ethernet subnet route for routing to a device on the Ethernet subnet.

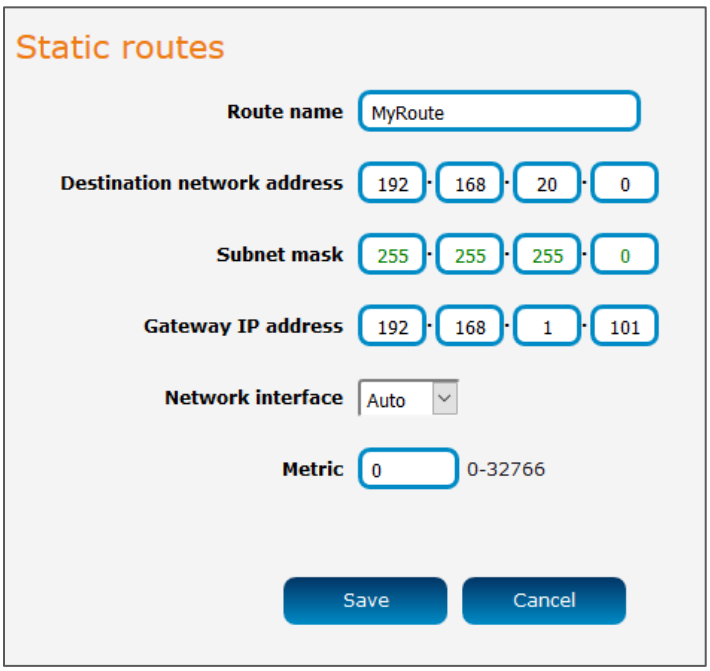
Adding Static Routes

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

1. In the **Route name** field, type a name for the route so that it can be identified in the static routing list.

2. From the **Network interface** drop-down list, select the interface for which you would like to create a static route.
3. In the **Destination IP address** field, enter the IP address of the destination of the route.
4. In the **Destination subnet mask** field, enter the subnet mask of the route.
5. In the **Gateway IP address** field, enter the IP address of the gateway that will facilitate the route.
6. In the **Metric** field enter the metric for the route. The metric value is used by the router to prioritise 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.

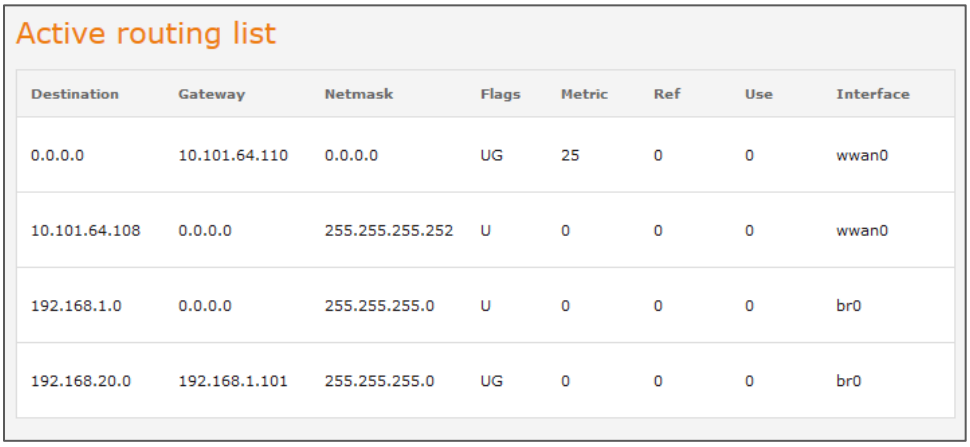
Figure 8-42 Adding a static route



Active routing list

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

Figure 8-43 Active routing list



Deleting static routes

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

Figure 8-44 Deleting a static route

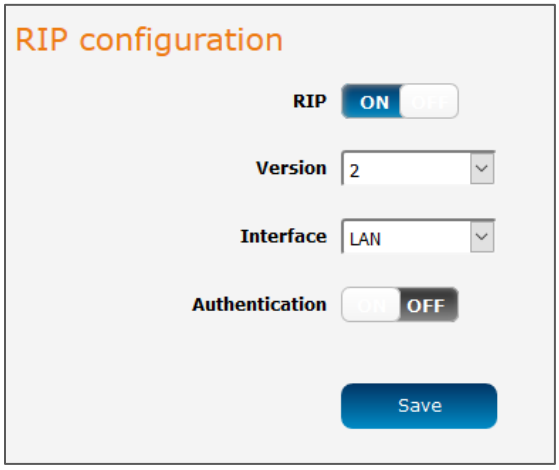
RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. Thus 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.

To access the RIP configuration page, click on the **Networking** menu at the top of the screen, click on the **Routing** menu on the left, then click on the **RIP** menu item.

Note: *Some routers will ignore RIP.*

Figure 8-45 RIP configuration



To enable Routing Information Protocol (RIP)

1. Click the **RIP** toggle key to switch it to the **ON** position.
2. Using the **Version** drop-down list, select the version of RIP that you would like to use.
3. Select the **Interface** for which you want RIP to apply. You can choose the **LAN** interface, the **WWAN** interface or **Both**.
4. If you wish 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 the **Save** button to confirm your settings.

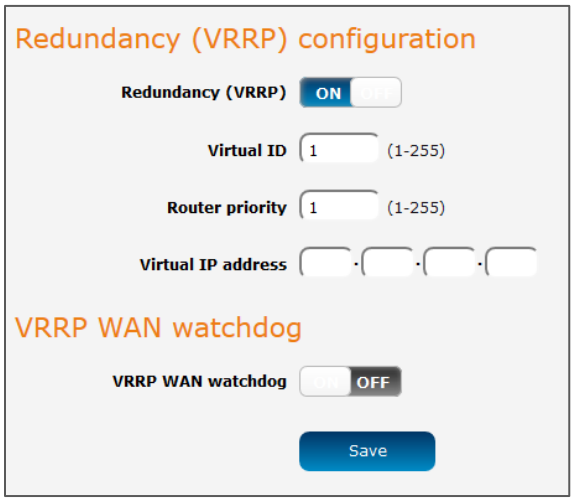
Redundancy (VRRP) configuration

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.

To access the Redundancy (VRRP) page, click on the **Networking** menu at the top of the screen, click on the **Routing** menu on the left, then click on the **Redundancy (VRRP)** menu item.

Figure 8-46 VRRP configuration



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

1. Click the **Redundancy (VRRP)** toggle key to **ON** in order to activate 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 the **Save** button to save the new settings.

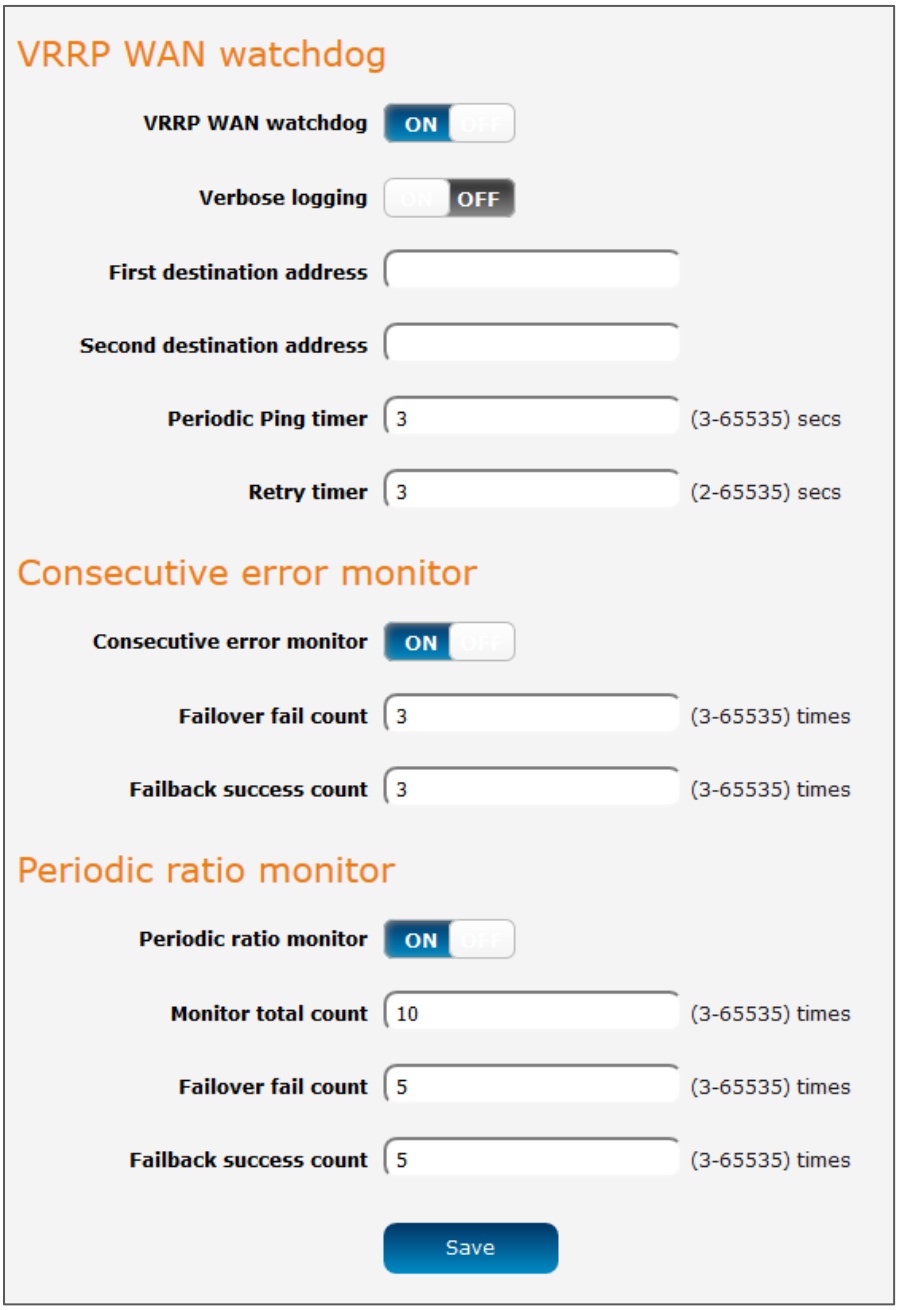
Note: *Configuring VRRP changes the MAC address of the Ethernet port and therefore if you want to resume with the web configuration you must use the new IP address (VRRP IP) or clear the arp cache (old MAC address) on a command prompt by typing:*

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

Using the VRRP WAN watchdog

By default, VRRP WAN watchdog is disabled. When it is disabled, VRRP monitors the status of the master and slave 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. Refer to the *Ping monitor* section for more information on how to configure the watchdog.

Figure 8-47 VRRP WAN watchdog configuration



Port forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the router. To access the Port forwarding page, click on the **Networking** menu at the top of the screen, click on the **Routing** menu on the left, then click on the **Port forwarding** menu item.

Figure 8-48 Port forwarding list

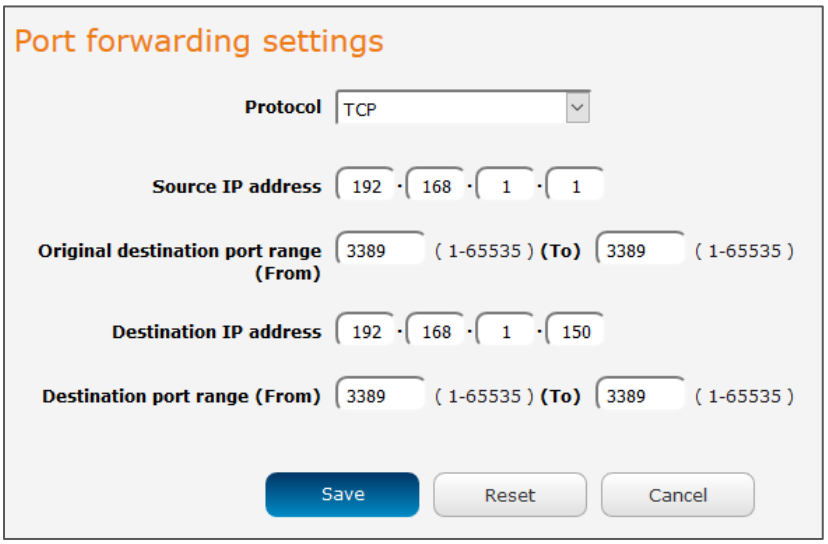
The purpose of the port forwarding feature is to allow mapping of inbound requests to a specific port on the WAN IP address to any connected device.

Adding a port forwarding rule

To create a new port forwarding rule:

1. Click the **+Add** button. The port forwarding settings screen is displayed.
2. 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 **All**.
3. In the **Source IP Address** field, enter a "friendly" address that is allowed to access the router or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the router.
4. The **Original destination port range (From)** and **(To)** fields are used to specify the port(s) on the source side that are to be forwarded. This allows you to send a range of consecutive port numbers by entering the first in the range in the (From) field and the last in the range in the (To) field. To forward a single port, enter the port in the (From) field and repeat it in the (To) field.
5. In the **Destination IP address** field, enter the IP address of the client to which the traffic should be forwarded.
6. The **Destination Port Range (From)** and **(To)** fields are used to specify the port(s) on the destination side that are to be forwarded. If the Source port range specifies a single port then the destination port may be configured to any port. If the Source port range specifies a range of port numbers then the Destination port range must be the same as the Source port range.
7. Click the **Save** button to confirm your settings.

Figure 8-49 Port forwarding settings



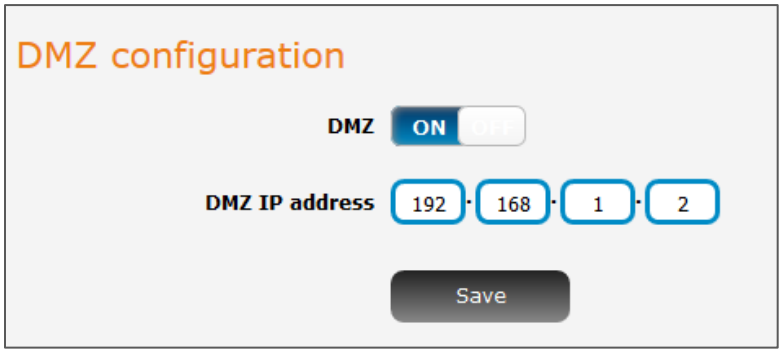
To delete a port forwarding rule, click the × button on the **Port forwarding list** for the corresponding rule that you would like to delete.

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, click on the **Networking** menu at the top of the screen, click on the **Routing** menu on the left, then click on the **DMZ** menu item.

Figure 8-50 DMZ configuration



1. Click the **DMZ** toggle key to turn the DMZ function **ON**.
2. Enter the IP Address of the device to be the DMZ host into the **DMZ IP Address** field.
3. Click the **Save** button to save your settings.

Router firewall

The Router firewall page is used to enable or disable the in-built firewall on the router. When enabled, the firewall performs stateful packet inspection on inbound traffic from the wireless WAN and blocks all unknown services, that is, all services not listed on the Services configuration page of the router.

With respect to the other Routing options on the Networking page, the firewall takes a low priority. The priority of the firewall can be described as:

DMZ > MAC/IP/Port filtering rules > MAC/IP/Port filtering default rule > Router firewall rules

In other words, the firewall is of the lowest priority when compared to other manual routing configurations. Therefore, a MAC/IP/Port filtering rule takes priority in the event that there is a conflict of rules. When DMZ is enabled, MAC/IP/Port filtering rules and the router firewall are ignored but the router will still honour the configuration of the Remote router access control settings listed under Administration Settings.

To access the DMZ page, click on the Networking menu at the top of the screen, click on the Routing menu on the left, then click on the Router firewall menu item.

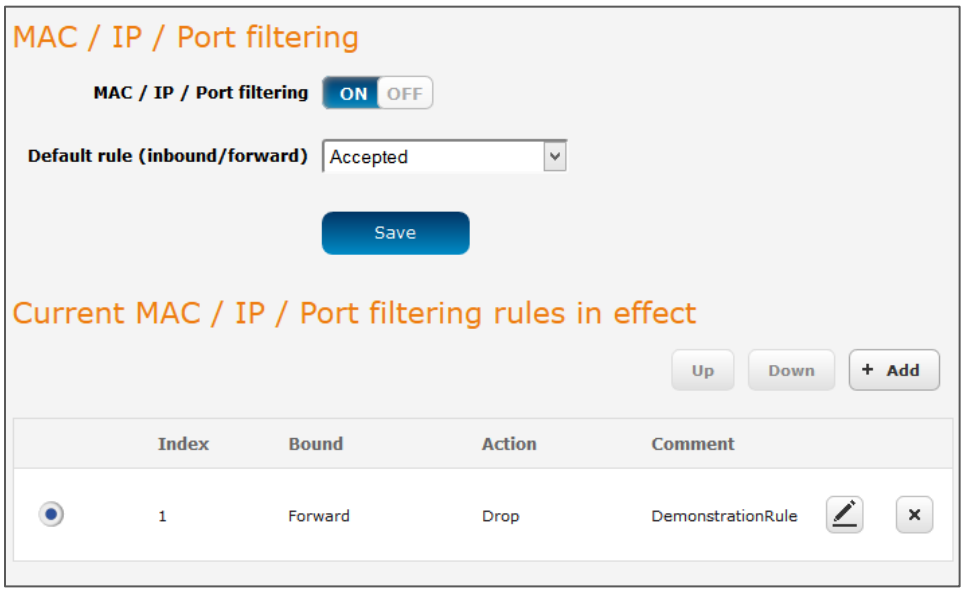
Figure 8-51 Router firewall toggle key

MAC / IP / Port filtering

The MAC/IP/Port filter feature 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.

To access the MAC / IP / Port filtering page, click on the Networking menu at the top of the screen, click on the Routing menu on the left, then click on the MAC / IP / Port filtering menu item.

Figure 8-52 MAC / IP / Port 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. Click the **MAC / IP / Port filtering** toggle key to switch it to the **ON** position.

2. Using the **Default rule (inbound/forward)** drop-down list, 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 the effect section, click the **+Add** button.

Figure 8-53 Current MAC / IP/ Port filtering rules in effect

5. Enter the details of the rule in the section that is displayed and click the **Save** button.

Figure 8-54 MAC / IP / Port filtering settings

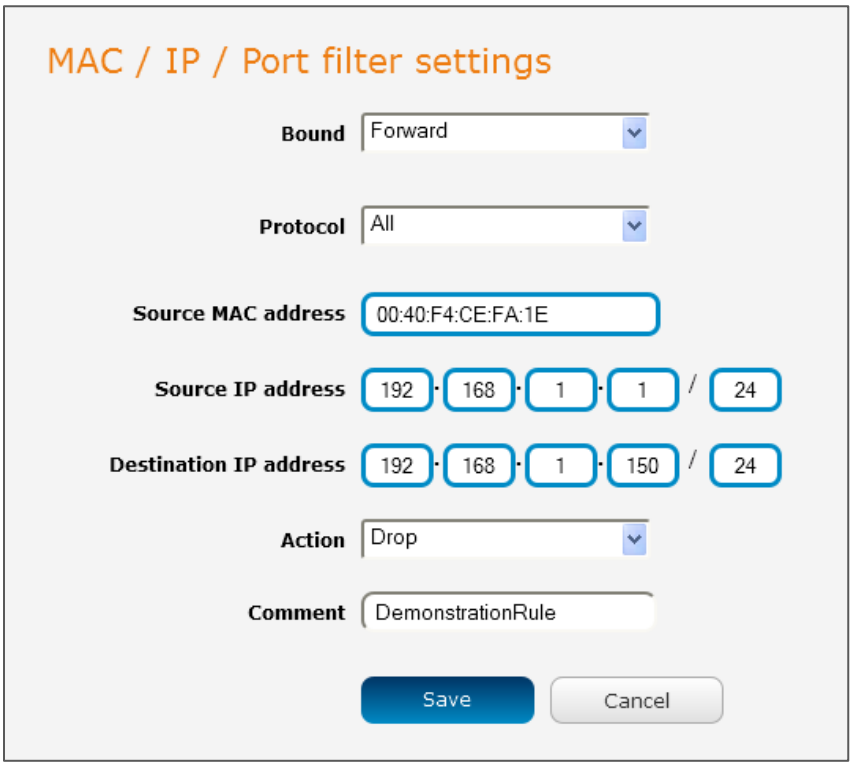


Table 8-8 Current MAC / IP / Port filtering rules in effect

Option	Description
Bound	Use the drop-down list to select the direction of the traffic for which you want to apply to the rule. Inbound refers to all traffic that is entering the router including data entering from the WAN and the

	LAN. Outbound refers to all traffic exiting the router including traffic leaving in the direction of the WAN and traffic leaving in the direction of the LAN. Forward specifies traffic that enters on the LAN or WAN side and is forwarded to the opposite end.
Protocol	Use the drop-down list to select the protocol for the rule. You can have the rule apply to all protocols, TCP, UDP, UDP/TCP, and ICMP.
Source MAC Address	Enter the MAC address in six groups of two hexadecimal digits separated by colons (:). e.g., 00:40:F4:CE:FA:1E
Source IP Address	Enter the IPv4 address that the traffic originates from and the subnet mask using CIDR notation.
Destination IP Address	Enter the IPv4 address that the traffic is destined for and the subnet mask using CIDR notation.
Action	Select the action to take for traffic which meets the above criteria. You can choose to Accept or Drop packets. When the default rule is set to Accept, you cannot create a rule with an Accept action since the rule is redundant. Likewise, if the default rule is set to Dropped you cannot create a rule with a Drop action.
Comment	[Optional] Use this field to enter a comment as a meaningful description of the rule.

6. The new rule is displayed in the filtering rules list. You can edit the rule by clicking the Edit button or delete the rule by clicking the × button.

Figure 8-55 Completed filtering rule

VPN

A Virtual Private Network (VPN) is a tunnel providing a private link between two networks or devices over a public network. Data to be sent via a VPN needs to be encapsulated and as such is generally not visible to the public network.

The advantages of a VPN connection include:

- Data Protection
- Access Control
- Data Origin Authentication

- Data Integrity

Each VPN connection has different configuration requirements. The following pages detail the configuration options available for the different VPN connection types.

Important: *The following descriptions are an overview of the various VPN options available. More detailed instructions are available in separate whitepapers on the Lantronix website.*

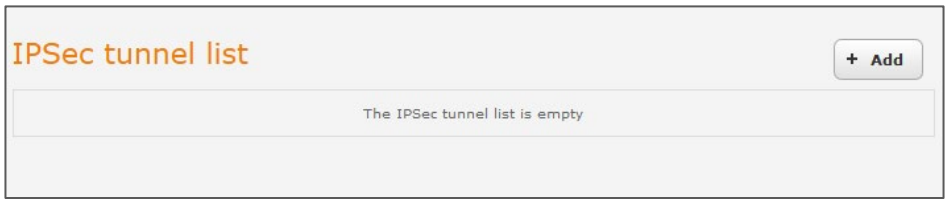
IPSec

IPSec operates on Layer 3 of the OSI model and as such can protect higher layered protocols. IPSec is used for both site to site VPN and Remote Access VPN. The NTC-220 Series router supports IPsec end points and can be configured with Site to Site VPN tunnels with third party VPN routers.

Configuring an IPSec VPN

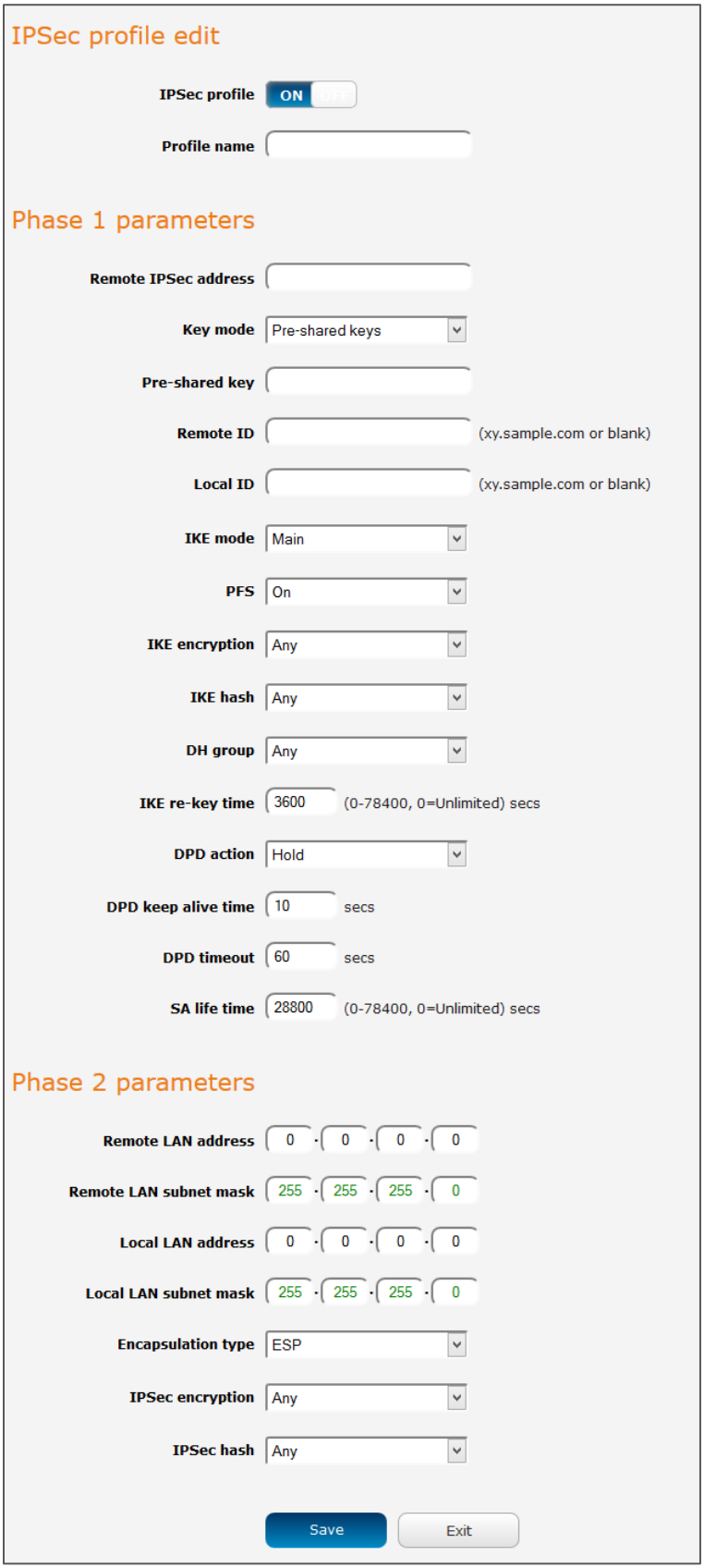
From the menu at the top of the screen, click Networking and under the VPN section, click IPSec. A list of configured IPSec VPN connections is displayed.

Figure 8-56 IPSec VPN List



Click the **+Add** button to begin configuring an IPSec VPN connection.

Figure 8-57 IPSec profile edit



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

Table 8-9 IPSec Configuration Items

Item	Definition
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 Key • RSA keys • Certificates • SCEP client
Pre-shared key	The pre-shared key is the key that peers used 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.
Update Time	Displays the last time the key was updated.
Local RSA Key Upload	Select the RSA key file for the local router here by clicking the Browse button.
Remote RSA Key Upload	Select the RSA key file for the remote router here by clicking the Browse button.
Private key Passphrase	The Private key passphrase of the router is the passphrase used when generating the router's private key using OpenSSL CA.
Key / Certificate	Select the type of key or certificate to use for authentication. You can select Local private key, Local public certificate, Remote public certificate, CA certificate, CRL certificate.
IPSec Certificate Upload	Select the IPSec certificate to upload by clicking the Browse button.
Remote ID	Specifies the domain name of the remote network.
Local ID	Specifies the domain name of the local network.
IKE mode	Select the IKE mode to use with the VPN connection. You can choose Main, Aggressive or Any.

PFS	Choose whether Perfect Forward Secrecy is ON or OFF for the VPN connection.
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.
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 desired 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.

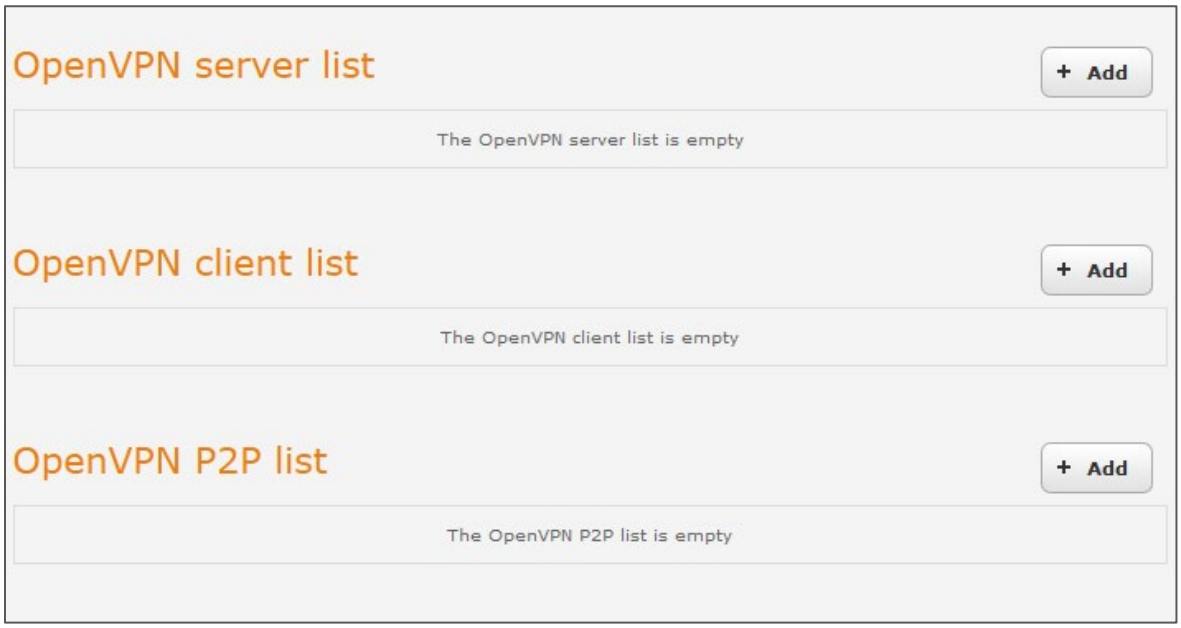
OpenVPN

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 several operating systems, including Windows, Linux, OS X, Solaris, OpenBSD, FreeBSD, NetBSD, and QNX.

Configuring an Open VPN connection

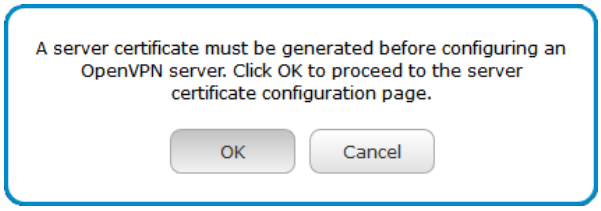
From the menu at the top of the screen, click Networking and from the VPN section on the left, click OpenVPN. A list of configured OpenVPN VPN connections is displayed.

Figure 8-58 OpenVPN VPN List



Configuring an OpenVPN Server

When you select the **+Add** button to add an OpenVPN server, the router checks whether there are existing server certificates. If no server certificate is found, you are informed that you must generate a certificate before configuring the OpenVPN server.



Click on the **OK** button to be taken to the **Server certificate** page. 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 and continue with the steps below.

To configure an OpenVPN Server:

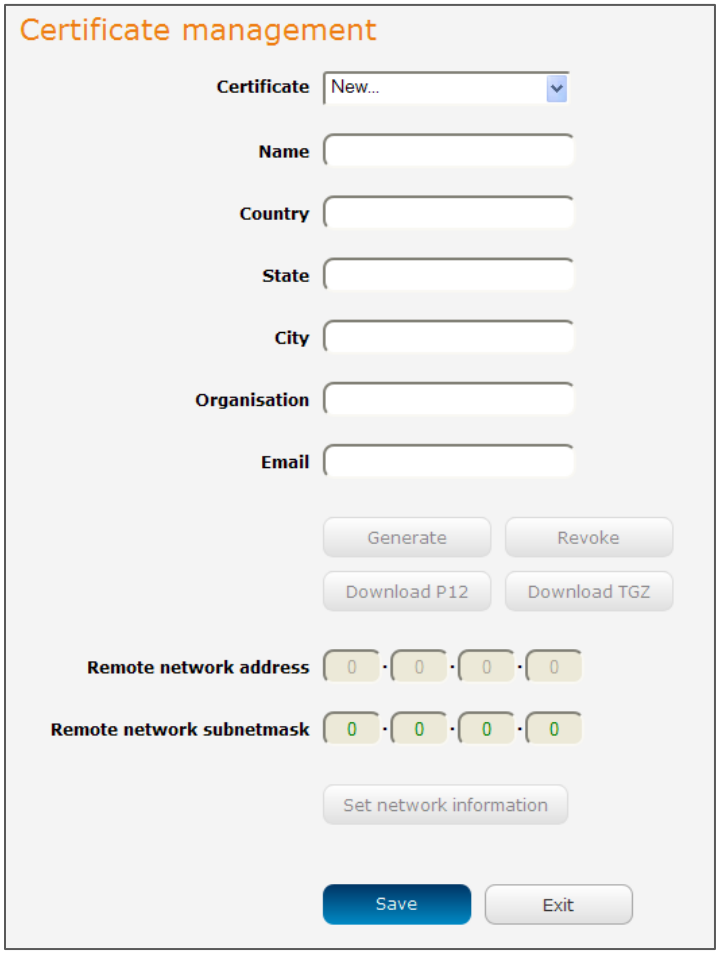
1. Click the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. Type a name for the OpenVPN server profile you are creating.

3. In the **Type** drop-down list, select the **OpenVPN connection type** (**TUN**/**TAP**). Default is **TUN**.
4. Use the **Server port** field to select a port number and then use the drop-down list to select a packet type to use for your OpenVPN Server. The default OpenVPN port is 1194 and default packet type is UDP.
5. 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.
6. The Server certificates section displays the details of the certificate. If you wish to change the certificate, click the **Change** button.
7. HMAC or Hash-based Message Authentication Code is a means of calculating a message authentication code through the use of 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, click the **Use HMAC Signature** toggle key so that it is in the **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.
8. Select an **Authentication type**. Authentication may be done using a Certificate or Username / Password.

Certificate Authentication

In the Certificate Management section, enter the required details to create a client certificate. All fields are required. When you have finished entering the details, click the Generate button.

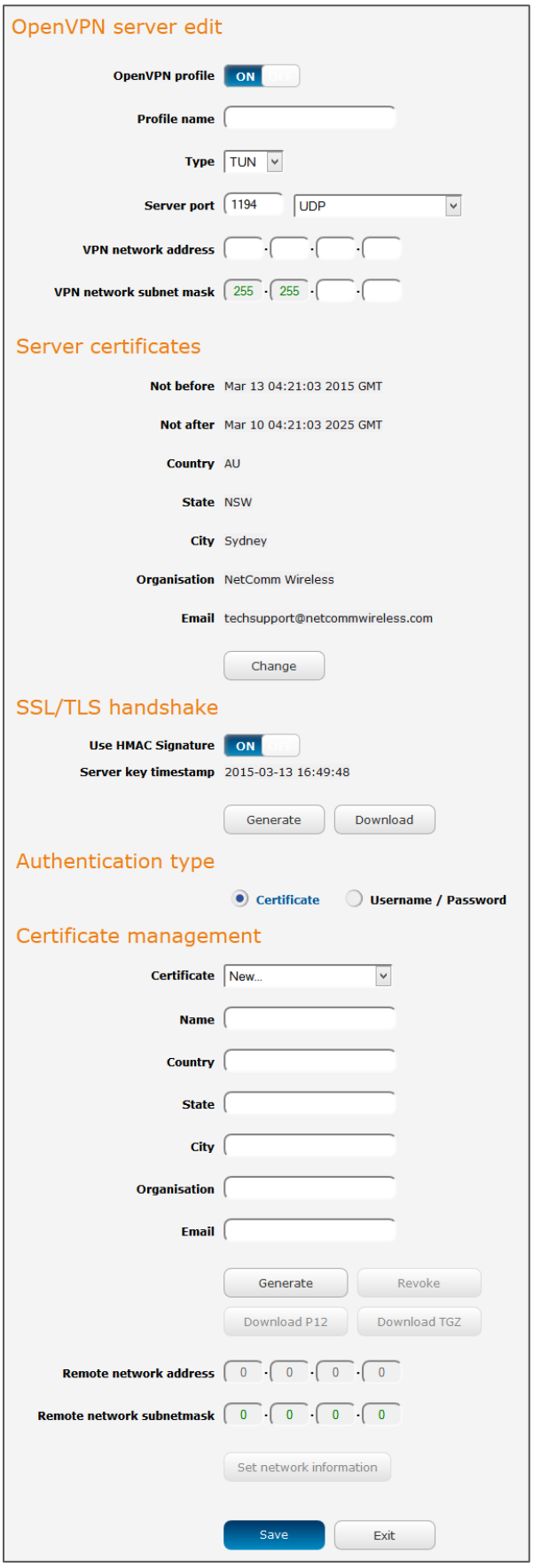
Figure 8-59 OpenVPN server configuration – Certificate management



When it is done, you can click the **Download P12** button or the **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, you can return to this screen and use the **Certificate** drop-down list to select the certificate and then press the Revoke button to disable it.

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.

Figure 8-60 OpenVPN server profile settings

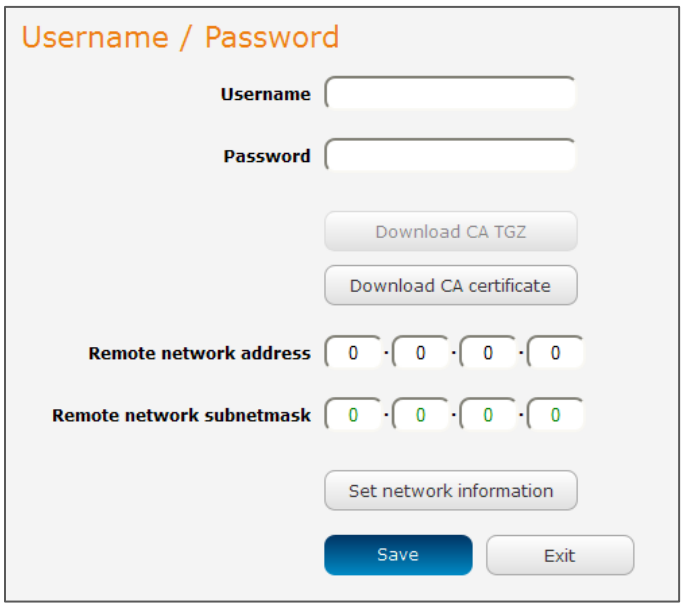


Username / Password Authentication

In the **Username/Password** section, enter the username and password you would like to use for authentication on the OpenVPN Server. Click the **Download CA certificate** or **Download CA TGZ** depending on file format button 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 8-61 OpenVPN Server – Username / Password section



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 finish configuring the OpenVPN server.

Configuring an OpenVPN Client

1. Click the OpenVPN profile toggle key to switch it to the ON position.
2. In the Profile name field, type a name for the OpenVPN client profile you are creating.
3. In the Server IP address field, type the WAN IP address /host domain name of the OpenVPN server.
4. Select OpenVPN connection type (TUN/TAP). Default is TUN.
5. Use the Server port field to select a port number and then use the drop-down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
6. 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.
7. Use the Authentication type options to select the Authentication type that you would like to use for the OpenVPN client.

Certificate Authentication

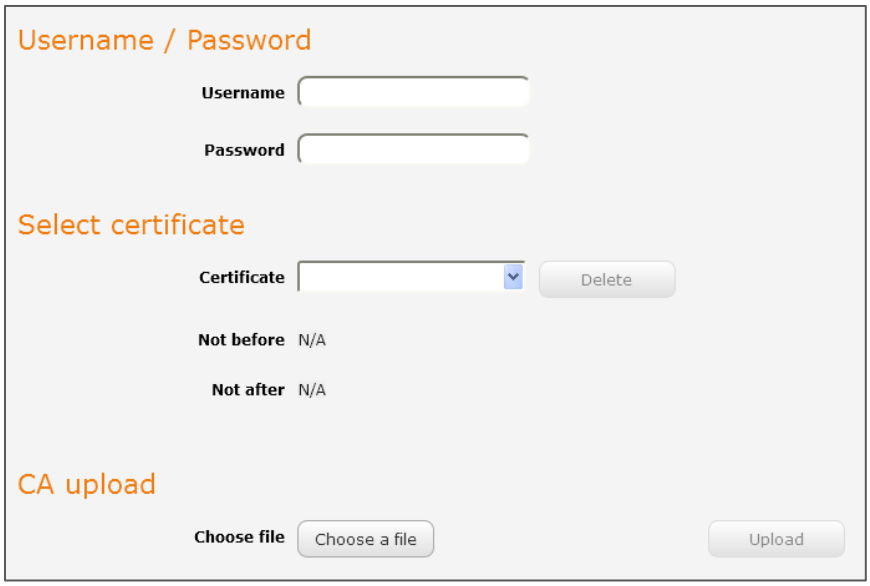
In the Certificate upload section at the bottom of the screen, click the Choose a file button and locate the certificate file you downloaded when you configured the OpenVPN server. When it has been selected, click the Upload button to send it to the router.

Figure 8-62 OpenVPN client – Certificate upload

Username / Password Authentication

1. Enter the username and password to authenticate with the OpenVPN server.

Figure 8-63 OpenVPN Client – Username/Password section



2. Use the **Choose a file** button to locate the CA certificate file you saved from the OpenVPN Server and then press the **Upload** button to send it to the router.
3. Click the **Save** button to complete the OpenVPN Client configuration.
4. If you have an additional SSL/TLS key created on the server, click on the **Use HMAC Signature** toggle key so that it is in the **ON** position. Select the **Choose a file** button then locate the key file on your computer. Click the **Upload** button to upload it to the router.
5. Click the **Save** button to save your settings.

Certificate and Username / Password Authentication

This is a combination of both the Certificate and Username / Password authentication methods providing additional levels of security since the client must know the username / password combination and be in possession of the certificate.

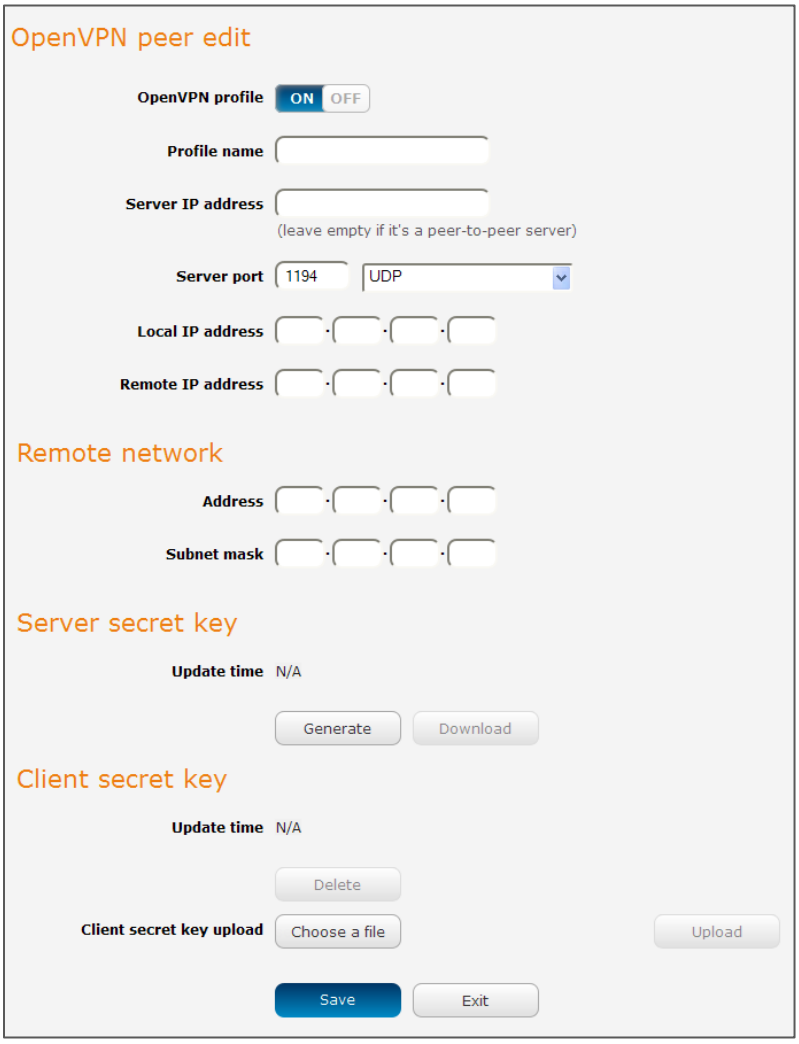
Configuring an OpenVPN P2P Connection

To configure an OpenVPN peer-to-peer connection:

1. Set the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. In the **Profile** name field, type a name for the OpenVPN P2P profile you are creating.

3. On the router designated as the server, leave the **Server IP address** field empty. On the router designated as the client, enter the WAN IP address/host domain name of the server.

Figure 8-64 OpenVPN P2P mode settings



4. Use the **Server port** field to select a port number and then use the drop-down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
5. 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 slave should have the reverse settings of the master.
6. Under the **Remote network** section, enter the network **Address** and network **Subnet mask**. The Network Address and Network Mask fields inform the Master node of the LAN address scheme of the slave.
7. Press the **Generate** button to create a secret key to be shared with the slave. When the timestamp appears, you can click the **Download** button to save the file to exchange with the other router.
8. When you have saved the secret key file on each router, use the **Choose a file** button to locate the secret key file for the master and then press the **Upload** button to send it to the slave. Perform the same for the other router, uploading the slave's secret key file to master.
9. When they are uploaded click the **Save** button to complete the peer-to-peer OpenVPN configuration.

PPTP client

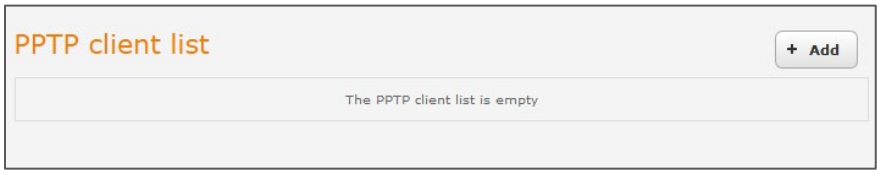
The Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks using a TCP and GRE tunnel to encapsulate PPP packets. PPTP operates on Layer 2 of the OSI model and is included on Windows computers.

Configuring the PPTP client

To configure the PPTP client:

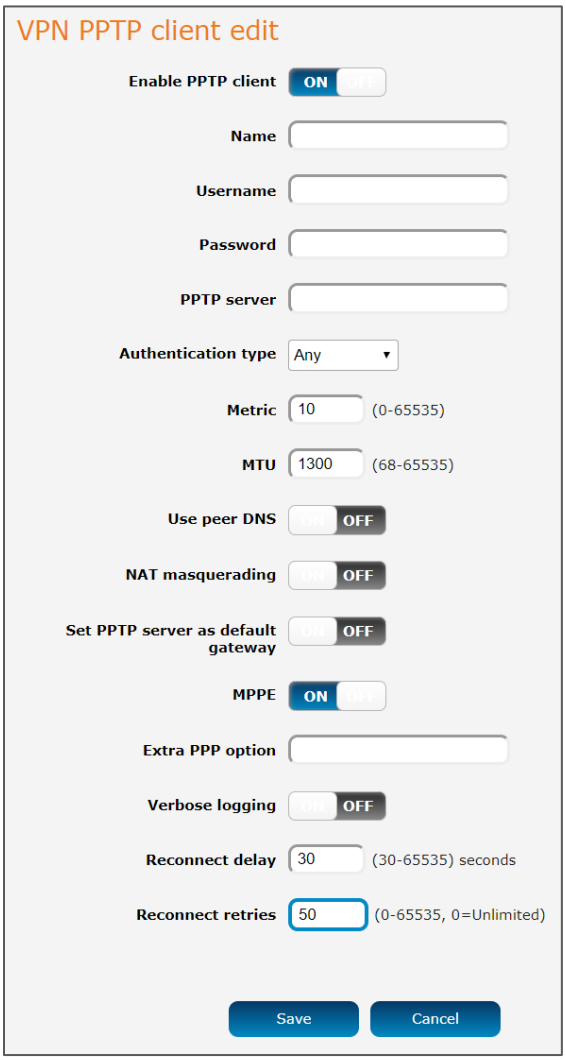
1. From the menu bar at the top of the screen, click **Networking** and then from the **VPN** drop-down menu on the left side of the screen, click **PPTP client**. The **PPTP client list** is displayed.

Figure 8-65 PPTP client list



2. Click the **+Add** button to begin configuring a new PPTP client profile. The **PPTP client edit** screen is displayed.

Figure 8-66 VPN PPTP client edit



3. Click the **Enable PPTP client** toggle key to switch it to the **ON** position.
4. In the P**rofile name** field, enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. Use the **Username** and **Password** fields to enter the username and password for the PPTP account.
6. In the **PPTP server** field, enter the IP address /host domain name of the PPTP server.
7. From the **Authentication type** drop-down list, select the Authentication type used on the server. If you do not know the authentication method used, select any and the router will attempt to determine the correct authentication type for you. There are 5 authentication types you can choose from:
    - **CHAP** – uses a three-way handshake to authenticate the identity of a client.
    - **MS-CHAP v1** – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista.
    - **MS-CHAP v2** - This is the Microsoft implementation of the Challenge Handshake Authentication Protocol which was introduced in Windows® NT 4.0 and is still supported today.
    - **PAP** – The Password Authentication Protocol uses a password as a means of authentication and as such, is commonly supported. PAP is not recommended because it transmits passwords unencrypted and is not secure.
    - **EAP** – Extensible Authentication Protocol. An Authentication protocol commonly used in wireless networks.
8. The **Metric** value helps the router to prioritise routes and must be a number between 0 and 65535. The default value is 30 and should not be modified unless you are aware of the effect your changes will have.
9. Enter the size of the **MTU** (Maximum Transmission Unit). The PPTP tunnel has a 40 byte overhead meaning the maximum value that this should be set to is 1300.
10. The **Use peer DNS** option allows you to select whether the remote clients will use the Domain Name Server of the PPTP server. Click the toggle key to set this to ON or OFF as required.
11. **NAT masquerading** allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. Click the toggle key to switch this to the ON position if you want to use this feature.
12. **Set PPTP server as default gateway** sets all outbound data packets to go out through the PPTP tunnel. Click the toggle key to switch this to the **ON** position if you want to use this feature.
13. The **MPPE** toggle key turns the Microsoft Point-to-Point Encryption feature **ON** or **OFF**. This is used to secure transmissions. Set this as desired.
14. In the **Extra PPP option** field, specify any extra commands or parameters that you wish to use when the PPP connection is established.
15. The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the System Log section of the router interface.
16. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the PPTP server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the PPTP server with connection requests, while the maximum time to wait is 65335 seconds.
17. The **Reconnect retries** is the number of connection attempts that the router will make in the event that the PPTP 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.
18. Click the **Save** button to save the changes. The VPN will attempt to connect after you click **Save**. Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.

GRE tunnelling

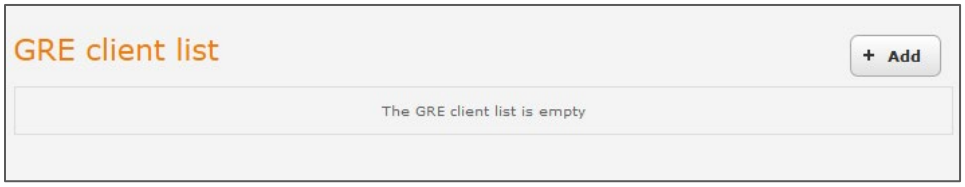
The Generic Route Encapsulation (GRE) protocol creates a point-to-point connection similar to a VPN between clients and servers or between clients only. GRE is used to encapsulate the data or payload.

Configuring GRE tunnelling

To configure GRE tunnelling:

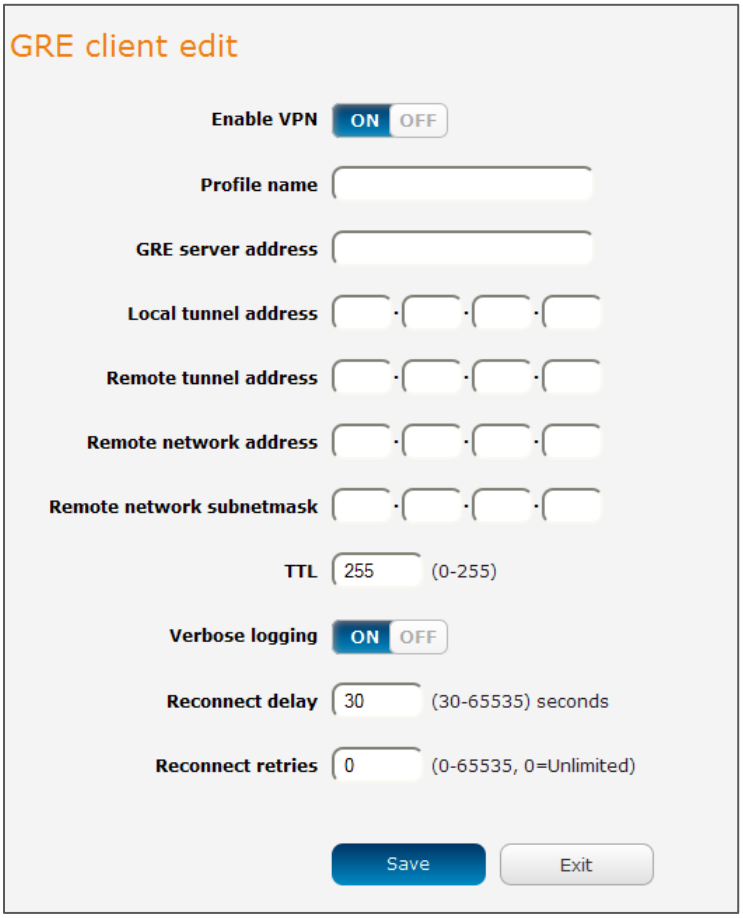
1. From the menu bar at the top of the screen, click **Networking** and then from the **VPN** section on the left side of the screen, click **GRE tunnelling**. The **GRE client list** is displayed.

Figure 8-67 GRE client list



2. Click the **+Add** button to begin configuring a new GRE tunnelling client profile. The **GRE client edit** screen is displayed.

Figure 8-68 GRE client edit



3. Click the **Enable VPN** toggle key to switch it to the **ON** position.
4. In the **Profile name**, enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. In the **GRE server address** field, enter the IP address or domain name of the GRE server.

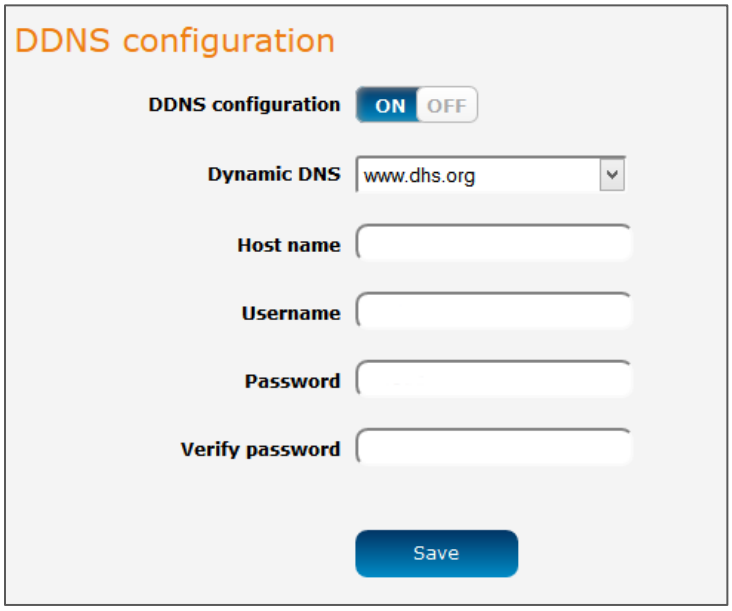
6. In the **Local tunnel address** field, enter the IP address you want to assign the tunnel locally.
7. In the **Remote tunnel address** field, enter the IP address you want to assign to the remote tunnel.
8. In the **Remote network address** field, enter the IP address scheme of the remote network.
9. In the **Remote network subnetmask** field, enter the subnet mask of the remote network.
10. 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 the route to 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.
11. The **Verbose logging** option sets the router to output detailed logs regarding the GRE tunnel in the System Log section of the router interface.
12. 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.
13. 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.
14. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Click the Status button at the top left of the interface to return to the status window and monitor the VPN's connection state.

9. Services

Dynamic DNS

The DDNS page is used to configure the Dynamic DNS feature of the router. A number of Dynamic DNS hosts are available from which to select. To access the Dynamic DNS page, click on the **Services** menu at the top of the screen then click on the **Dynamic DNS** menu item on the left.

Figure 9-1 Dynamic DNS settings



Dynamic DNS provides a method for the router to update an external name server with the current WAN IP address.

To configure dynamic DNS:

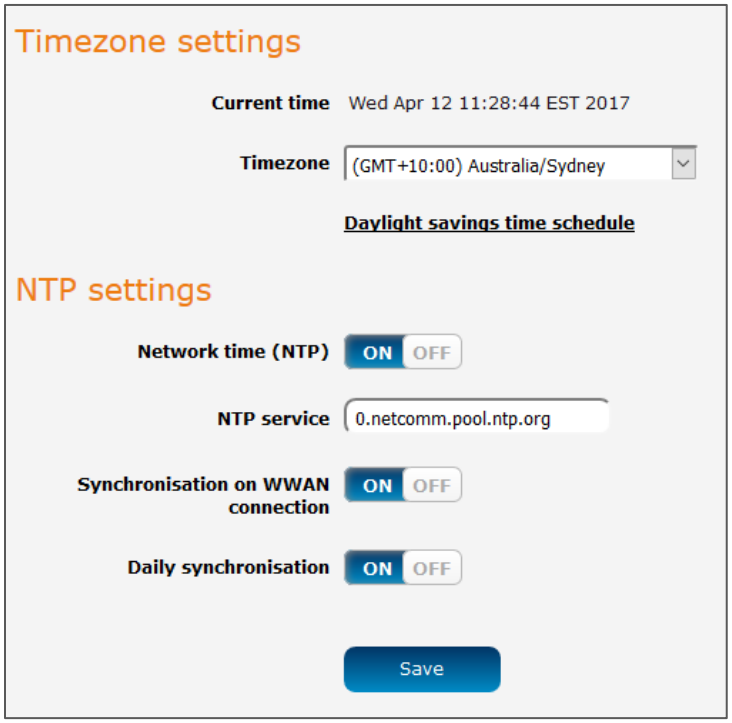
1. Click the **DDNS configuration** toggle key to switch it to the **ON** position.
2. From the **Dynamic DNS** drop-down list, select the Dynamic DNS service that you wish to use. The available DDNS services available are:
    - www.dhs.org
    - www.dyndns.org
    - www.easydns.com
    - www.justlinux.com
    - www.no-ip.com
    - www.tzo.com
    - www.zoneedit.com
3. Enter your hostname in the **Host name** field.
4. In the **Username** and **Password** fields, enter the logon credentials for your DDNS account. Enter the password for the account again in the **Verify password** field.
5. Click the **Save** button to save the DDNS configuration settings.

Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the NTC-220 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 NTP server available publicly on the internet may be used. The default NTP server is 0.netcomm.pool.ntp.org.

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

Figure 9-2 NTP settings



Configuring Timezone settings

To configure time zone settings:

1. 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 link appears below the drop-down list. Click the link to see the start and end times for daylight savings.
2. When you have selected the correct time zone, click the **Save** button to save the settings.

Configuring NTP settings

To configure NTP settings:

1. Click 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 wish to use.
3. The **Synchronization on WWAN connection** toggle key enables or disables the router from performing a synchronization of the time each time a mobile broadband connection is established.

4. The **Daily synchronization** toggle key enables or disables the router from performing a synchronization of the time each day.
5. When you have finished configuring NTP settings, click the **Save** button to save the settings.

Data stream manager

The data stream manager provides you with the ability 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.

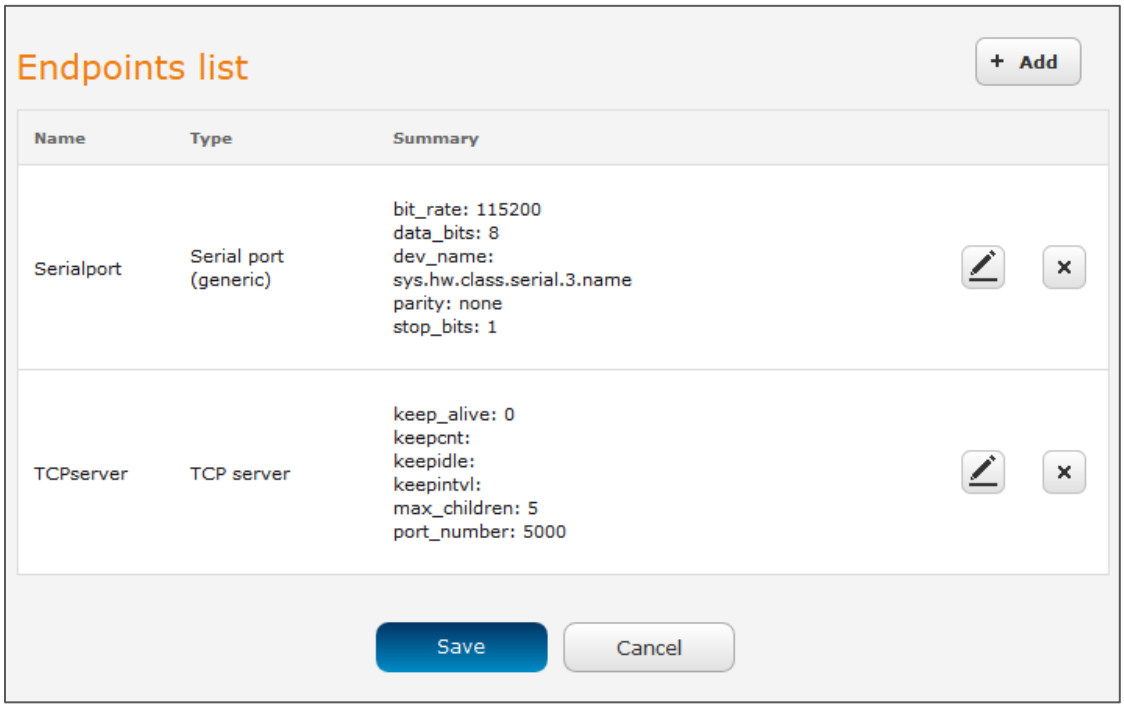
Endpoints

The first thing to be done to create a data stream is to define the endpoints. There are 15 types of endpoints that may be configured:

- 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

To access the **Endpoints list** page, click on the **Services** menu at the top of the screen, click on the **Data stream manager** menu then click on the **Endpoints** menu item on the left.

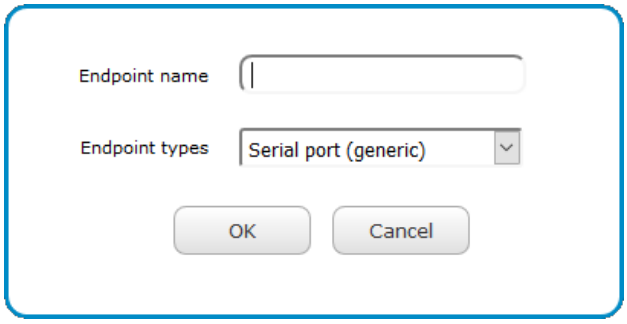
Figure 9-3 Endpoints list



To create an endpoint:

1. Click the **+Add** button on the right side of the page. A pop-up window appears.

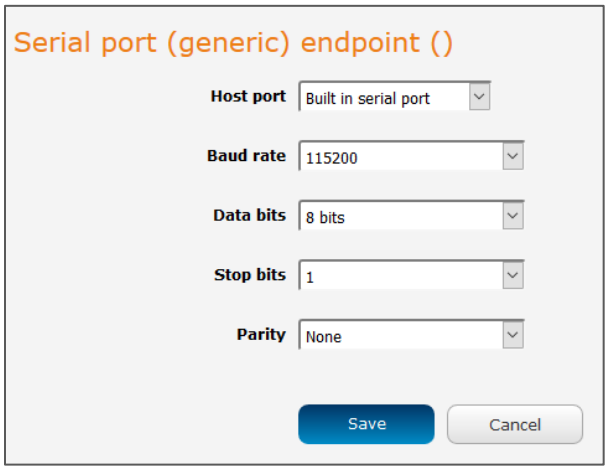
Figure 9-4 Creating an endpoint



2. In the **Endpoint name** field, type a name for this endpoint. The name can contain alphanumeric characters only i.e. A-Z, a-z, 0-9.
3. Use the **Endpoint types** drop-down list to select the type of endpoint to configure.

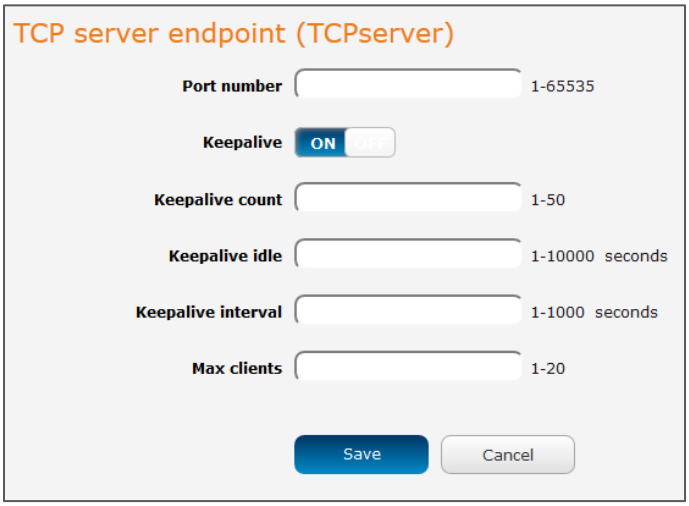
Serial port (generic): When a USB to Serial cable is used, this creates a generic serial port as an endpoint defaulting to the commonly used settings as shown below.

Figure 9-5 Serial port (generic) endpoint configuration



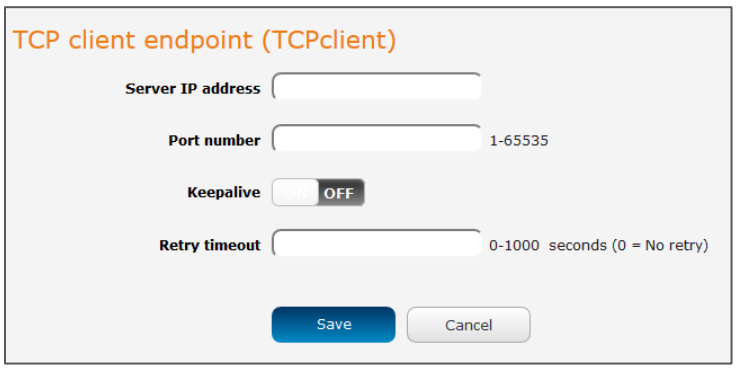
TCP server: This creates a TCP server endpoint with the following options available.

Figure 9-6 TCP server endpoint configuration



TCP client: 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 9-7 TCP client endpoint configuration

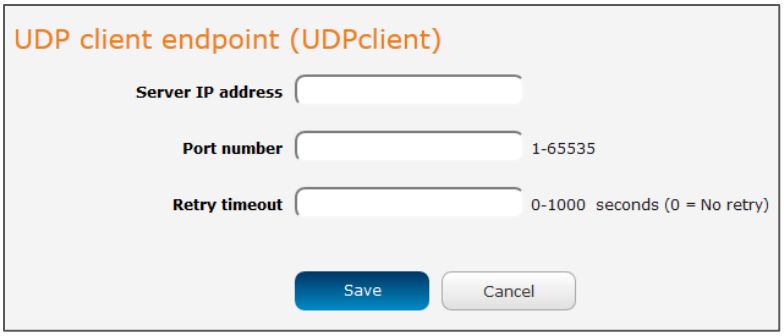


UDP server: This creates a UDP server endpoint with the following options available.

Figure 9-8 UDP server endpoint configuration

UDP client: 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 9-9 UDP client endpoint configuration



GPS data: This creates a GPS data endpoint.

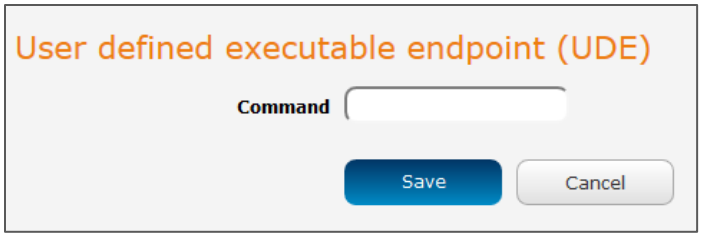
Figure 9-10 GPS data endpoint configuration

User defined executable: 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.

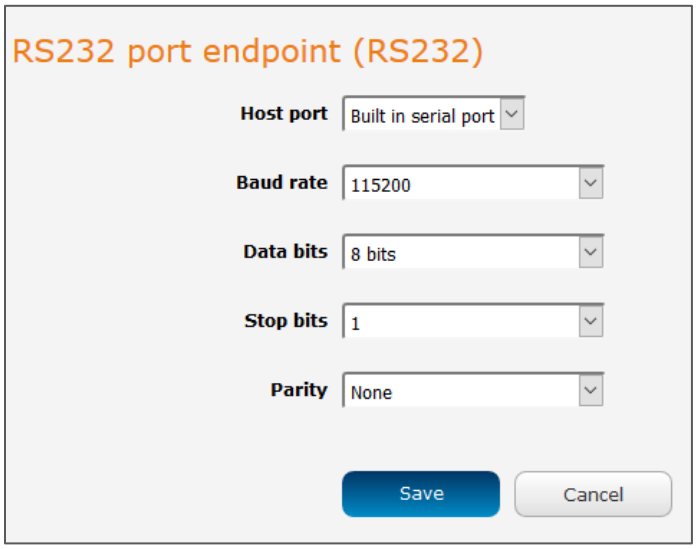
Figure 9-11 User defined executable endpoint configuration



RS232 / RS485 / RS422 port: 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 9-12 RS232 / RS485 / RS422 port configuration options



Note: *For detailed information about half duplex RS-485 and full duplex RS-422 refer to* *Appendix F – Serial port wiring section on page 209.*

Modem emulator - 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-220 Series router emulates the dial-up modem's behaviour and passes the serial data over the IP network.

Figure 9-13 Modem emulator endpoint configuration

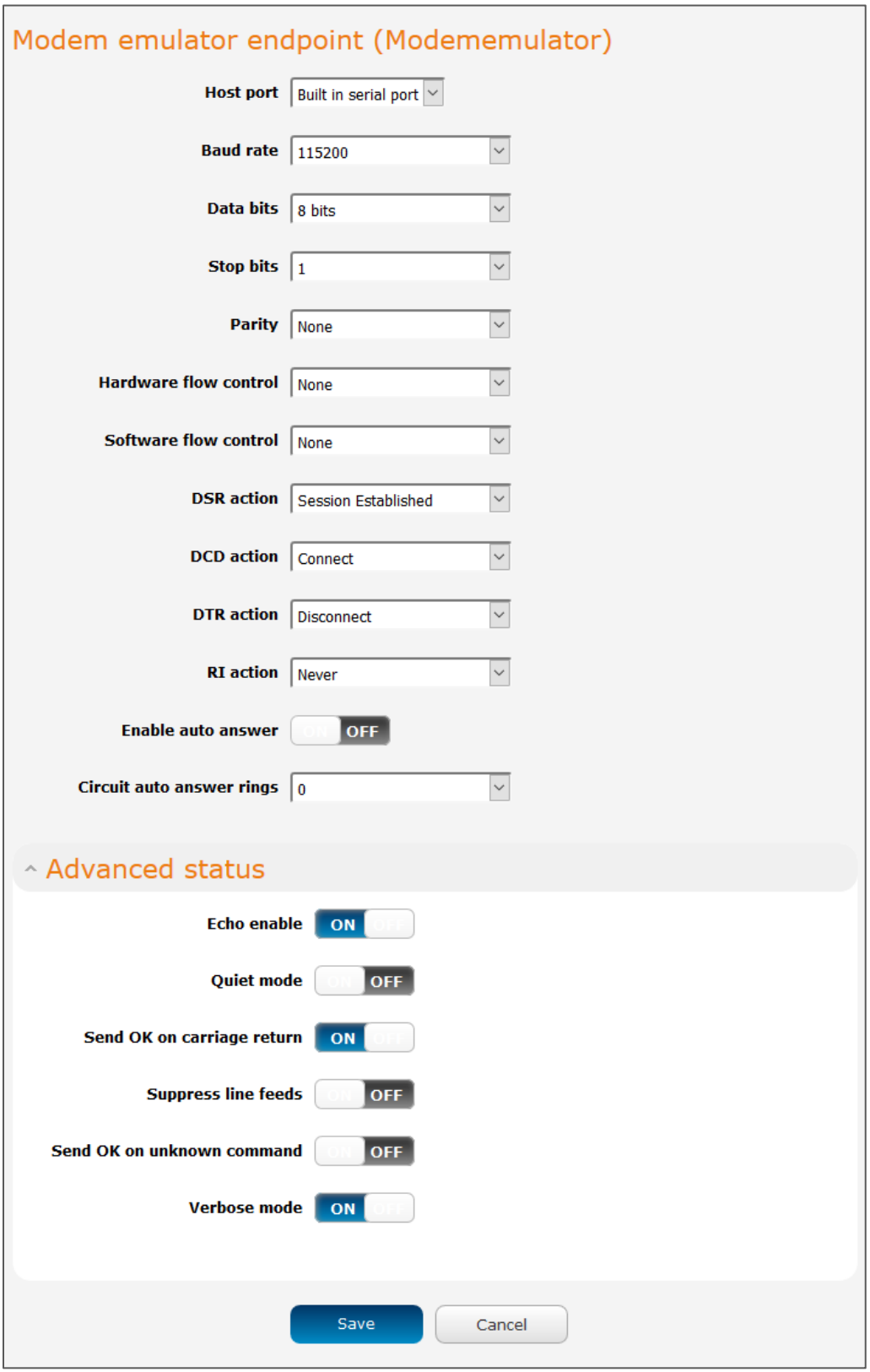


Table 9-1 Modem emulator endpoint options

Item	Description
Host port	Use the drop-down list to 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	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	The default serial line data bits setting used is 8. Options include 5 – 8 bits.
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	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	• **Off** – Serial port flow control off • **Hardware** - Serial port uses RTS/CTS flow control
Software flow control	Enables or disables software flow control.
DSR action	Sets 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	Determines how the router controls the state of the serial port Data Carrier Detect (DCD) line. • **Always On** – DCD is always on.

	• **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	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	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	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: This creates a point-to-point server endpoint with the following options.

Figure 9-14 PPP server endpoint configuration

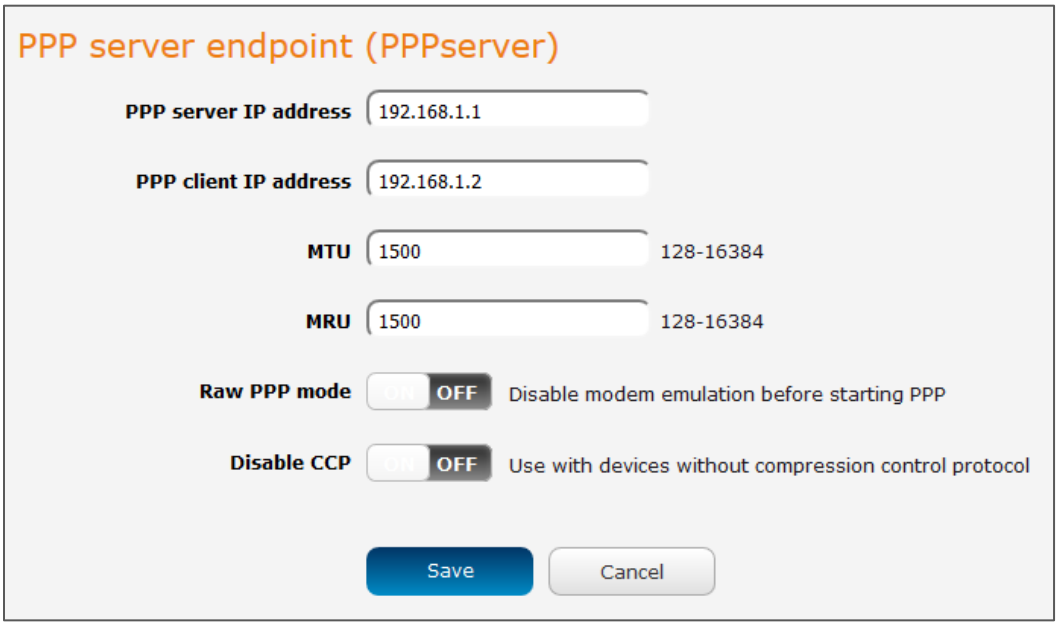


Table 9-2 PPP server endpoint options

Item	Description
PPP server IP address	The IP address of the PPP server. This defaults to the router's current IP address.
PPP client IP address	The IP address of the PPP client. This defaults to the next IP address in the DHCP range after the router's address.
MTU	The maximum transmission unit size of packets sent by the PPP server.
MRU	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: 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.

Table 9-3 IP modem endpoint configuration

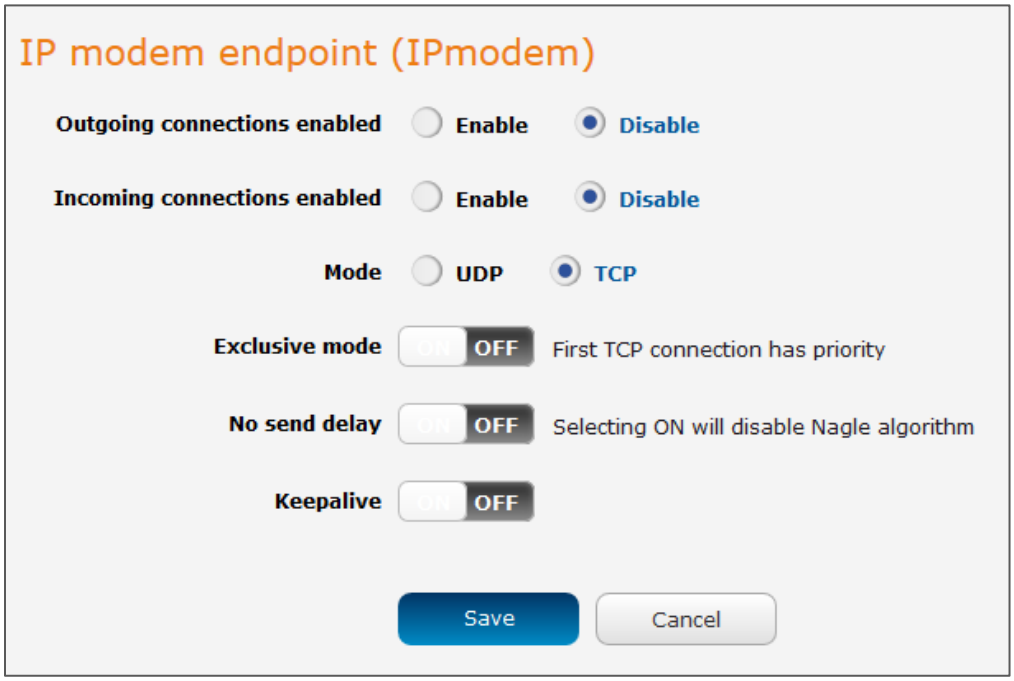


Table 9-4 IP modem endpoint options

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 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.
Keepalive count	The number of keepalive messages to send.
Keepalive idle	The duration between two keepalive transmissions when in idle condition.
Keepalive interval	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 9-15 TCP connect-on-demand endpoint configuration

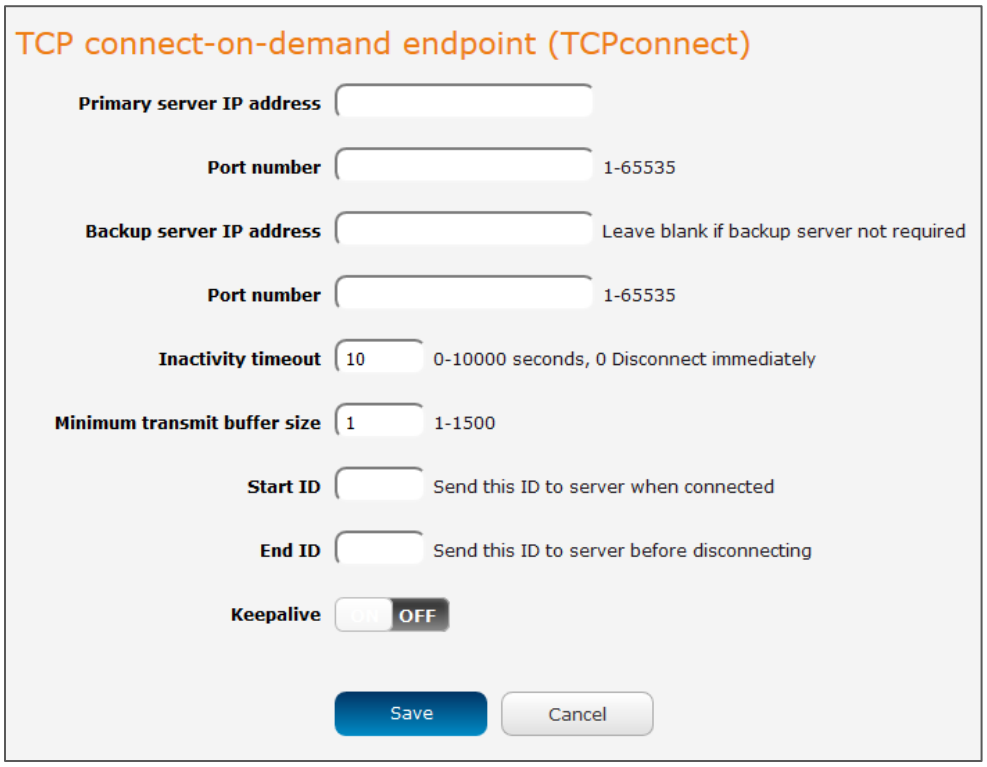
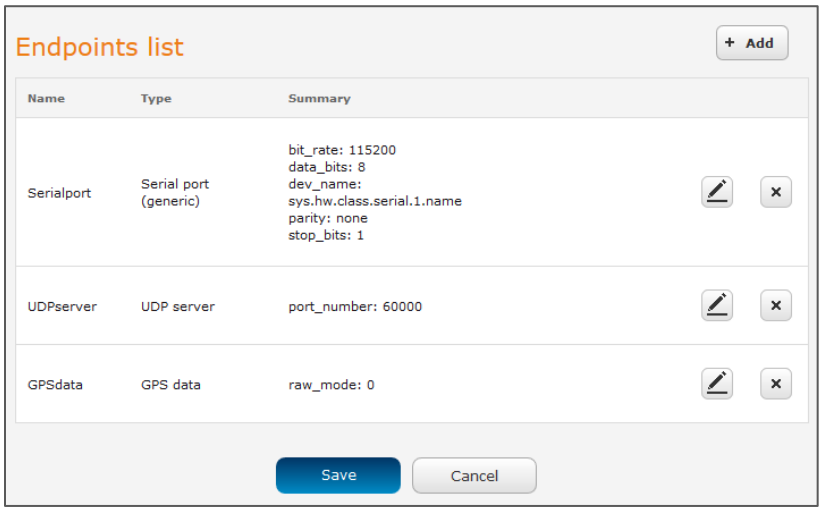


Table 9-5 TCP connect-on-demand endpoint options

Item	Description
Primary server IP address	The IP address of the TCP server to which the router should attempt the initial connection.
Port number	The port number that the TCP server operates on.
Backup server IP address	If connection to the primary server fails, the router will attempt to connect to this address.
Port number	The port number that the backup TCP server operates on.
Inactivity timeout	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	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.
Keepalive count	The number of keepalive messages to send.
Keepalive idle	The duration between two keepalive transmissions when in idle condition.
Keepalive interval	The duration between two successive keepalive retransmissions.

4. Click the **OK** button. The router displays a screen with configuration options for your chosen endpoint type.
5. Enter the options for your endpoint as required.
6. Click the **Save** button. The Endpoints list is displayed with the newly created endpoint listed and a summary of the settings your configured.

Figure 9-16 Endpoints list



Streams

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. To access the Streams page, click on the Services menu at the top of the screen, click on the Data stream manager menu then click on the Streams menu item on the left.

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.

Every 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 stream:

1. Click the **+Add** button on the right side of the page.

Figure 9-17 Data stream list

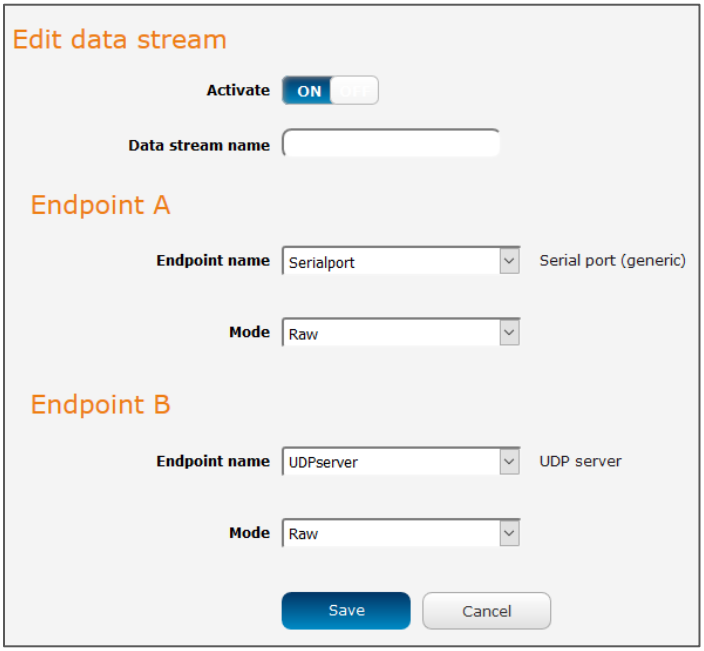
The Edit data stream page is displayed.

2. In the **Data stream name** field, enter a name for the Data stream.
3. Under **Endpoint A**, use the Endpoint name drop-down list to select one of the endpoints you created previously. This endpoint should be the starting point of the stream. Use the Mode drop-down list to 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.

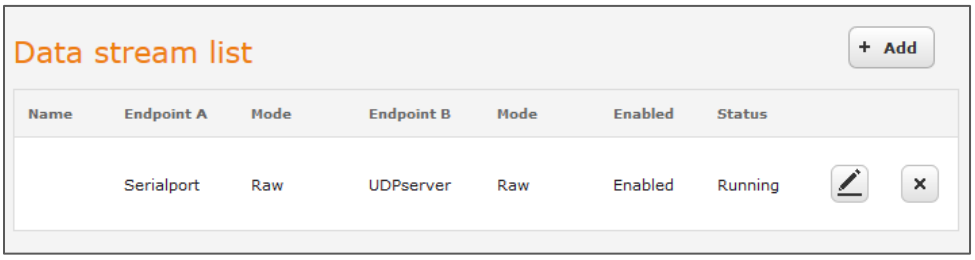
4. Under **Endpoint B**, use the Endpoint name drop-down list to select one of the endpoints you created previously. This endpoint should be the destination of the stream. The screenshot below shows a configuration sending data received on an attached serial port to a TCP server running on the router. Use the Mode drop-down list to 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.

Figure 9-18 Edit data stream



5. Click the **Save** button. The new stream appears in the **Data stream list**.

Figure 9-19 Data stream list



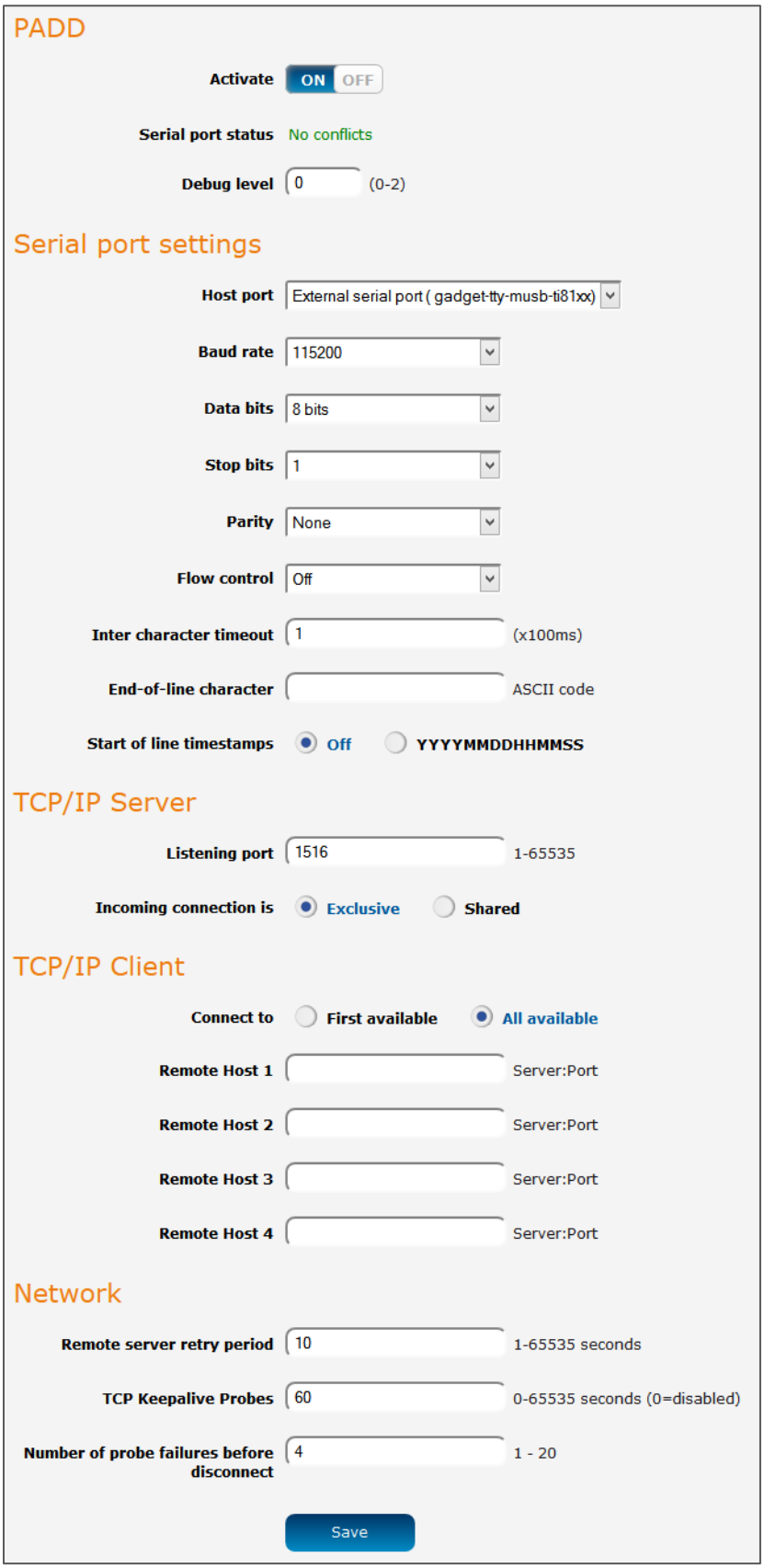
PADD

PAD Daemon is a tool used to encapsulate raw serial data into a TCP packet to be transported over IP to another end point. The server receiving the TCP packets unpacks the data and the original raw serial data is passed out of its serial port to the attached device, thereby creating an invisible IP network to the two serial devices.

The PAD Daemon runs as a background process which can be accessed via the web configuration interface. The PADD configuration page is located under “Services > PADD”. The PADD is used usually with multiple connections or when redundant connections are needed. The PADD has two modes: the PADD TCP/IP Server mode and PADD TCP/IP Client Mode. When PADD is enabled, both the PADD server mode and PADD client mode can be run at the same time.

To access the PADD configuration page, click on the **Services** menu at the top of the screen then click on the **PADD** menu item on the left.

Figure 9-20 PADD



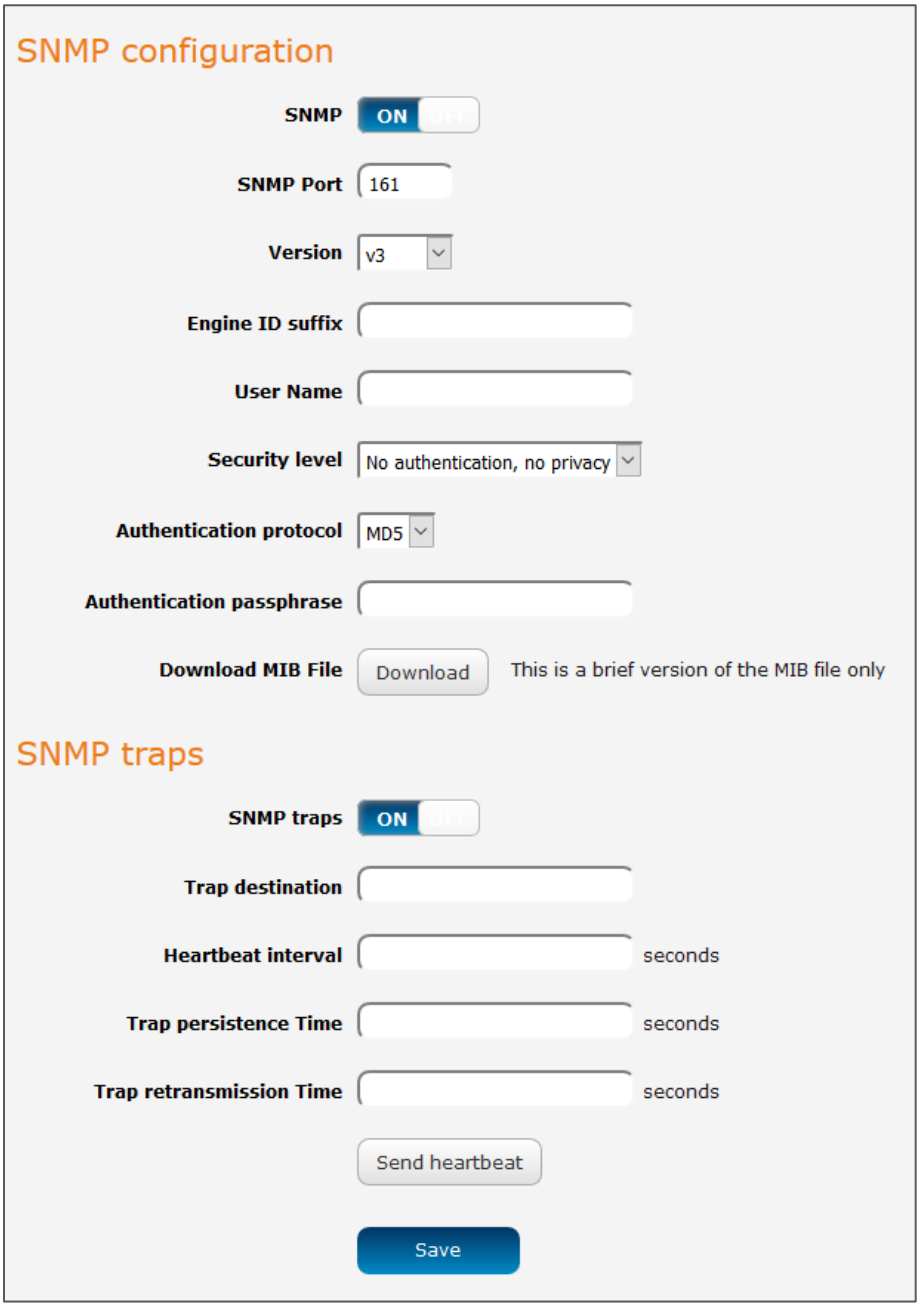
Remote management

SNMP

SNMP configuration

The SNMP page is used to configure the SNMP features of the router. To access the SNMP configuration page, click on the **Services** menu at the top of the screen then click on the **SNMP** menu item on the left.

Figure 9-21 SNMP configuration



SNMP (Simple Network Management Protocol) is used to remotely monitor the router for conditions that may warrant administrative attention. It can be used to retrieve information from the router such as the signal strength, the system time and the interface status.

Configuring SNMP

To configure SNMP:

1. Click the **SNMP** toggle key to switch it to the **ON** position.
2. In the **SNMP port** field, enter a port number to use for SNMP.
3. Use the **Version** drop-down list to select an SNMP version to use. When SNMP is turned on, the router selects v3 as default because v1 and v2 are known to be insecure, therefore you should use v1 and v2 of SNMP with caution.

v3 Configuration

Complete the details as described in the screenshot and table below then click the **Save** button.

Figure 9-22 SNMP v3 Configuration

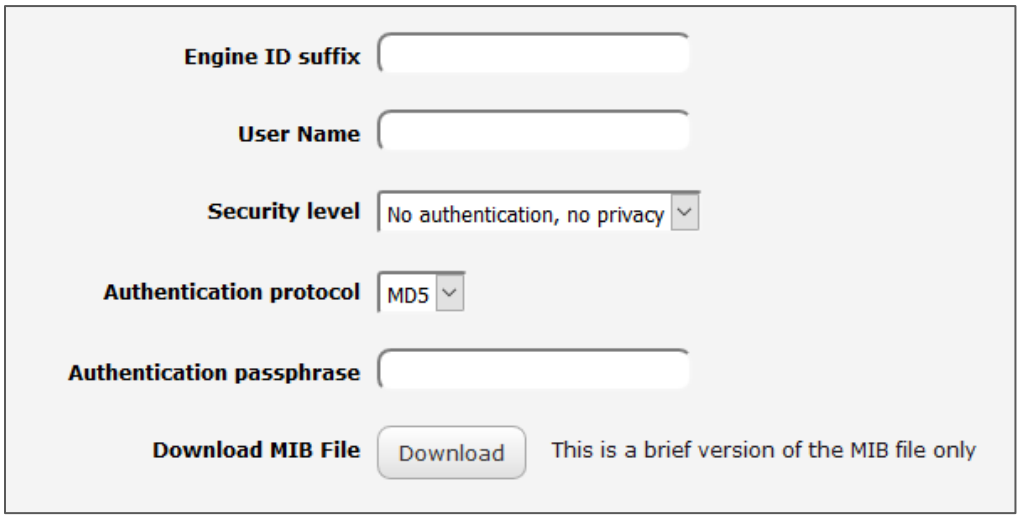


Table 9-6 SNMP v3 Configuration

Item	Description
Engine ID suffix	Enter the Engine ID suffix generated by the SNMP server.
User Name	Enter the SNMP username.
Security level	Use the drop-down list to select the desired security level.
Authentication protocol	Select the authentication protocol (MD5/SHA). This is only required if Security level is set to enforce authentication.
Authentication passphrase	Select the authentication passphrase. This is only required if Security level is set to enforce authentication.
Privacy protocol	Select the privacy protocol (DES/AES). This is only required if Security level is set to enforce privacy.
Privacy passphrase	Select the privacy passphrase. This is only required if Security level is set to enforce privacy.

v1/v2 Configuration

Enter Read-only community name and Read-write community name which are used for client authentication.

Important: *Community names are used as a type of security to prevent access to reading and/or writing to the router's configuration. It is recommended that you change the Community names to something other than the default settings when using this feature.*

Click the Save button to save any changes to the settings.

The Download button displays the Management Information Base (MIB) of the router. The MIB displays all the objects of the router that can have their values set or report their status. The MIB is formatted in the SNMP-related standard RFC1155.

SNMP traps

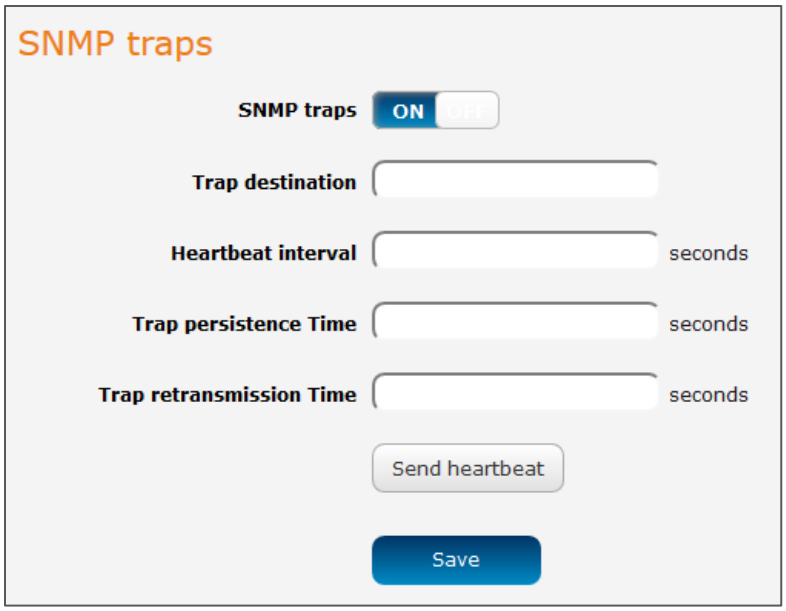
SNMP traps are messages from the router to the Network Management System sent as UDP packets. They are often used to notify the management system of any significant events such as whether the link is up or down.

Configuring SNMP traps

To configure SNMP traps:

1. In the **Trap destination** field, enter the IP address to which SNMP data is to be sent.
2. In the **Heartbeat interval** field, enter the number of seconds between SNMP heartbeats.
3. Use the **Trap persistence** time to specify the time in seconds that an SNMP trap persists.
4. Use the **Trap retransmission** time to specify the length of time in seconds between SNMP trap retransmissions.

Figure 9-23 SNMP traps



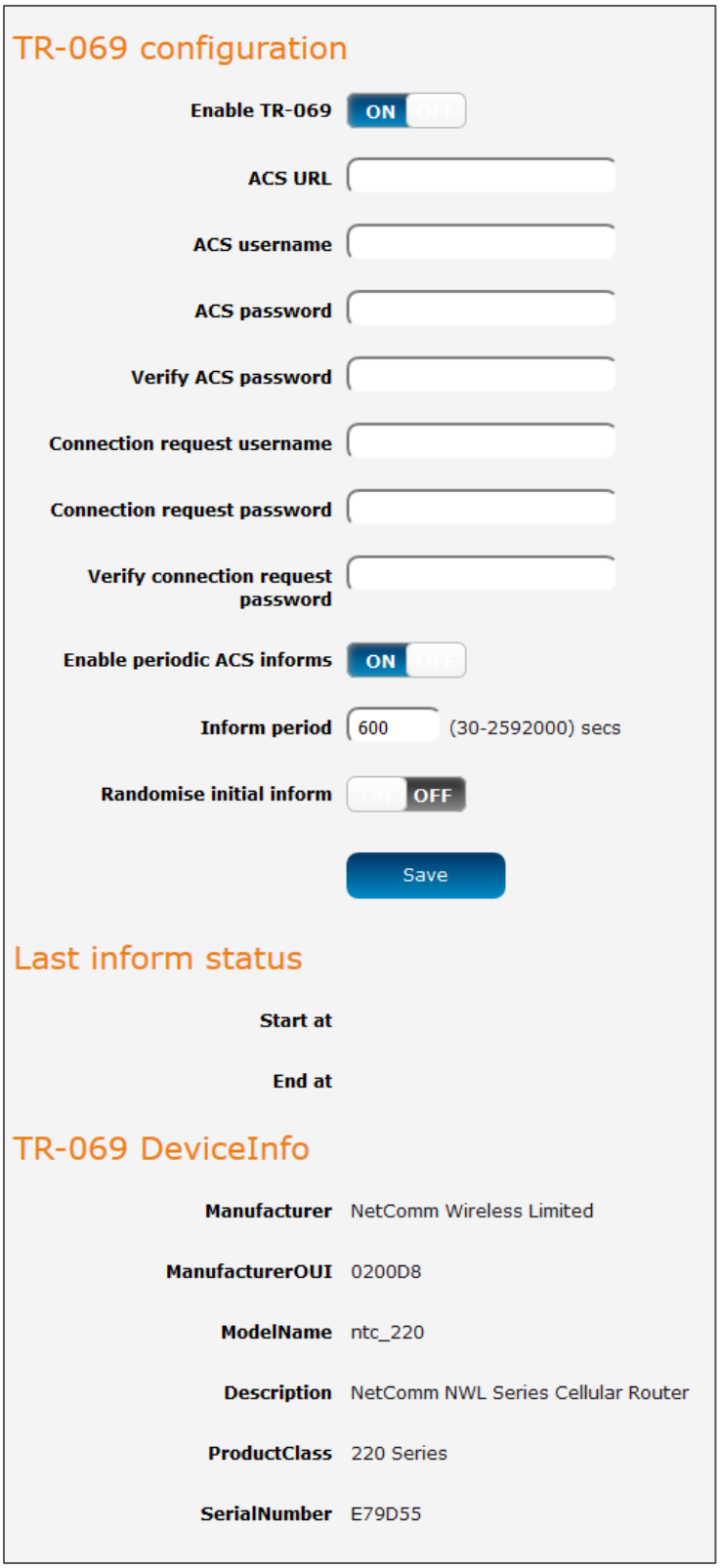
To send a manual SNMP Heartbeat, click the **Send heartbeat** button. When you have finished configuring the SNMP traps, click the **Save** button to save the settings.

Important: *When a factory reset is performed via SNMP, the SNMP settings are not preserved. Ensure that you have physical access to the router if you plan to perform a factory reset.*

TR-069

To access the TR-069 configuration page, click the **Services** menu item, then select the **TR-069** menu item on the left.

Figure 9-24 TR-069 configuration



The TR-069 (Technical Report 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 Lantronix 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.

TR-069 configuration

To configure TR-069:

1. Click the **Enable TR-069** toggle key to switch it to the **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server’s full domain name or IP address.
3. Use 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. 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** in order to turn on the periodic ACS inform messages.
8. In the **Inform Period** field, enter the number of seconds between the inform messages.
9. Click the **Save** button to save the settings.

OMA-Lightweight M2M

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, select the **Enable LwM2M** toggle key so that it is in the **ON** position.

Figure 9-25 LwM2M client configuration

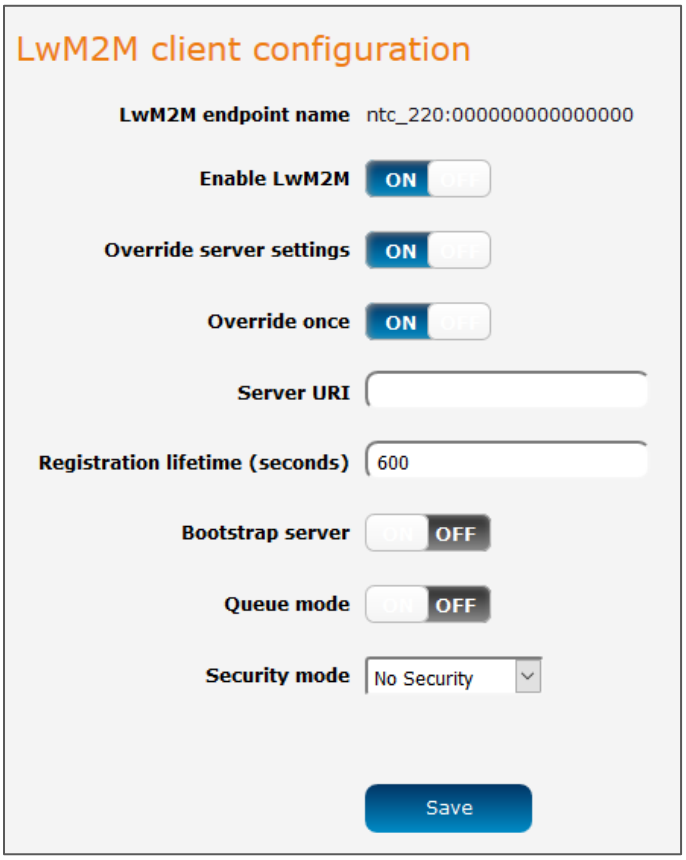


Table 9-7 LwM2M client configuration

Item	Description
LwM2M Endpoint Name	This is the unique ID the device will use to identify itself with LwM2M servers.
Enable LwM2M	Toggle key which enables or disables the LwM2M function.
Override Server Settings	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	When 'Override Settings' is enabled, this option allows you to specify whether the new server details they provide will be applied once when the client is restarted (normal flow for configuring/reconfiguring the client) or, when disabled,

	applied every time the client restarts (used for debugging/troubleshooting.)
Server URI	When 'Override Settings' is enabled, this allows you to specify the URI of the LwM2M server to connect to. 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	When 'Override Settings' is enabled, this allows you to specify the interval (in seconds) at which the LwM2M client will send registration updates (i.e. heartbeat messages) to the server.
Bootstrap Server	When 'Override Settings' is enabled, this allows you to specify whether the new server is a LwM2M bootstrap server.
Queue Mode	When 'Override Settings' is enabled, this allows you to specify whether to report the UDP binding mode to the server as queued ("UQ" binding mode) or not ("U" binding mode.)
Security Mode	When 'Override Settings' is enabled, this allows you to choose the security mode that will be used to connect to the LwM2M server. Currently supported options are 'No Security' and 'Pre-Shared Key'.
Client Identity	When PSK security mode is selected this field is where you must specify the identity string associated with your pre-shared key.
Client Pre-Shared Key	When PSK security mode is selected this field is where you must provide the pre-shared key. The key must be entered as a hexadecimal string.

The table below lists the supported object IDs on the NTC-220. For further information on the objects, refer to the Open Mobile Alliance LWM2M registry.

Table 9-8 Supported LWM2M 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.

GPS

On models with a built-in GPS, you are able to use location-based services, monitor field deployed hardware or find your current location. 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.

***Note:** The **NTC-223** model does not support GPS and this section does not apply to it.*

NMEA support

The router supports the National Marine Electronics Association NMEA-0183 compatible (V2.3) standard of sending GPS data. The standard includes “sentences” used to identify the type of data being sent and therefore defines the way the data is interpreted. The supported GPS related sentences are listed below:

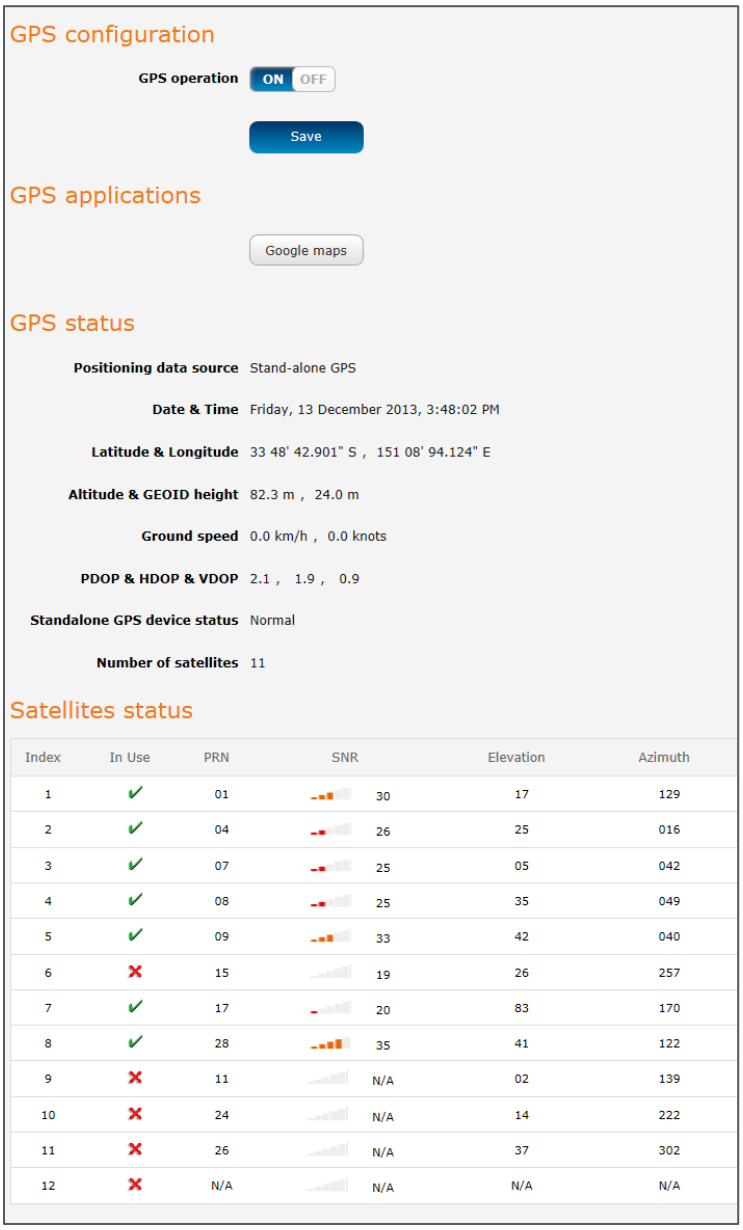
- **GPGGA** – Global Positioning System Fix Data, Time, Position and fix related data for a GNSS receiver
- **GPRMC** – Recommended minimum data for GPS
- **GPGSV** – Detailed satellite data
- **GPGSA** – Overall satellite data
- **GPVTG** – Vector track and speed over the Ground

GPS configuration

To access the GPS configuration screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **GPS configuration** menu item.

To use the GPS function, set the **GPS operation** toggle key to **ON** and click the **Save** button.

Figure 9-26 GPS configuration



The Google maps button provides a quick short cut to show your router's current position on a map.

Mobile Station Based Assisted GPS configuration

To access the Mobile Station Based Assisted GPS configuration screen, select the Services item from the top menu bar then the GPS item on the left. Finally, select the MSB (A-GPS) menu item.

Mobile Station Based Assisted GPS (MSB A-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.

To set up automatic updates of GNSS data, set the **A-GPS Enable** toggle key to the **ON** position and use the drop-down lists to configure the automatic retry options. Each retry, the router checks for an updated GNSS data file and downloads the GNSS data if newer than the currently stored data.

Important: *When new GNSS data is available and the router performs an update, up to 40MB of data may be downloaded. Please keep this in mind if your mobile broadband plan has usage restrictions.*

Figure 9-27 Mobile Stations Based Assisted GPS configuration options

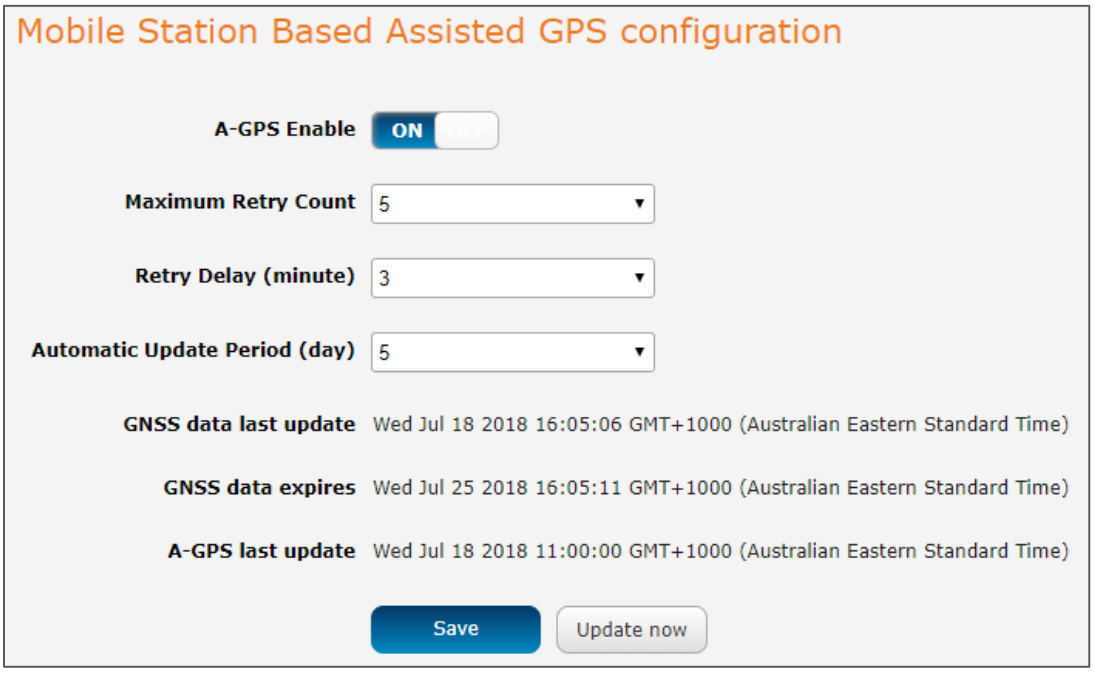


Table 9-9 Mobile Station Based Assisted GPS configuration options

Item	Description
A-GPS Enable	Enables or disables the mobile station based assisted GPS function.
Maximum Retry Count	Sets the maximum number of times the router should attempt to triangulate its position.
Retry delay (minute)	Sets the number of minutes the router should wait between attempts to triangulate its position.
Automatic Update Period (day)	Sets the number of days that the router should automatically update the A-GPS data. The maximum update period is 7 days.

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

You may manually force the router to check for an update regardless of the next scheduled update time by clicking the **Update Now** button.

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

Odometer

To access the Odometer screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **Odometer** menu item.

The GPS may be used to record the distance that the router has travelled. To do this, set the **Odometer** toggle key to the **ON** position as in the screenshot below. You can toggle the unit of measurement by clicking the Display imperial / Display metric button. The threshold setting adjusts the router's sensitivity to movement so that movement within the specified radius from the starting point does not register as distance travelled. When you have finished configuring the Odometer settings, click the **Save** button to ensure the settings are stored on the router.

Figure 9-28 Odometer options

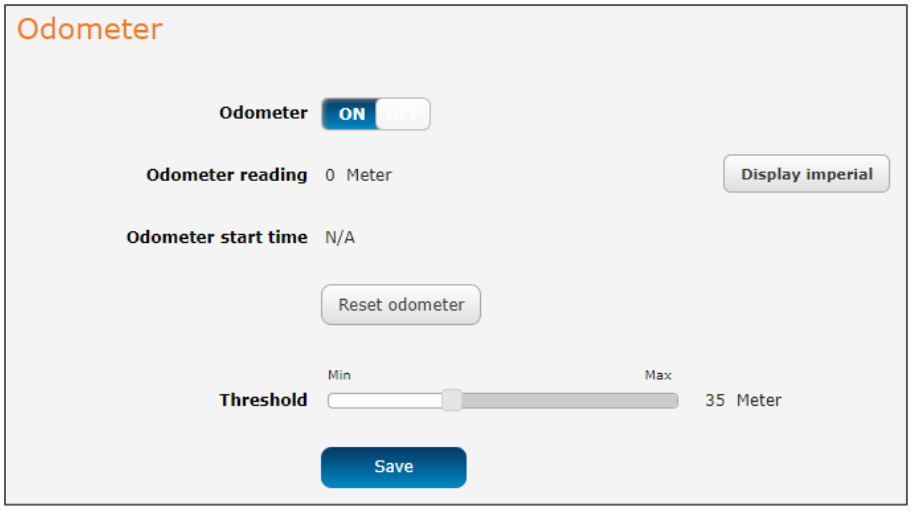


Table 9-10 Odometer configuration options

Item	Description
Odometer reading	The number of metres/kilometres that the device has travelled since the time listed in the Odometer start time field.
Display imperial / Display metric	Toggles the Odometer reading between metric and imperial measurements.
Odometer start time	The time that recording of distance travelled began.
Reset odometer	Resets the odometer reading to 0 and the Odometer start time to the current time.
Odometer	Toggles the Odometer function on and off.
Threshold	Specifies the minimum distance that the router must travel from its current position before the Odometer reading increases.

Geofence

To access the Geofence screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **Geofence** menu item.

Geofence allows you to designate a circular area and then uses the router's GPS position to monitor when the NTC-220 Series router moves out of or into that area. You can configure notifications to be sent when the unit enters or exits the region. Notification types are set on the Event notification configuration page, see below.

Figure 9-29 Geofence options

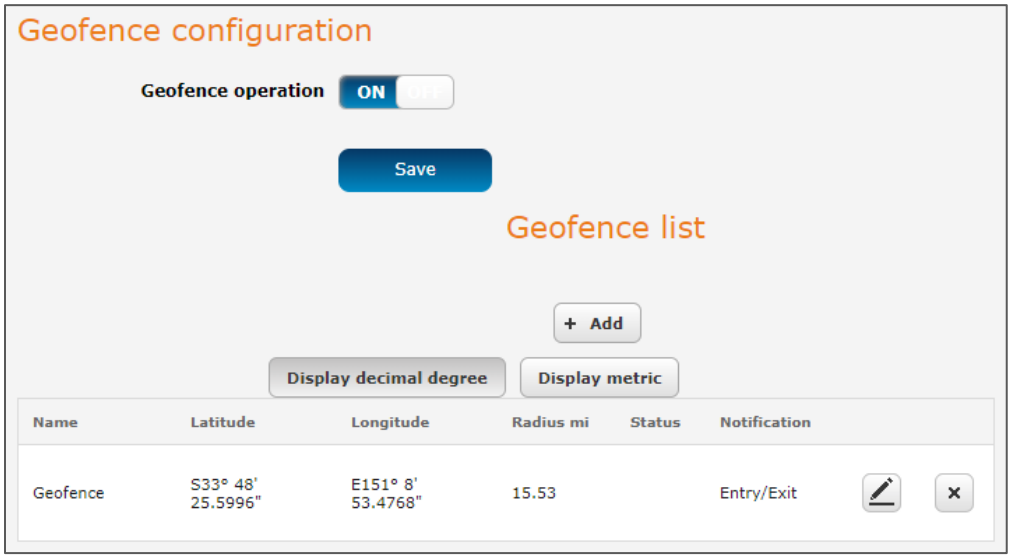


Table 9-11 Geofence user interface

Item	Description
Geofence operation button	Toggles Geofence operation On or Off. When on your currently defined Geofences appear in the Geofence list, see below.
Save button	Saves any changes made on this page
Add button	Click to add a new Geofence definition. The add Geofence configuration screen will open, see next section below.
Geofence list	This table contains all your currently defined Geofences.
Display DMS / Display Decimal degree button	Toggle the Latitude and Longitude coordinates display between Decimal degree coordinates, see above graphics, or the more traditional DMS (degrees, minutes, seconds) coordinates, see below:

	
Display imperial/ Display metric button	Toggle between metric (kilometres) or imperial (miles) display of the radius of the Geofence.
Status	In if the router is inside the radius. Out if the router is outside the radius.
Notification	The event notification currently selected for this Geofence, see Add Geofence in next section for a description of the available notification types.
Edit button	Click this to edit an existing Geofence in the list. The user interface is the same as the add Geofence configuration screen, see next section below.

Add Geofence

Click the **+Add** button to create a new Geofence (note that editing an existing Geofence uses the same configuration page).

Figure 9-30 Configure Geofences

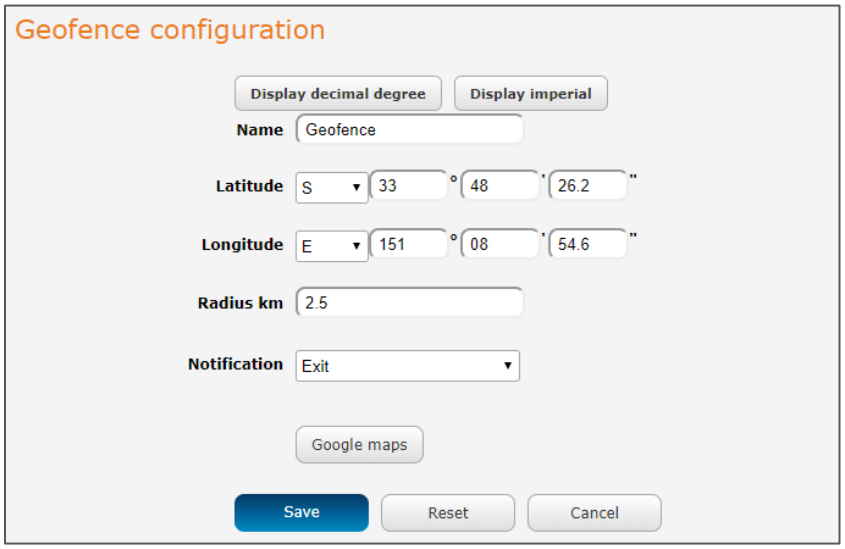


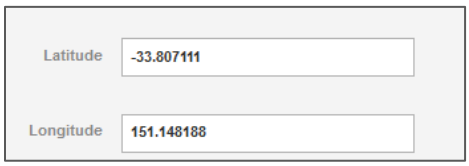
Table 9-12 Add Geofence options

Item	Description
Name	When you Add a new Geofence you will be prompted to enter a meaningful name. This will be its reference in the Geofence list page.

<table>
<tr><td>Display DMS / Display decimal degree button</td><td>Toggle this button to enter the Latitude and Longitude coordinates using either the more traditional DMS (degrees, minutes, seconds) coordinates or using decimal degrees.

When Display DMS is selected you have to select North (N) or South (S) for your Latitude, depending on whether your location is north or south of the equator and you must select east (E) or west (W) of the prime meridian (Greenwich England to the international date line) and then enter the coordinates as:

<table><tr><th>Degrees</th><th>Minutes</th><th>Seconds</th></tr><tr><td>0° - 360°</td><td>0’ – 60’</td><td>0.0000” – 59.9999”</td></tr><tr><td>Whole degrees only</td><td>Whole minutes only</td><td>Seconds and fractions of a second to thousandths (4)</td></tr></table>
When Display decimal degree is selected you have to enter the Latitude and Longitude coordinates using Decimal degree coordinates:

Note that in the southern hemisphere you must enter a negative Latitude coordinate (–) and in the western hemisphere (North and South America, from the prime meridian to the international date line) you must enter a negative Longitude coordinate (–).</td></tr>
<tr><td>Display imperial / Display metric button</td><td>Toggle between imperial and metric to display the Radius in miles (mi) or kilometres (km), respectively.</td></tr>
<tr><td>Radius mi / km text box</td><td>Set the radius of the Geofence to be activated when the Notification type (see next) is triggered at the distance specified.</td></tr>
<tr><td>Notification</td><td>Four notification states are available:

• 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.</td></tr>
</table>

	• **Entry** – A notification is triggered when the router enters into 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 over the Geofence radius line. The type or types of notification (SMS, email, etc.) is set in the Event notification configuration page, see below.
Google maps button	The **Google maps** button serves two 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.
Save button	Saves the new Geofence (Add) or saves the changes to an existing Geofence (Edit).
Reset button	Clears all entries on the page.
Cancel button	Closes the **Add/Edit** page and returns to the Geofence list without saving any changes.

IO configuration

The NTC-220 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.

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 3.3 V or 8.2 V.

Figure 9-31 IO configuration options

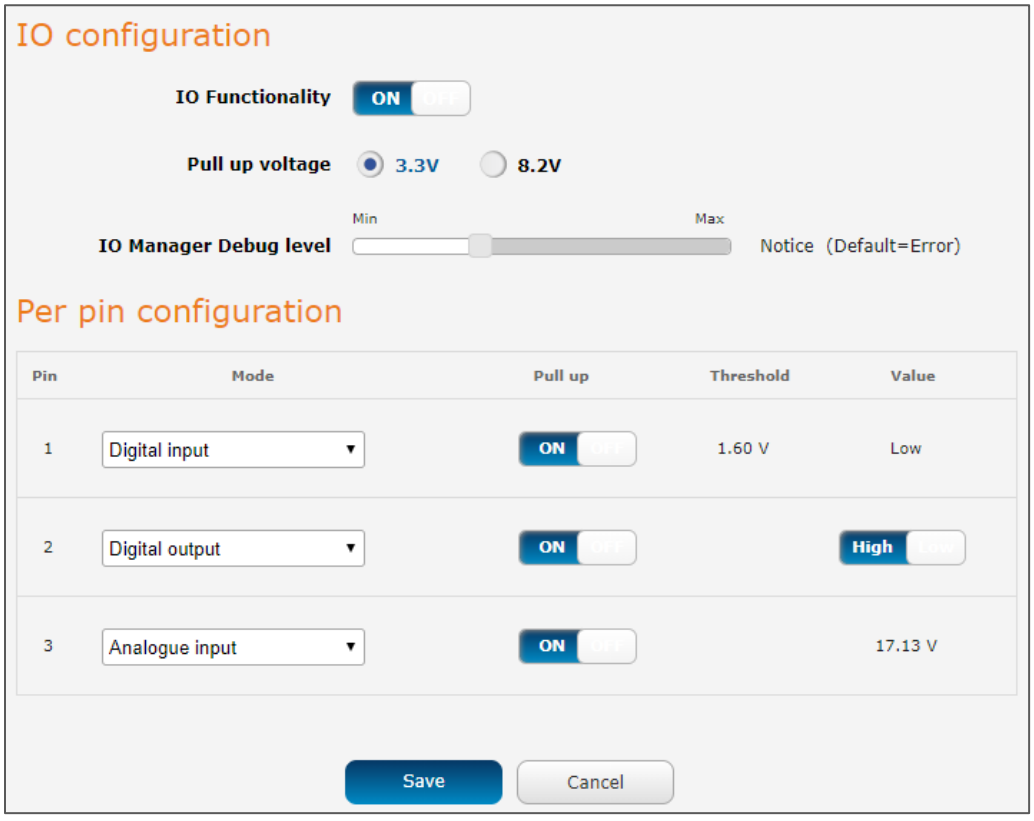


Table 9-13 IO configuration options

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.
Per pin configuration	
Pin	The I/O pin number corresponding to the pin on the four-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 3.3V and 8.2V 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 3.3V and 8.2V 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 0V. When set to High, the output of the I/O pin is 5V. • **Analogue input** – The corresponding pin accepts an analogue signal. Pull up may be on or off and both 3.3V and 8.2V 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 8.2V. 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. 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 3.3V or 8.2V.
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.
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.

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.*

Event notification

The event notification feature is an advanced remote monitoring tool providing you with the ability to send alerts via SMS, e-mail, TCP or UDP when pre-defined system events occur.

Notification configuration

The Notification configuration screen is used to select the event types, methods of notification and the destinations for the notifications. Up to four types of alerts for a particular event may be sent to a single destination profile containing the contact details.

To access the Event notification configuration page, click the Services menu item, select the Event configuration menu item on the left, then select the Notification configuration menu item.

Figure 9-32 Event notification options

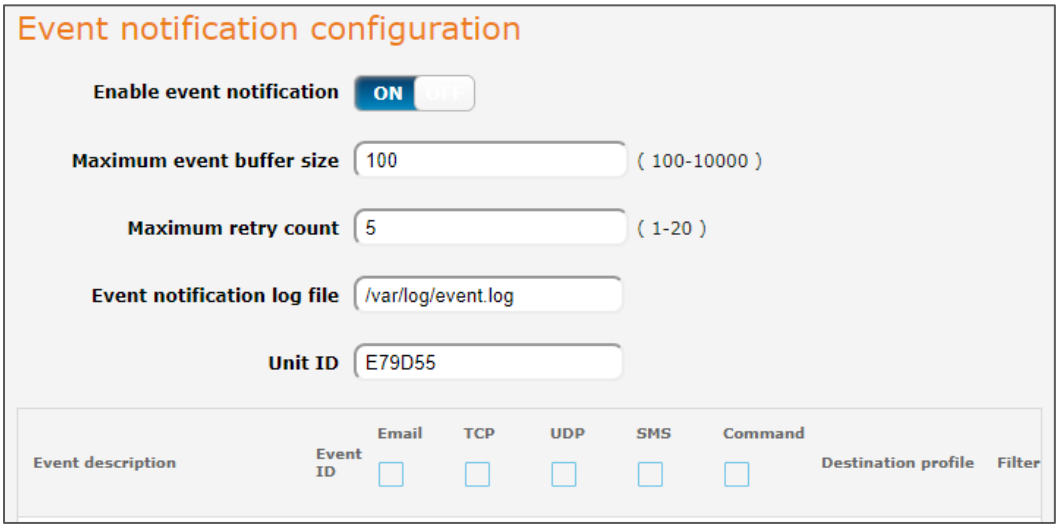
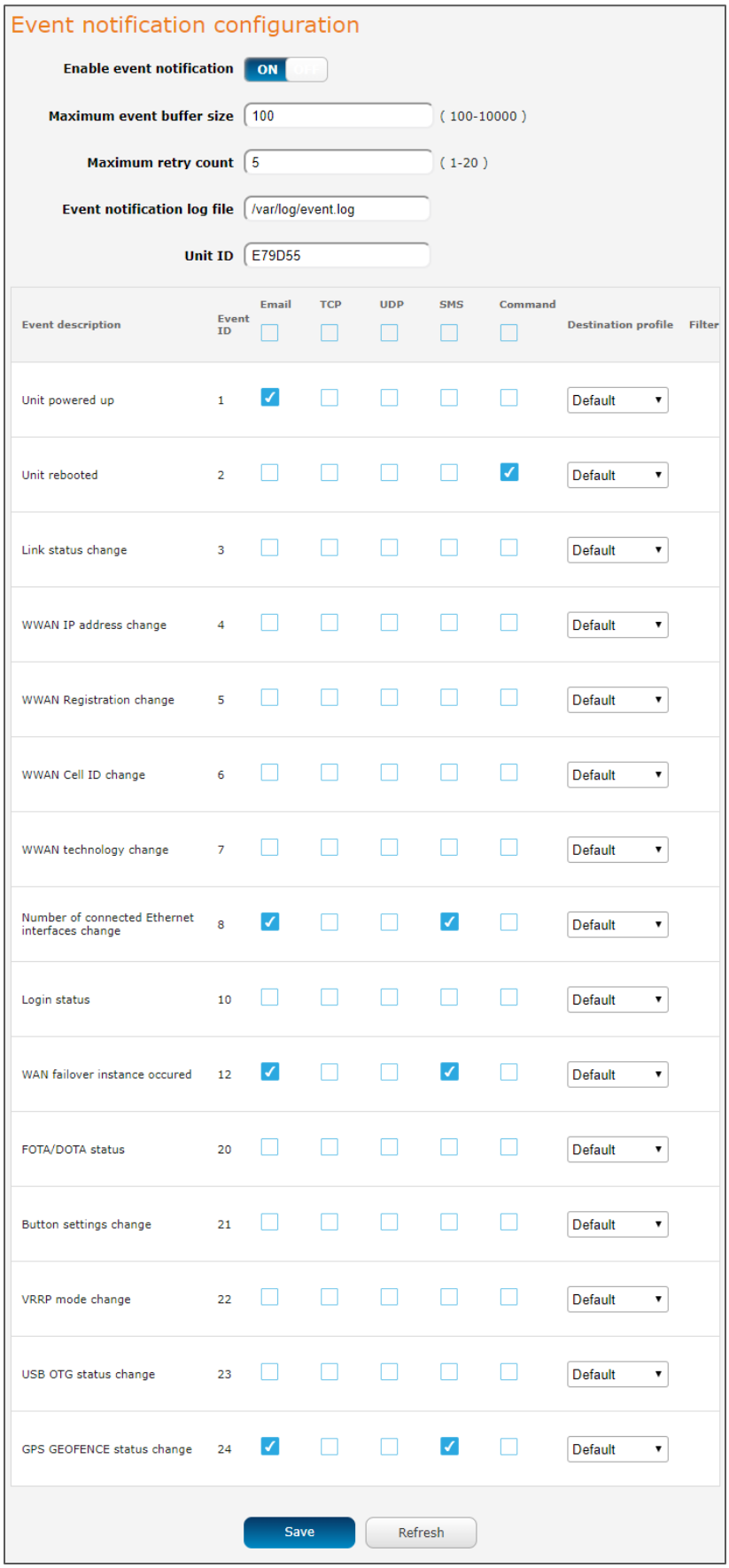


Table 9-14 Event notification configuration options

Item	Description
Enable event notification	Toggles the event notification feature on and off.
Maximum event buffer size	Specifies the buffer size for event notifications which failed to be delivered or are yet to be sent. The minimum size is 100 and the maximum is 10000.
Maximum retry count	Specifies the maximum number of attempts that the router will make to deliver an event notification. The range is between 1 and 20.
Event notification log file	Specifies to the location and name of the file used to log the event notification activity.
Unit ID	The Unit ID field is used to specify an identifier for the router which are sent in the event notifications so that you know which router has an event.

Figure 9-33 Event notification configuration



Event types

There are twenty-one events for which you can configure alerts. Hovering the mouse over the event description provides more details of event notification type.

Table 9-15 Event notification – event types

Event	Event ID	Description	Example message
Unit powered up	1	Notification is sent when the unit is powered up through connection of a power source or after a soft-reset.	Power is up
Unit rebooted	2	Notification is sent when the unit is rebooted via Web UI, SMS diagnostics or via command line/telnet session.	Rebooting triggered by internal application
Link status change	3	Notification is sent if the status of the data connection profile or any IPSec/OpenVPN/PPTP/GRE tunnel endpoint changes i.e. the link goes up or down.	Profile 1 WWAN status changed : down -> up
WWAN IP address change	4	Notification is sent if an active data connection profile's WWAN IP address changes.	WWAN IP address changed : N/A --> 10.103.4.149
WWAN Registration change	5	Notification is sent if the network registration status changed between "registered", "unregistered" or "roaming".	WWAN registration status changed : Not registered --> Registered to home network
WWAN Cell ID change	6	Notification is sent if the router connects to a different cell, marked by a changed in the Cell ID.	Cell ID changed : --> 15224145 Cell ID changed : 15224148 --> 15224145
WWAN technology change	7	Notification is sent if the router connects to a different network technology, e.g. 3G/2G.	WWAN network changed : N/A() --> 3G(UMTS) WWAN network changed : 3G(UMTS) --> 2G(GSM)
Number of connected Ethernet interfaces change	8	Notification is sent if there is a change to the number of directly connected Ethernet interfaces.	Ethernet device number changed : 0 -> 1
Login status	10	Notification is sent if there was a failure to log in to the router via the Web UI.	WEBUI login failed, username root, password

FOTA/DOTA status	20	Notification is sent with the result of the Firmware Over-The-Air via SMS or TR-069.	FOTA/DOTA: upgrading firmware successful
Button settings change	21	Notification is sent when the reset button enabled or disabled in the web user interface.	Reset button is enabled
VRRP mode change	22	Notification is sent if a device configured as a slave becomes a master router or returns to slave status.	VRRP is in backup mode
USB OTG status change	23	When a USB device is connected.	USB OTG status changed: disabled → connected
GPS GEOFENCE status change	24	Notification is sent based on the Geofence settings.	GPS GEOFENCE status changed (latitude: -33.807242, longitude: 151.148293, radius 15 km): out → in

Destinations

A "destination" is a profile on the router containing the contact details of a recipient of event notification alerts i.e. the e-mail address, SMS number, TCP or UDP server addresses of the recipient. The destination profile must contain the details of at least one destination type in order to be used.

Configuring Event notification

To configure the event notification feature:

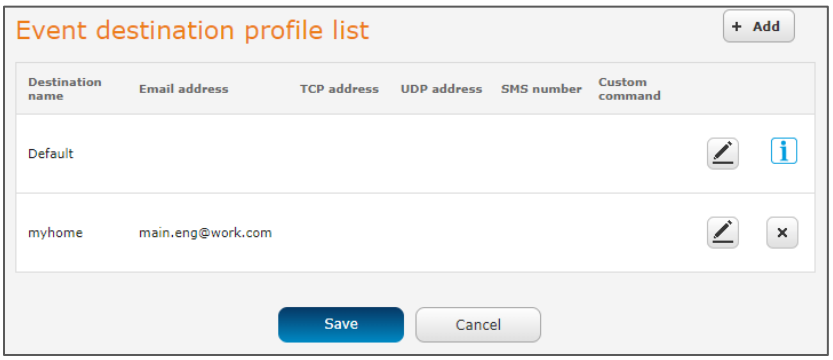
1. Click the Services menu item at the top of the screen. From the Event notification menu on the left of the screen, select the Destination configuration menu item.
2. Click the +Add button at the top right corner of the window. The Event destination edit screen is displayed.
3. In the Destination name field enter a name for the destination profile then enter the contact details for each type of destination i.e. Email address, TCP address and port, UDP address and port and/or SMS number.
4. Click the Save button when you have entered the required details.
5. From the Event notification menu on the left of the screen, select the Notification configuration menu item.
6. Select the Enable event notification toggle key to turn it to the ON position.
7. If desired, set the Maximum event buffer size, Maximum retry count, Event notification log file and Event notification prefix fields. See table 29 for descriptions of these options.
8. From the Destination profile column, use the drop-down menus to select the desired destination profiles to use for the corresponding events, then select the checkboxes for the types of notifications to send to the chosen destination profile. If the Destination profile does not contain the required contact details, a pop-up warns you to enter the required details in the Destination profile.
9. Click the Save button.

Note: *If you have selected the Email notification type for any of the events, you must also configure Email client settings to allow the router to send e-mail messages.*

Destination configuration

The Destination configuration screen displays a list of the destination “profiles” that have been configured on the device as well as providing the option to add new profiles.

Figure 9-34 Event destination list



To add a new destination profile:

1. Click the **+Add** button at the top right corner of the window. The Event destination profile edit screen is displayed.
2. In the **Destination name** field enter a name for the destination profile.
3. Then for each destination enter the contact details relevant to that destination type i.e.: Email address, TCP address and port, UDP address and port and/or SMS number.
4. In addition to entering details for specific destination types, you can also add a custom command to perform certain tasks when an event is triggered. Any command or script that can be executed from a terminal command prompt, including any executable and parameters, can be entered in the Custom Command field.
5. Click the **Save** button when you have entered the required details.

To edit a destination profile:

1. From the Event destination list, click the edit button for the corresponding destination profile. The Event destination edit page is displayed. Make the required changes.
2. Click the **Save** button.

To delete a destination profile:

1. From the Event destination list, select the delete button for the corresponding destination profile that you would like to delete. If the destination profile is linked to an event notification type, the i button is displayed instead of the delete button. In this case, you must go to the Notification configuration screen and remove the check marks from all the notification types for each event for which the destination profile is configured. When you have done that, return to the Event destination list and select the delete button.
2. Click the **Save** button.

Email settings

The Email settings screen allows the configuration of the email account that is used to send emails in features such as Event notification.

To access the Email settings page, click the **Services** menu item then select the **Email settings** menu item on the left.

Figure 9-35 Email client settings

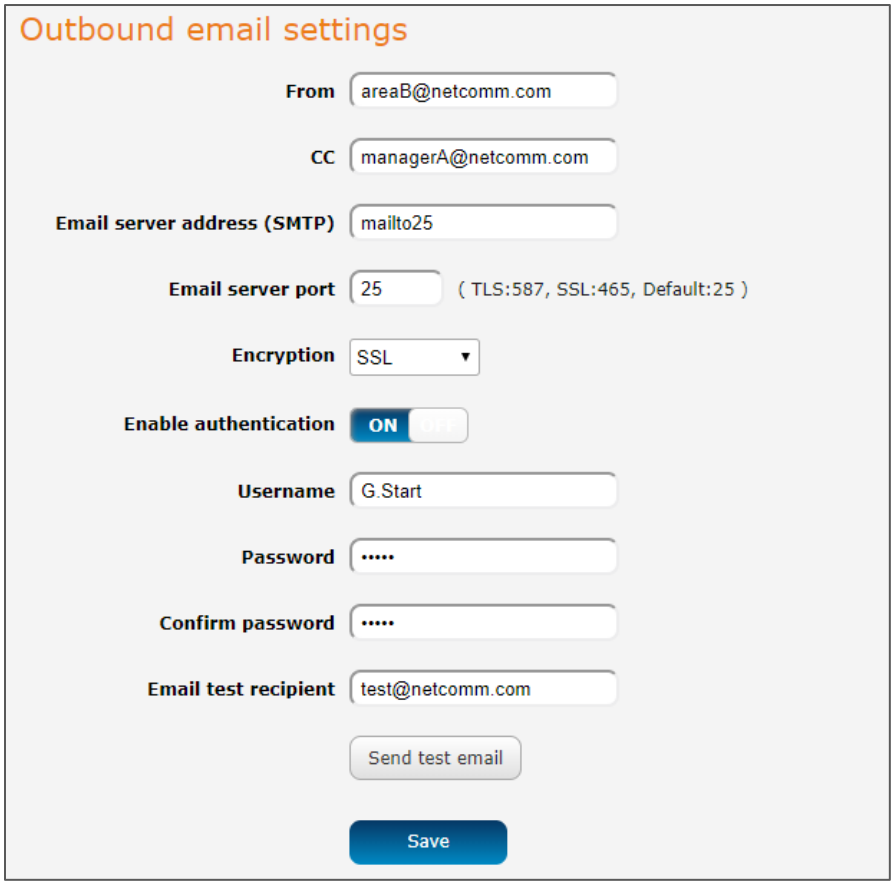


Table 9-16 Email client settings

Item	Description
From	Enter the email address of the account you will be using to send emails.
CC	(Optional) Enter an email address which will be copied on all messages sent.
Email server address (SMTP)	Enter the SMTP server address of the email server. This may be an IP address or a hostname.
Email server port	Enter the Email server's SMTP port.
Encryption	Choose from SSL or STARTTLS encryption methods or select None to use no encryption. The main point of difference between SSL

	and STARTTLS is that SSL opens a secure connection first, and then begins the SMTP transaction. STARTTLS starts the SMTP transaction and then looks for support for TLS in the response message.
Username	Enter the username of the account to be used for sending emails.
Password	Enter the password of the account to be used for sending emails.
Confirm password	Enter the password of the account to be used for sending emails once more for confirmation.
Email test recipient	Enter an email address to send a test message to, then click the Send test email button.

SMS messaging

The NTC-220 Series router offers an advanced SMS feature set, including sending messages, receiving messages, redirecting incoming messages to another destination, as well as supporting remote commands and diagnostics messages.

Some of the functions supported include:

- 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-220 Series router to download and install a firmware upgrade
- Ability to trigger the NTC-220 Series router to download and apply a configuration file

To access the SMS messaging functions of the NTC-220 Series router, click on the Services menu item from the top menu bar, and then select one of the options under the SMS messaging section on the left-hand menu.

Setup

The Setup page provides the options to enable or disable the SMS messaging functionality and SMS forwarding functionalities of the router. SMS messaging is enabled by default.

Figure 9-36 General SMS Configuration

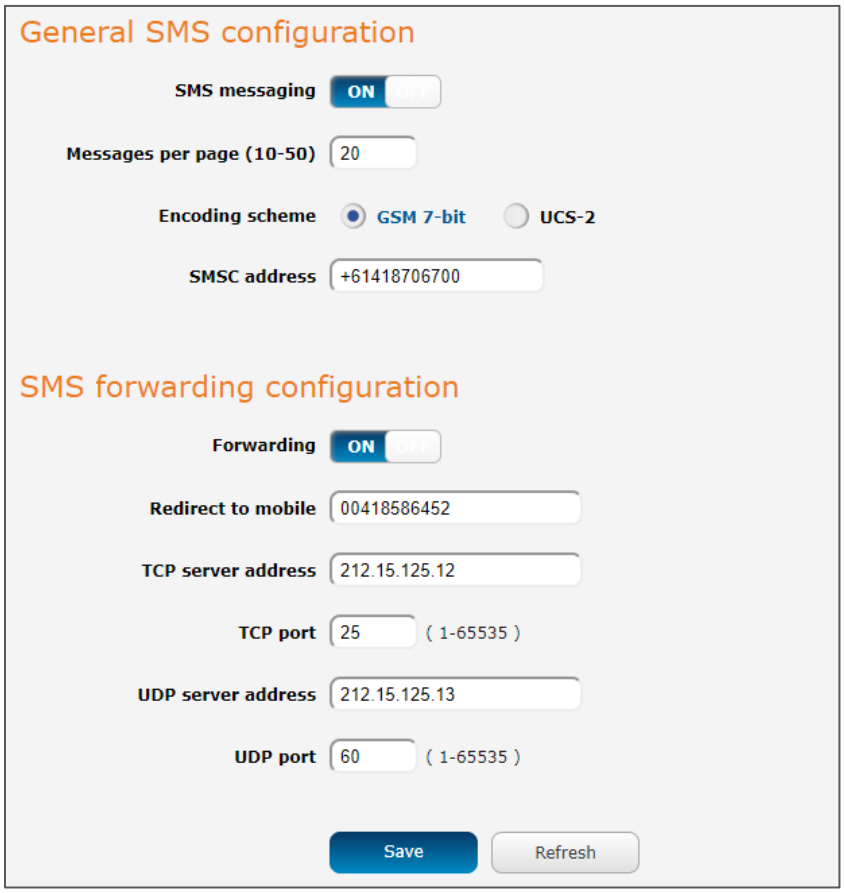


Table 9-17 SMS Setup Settings

Option	Definition
General SMS configuration	
SMS messaging	Toggles the SMS functionality of the router on and off.
Messages per page (10-50)	The number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding scheme	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 the sending of Unicode characters and permits a message to be up to 50 characters in length.
SMS forwarding configuration	

Forwarding	Toggles the SMS forwarding function of the router on and off.
Redirect to mobile	Enter a mobile number as the destination for forwarded SMS messages.
TCP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP.
TCP port	The TCP port on which to connect to the remote destination.
UDP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP.
UDP port	The UDP port on which to connect to the remote destination.

SMS forwarding configuration

Incoming text messages can be redirected to another mobile device and/or a TCP/UDP message server.

Redirect to mobile

You can forward incoming text messages to a different destination number. This destination number can be another mobile phone or a router phone number.

For Example:

If someone sends a text message and Redirect to mobile is set to “+61412345678”, the text message is stored on the router and forwarded to “+61412345678” at the same time.

To disable redirection to a mobile, clear the Redirect to mobile field and click the Save button.

Redirect to TCP / UDP server address

You can also forward incoming text messages to a TCP/UDP based destination. The TCP or UDP server can be any kind of public or private server if the server accepts incoming text-based messages.

The TCP/UDP address can be an IP address or domain name. The port number range is from 1 to 65535. Please refer to your TCP/UDP based SMS server configuration for which port to use.

For Example:

If someone sends a text message and TCP server address is set to “192.168.20.3” and TCP port is set to “2002”, this text message is stored in the router and forwarded to “192.168.20.3” on port “2002” at the same time.

To disable redirection to a TCP or UDP address, clear the TCP server address and UDP server address fields and click the Save button.

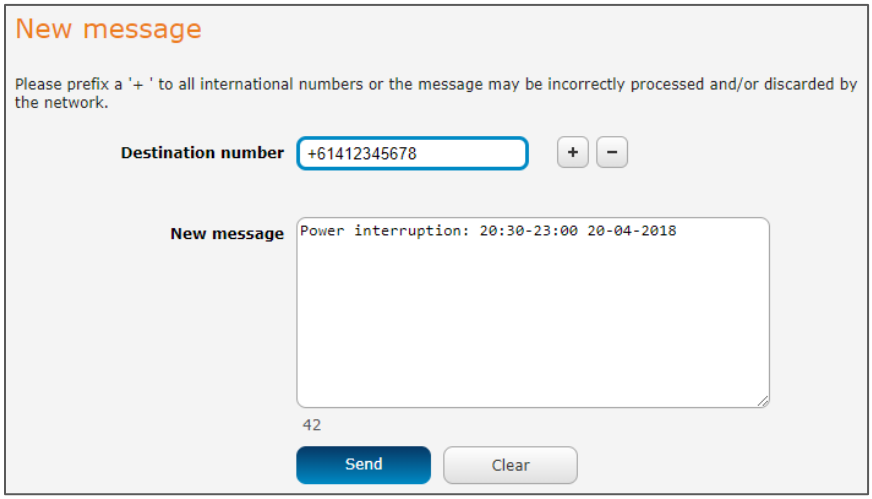
New message

The New message page can be used to send SMS text messages to a single or multiple recipients. To access the New message page, click on the Services menu item from the top menu bar, select the SMS messaging menu on the left then select the New message menu item.

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” if the message failed to send. 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, click the + button and to remove the last destination in the list, click the − button.

Figure 9-37 SMS – New Message



Destination numbers should begin with the "+" symbol followed by the country calling code. To send a message to a destination number, enter the "+" symbol followed by the country calling code and then the destination number.

For example:

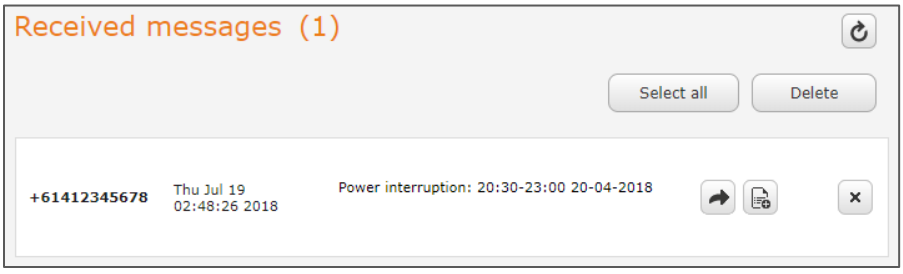
To send a message to the mobile destination number 0412345678 in Australia (country calling code 61), enter "+61412345678".

After entering the required recipient numbers, type your SMS message in the New message 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 the Send button.

Inbox / Sent Items

The Inbox displays all received messages that are stored on the router while Sent Items displays all sent messages. To access the Inbox page, click on the Services menu item from the top menu bar, select the SMS messaging menu on the left then select the Inbox menu item.

Figure 9-38 SMS Inbox



To access the Sent items page, click on the Services menu item from the top menu bar, select the SMS messaging menu on the left then select the Sent items menu item.

Figure 9-39 SMS Outbox

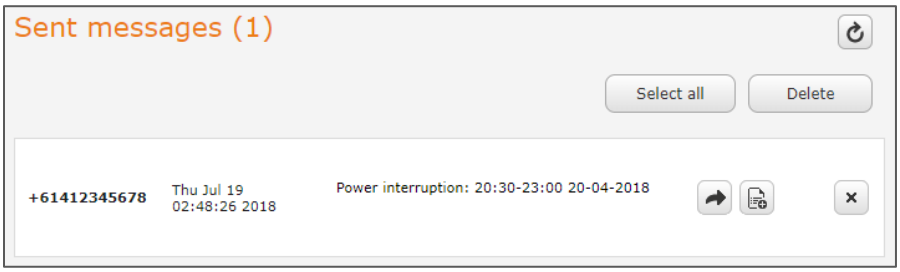


Table 9-18 Inbox/Outbox icons

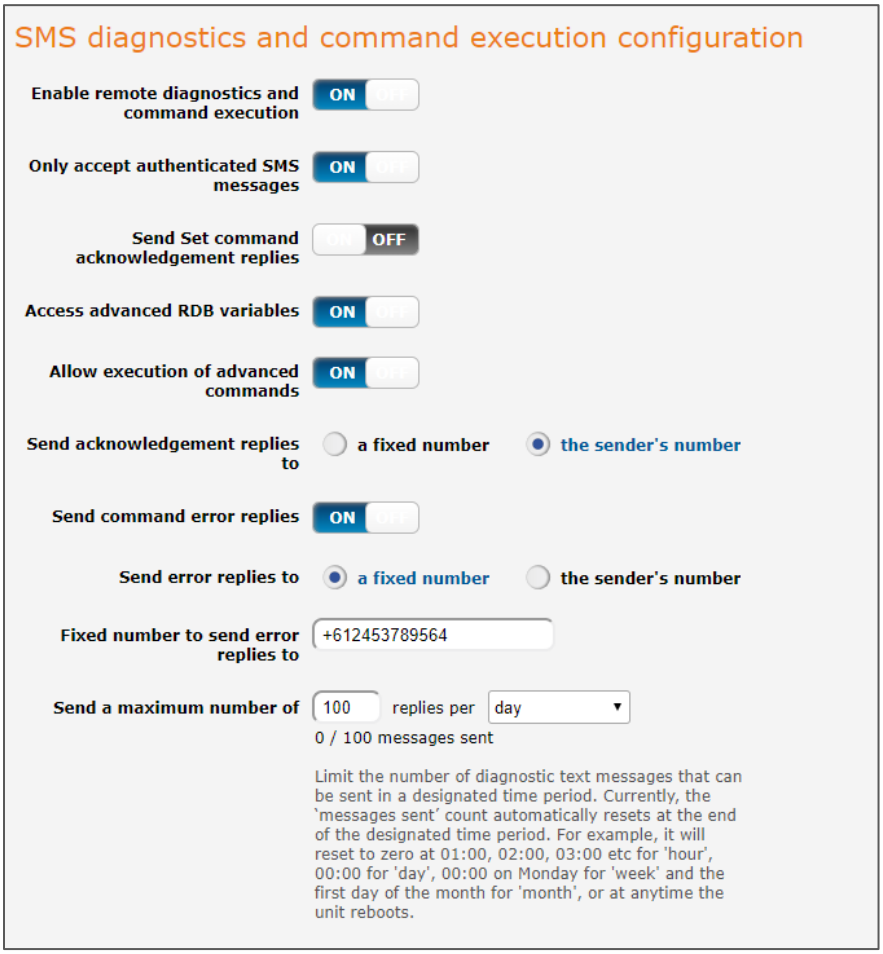
Icon	Name	Description
	Forward	Click this button to open a new message window where you can forward the corresponding message to another recipient.
	Reply	Click this button to open a new message window where you can reply to the sender.
	Add to White list	Click this button to add the sender's mobile number to the white list on the router.
	Delete	Click this button to delete the corresponding message.
	Refresh	Click this button to refresh the inbox or outbox to see new messages.

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.

To access the Diagnostics page, click on the Services menu item then select the SMS menu on the left and finally select Diagnostics beneath it.

Figure 9-40 SMS diagnostics and command execution configuration



SMS diagnostics and command execution configuration

The options on this page are described below.

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 in order to restore normal operation.*

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.*

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.

Send Set command acknowledgement replies

The NTC-220 Series router will automatically reply to certain types of commands received, such as get commands, or execute commands. However, acknowledgement replies from the NTC-220 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 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

By default, this option is turned on and 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

By default, this option is turned on and 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

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.

Fixed number to send replies to

This field defines the destination number to which error messages are sent after the execution of a get, set, or exec command. This field is only displayed when Send Error SMS to is set to Fixed Number.

Send command error replies

Enables or disables the sending of an error message resulting from the execution of a get, set, or exec command. All error replies are stored in the Outbox after they have been sent.

Send error replies to

When Send command error replies is set to ON, this option is used to specify where the error SMS is sent. Use the radio buttons to select either a fixed number or the sender's number. When set to the sender's number the router will reply to the originating number of the SMS diagnostic or command. When set to a fixed number the router will send the error messages to the number specified in the following field.

Send a maximum number of

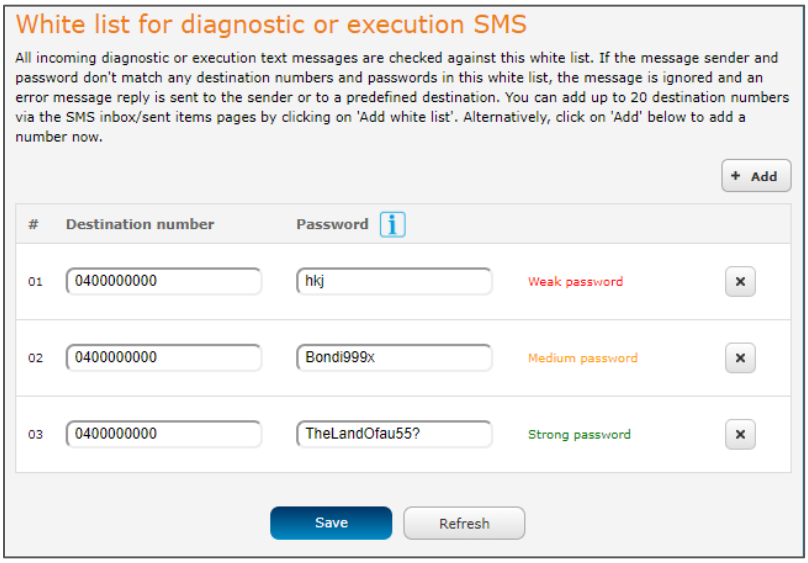
You can set the maximum number of acknowledgement and error messages sent when an SMS diagnostic or command is executed. The maximum limit can be set per hour, day, week or month. The router will send a maximum of 100 replies per day by default.

The number of messages sent is shown below the options. The total transmitted message count resets after a reboot or at the beginning of the time frame specified.

White list for diagnostic or execution SMS

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.

Figure 9-41 White list for diagnostic or execution SMS



Up to 20 numbers may be stored in the white list. To add a number to the white list, click the "+Add" button.

The White list numbers and passwords can be cleared by pressing the × button to the right of each entry. To add a number to the white list, enter it in the Destination number field and define a password in the Password field. The SMS white list password must meet the following criteria for a strong password:

- Be a minimum of eight characters and no more than 128 characters in length.

- Contain at least one upper case, one lower case character and one number.
- Contain at least one of the following special characters: !*()?/

When you have finished adding numbers click the Save button to save the entries.

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** click 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, click 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 click 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. Click 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 acknowledgment 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 9-19 SMS Diagnostic 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 9-20 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: 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
7	codconnect	Causes the router to activate the PDP context when the Connect on demand feature is enabled.
8	coddisconnect	Causes the router to de-activate the PDP context when the Connect on demand feature is enabled.
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 9-21 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.
set cod	`set cod=1`	Enables or disables Connect on demand.

get cod	**get cod**	Returns the enable/disable status of the Connect on demand feature.
get codstatus	**get codstatus**	Returns the connection status of the Connect on demand feature.
set coddialport	**set coddialport=on,53**	Sets the Connect on demand feature to connect only when traffic is received on the specified port.
get coddialport	**get coddialport**	Returns the Connect on demand port filter status and list or filtered ports.
set codonline	**set codonline=20**	Sets the router to stay online for at least X minutes when data activity is detected.
get codonline	**get codonline**	Returns the number of minutes the router is configured to stay online when data activity is detected.
set codminonline	**set codminonline=10**	Sets the router to stay online for a minimum of X minutes after connecting.
get codminonline	**get codminonline**	Returns the minimum number of minutes the router should stay online after connecting.
set codredial	**set codredial=5**	Sets the number of minutes that the router should not attempt to redial after hanging up.
get codredial	**get codredial**	Returns the number of minutes that the router is configured to not attempt to redial after hanging up.
set coddisconnect	**set coddisconnect=0**	Sets the number of minutes after which the router should disconnect regardless of traffic.
get coddisconnect	**get coddisconnect**	Returns the number of minutes the router is configured to disconnect regardless of traffic.
set codconnectreg	**set codconnectreg=30**	Sets the number of minutes that the router should regularly attempt to connect.
get codconnectreg	**get codconnectreg**	Returns the number of minutes that the router is configured to regularly attempt to connect.
set codrandomtime	**set codrandomtime=3**	Sets the number of minutes that the router should randomise the dial time by.
get codrandomtime	**get codrandomtime**	Returns the number of minutes that the router is configured to randomise the dial time by.
set codverbose	**set codverbose=1**	Sets verbose logging on or off.
get codverbose	**get codverbose**	Returns the status of verbose logging.

set codignore.icmp	**set codignore.icmp=1**	Sets the router to ignore ICMP packets triggering data activity detection.
get codignore.icmp	**get codignore.icmp**	Returns the status of the Ignore ICMP option.
set codignore.tcp	**set codignore.tcp=1**	Sets the router to ignore TCP packets triggering data activity detection.
get codignore.tcp	**get codignore.tcp**	Returns the status of the Ignore TCP option.
set codignore.udp	**set codignore.udp=1**	Sets the router to ignore UDP packets triggering data activity detection.
get codignore.udp	**get codignore.udp**	Returns the status of the Ignore UDP option.
set codignore.dns	**set codignore.dns=1**	Sets the router to ignore DNS traffic triggering data activity detection.
get codignore.dns	**get codignore.dns**	Returns the status of the Ignore DNS option.
set codignore.ntp	**set codignore.ntp=1**	Sets the router to ignore NTP traffic triggering data activity detection.
get codignore.ntp	**get codignore.ntp**	Returns the status of the Ignore NTP option.
set codignore.ncsi	**set codignore.ncsi=1**	Sets the router to ignore NCSI traffic triggering data activity detection.
get codignore.ncsi	**get codignore.ncsi**	Returns the status of the Ignore NCSI option.
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/3G/2G) 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 pppoe	**get pppoe**	Returns the PPPoE status, currently configured dial string and service name
set pppoe	**set pppoe=1,1,1,test**	Sets PPPoE on, debug logging on, Forward WAN IP on, and service name to “test”.
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).
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 9-22 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 link.profile.1.iplocal link.profile.1.status	profile	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal, status) 1,apn,username,password, chap,202.44.185.111,up 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	WCDMA850

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, 3G, 2G)
- 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 9-23 Network types returned by get plmnscan SMS command

Network type	Description
9	Indicates an LTE network.
7	Indicates a 3G network
1	Indicates a 2G network

Table 9-24 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.

Command format:

```
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=505,1
```

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/3G/2G) is specified, it is selected automatically.

```
set forceplmn=505,1,7
```

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 “7” is the 3G network type.

Table 9-25 Mobile Network Provider codes (Australia)

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

Table 9-26 Network types

Network type code	Network Type
9	Indicates an LTE network.
7	Indicates a 3G network
1	Indicates a 2G network

Notes:

If the manual selection fails, the device will fall back to the previous ‘good’ network.

When enabled, the SMS acknowledgement reply reflects the success or failure of the manual selection with respect to the set command and includes the final MNC/MCC that was configured.

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:

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 9-27 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`
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 wake up the router, turn on the default gateway and trigger the 'connect on demand' profile if in waiting state.	**A zero byte class 1 flash SMS**
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 turn off PPPoE	**set pppoe=0**
Send SMS to retrieve the PPPoE status, currently configured dial string and service name	**get pppoe**
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**
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**

10. System

Log

The Log pages are used to display or download the System log, Event notification logs and IPSec logs on the router.

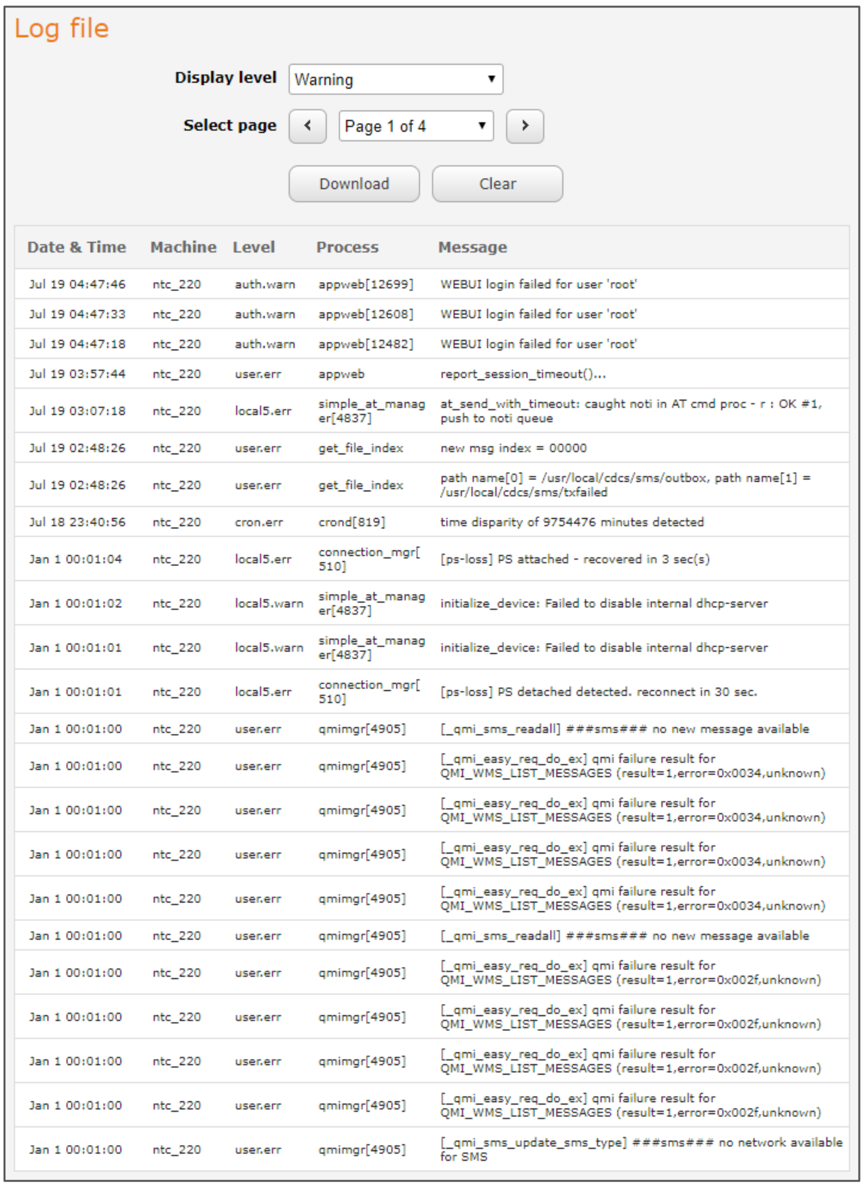
System log

The System Log enables you to troubleshoot any issues you may be experiencing with your NTC-220 Series router. To access the System Log page, click on the System menu. The System Log is displayed.

Log file

Use the Display level drop-down list to select a message level to be displayed.

Figure 10-1 System log file



Date & Time	Machine	Level	Process	Message
Jul 19 04:47:46	ntc_220	auth.warn	appweb[12699]	WEBUI login failed for user 'root'
Jul 19 04:47:33	ntc_220	auth.warn	appweb[12608]	WEBUI login failed for user 'root'
Jul 19 04:47:18	ntc_220	auth.warn	appweb[12482]	WEBUI login failed for user 'root'
Jul 19 03:57:44	ntc_220	user.err	appweb	report_session_timeout()...
Jul 19 03:07:18	ntc_220	local5.err	simple_at_manager[4837]	at_send_with_timeout: caught noti in AT cmd proc - r : OK #1, push to noti queue
Jul 19 02:48:26	ntc_220	user.err	get_file_index	new msg index = 00000
Jul 19 02:48:26	ntc_220	user.err	get_file_index	path name[0] = /usr/local/cdcs/sms/outbox, path name[1] = /usr/local/cdcs/sms/txfailed
Jul 18 23:40:56	ntc_220	cron.err	crond[819]	time disparity of 9754476 minutes detected
Jan 1 00:01:04	ntc_220	local5.err	connection_mgr[510]	[ps-loss] PS attached - recovered in 3 sec(s)
Jan 1 00:01:02	ntc_220	local5.warn	simple_at_manager[4837]	initialize_device: Failed to disable internal dhcp-server
Jan 1 00:01:01	ntc_220	local5.warn	simple_at_manager[4837]	initialize_device: Failed to disable internal dhcp-server
Jan 1 00:01:01	ntc_220	local5.err	connection_mgr[510]	[ps-loss] PS detached detected. reconnect in 30 sec.
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_sms_readall] ###sms### no new message available
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x0034,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x0034,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x0034,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x0034,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_sms_readall] ###sms### no new message available
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x002f,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x002f,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x002f,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_easy_req_do_ex] qmi failure result for QMI_WMS_LIST_MESSAGES (result=1,error=0x002f,unknown)
Jan 1 00:01:00	ntc_220	user.err	qmimgr[4905]	[_qmi_sms_update_sms_type] ###sms### no network available for SMS

Select a Display level from the drop-down menu to filter the message display.

Table 10-1 System log detail levels

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

To download the System log for offline viewing, right-click **Download** button and choose **Save as..** to save the file. The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore, to be displayed correctly with new lines shown, it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

To clear the System log, click the **Clear** button.

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 10-2 Diagnostic log

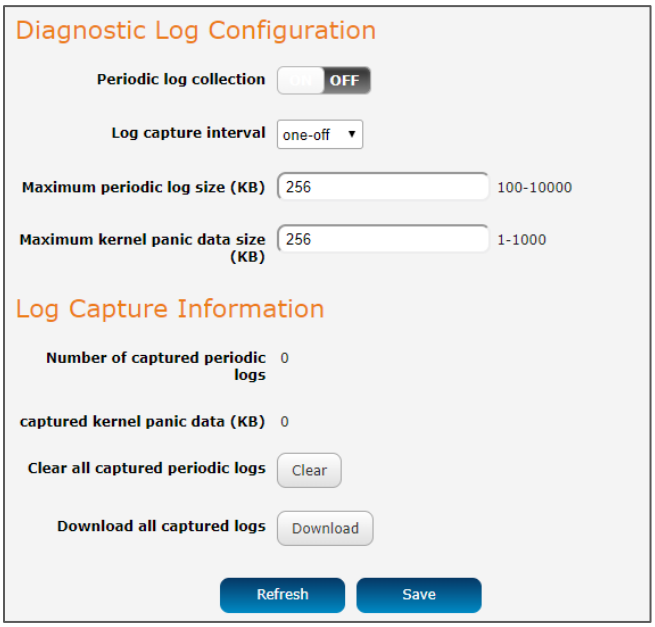


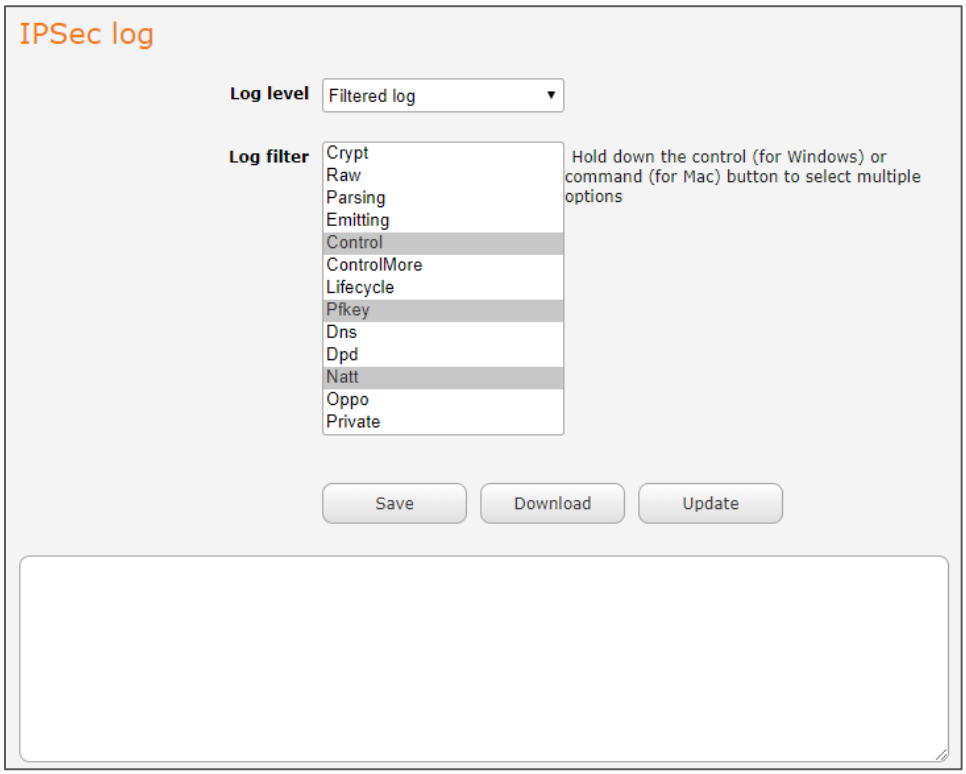
Table 10-2 Diagnostic log

Item	Description
Diagnostic log configuration	
Periodic log collection	Turn on this toggle key to enable diagnostic log collection.
Log capture interval	Specifies the interval at which the router should collect diagnostic log data.
Maximum periodic log size (KB)	Specifies the maximum size of the log file in kilobytes.
Maximum kernel panic data size (KB)	Specifies the maximum size of the kernel panic data file in kilobytes.
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.
Clear all captured periodic logs	Press the “Clear” button to clear all captured periodic logs.
Download all captured logs	Press the “Download” button to download all captured logs.

IPSec log

The IPSec log section provides the ability for you to download the log for the IPSec VPN function. This can assist in troubleshooting any problems you may have with the IPSec VPN. To access the IPSec log page, click on the **System** menu item then select the **Log** menu on the left and finally select **IPSec log** beneath it.

Figure 10-3 IPSec log



Use the **Log level** drop-down list to specify the type of detail you want to capture in the log and then click the Save button. When you change the logging level, any active IPSec VPN tunnels will be disconnected as a change in logging level requires the IPSec service to be restarted.

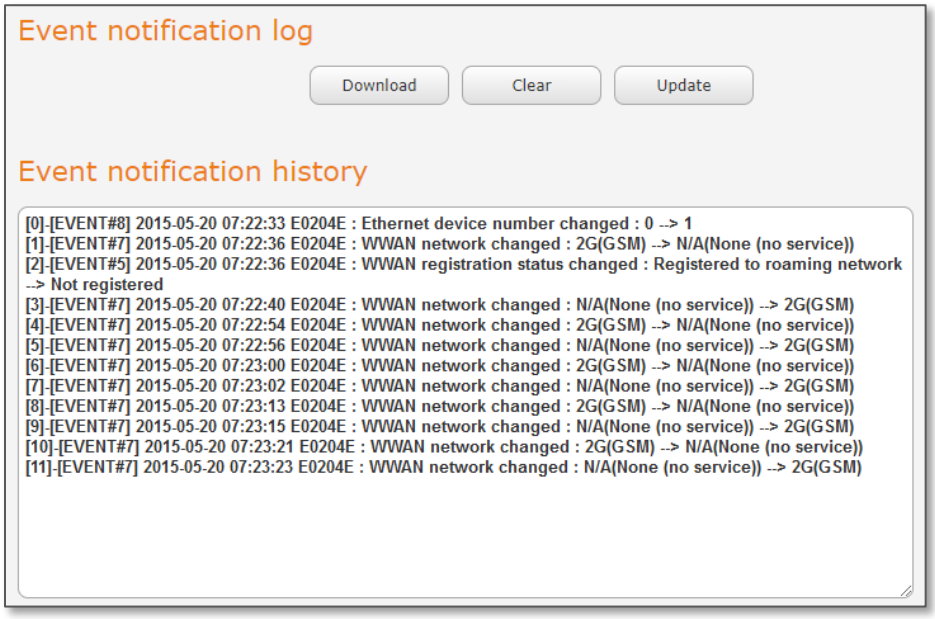
When the Log level is set to **Filtered log** the Log filter drop-down menu contains 13 filters. Select one or multiple filters (hold down **Ctrl** and select for Windows, **Cmd** and select for Mac) and click **Save** to apply the filter(s).

The **Update** button forces a refresh of the display to show any entries since the display was last loaded. To download the IPSec log, click the **Download** button and you will be prompted to save the file.

Event notification log

The **Event notification log** section provides the ability for you to download the log for the Event notification function. This can assist in troubleshooting any problems you may have with the Event notification feature. To access the Event notification log page, click on the **System** menu item then select the **Log** menu on the left and finally select **Event notification log** beneath it.

Figure 10-4 Event notification log



Use the **Download** button to download the log file. The **Update** button forces a refresh of the log display.

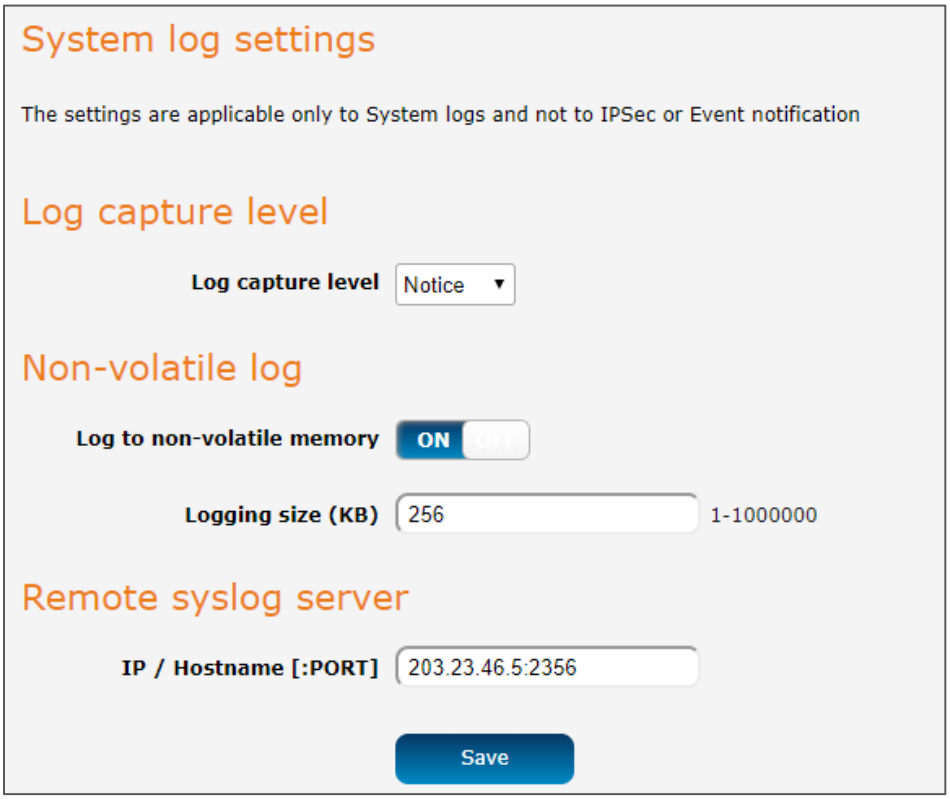
System log settings

To access the System log settings page, click on the **System** menu item then select the **Log** menu on the left and then select **System log** settings from the drop-down menu.

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 10-5 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 10-3 System log detail levels

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

Error	Show error condition messages only.

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.

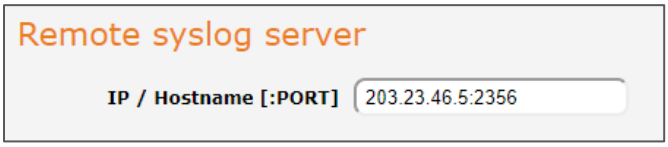
Remote syslog server

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-220 Series router to output log data to a remote syslog server:

1. Click on the **System** menu from the top menu bar. The **System log** item is displayed.
2. Under the **Remote syslog server** section, enter the IP address or hostname of the syslog server in the **IP / Hostname [PORT]** field.

Figure 10-6 Remote syslog server configuration



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.

3. Click the **Save** button to save the configuration.

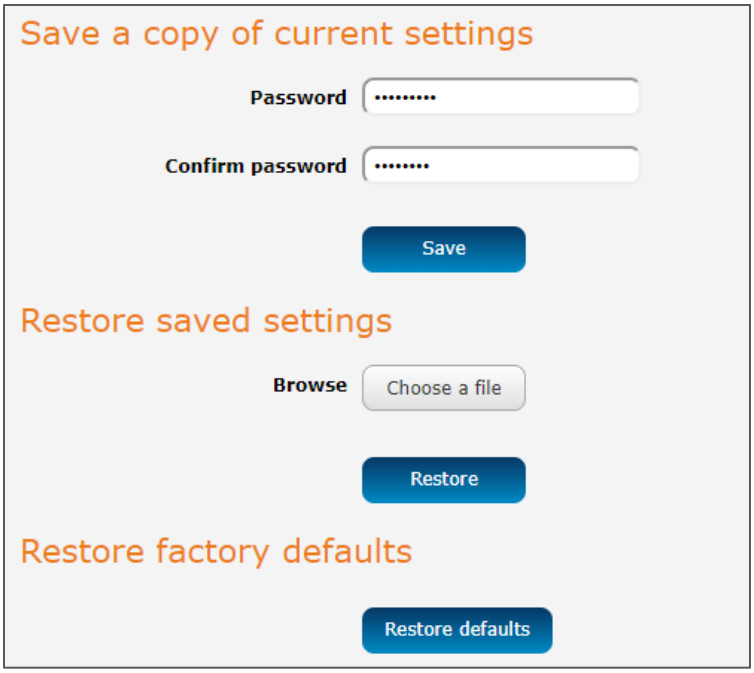
System configuration

Settings backup and restore

The settings backup and restore page is used 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 a large number of NTC-220 Series routers by configuring one router with your desired settings, backing them up to a file and then restoring that file to multiple NTC-220 Series routers.

To access the Settings backup and restore page, click on the **System** menu item then select the **System configuration** menu on the left and finally select **Settings backup and restore** beneath it.

Figure 10-7 Settings backup and restore



Back up your router's configuration

1. Log in to the web configuration interface, click the System menu and select Settings backup and restore.
2. If you want to password protect your backup configuration files, enter your password in the fields under Save a copy of current settings and click Save.

If you do not want to password protect your files, just click on Save. The router will then prompt you to select a location to save the settings file.

***Note**:*

*It is **NOT possible** to edit the contents of the file downloaded; if you modify the contents of the configuration file in any way you will not be able to restore it later.*

*You may change the name of the file if you wish but the filename extension must remain as "**.cfg**"*

Restore your backup configuration

1. In the web configuration interface click on the **System** menu and select **Settings backup and restore**.
2. From the **Restore saved settings** section, click on **Browse** or **Choose a file** and select the backup configuration file on your computer.
3. Click **Restore** to copy the settings to the new NTC-220 Series router. The router will apply these settings and inform you it will reboot - click on **OK**.

Restoring the router's factory default configuration

Click the **Restore defaults** button to restore the factory default configuration. The router asks you to confirm that you wish to restore factory default settings. If you wish to continue with the restoring of factory defaults, click **OK**.

Note: *All current settings on the router will be lost when performing a restore of factory default settings. The device IP address will change to 192.168.1.1 and the default username root and default password user will be configured.*

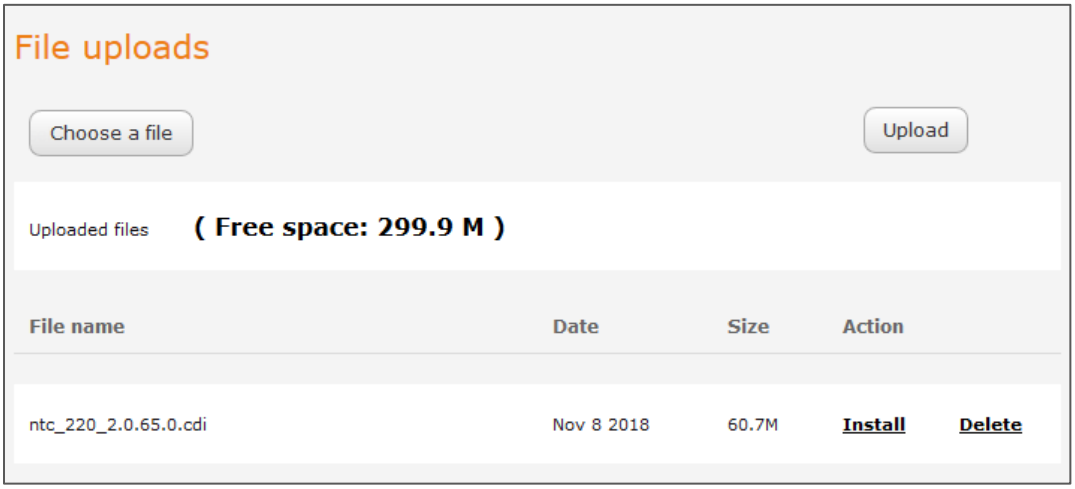
Upload

To access the Upload page, click on the **System** menu, then **System Configuration** and then **Upload**.

The Upload page allows you to upload firmware files, HTTPS certificates or user-created application packages to the NTC-220 Series router. When firmware files have been uploaded, they can also be installed from this page. PDF files, such as this user guide may also be uploaded for access on the router's help page.

For more information on application development, contact Lantronix about our Software Development Kit.

Figure 10-8 Upload page



Updating the Firmware

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

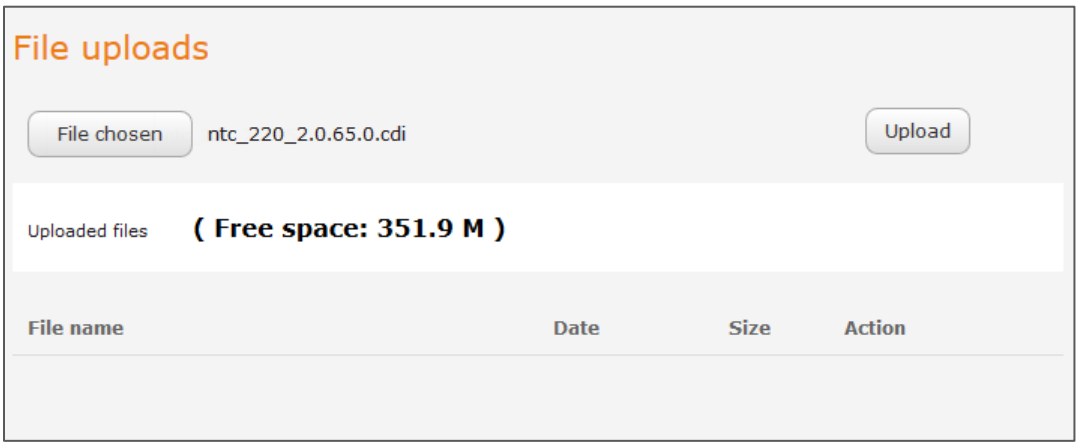
Note: *In order to perform an update, you must be logged into the router with the root manager account (see the Advanced configuration section for more details).*

To update the NTC-220 Series router's firmware:

1. Power on the router as described in the Installing the router section.

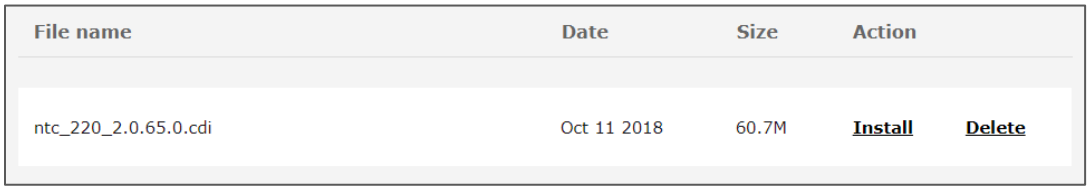
2. Log in to the router with the root user account (See the Advanced configuration section for details)
3. Select the **System** item from the top menu bar, select the **System configuration** item from the menu on the left and then select the **Upload** menu item.
4. Under the **File uploads** section, click the **Choose a file** button. Locate the firmware image file on your computer and click **Open**. The firmware image is named **ntc_220_x.xx.xx.x.cdi** or **vzw_220_x.xx.xx.x.cdi** (NTC-225) where the 'x' characters represent the version number.
5. Click the **Upload** button. The firmware image is uploaded to the storage on the router.

Figure 10-9 File upload



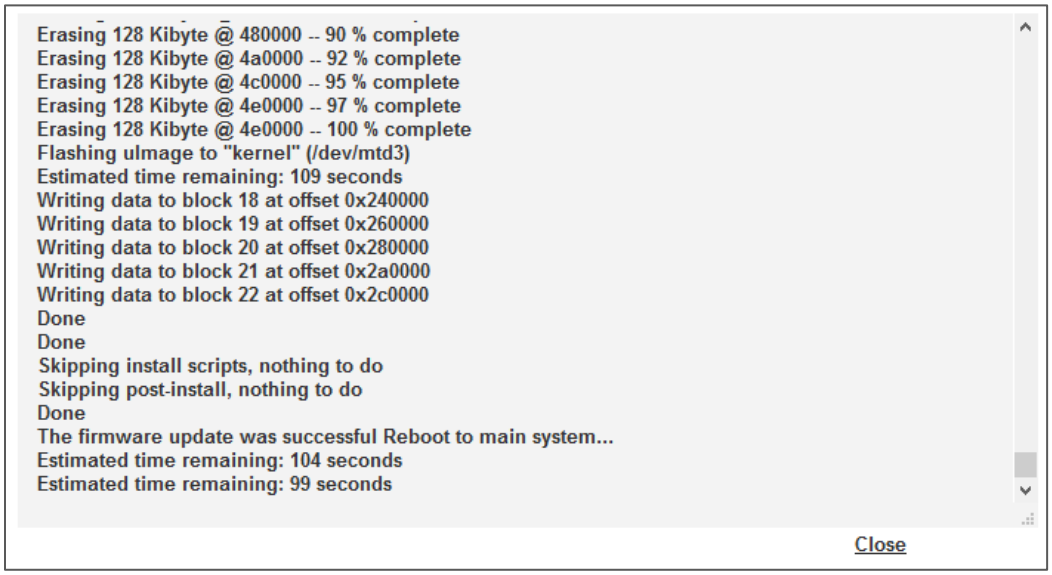
6. The uploaded firmware is listed in the Uploaded files section. Click the **Install** link next to the file to begin installing the firmware and then click **OK** on the confirmation window that appears.

Figure 10-10 Uploaded files



7. The firmware is flashed and when it is complete, the router displays "The firmware update was successful" and returns to the main Upload screen.

Figure 10-11 Firmware flash process complete



Note: *Do not remove the power when the router's LEDs are flashing as this is when the firmware update is in process.*

The installation is complete when the countdown reaches zero. The router attempts to redirect you to the Status page.

Figure 10-12 Installation process complete

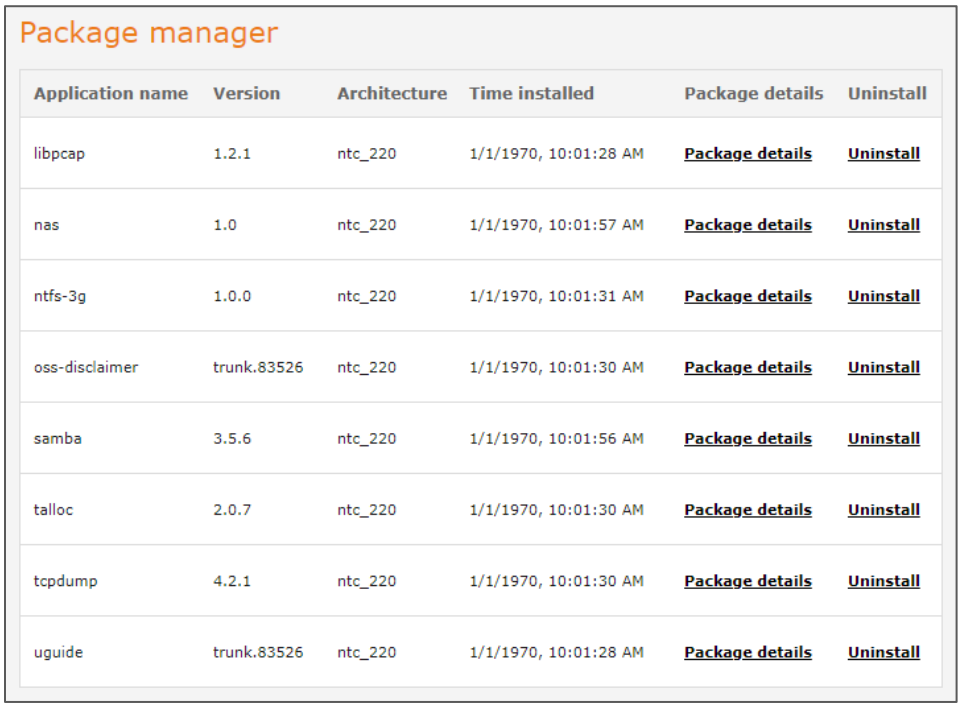
8. Hold down the reset button on the router for 15-20 seconds to reboot and restore the factory default settings of the router. See the *Restoring factory default settings* section for more information.

Package manager

The Package manager page is used to provide details of any user installed packages on the router and allow them to be uninstalled.

For more information on application development, contact your sales representative about the Software Development Kit.

Figure 10-13 Software applications manager



The Application name, Version number of the application, the architecture type and time of installation are all displayed. Clicking the **Package details** link will display a pop-up window with further details of the package.

To uninstall any software applications, click the **Uninstall** link. The NTC-220 Series User Guide PDF (this document) and the Open-Source Software Disclaimer are installed as packages and may be uninstalled to recover some storage space if required.

Firmware signature (not available on NTC-225)

By default, the **Enable firmware signature check** toggle key to **ON** and the router is configured to verify the signature of the firmware loaded onto it. This ensures that the firmware that is installed on the router is certified.

Figure 10-14 Firmware signature

Details for currently verified signatures will appear in the **Public key list** table.

The administrator may disable this feature for the purposes of development by turning the **Enable firmware signature check** toggle key to the **OFF** position and clicking the **Save** button.

Once the change has been made, the message "*Success! Your firmware signature check option changes were successfully saved and applied*." appears.

Administration

Administration settings

To access the Administration Settings page, click on the System menu then the Administration menu on the left and then click on Administration settings.

The Administration settings page is used to enable or disable protocols used for remote access and configure the passwords for the user accounts used to log in to the router.

The page is divided into four sections:

- Remote router access control
- Local router access control
- Web User Interface account
- Telnet/SSH account

Figure 10-15 Administration page

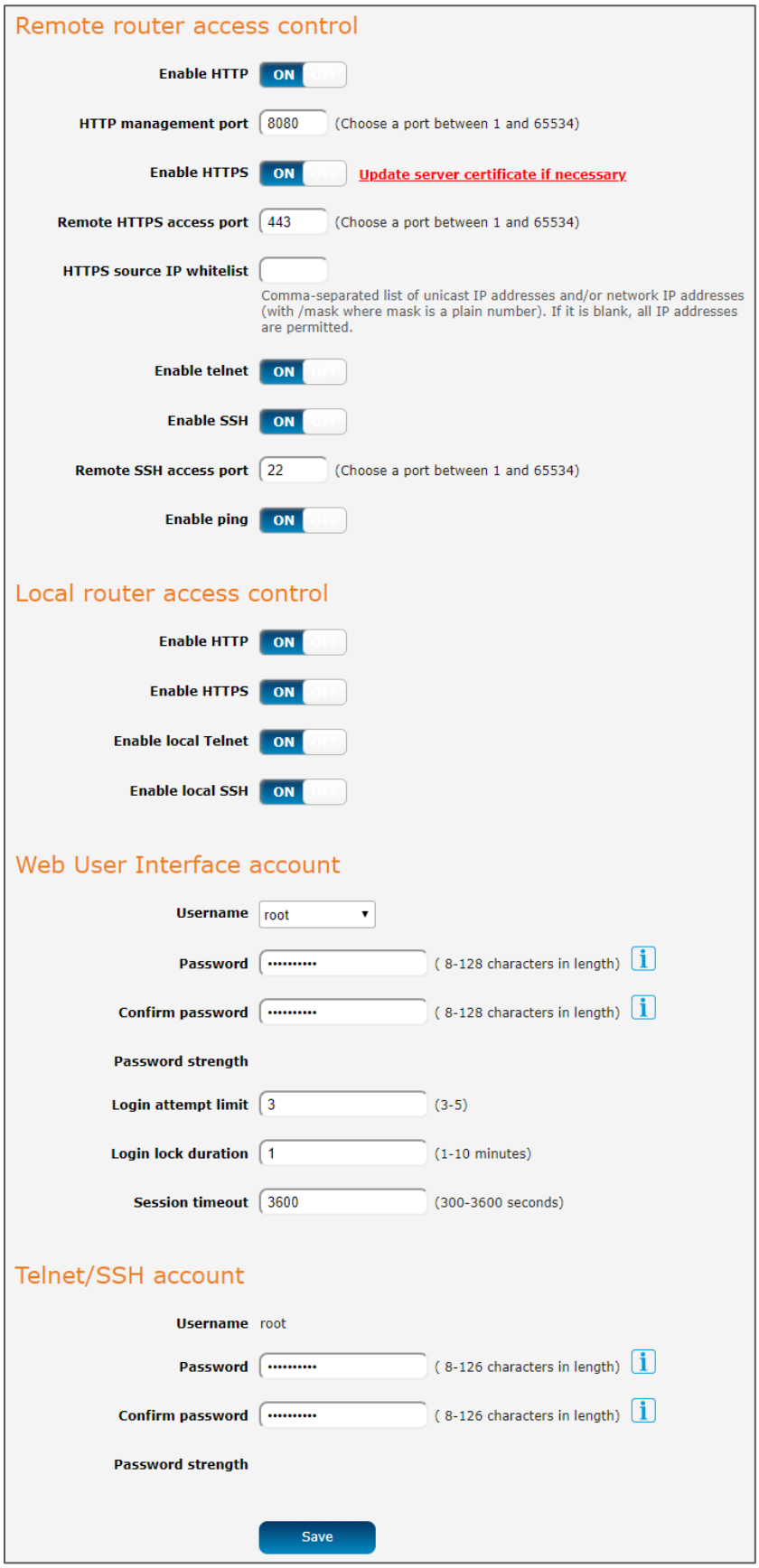
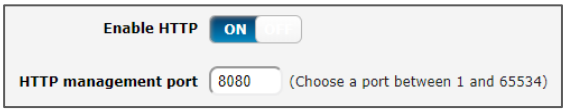
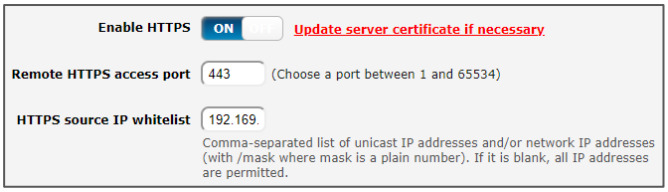
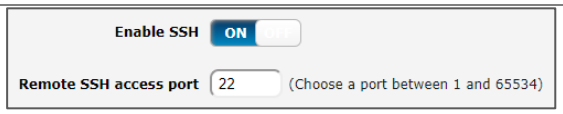


Table 10-4 Administration configuration options

Option	Definition
Remote router access control Note that all remote router access control settings are disabled by default. 	
Enable HTTP	Enable or disable remote HTTP access to the router.
HTTP management 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.
Enable HTTPS	Enable or disable remote HTTPS access to the router using a secure connection.
Remote HTTPS access port	When HTTPS is enabled (see previous) 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 whitelist	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. Note that if this field is left blank, all IP addresses will be permitted to access the router.
Enable Telnet	Enable or disable remote telnet (command line) access to the router.
Enable SSH	Enable or disable Secure Shell on the router.
Remote SSH Access Port	When SSH is enabled (see previous) you can set the remote SSH access port.

	 Enter the port number for remote SSH access. The port number must be between 1 and 65534.
Enable FTP	Enable or disable the File Transfer Protocol on the router for remote connections.
Enable FTPS	Enable or disable the Secure File Transfer Protocol on the router for remote connections.
Enable Ping	Enable or disable remote ping responses on the WWAN connection.
Local router access control	
Enable HTTP	Enable or disable local HTTP access to the router. The default setting is disabled.
Enable HTTPS	Enable or disable local secure HTTP access (https). The default setting is enabled.
Enable local Telnet	Enable or disable local telnet (command line) access to the router. The default setting is disabled.
Enable local SSH	Enable or disable local Secure Shell on the router. The default setting is enabled.
Enable local FTP	Enable or disable the File Transfer Protocol on the router for local connections.
Enable local FTPS	Enable or disable the Secure File Transfer Protocol on the router for local connections.
Web User Interface account	
Username	Use the drop-down list to select the root or user account to change its web user interface password.
Password	Enter the desired web user interface password. When logged in with the root account the password will display in clear text, otherwise the password is masked. Only the root account can view and change passwords.
Password strength	The NTC-220 Series router includes algorithms to ensure that the password you enter is strong.

	Any password configured on the router must now meet the following criteria: • Be a minimum of eight characters and no more than 128 characters in length. • Contain at least one upper case, one lower case character and one number. • Contain at least one special character, such as: `~!@#$%^&*()-_=+[{]}|;:'",<.>/?. Additionally, the password must also 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 and US television and movies and other common patterns such as dates, repeated characters (aaa), sequences (abcd), keyboard patterns (qwertyuiop) and substitution of numbers for letters.
Login attempt limit	Set the number of unsuccessful login attempts that are allowed before the login lock applies (see next item). You can choose 3, 4 or 5 login attempts. The default is 3.
Login lock duration	Set the time users must wait before they can attempt to login after reaching the login attempt limit, see previous item above. The duration can be set from one minute to ten minutes. The default is one minute.
Session timeout	Set the time in seconds that the system must remain idle before it automatically logs out. 1800 seconds (30 minutes) is the default. You can choose a time between 300 seconds (5 minutes) and 3600 seconds (one hour).
Telnet/SSH account	
Username	Displays the Telnet/SSH.username. This may not be changed.
Password	Enter the desired Telnet/SSH password.
Confirm password	Re-enter the desired Telnet/SSH password.

Accessing the router configuration pages remotely

To access the router's configuration pages remotely:

1. Open a new browser window and navigate to the WAN IP address and assigned port number of the router, for example, http://123.209.130.249:8080

Note: *You can find the router's WAN IP address by clicking on the "Status" menu. The WWAN IP field in the WWAN Connection Status section shows the router's WAN IP address.*

2. Enter the username and password to login to the router and click Log in.

Note: *To perform functions like Firmware upgrade, device configuration backup and to restore and reset the router to factory defaults, you must be logged in with the root manager account.*

Server certificate

What is HTTP Secure?

HTTP Secure or HTTPS is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured through the use of certificates issued by trusted certificate authorities such as VeriSign. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.

There are two main differences between how HTTPS and HTTP connections work:

- HTTPS uses port 443 while HTTP uses port 80 by default.
- Over an HTTPS connection, all data sent and received is encrypted with SSL while over an HTTP connection, all data is sent unencrypted.

The encryption is achieved by using a pair of public and private keys on both sides of the connection. In cryptography, a key refers to a numerical value used by an algorithm to alter information (encrypt it), making the information secure and visible only to those who have the corresponding key to recover (decrypt) the information. The public key is used to encrypt information and can be distributed freely. The private key is used to decrypt information and must be secret by its owner.

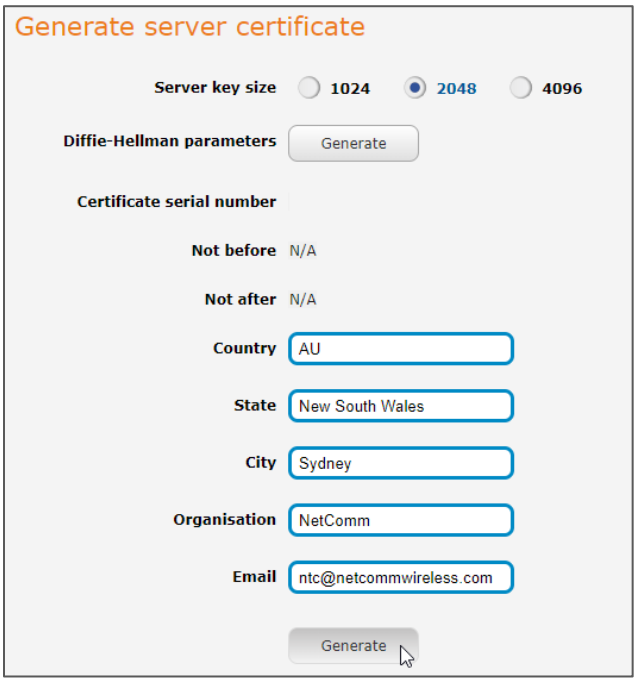
Each NTC-220 Series router contains a self-signed digital certificate which is identical on all NTC-220 Series routers. For a greater level of security, the router also supports generating your own unique key. Additionally, you may use third party software to generate your own self-signed digital certificate or purchase a signed certificate from a trusted certificate authority and then upload those certificates to the router.

Generating your own self-signed certificate

To generate your own self-signed certificate:

1. Click the System item from the top menu bar, then Administration from the side menu bar and then Server certificate.
2. Select a Server key size. A larger key size takes longer to generate but provides better security.
3. Click the Generate button to begin generating Diffie-Hellman parameters.
4. Enter the certificate details using the appropriate fields. All fields must be completed to generate a certificate.

Figure 10-16 Generate server certificate



Note: *The Country field must contain a code for the desired country from the list below.*

Table 10-5 Country codes

Code	Country	Code	Country	Code	Country	Code	Country
AX	Åland Islands	**ER**	Eritrea	**LS**	Lesotho	**SA**	Saudi Arabia
AD	Andorra	**ES**	Spain	**LT**	Lithuania	**SB**	Solomon Islands
AE	United Arab Emirates	**ET**	Ethiopia	**LU**	Luxembourg	**SC**	Seychelles
AF	Afghanistan	**FI**	Finland	**LV**	Latvia	**SE**	Sweden
AG	Antigua and Barbuda	**FJ**	Fiji	**LY**	Libya	**SG**	Singapore
AI	Anguilla	**FK**	Falkland Islands (Malvinas)	**MA**	Morocco	**SH**	St. Helena
AL	Albania	**FM**	Micronesia	**MC**	Monaco	**SI**	Slovenia
AM	Armenia	**FO**	Faroe Islands	**MD**	Moldova	**SJ**	Svalbard and Jan Mayen Islands
AN	Netherlands Antilles	**FR**	France	**ME**	Montenegro	**SK**	Slovak Republic

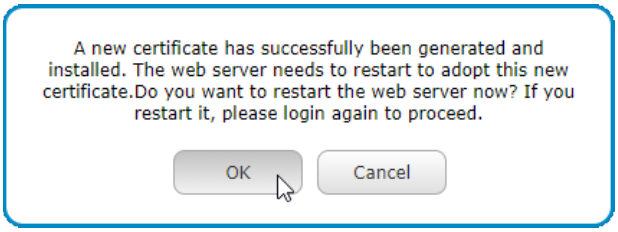
AO	Angola	**FX**	France, Metropolitan	**MG**	Madagascar	**SL**	Sierra Leone
AQ	Antarctica	**GA**	Gabon	**MH**	Marshall Islands	**SM**	San Marino
AR	Argentina	**GB**	Great Britain (UK)	**MK**	Macedonia	**SN**	Senegal
AS	American Samoa	**GD**	Grenada	**ML**	Mali	**SR**	Suriname
AT	Austria	**GE**	Georgia	**MM**	Myanmar	**ST**	Sao Tome and Principe
AU	Australia	**GF**	French Guiana	**MN**	Mongolia	**SU**	USSR (former)
AW	Aruba	**GG**	Guernsey	**MO**	Macau	**SV**	El Salvador
AZ	Azerbaijan	**GH**	Ghana	**MP**	Northern Mariana Islands	**SZ**	Swaziland
BA	Bosnia and Herzegovina	**GI**	Gibraltar	**MQ**	Martinique	**TC**	Turks and Caicos Islands
BB	Barbados	**GL**	Greenland	**MR**	Mauritania	**TD**	Chad
BD	Bangladesh	**GM**	Gambia	**MS**	Montserrat	**TF**	French Southern Territories
BE	Belgium	**GN**	Guinea	**MT**	Malta	**TG**	Togo
BF	Burkina Faso	**GP**	Guadeloupe	**MU**	Mauritius	**TH**	Thailand
BG	Bulgaria	**GQ**	Equatorial Guinea	**MV**	Maldives	**TJ**	Tajikistan
BH	Bahrain	**GR**	Greece	**MW**	Malawi	**TK**	Tokelau
BI	Burundi	**GS**	S. Georgia and S. Sandwich Isls.	**MX**	Mexico	**TM**	Turkmenistan
BJ	Benin	**GT**	Guatemala	**MY**	Malaysia	**TN**	Tunisia
BM	Bermuda	**GU**	Guam	**MZ**	Mozambique	**TO**	Tonga
BN	Brunei Darussalam	**GW**	Guinea-Bissau	**NA**	Namibia	**TP**	East Timor
BO	Bolivia	**GY**	Guyana	**NC**	New Caledonia	**TR**	Turkey

BR	Brazil	**HK**	Hong Kong	**NE**	Niger	**TT**	Trinidad and Tobago
BS	Bahamas	**HM**	Heard and McDonald Islands	**NF**	Norfolk Island	**TV**	Tuvalu
BT	Bhutan	**HN**	Honduras	**NG**	Nigeria	**TW**	Taiwan
BV	Bouvet Island	**HR**	Croatia (Hrvatska)	**NI**	Nicaragua	**TZ**	Tanzania
BW	Botswana	**HT**	Haiti	**NL**	Netherlands	**UA**	Ukraine
BZ	Belize	**HU**	Hungary	**NO**	Norway	**UG**	Uganda
CA	Canada	**ID**	Indonesia	**NP**	Nepal	**UM**	US Minor Outlying Islands
CC	Cocos (Keeling) Islands	**IE**	Ireland	**NR**	Nauru	**US**	United States
CF	Central African Republic	**IL**	Israel	**NT**	Neutral Zone	**UY**	Uruguay
CH	Switzerland	**IM**	Isle of Man	**NU**	Niue	**UZ**	Uzbekistan
CI	Cote D'Ivoire (Ivory Coast)	**IN**	India	**NZ**	New Zealand (Aotearoa)	**VA**	Vatican City State (Holy See)
CK	Cook Islands	**IO**	British Indian Ocean Territory	**OM**	Oman	**VC**	Saint Vincent and the Grenadines
CL	Chile	**IS**	Iceland	**PA**	Panama	**VE**	Venezuela
CM	Cameroon	**IT**	Italy	**PE**	Peru	**VG**	Virgin Islands (British)
CN	China	**JE**	Jersey	**PF**	French Polynesia	**VI**	Virgin Islands (U.S.)
CO	Colombia	**JM**	Jamaica	**PG**	Papua New Guinea	**VN**	Viet Nam
CR	Costa Rica	**JO**	Jordan	**PH**	Philippines	**VU**	Vanuatu
CS	Czechoslovakia (former)	**JP**	Japan	**PK**	Pakistan	**WF**	Wallis and Futuna Islands
CV	Cape Verde	**KE**	Kenya	**PL**	Poland	**WS**	Samoa
CX	Christmas Island	**KG**	Kyrgyzstan	**PM**	St. Pierre and Miquelon	**YE**	Yemen

CY	Cyprus	**KH**	Cambodia	**PN**	Pitcairn	**YT**	Mayotte
CZ	Czech Republic	**KI**	Kiribati	**PR**	Puerto Rico	**ZA**	South Africa
DE	Germany	**KM**	Comoros	**PS**	Palestinian Territory	**ZM**	Zambia
DJ	Djibouti	**KN**	Saint Kitts and Nevis	**PT**	Portugal	**COM**	US Commercial
DK	Denmark	**KR**	Korea (South)	**PW**	Palau	**EDU**	US Educational
DM	Dominica	**KW**	Kuwait	**PY**	Paraguay	**GOV**	US Government
DO	Dominican Republic	**KY**	Cayman Islands	**QA**	Qatar	**INT**	International
DZ	Algeria	**KZ**	Kazakhstan	**RE**	Reunion	**MIL**	US Military
EC	Ecuador	**LA**	Laos	**RO**	Romania	**NET**	Network
EE	Estonia	**LC**	Saint Lucia	**RS**	Serbia	**ORG**	Non-Profit Organization
EG	Egypt	**LI**	Liechtenstein	**RU**	Russian Federation	**ARPA**	Old style Arpanet
EH	Western Sahara	**LK**	Sri Lanka	**RW**	Rwanda		

5. When you have entered all the required details, press the **Generate** button. The certificate takes several minutes to generate. When the certificate has been generated, you are informed that it has been successfully generated and installed. The web server on the router restarts and you are logged out of the router. Click **OK** to be taken back to the login screen.

Figure 10-17 New certificate successfully generated message



SSH key management

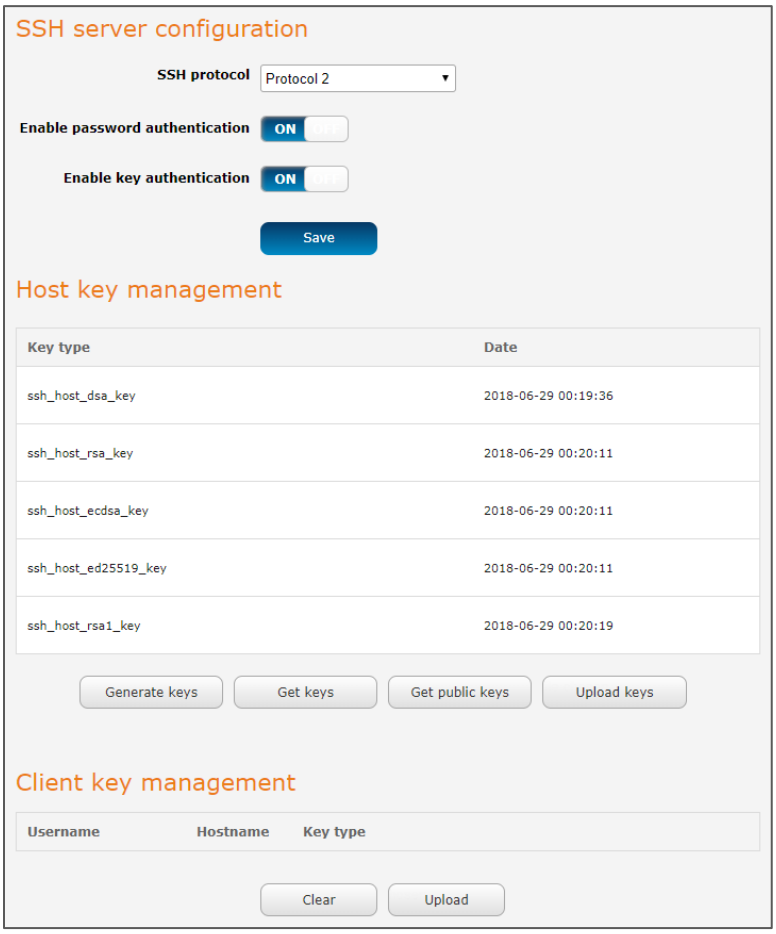
Secure Shell (SSH) is UNIX-based command interface and network protocol used to gain secure access to a remote computer, execute commands on a remote machine or to transfer files between machines. It was designed as a replacement for Telnet and other insecure remote shell protocols which send information, including passwords, as plain text.

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, click on the **System** menu then the **Administration** menu on the left and then click on **SSH key management**.

Figure 10-18 SSH Server Configuration



SSH Server Configuration

To configure the SSH server settings:

1. Use the SSH Protocol drop-down list to select the protocol that you want to use. Protocol 2 is more recent and is considered more secure.
2. Select the types of authentication you want to use by clicking the Enable password authentication and Enable key authentication toggle keys on or off. Note that you may have both authentication methods on but you may not turn them both off.
3. Click the **Save** button to confirm your settings.

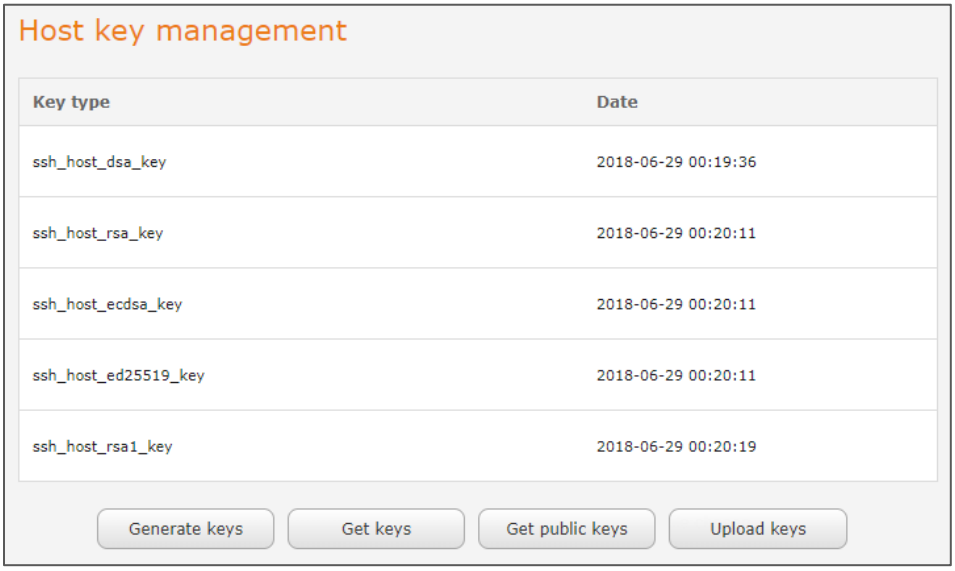
Host key management

SSH keys provide a means of identification using public key cryptography and challenge response authentication. This means that a secure connection can be established without transmitting a password, thereby greatly reducing the threat of someone eavesdropping and guessing the correct credentials.

SSH Keys always come in pairs with one being a public key and the other a private key. The public key may be shared with any server to which you want to connect. When a connection request is made, the server uses the public key to encrypt a challenge (a coded message) to which the correct response must be given. Only the private key can decrypt this challenge and produce the correct response. For this reason, the private key should not be shared with those who you do not wish to give authorization.

The Host key management section displays the current public keys on the router and their date and timestamp. These public keys are provided in different formats, including DSA, RSA and ECDSA. Each format has advantages and disadvantages in terms of signature generation speed, validation speed and encryption/decryption speed. There are also compatibility concerns to consider with older clients when using ECDSA, for example.

Figure 10-19 Host key management



Generating new keys

The complete set of keys can be re-generated by selecting the Generate keys button. This key generation process takes approximately 30 seconds to complete.

Downloading keys

The Get keys button allows you to download the complete set of public and private keys while the Get public keys button will download only the set of public keys.

Uploading your own key files

You can generate your own SSH keys and upload them to the router. To generate keys on a Linux-based machine, use the following commands:

```
mkdir keys
cd keys
ssh-keygen -t rsa1 -f ssh_host_key -N ""
ssh-keygen -t dsa -f ssh_host_dsa_key -N ""
ssh-keygen -t rsa -f ssh_host_rsa_key -N ""
```

```
ssh-keygen -t ecdsa -f ssh_host_ecdsa_key -N ""
zip -e -P "PASSWORDHERE" -j keys.zip *
```

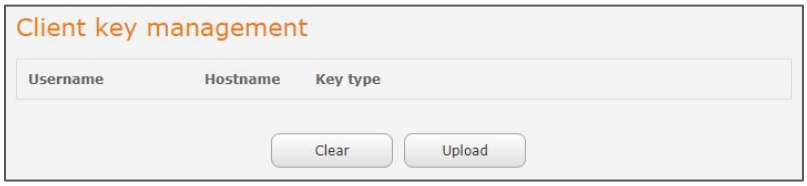
Click the Upload keys button then locate the generated keys to upload them to the router.

Client key management

The **Client Key Management** section is used for uploading the public key file of clients.

To upload a client public key, click the **Upload** button, browse to the file and click **Open**.

Figure 10-20 Client key management

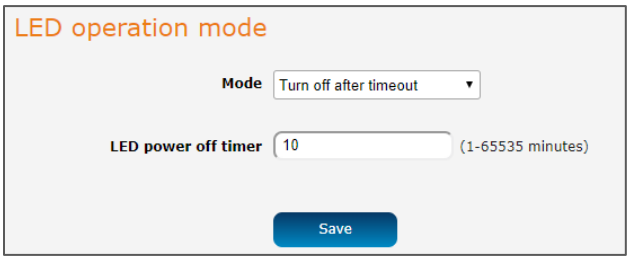


When the file is uploaded, it is examined for validity. If the key file is not a valid public key, it will not be uploaded.

LED operation mode

The eight LED indicators may be turned off after a timeout period for aesthetic or power saving reasons. To access the **LED Operation Mode** page, click the **System** menu, then **Administration** on the left and finally select **LED Operation Mode**.

Figure 10-21 LED Operation Mode



The **Mode** drop-down list sets the operation mode of the LEDs on the front panel of the router. To set the lights to operate at all times, set this to Always on. To set the lights to turn off after a specified period, select Turn off after timeout. When configured to turn off after timeout, use the **LED power off timer** field to specify the time in minutes to wait before turning off the LED indicators.

The **LED Power Off Timer** must be an integer between 1 and 65535 minutes.

The wait period begins from the time the **Save** button is clicked. When the wait period expires, the LEDs will turn off. If the router is rebooted, the LED power off timer is reset. The router will boot up and wait for the configured time before turning off again.

Watchdogs

The **Ping watchdog** 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.

Please be very careful when considering 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). This is because the ping watchdog feature expects to be able to access the internet at all times and will always eventually reboot the router if access isn't restored by the time the various timers and retries expire.

It is due to the nature of the ping watchdog being a last resort standalone backup mechanism that 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. Therefore, 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.

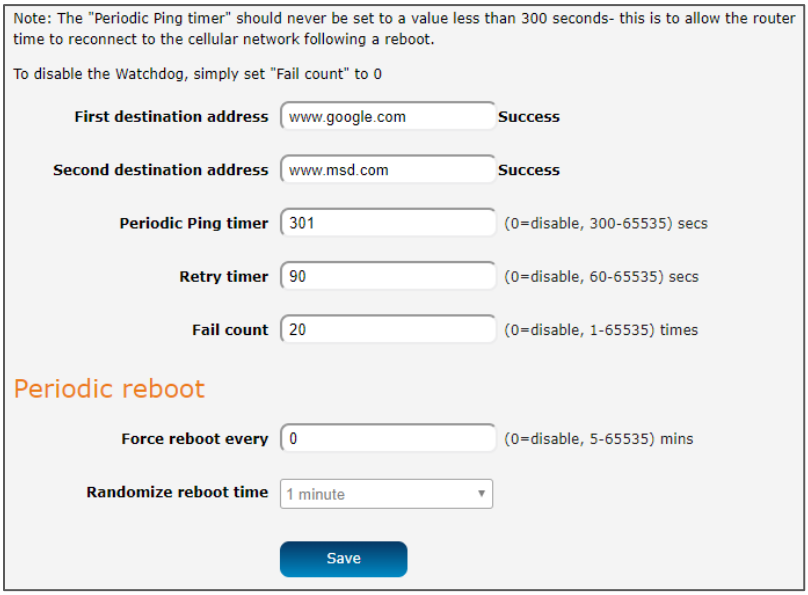
The feature operates as follows:

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 C above fail then number of time configured in "Fail count", the router reboots.
5. If any ping succeeds, the router returns to step A and does not reboot.

Important: *The "Periodic Ping timer" should not be set to a value of less than 300 seconds to allow the router time to reconnect to the cellular network following a reboot.*

To disable the Ping watchdog, set **Fail count** to 0.

Figure 10-22 Ping watchdog settings



Configuring Periodic Ping settings

The Periodic Ping settings configure the router to transmit controlled ping packets to 2 specified IP addresses. If the router does not receive responses to the pings, the router will reboot.

To configure the ping watchdog:

1. 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.
2. 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.
3. In the **Periodic Ping timer** field, enter an integer 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.
4. In the **Retry timer** field, enter an integer 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. Setting this to 0 disables the ping watchdog function
5. 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.

Disabling the Ping watchdog function

To disable the Ping watchdog function, set **Fail Count** to **0**.

Important: *The traffic generated by the periodic ping feature is usually counted as chargeable data usage. Please keep this in mind when selecting how often to ping.*

Configuring a 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.

1. 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.
2. If you have configured a forced reboot time, you can use the Randomise reboot time drop-down list to select a random reboot timer. Randomising 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 Randomise reboot time setting. After that randomly selected time has elapsed, the router reboots.
3. Click the **Save** button to save the settings.

Important: *The randomise 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 Randomise reboot time*

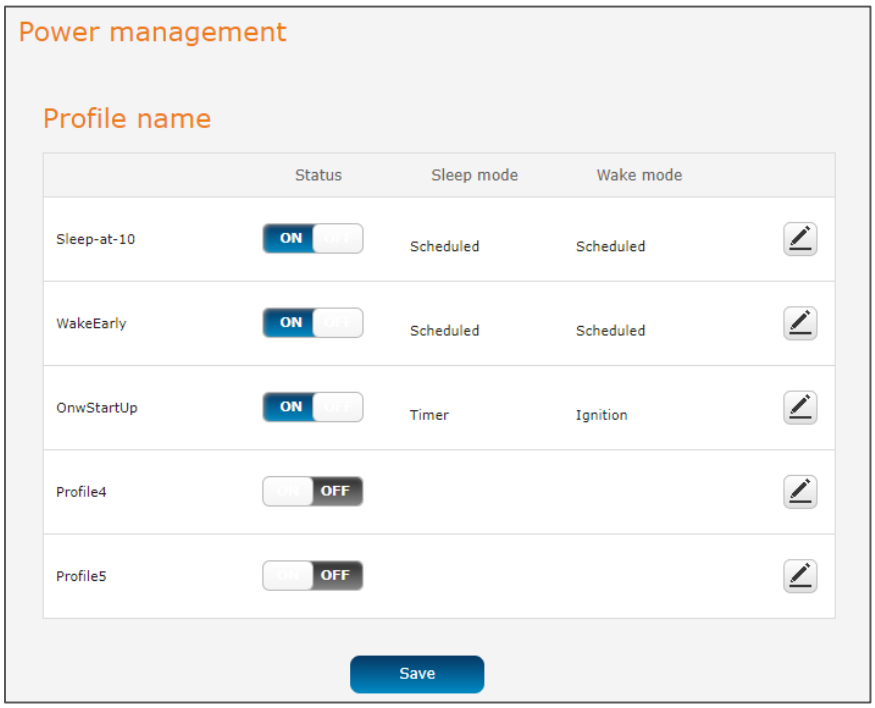
Power management

The Power management page provides you with an overview of the power profiles and the ability to configure them. Up to five power profiles may be configured and all of them may be active simultaneously. The Status column indicates whether the profile is active, while the **Sleep mode** and **Wake mode** columns summarise the method used to sleep or wake the modem.

To access the Low power mode page, click the **System** menu item, then select the **Low power mode** menu item on the left.

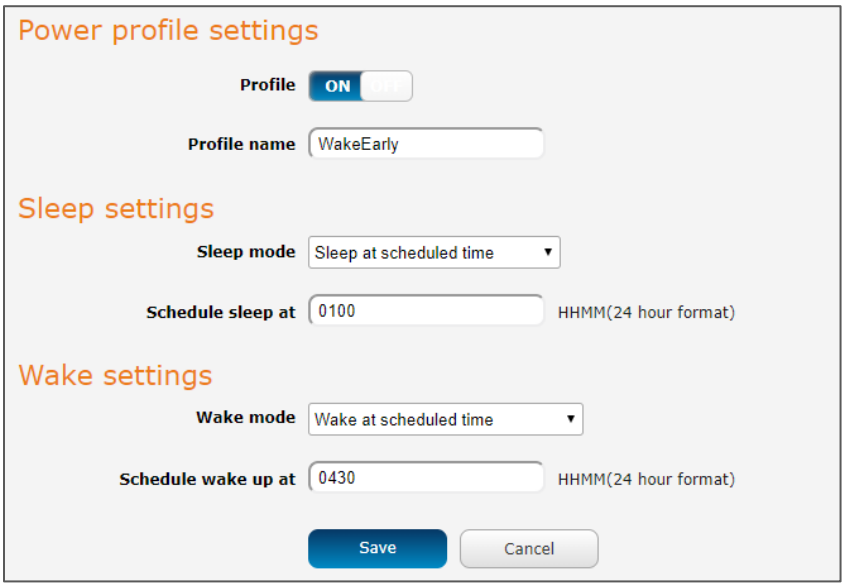
Important: *When configuring multiple power profiles, be careful so that they do not overlap or conflict with one another, for example, configuring a schedule which wakes up the unit when another profile has it scheduled to be in low power mode.*

Figure 10-23 Power management



To edit a power profile, click the edit icon of the appropriate profile.

Figure 10-24 Power management – Power profile settings



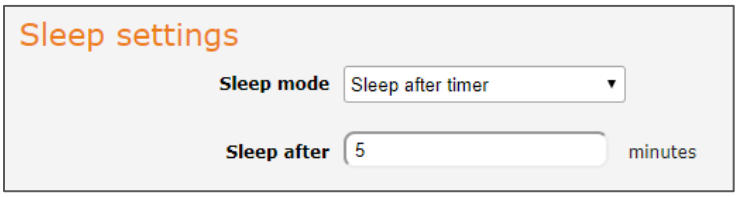
Sleep settings

Use the **Sleep mode** drop-down list to select a condition under which the router should enter the sleep state.

Sleep after timer

When this mode is selected, the router will enter the sleep state after the number of minutes specified in the **Sleep after** field, regardless of the state of the ignition pin.

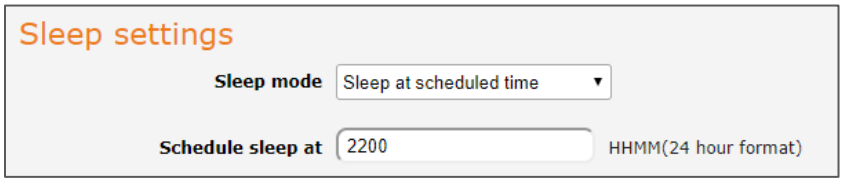
Figure 10-25 Sleep after timer



Sleep at scheduled time

When this mode is selected, the router goes to sleep at the time specified in the **Schedule sleep at** field, regardless of the state of the ignition pin. Enter the time in 24 hour format without the semi-colon.

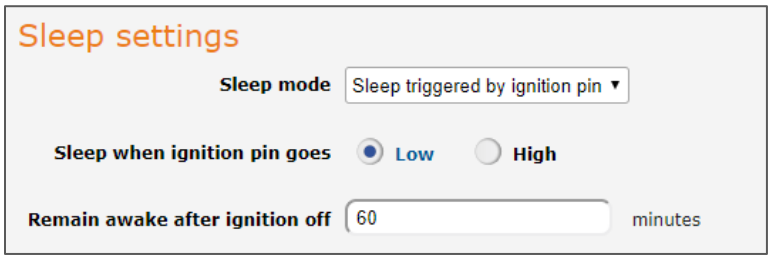
Figure 10-26 Sleep at scheduled time



Sleep triggered by ignition pin

This mode sets the router to enter sleep state when the signal on the ignition pin reaches the specified value.

Figure 10-27 Sleep triggered by ignition pin



Use the **Sleep when ignition pin goes** setting to select **Low** or **High**. By default, this is set to **Low**. Additionally, the router will stay on for the number of minutes specified in the **Remain awake after ignition off** field. The minimum value for this field is 2 minutes with the maximum being 255 minutes.

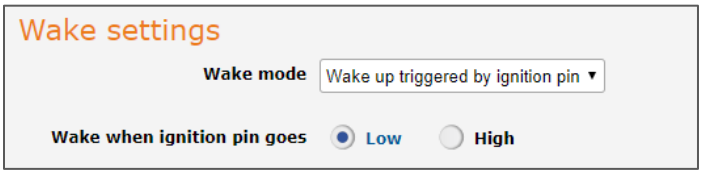
Wake settings

Use the **Wake mode** drop-down list to select a condition under which the router should return from the sleep state.

Wake triggered by ignition pin

This mode sets the router to wake up when the signal on the ignition pin reaches the specified value.

Figure 10-28 Wake up triggered by ignition pin

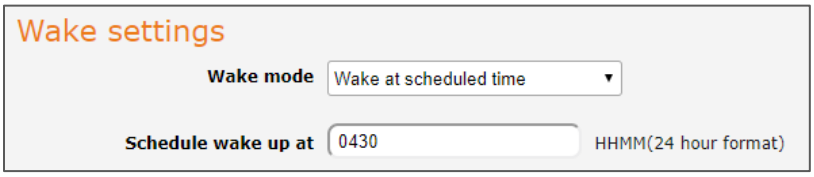


Use the **Wake up when ignition pin goes** setting to select **Low** or **High**. By default, this is set to **High**.

Wake up at scheduled time

When this mode is selected, the router wakes up at the time specified in the **Schedule wake up at** field, regardless of the state of the ignition pin. Enter the time in 24-hour format without the semi-colon.

Figure 10-29 Wake up at scheduled time



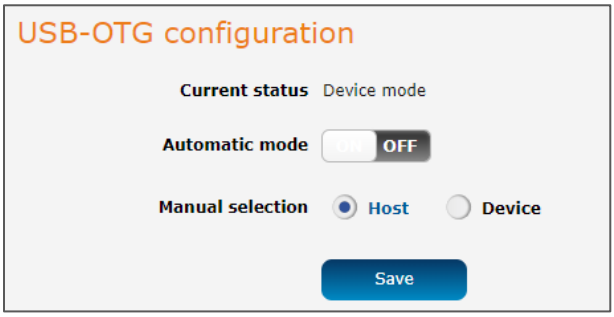
USB-OTG

The USB port can be enabled or disabled on the USB OTG configuration page (**System > USB OTG**). By default, the port is enabled.

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.

Figure 10-30 USB-OTG configuration



A notification can be sent each time a change to these settings is saved. To configure notification settings, go to **Services > Event notification > Notification configuration** and select a notification type and destination for event 23.

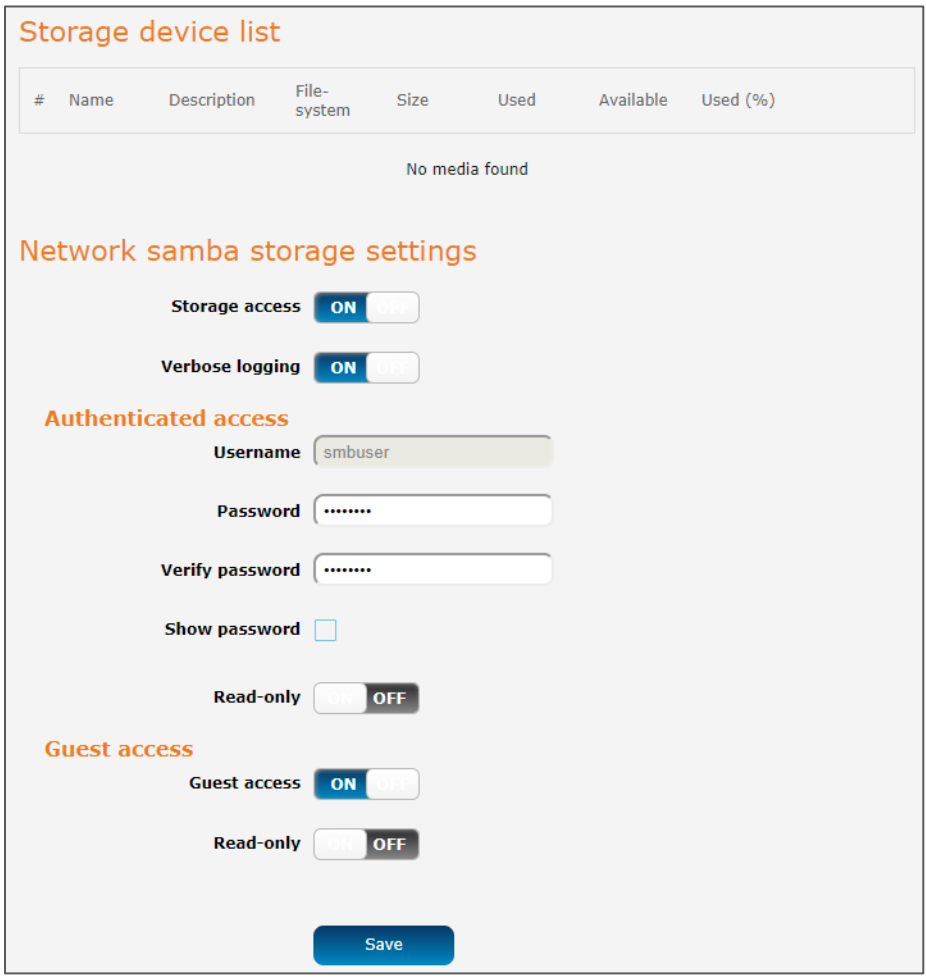
Storage

The Storage page provides configuration options with relation to USB and SD storage devices. To access the **Storage** page, click the **System** menu item, then select the **Storage** menu item on the left.

Storage device list

The **Storage devices 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.

Figure 10-31 Storage



Network Samba storage settings

Storage devices connected to the router can be shared using the Samba protocol. The table below describes the configuration options for the Network Samba storage settings.

Table 10-6 Network Samba storage settings

Item	Definition
Storage access	Turns the Samba sharing function on or off.
Verbose logging	When turned on, this provides 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	The password to be used for authenticated access to the storage device.
Verify password	The password to be used for authenticated access to the storage device.
Show password	Displays the passwords in the authenticated access fields.
Read-only	When turned on, this provides 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	Enables or disables guest access to the storage device.
Read-only	When turned on, this provides 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.

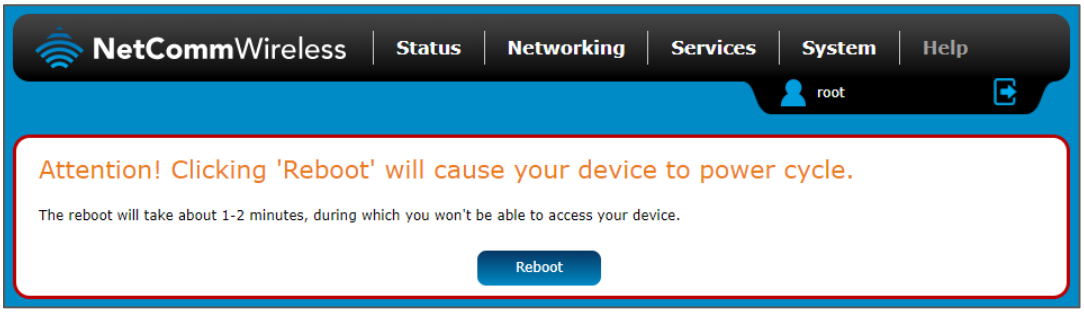
Reboot

The **Reboot** option performs a soft reboot of the router. This can be useful if you have made configuration changes you want to implement.

To reboot the router:

1. Click the **System** menu item from the top menu bar.
2. Click the **Reboot** button from the menu on the left side of the screen.
3. The router displays a warning that you are about to perform a reboot.
4. If you wish to proceed, click the **Reboot** button.
5. A warning popup will advise that "It may take 1-2 minutes to reboot your device. Are you sure you want to continue?" Click **OK** to continue with the reboot process

Figure 10-32 Reboot confirmation



Note: *It can take up to 2 minutes for the router to reboot.*

Logging out

To log out of the router, click the icon at the top right corner of the web user interface.

11. Open-source disclaimer

This product contains Open Source software that has been released by the developers of that software under specific licensing requirements such as the “General Public License“ (GPL) Version 2 or 3, the “Lesser General Public License“ (LGPL), the “Apache License“ or similar licenses.

For detailed information on the Open Source software, the copyright, the respective licensing requirements and ways of obtaining the source code, please contact our technical support team by going to https://lantronix.com/technical-support.

12. Safety and product care

Electrical safety

Accessories

Only use approved accessories.

Do not connect with incompatible products or accessories.

Connection to a car

Seek professional advice when connecting a device interface to the vehicle electrical system.

Distraction

Operating machinery

Full attention must be given to operating the machinery in order to reduce the risk of an accident.

Driving

Full attention must be given to driving at all times in order to reduce the risk of an accident. Using the device in a vehicle can cause distraction and can lead to an accident. You must comply with local laws and regulations restricting the use of mobile communication devices while driving.

Product handling

You alone are responsible for how you use your device and any consequences of its use.

You must always switch off your device wherever the use of a mobile phone is prohibited. Do not use the device without the clip-on covers attached, and do not remove or change the covers while using the device. Use of your device is subject to safety measures designed to protect users and their environment.

Always treat your device and its accessories with care and keep it in a clean and dust-free place.

Do not expose your device or its accessories to open flames or lit tobacco products.

Do not expose your device or its accessories to liquid, moisture or high humidity.

Do not drop, throw or try to bend your device or its accessories.

Do not use harsh chemicals, cleaning solvents, or aerosols to clean the device or its accessories.

Do not paint your device or its accessories.

Do not attempt to disassemble your device or its accessories, only authorised personnel must do so.

Do not expose your device or its accessories to extreme temperatures. Ensure that the device is installed in an area where the temperature is within the supported operating temperature range:

- Class A: -30° C to +70° C
- Class B: -40° C to +85° C (with possible performance deviation)

Do not use your device in an enclosed environment or where heat dissipation is poor. Prolonged use in such space may cause excessive heat and raise ambient temperature, which will lead to automatic shutdown of your

device or the disconnection of the mobile network connection for your safety. To use your device normally again after such shutdown, cool it in a well-ventilated place before turning it on.

Please check local regulations for disposal of electronic products.

Do not operate the device where ventilation is restricted

Installation and configuration should be performed by trained personnel only.

Do not use or install this product near water to avoid fire or shock hazard. Avoid exposing the equipment to rain or damp areas.

Arrange power and Ethernet cables in a manner such that they are not likely to be stepped on or have items placed on them.

Ensure that the voltage and rated current of the power source match the requirements of the device. Do not connect the device to an inappropriate power source.

Small children

Do not leave your device and its accessories within the reach of small children or allow them to play with it.

They could hurt themselves or others or could accidentally damage the device.

Your device contains small parts with sharp edges that may cause an injury or which could become detached and create a choking hazard.

Demagnetisation

To avoid the risk of demagnetisation, do not allow electronic devices or magnetic media close to your device for a long time.

Avoid other magnetic sources as these may cause the internal magnetometer or other sensors to malfunction and provide incorrect data.

Electrostatic discharge (ESD)

Do not touch the SIM card’s metal connectors.

Air Bags

Do not place the device in the area near or over an air bag or in the air bag deployment area

Mount the device safely before driving your vehicle.

Emergency & other situations requiring continuous connectivity

This device, like any wireless device, operates using radio signals, which cannot guarantee connection in all conditions. Therefore, you must never 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.

Device heating

Your device may become warm during normal use.

Faulty and Damaged Products

Do not attempt to disassemble the device or its accessory.

Only qualified personnel should service or repair the device or its accessory.

If your device or its accessory has been submerged in water or other liquid, punctured, or subjected to a severe fall, do not use it until you have taken it to be checked at an authorised service centre

Interference

Care must be taken when using the device in close proximity to personal medical devices, such as pacemakers and hearing aids.

Pacemakers

Pacemaker manufacturers recommend that a minimum separation of 15cm be maintained between a device and a pacemaker to avoid potential interference with the pacemaker.

Hearing aids

People with hearing aids or other cochlear implants may experience interfering noises when using wireless devices or when one is nearby.

The level of interference will depend on the type of hearing device and the distance from the interference source, increasing the separation between them may reduce the interference. You may also consult your hearing aid manufacturer to discuss alternatives.

Medical devices

Please consult your doctor and the device manufacturer to determine if operation of your device may interfere with the operation of your medical device.

Hospitals

Switch off your wireless device when requested to do so in hospitals, clinics or health care facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Aircraft

Switch off your wireless device whenever you are instructed to do so by airport or airline staff.

Consult the airline staff about the use of wireless devices on board the aircraft, if your device offers a ‘flight mode’ this must be enabled prior to boarding an aircraft.

Interference in cars

Please note that because of possible interference to electronic equipment, some vehicle manufacturers forbid the use of devices in their vehicles unless an external antenna is included in the installation.

Explosive environments

Petrol stations and explosive atmospheres

In locations with potentially explosive atmospheres, obey all posted signs to turn off wireless devices such as your device or other radio equipment.

Areas with potentially explosive atmospheres include fuelling areas, below decks on boats, fuel or chemical transfer or storage facilities, areas where the air contains chemicals or particles, such as grain, dust, or metal powders.

Blasting caps and areas

Turn off your device or wireless device when in a blasting area or in areas posted turn off “two-way radios” or “electronic devices” to avoid interfering with blasting operations.

13. Compliance

Manufacturer's Name & Address:

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

Product Family:

NTC-220 Series
Conforms to the following standards or other normative documents:

Country	Models	Specification
Australia – RCM	NTC-221	Yes
Canada – IC	NTC-224 and NTC-227	Contains IC: 8847A-NTC224 IC: 8847A-227
Europe – CE	NTC-221, NTC-222, and NTC-227	See EU Declaration of Conformity
Europe – E-mark	NTC-222 and NTC-227	Yes
Japan – Japan-JPA	NTC-223	Yes
None – CB	NTC-221, NTC-222, NTC-223, NTC-224, and NTC-225	Yes
USA – FCC	NTC-221, NTC-224, NTC-225, and NTC-227	Contains FCC ID: XIA-221 FCC ID: XIA-NTC224 FCC ID: XIA-NTC225 FCC ID: XIA-227

FCC Compliance

Federal Communications Commission Notice (United States): Before a wireless device model is available for sale to the public, it must be tested and certified to the FCC that it does not exceed the limit established by the government-adopted requirement for safe exposure.

FCC Regulations

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio

communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorientate or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

RF Exposure

Your device contains a transmitter and a receiver. When it is on, it receives and transmits RF energy. When you communicate with your device, the system handling your connection controls the power level at which your device transmits.

- This device meets the government’s requirements for exposure to radio waves.
- This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.
- This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. To ensure compliance with RF exposure guidelines the device must be used with a minimum of 23 cm separation from the body. Failure to observe these instructions could result in your RF exposure exceeding the relevant guideline limits.

External Antenna

Any optional external antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Please consult the health and safety guide of the chosen antenna for specific body separation guidelines as a greater distance of separation may be required for high-gain antennas.

Any external antenna gain must meet RF exposure and maximum radiated output power limits of the applicable rule section.

IC regulations

This Class B digital apparatus complies with Canadian ICES-003.

This device complies with ISED licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et

(2) l’utilisateur de l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.”

RF Exposure Information (MPE)

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Cet équipement est conforme aux limites d’exposition aux rayonnements ISED établies pour un environnement non contrôlé.

Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

External antenna

RSS-Gen 8.3 (transmitters equipped with detachable antennas)

This radio transmitter has been approved by ISED to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated.

Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio a été approuvé par ISED pour fonctionner avec les types d’antenne énumérés ci-dessous et ayant un gain admissible maximal et l’impédance requise pour chaque type d’antenne.

Les types d’antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l’exploitation de l’émetteur.

Appendix A. Default Settings

The following tables list the default settings for the NTC-220 Series router.

Table B-1 LAN Management Default Settings

LAN (MANAGEMENT)	
Static IP Address	**192.168.1.1**
Subnet Mask	**255.255.255.0**
Default Gateway	**192.168.1.1**

Default root and admin passwords are printed on the label on the bottom of the router and on the back of the Quick Start Guide which came in the box with your device.

Restoring factory default settings

Restoring factory defaults will reset the NTC-220 Series router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-220 Series router such as:

- You have lost your username and password and are unable to login to the web configuration page;
- You are asked to perform a factory reset by support staff.

There are two methods you can use to restore factory default settings on your NTC-220 Series router:

- Using the web-based user interface
- Using the reset button on the interface panel of the router (if the button is enabled)

Using the web-based user interface

To restore your router to its factory default settings, please follow these steps:

1. Open a browser window and navigate to the IP address of the router (default address is **https://192.168.1.1**). Login to the router using root as the User Name and admin as the password.
2. Click the **System** item from the top menu bar, then **System configuration** on the left menu and then click **Settings backup and restore**.
3. Under the Restore factory defaults section, click the Restore defaults button. The router asks you to confirm that you wish to restore factory defaults. Click **OK** to continue. The router sets all settings to default. Click **OK** again to reboot the router.
4. When the Power light returns to a steady red, the reset is complete. The default settings are now restored.

Using the reset button on the interface panel of the router

If the reset button is enabled, use a pen to depress the Reset button on the device for 15-20 seconds. The router will restore the factory default settings and reboot.

When you have reset your NTC-220 Series router to its default settings you will be able to access the device's configuration web interface using **https://192.168.1.1** with username user or root and password admin.

Appendix B. Recovery mode

The NTC-220 Series router features two independent operating systems, each with its own file systems. These two systems are referred to as 'Main' and 'Recovery'. It is always possible to use one in order to restore the other in the event that one system becomes damaged or corrupted (such as during a firmware upgrade failure). The recovery console provides limited functionality and is typically used to restore the main firmware image in the case of a problem.

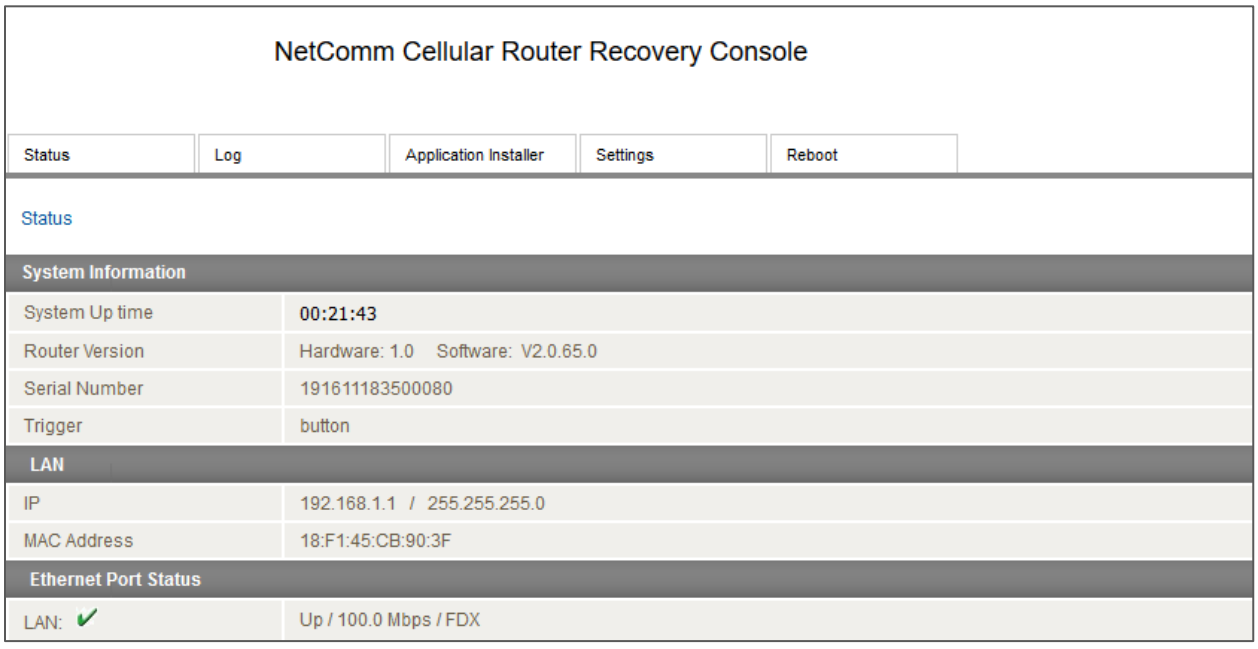
Accessing recovery mode

Both systems have web interfaces that can be used to manipulate the other inactive system. The NTC-220 Series router starts up by default in the Main system mode, however the router may be triggered to start in recovery mode if desired.

To start the router in recovery mode:

1. If the reset button is enabled, press and hold the physical reset button on the interface panel of the router for 5 to 15 seconds. When the LEDs on the front panel change to amber and countdown in a sequence, release the reset button. The router then boots into recovery mode.
2. In your browser, navigate to **http://192.168.1.1**. The router's recovery mode is hardcoded to use this address regardless of the IP address that was configured in the main system. The router's recovery console is displayed.

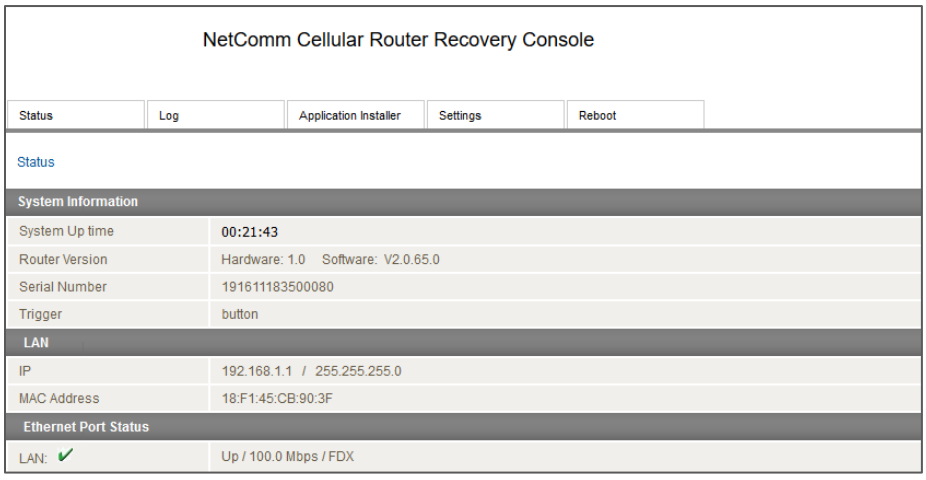
Figure C-1 Recovery console



Status

The status page provides basic information such as the system up time, hardware and software router versions, the router's serial number, the method used to trigger the recovery mode, the IP and MAC address of the router and the status of the Ethernet port.

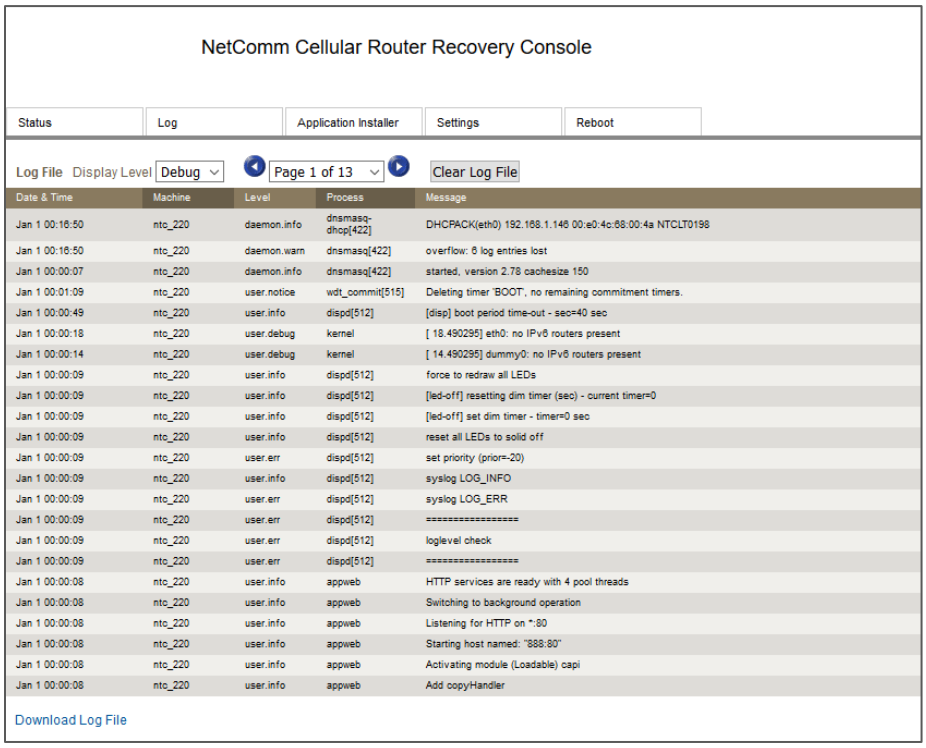
Figure C-2 Recovery mode – Status



Log

The log page displays the system log which is useful in troubleshooting problems which may have led to the router booting up in recovery mode. The only functionality provided here is the ability to clear the system log, filter by log level and downloading of the log file.

Figure C-3 Recovery mode – Log

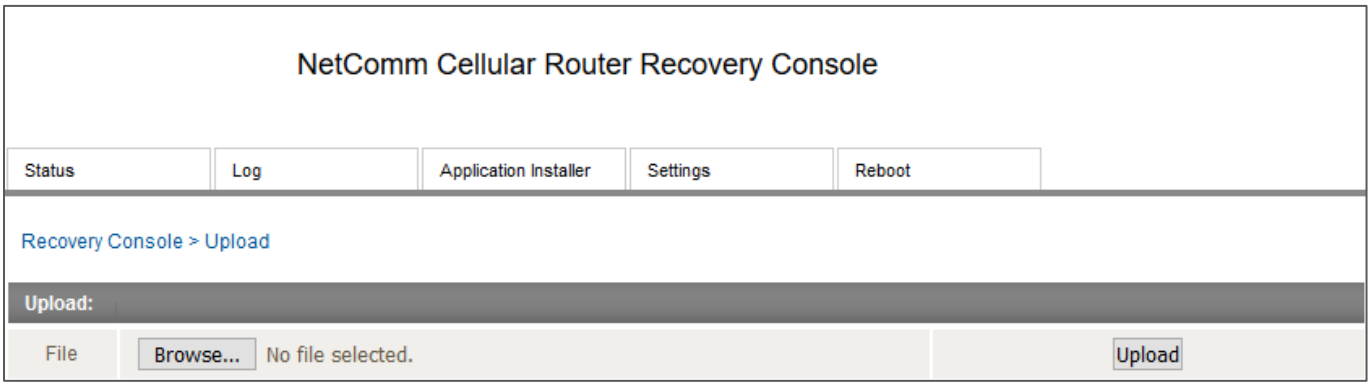


Application Installer

The Application installer is designed to upload and install main firmware images, upload recovery firmware images, custom applications and HTTPS certificates. Use the **Browse** button to select a file to be uploaded to the router. When it has been selected, press the **Upload** button. The file is sent to the router and when the transfer is complete, the file appears in the **Uploaded files list**. From the Uploaded files list, you are able to either **Install** or **Delete** a file.

⚠	***Important:*** *The Application Installer page may exhibit incorrect behaviour on Google Chrome™ and Mozilla Firefox when the web interface was previously rendered via HTTPS and has switched to HTTP. This is usually the case when you have rebooted from the Main image into Recovery mode. To work around this issue, clear the router cookies and refresh the page.*

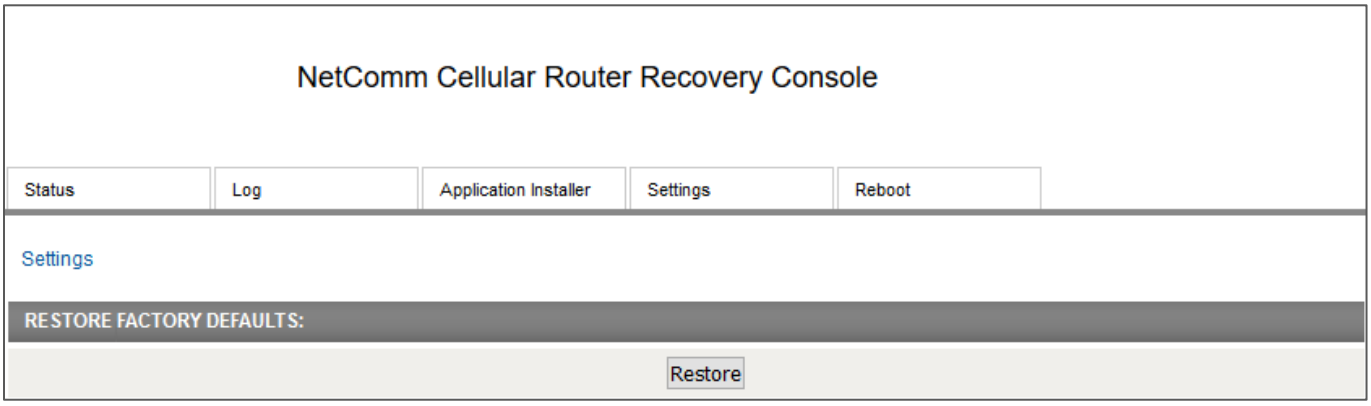
Figure C-4 Recovery mode – Application Installer



Settings

The settings page provides the option of restoring the router to factory default settings. Click the **Restore** button to set the router back to the original factory settings.

Figure C-5 Recovery mode – Settings

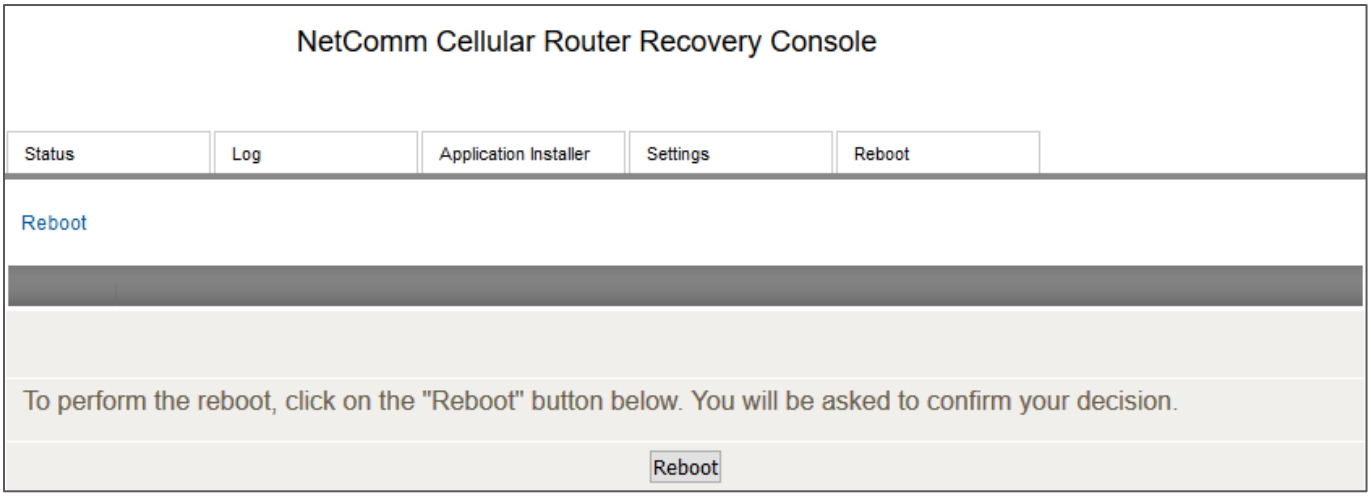


Reboot

The reboot page allows you to reboot the router when you have finished using recovery mode. When rebooting the router from recovery mode, the router boots into the main firmware image unless there is some fault preventing it from doing so, in which case the recovery console will be loaded.

Click the Reboot button to reboot the router to the main firmware image.

Figure C-6 Recovery mode – Reboot



Appendix C. HTTPS – Uploading a self-signed certificate

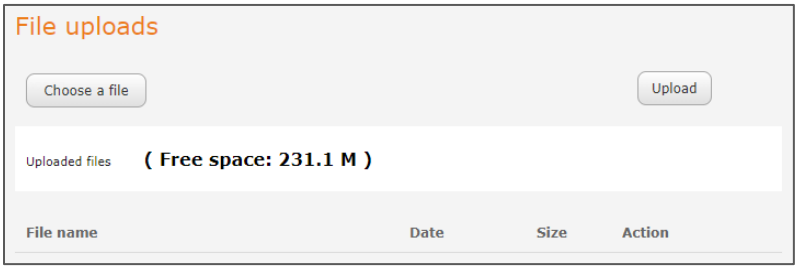
If you have your own self-signed certificate or one purchased elsewhere and signed by a Certificate Authority, you can upload it to the NTC-220 Series router using the **Upload** page.

Important: Your key and certificate files must be named server.key and server.crt respectively otherwise they will not work.

To upload your certificate:

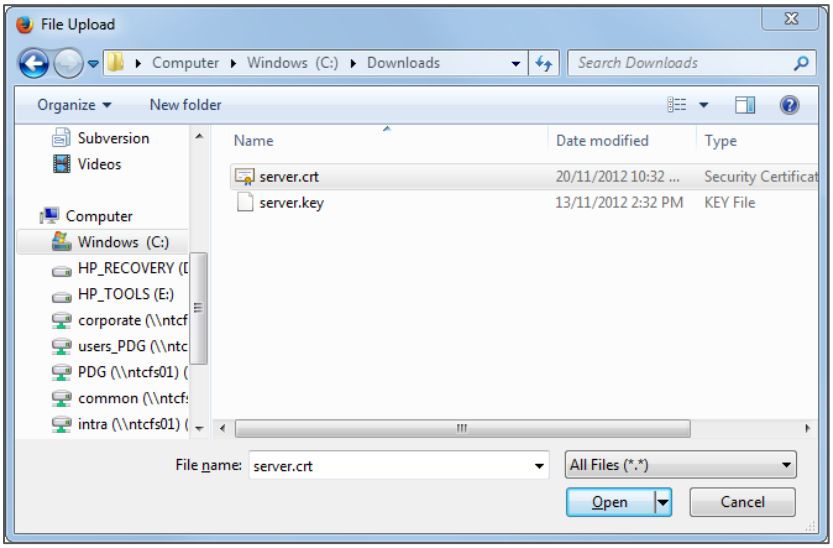
1. Click on the **System** item from the top menu bar. From the side menu bar, select **System Configuration** and then **Upload**. The file upload screen is displayed.

Figure D-1 Upload page



2. Click the **Choose a File** button and locate your server certificate file and click **Open**.

Figure D-2 Browse for server.crt

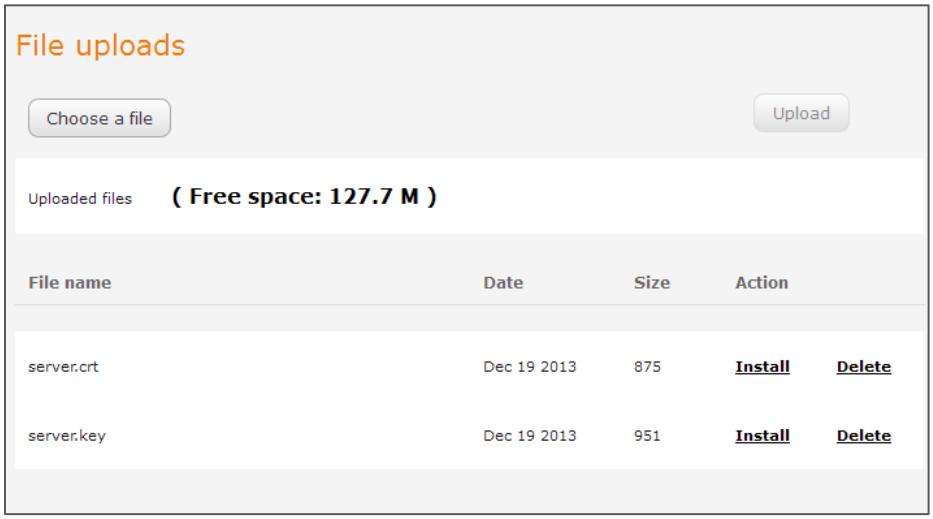


3. Click the **Upload** button to begin uploading it to the router. The file appears in the list of files stored on the router.

Figure D-3 Server certificate file uploaded

4. Repeat steps 2 and 3 for the server key file.
5. Click the **Install** link next to the server.crt file, then click **OK** on the prompt that is displayed. The certificate file is installed. Repeat this for the key file. When each file is installed it is removed from the list of stored files.

Figure D-4 Installing the server.crt file



Appendix D. RJ45 connectors

The RJ45 connectors provide an interface for a data connection and for device input power using the pin layout shown below.

Figure E-1 The RJ-45 connector

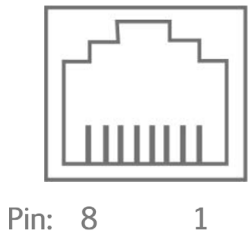


Table E-1 RJ-45 connector pin outs

Pin	Colour	Signal (802.3af mode a)	signal (802.3af mode b)
1	White/Orange stripe	Rx +	Rx + DC +
2	Orange Solid	Rx -	Rx - DC +
3	White/Green stripe	Tx +	Tx + DC -
4	Blue solid	DC +	unused
5	White/Blue stripe	DC +	unused
6	Green solid	Tx -	Tx - DC -
7	White/Brown stripe	DC -	unused
8	Brown solid	DC -	unused

Appendix E. Serial port wiring

Figure F-1 DE9 Male connector (Pin side view)

The NTC-220 Series router has a serial interface and acts as the data communications equipment (DCE). The wiring tables below indicate the DCE and DTE devices as well as the signal direction.

Shielding cable can optionally be soldered to the chassis and connected to ground.

Table F-1 RS-232 Wiring

DTE Device (Computer)			SIGNAL DIRECTION	DCE Device (NTC-220 Router)		
PIN	NAME	DESCRIPTION		DESCRIPTION	NAME	PIN
1	DCD	Data carrier detect	←	Data carrier detect	DCD	1
2	RXD	Receive Data	←	Receive Data	RXD	2
3	TXD	Transmit Data	→	Transmit Data	TXD	3
4	DTR	Data Terminal Ready	→	Data Terminal Ready	DTR	4
5	GND	Ground	—	Ground	GND	5
6	DSR	Data Set Ready	←	Data Set Ready	DSR	6
7	RTS	Request to Send	→	Request to Send	RTS	7
8	CTS	Clear to Send	←	Clear to Send	CTS	8
9	RI	Ring Indicator	←	Ring Indicator	RI	9
-	FGND	Shield (Soldered to D9 metal shield)	—	Shield (Soldered to D9 metal shield)	FGND	-

Table F-2 RS-485 Half Duplex Wiring

RS-485 HALF DUPLEX WIRING			
PIN	SIGNAL	NAME	DESCRIPTION
1	—	A	Differential pair A
2	+	B	Differential pair B

RS-485 HALF DUPLEX WIRING			
PIN	**SIGNAL**	**NAME**	**DESCRIPTION**
5		GND	Ground

Table F-3 RS-485 (RS-422) Full Duplex Wiring

RS-485 (RS-422) FULL DUPLEX WIRING			
PIN	**SIGNAL**	**NAME**	**DESCRIPTION**
1	—	RXA	Receive (Differential pair A)
2	+	RXB	Receive (Differential pair B)
3	+	TXB	Transmit (Differential pair B)
4	—	TXA	Transmit (Differential pair A)
5		GND	Ground

Appendix F. Obtaining a list of RDB variables

Important: *Modifying the RDB can cause your device to malfunction if you are not aware of the specific functions of each variable. Please take care whenever making changes to any RDB variable. These instructions are provided for your information only. Lantronix shall be liable for any loss that arises from the misuse of this information.*

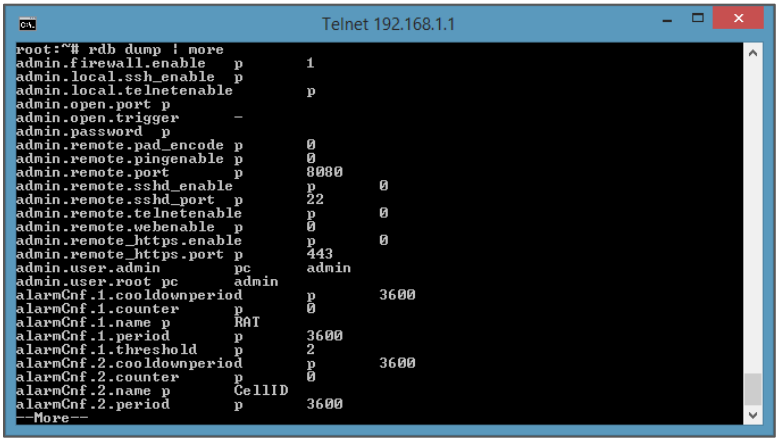
The RDB is a database of variables that contain settings on the router. You can retrieve (get) and set the values of these variables through the command-line or via SMS Diagnostics. To access a full list of the RDB variables, follow these steps:

1. Log in to the web user interface as described in the *Advanced configuration* section of this guide.
2. Click the **System** menu at the top of the screen, then select the **Administration** menu on the left. Finally, select the **Administration settings** menu item.
3. Click the **Enable Telnet** toggle key so that it is in the **ON** position.

4. Under the **Telnet/SSH account** section, enter a telnet password and then re-enter it in the **Confirm password** field.
5. Click the **Save** button at the bottom of the screen.
6. Open a terminal client such as PuTTY and telnet to the router using its IP address.

7. At the login prompt, type root and press **Enter**.
8. At the password prompt, enter the password that you configured in step 4.
9. At the root prompt, enter the command **`rdb dump | more`**.

This will display a list of every rdb variable on the router one page at a time:



Note: *Omitting the | more parameter will dump a complete list without pagination. For easier access, some terminal clients such as PuTTY have the ability to log all telnet output to a text file.*

Appendix G. Using USB devices

The NTC-220 Series router features a Micro USB 2.0 OTG port capable of supplying 0.5A to connected devices. The Micro USB port supports both USB storage devices as well as certain USB accessories, including USB-to-Ethernet adapters and USB-to-Serial cables.

Accessing USB storage devices

When a USB storage device is inserted, the router automatically mounts the storage. To access storage devices:

Windows

1. Open Windows Explorer.
2. In the address bar, type in the network address of the router (**\\my.router** or **\\192.168.1.1** by default), and press **Enter**. The storage devices are labelled Disk A, Disk B or Disk C.

Mac OS

1. In Mac OS, open a Finder window.
2. Select **Go > Connect to Server**.
3. Enter the server address **smb://my.router** or **smb://192.168.1.1**
4. Select the volumes you want to mount. Storage devices are labelled Disk A, Disk B or Disk C.

Linux / Smartphones

You can use any Samba client on Linux and Smartphones to access the connected storage devices by navigating to "**my.router**" or "**192.168.1.1**" in your chosen Samba client.

Host and Device mode

The USB port automatically detects whether to run in host or device mode. When in host mode, the router automatically mounts USB storage, USB-to-serial and USB-to-Ethernet devices. When in device mode, the router supports Ethernet and serial over USB. It is also possible to configure the USB Ethernet port as a WAN port.

Appendix H. Inputs/Outputs

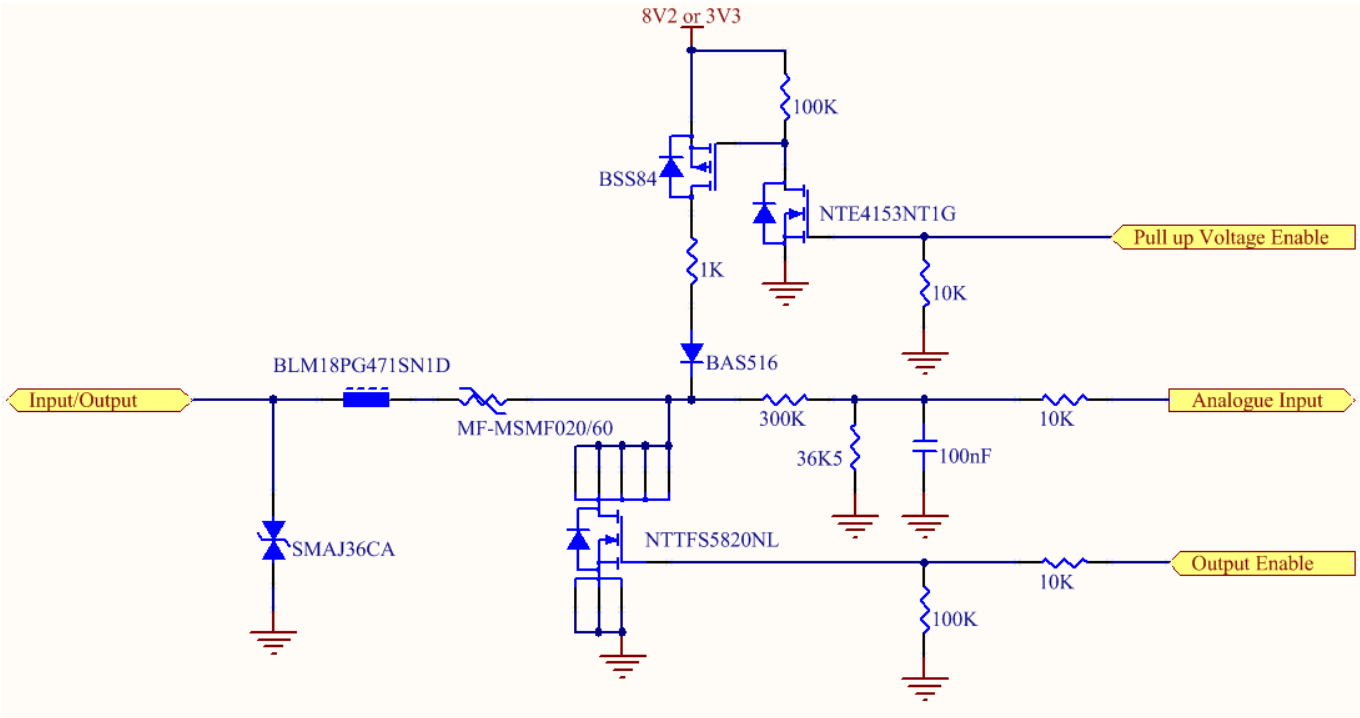
Overview

The NTC-220 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 0V 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 200 mA at 230 °C. 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 8.2 V by software. The Analogue Input pin can read values from 0 V to 30 V. 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.

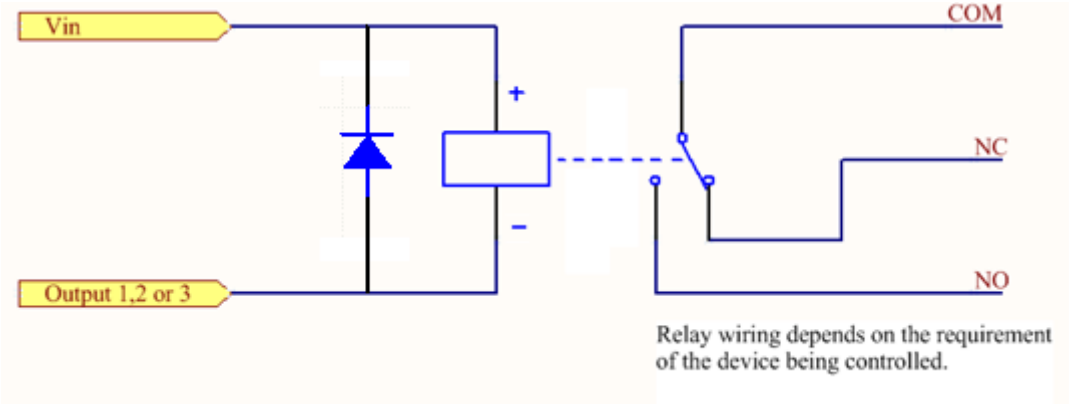
Wiring Examples

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.*

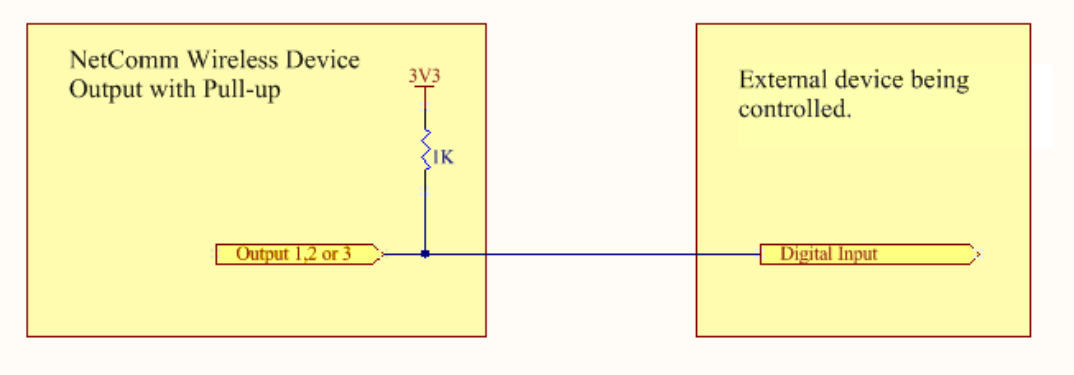
Open Collector Output driving a relay

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.



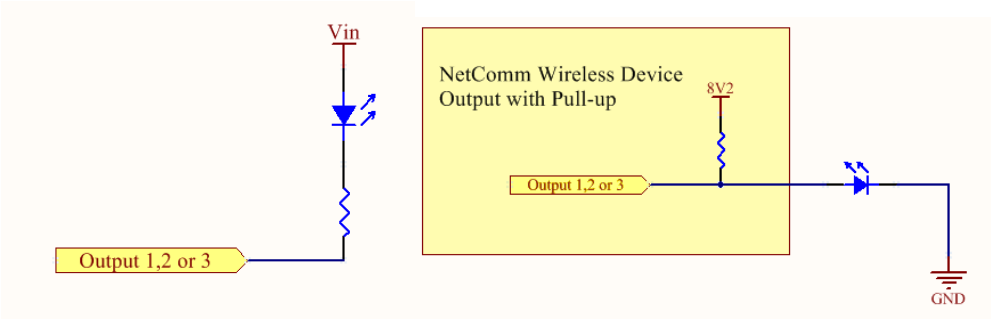
Logic level Output

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

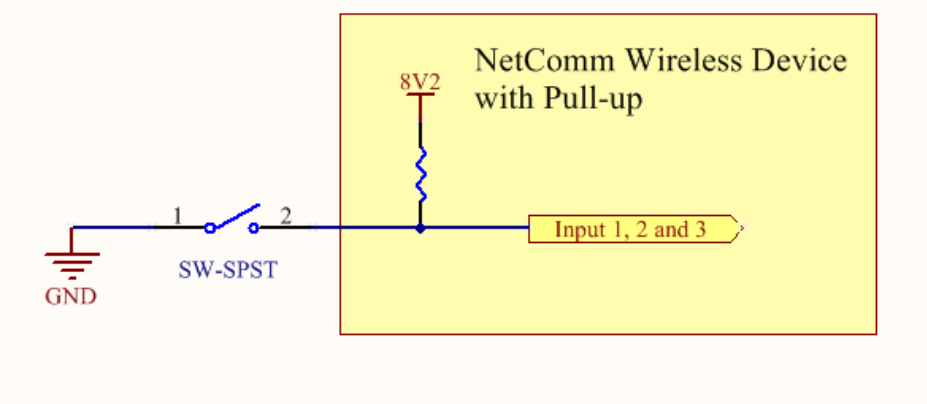
An LED can be controlled by simply providing an open collector ground to an externally powered LED Resistor value and Voltage will need to suit the LED type used. Alternatively, an LED can be powered using 8V2 via 1 K resistor. The suitability of the LED will need to be investigated.



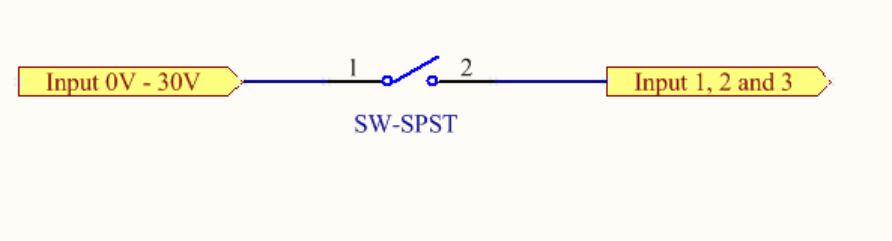
Digital inputs

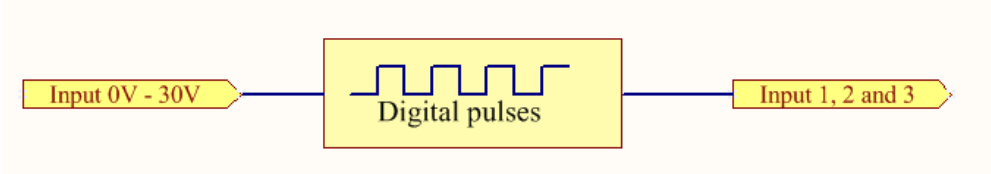
There are several ways to connect a digital input. A digital input can be anything from a simple switch to a digital waveform or pulses. The unit will read the voltage in as an analogue input and the software will decode it in a certain way depending on your configuration.

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



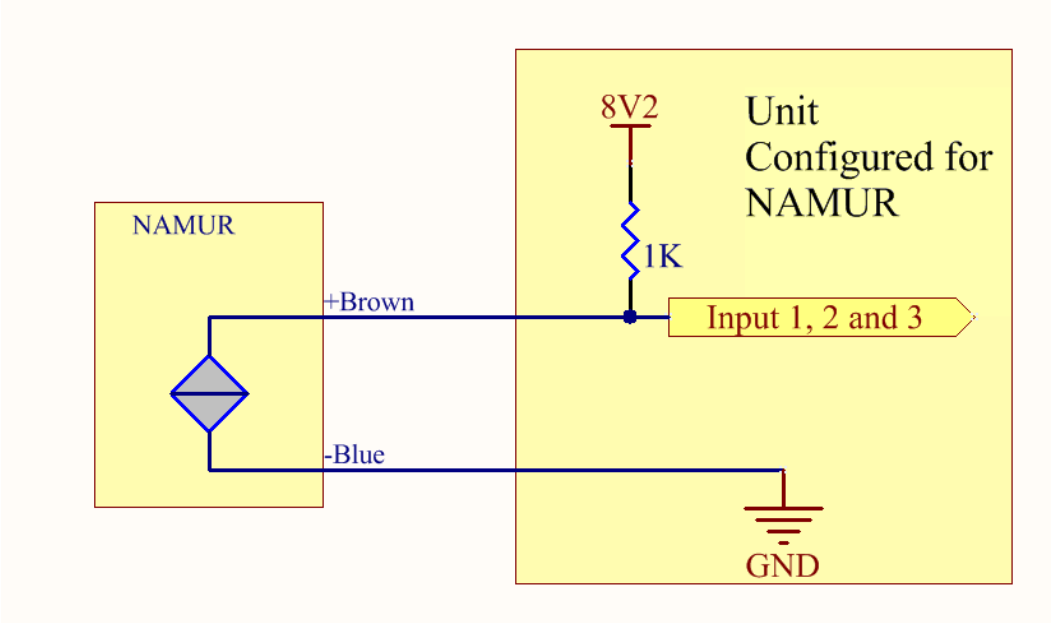
The following input detects an input going high. The turn on/off threshold can be set in the software.





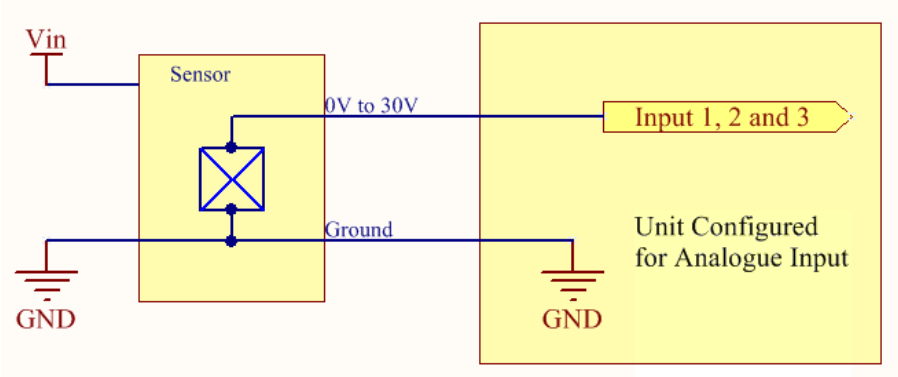
NAMUR Sensor

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.



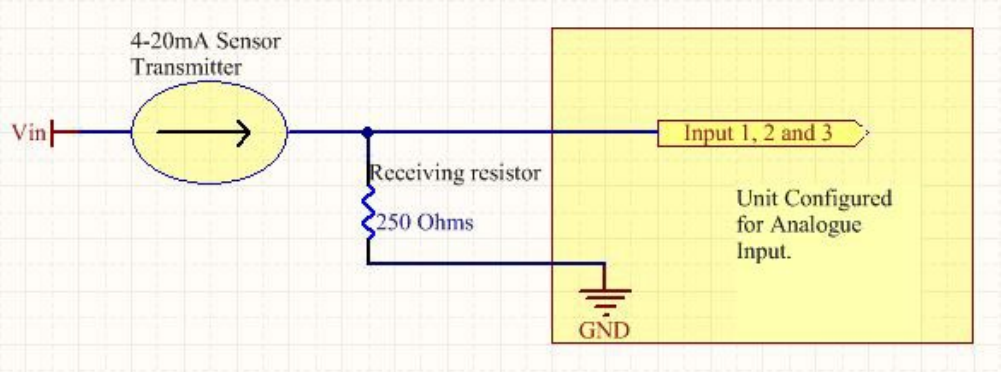
Analogue Sensor with Voltage output

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 0V 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.



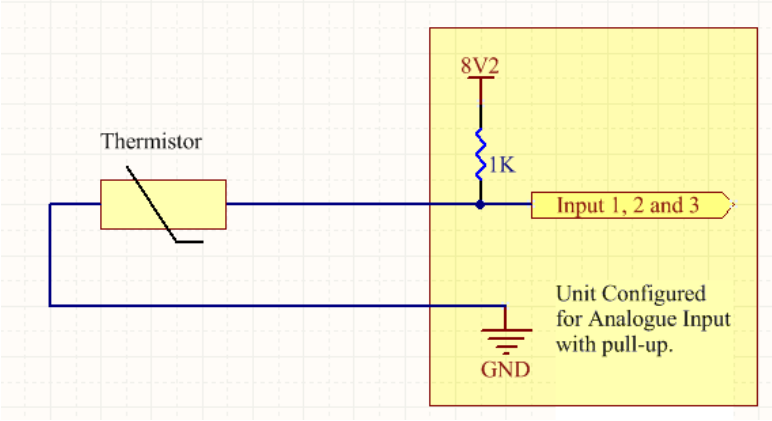
Analogue Sensor with 4 to 20 mA output

Another common type of sensor type is the 4-20 mA current loop sensor. It provides a known current through a fixed resistor, usually 250 ohms thus producing a voltage of 0 v to 5 V 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.



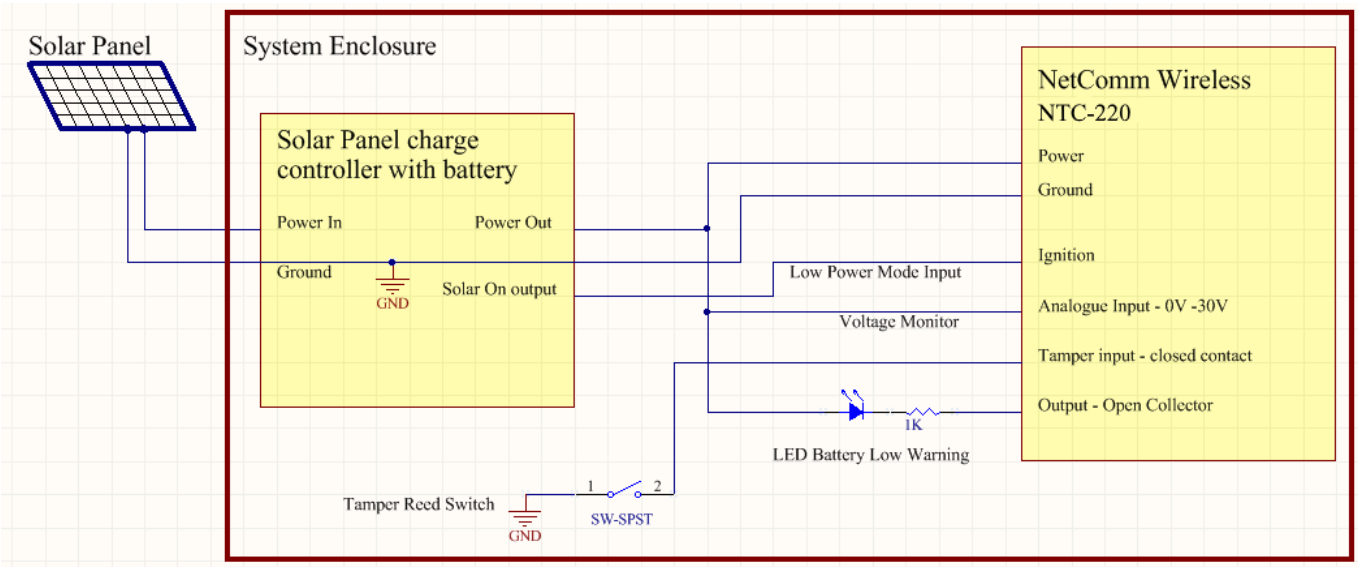
Analogue Sensor with Thermistor

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 1 K resistor activated. The voltage received depends on the combination of resistors and the value of the resistance of the sensor itself.

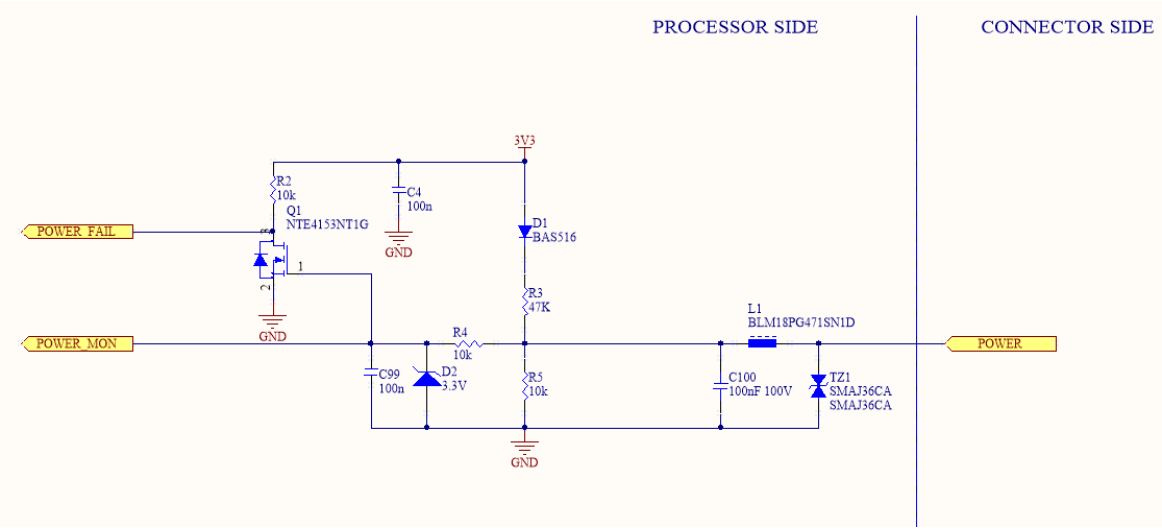


System Example –Solar powered Router with battery backup

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.


Solar Panel
System Enclosure
Solar Panel charge controller with battery
Power In
Power Out
Ground
GND
Solar On output
NetComm Wireless
NTC-220
Power
Ground
Ignition
Low Power Mode Input
Analogue Input - 0V -30V
Voltage Monitor
Tamper input - closed contact
Output - Open Collector
1K
LED Battery Low Warning
Tamper Reed Switch
1
2
SW-SPST
GND

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 0.5 V 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 0.5-3 V 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 3.3 V (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 30 V and clamps to anything above 36 V.

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

Appendix I. NetComm Revision History

This document covers the following products:

NTC-221, NTC-222, NTC-223, NTC-224, NTC-225, & NTC-227

Table J-1 NetComm Revision History

Ver.	Document description	Date
v1.0	First document release	8 November 2018
v1.1	New format and changes to signal strength LED mapping.	11 March 2019
v1.2	Updated signal strength LED mapping, added Appendix F: Serial Port Wiring details.	25 March 2019
v1.3	Added text explaining password on label, firmware signature function and GPS notes.	13 May 2019
v1.4	Added explanation of new Skip button	23 May 2019
v1.5	Corrected signal strength description	29 May 2019
v1.6	Updated Data stream manager description	4 June 2019
v1.7	Corrected Network LED display description	29 July 2019
v1.8	Added supported LWM2M objects	28 April 2020
v1.9	Added single and dual stack IPv6 and IPv4v6 PDP type settings.	10 June 2020
v2.0	Added band options for the NTC-227 to Operator settings description.	10 August 2021
v2.1	Altered contact details in the Open-Source disclaimer	2 December 2021