LANTRONIX®



NTC-500 Series User Guide

NTC-501
NTC-502

Part Number PMD-00315
Revision C October 2026

Intellectual Property

© 2026 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

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

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

Warranty

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

Contacts

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

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

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

Disclaimer

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

Important Notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. Lantronix accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Lantronix NTC-500 Series router 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.

Trademark Notice

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

Revision History

Date	Rev.	Comments
June 2025	A	Reformatted to Lantronix For prior document history, see *Appendix B. NetComm Document History*
August 2026	B	Updated for Firmware Release 2.4 (3.4) which includes the following: • Added 4G LTE neighbouring cell information and 5G NR neighbouring cell information to status page • Added Unlock timer setting to Cell Lock List • Added Active SIM parameter and Auto Enable feature to WAN profile settings • Updated OpenVPN P2P configuration settings • Added Percepxion • Added TR-369 • Added LDAP settings • Added 5G NR extended information details to Field Test Updated compliance information
October 2026	C	Updated for Firmware Release 3.5.0.0 which includes the following: • Added Pairpoint Secure VPN • Added section adding new users

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

Contents

1. Overview 9

Introduction 9

Target audience 9

Prerequisites 9

Notation 9

2. Product introduction 10

Product overview 10

Product features 10

Package contents 10

3. Physical dimensions and indicators 11

Physical dimensions 11

Interfaces 12

LED indicators 13

Signal strength LEDs 14

LED update interval 14

Ethernet port LED indicators 14

4. Placement of the router 15

Antenna installation 15

Mounting options 16

DIN rail mounting bracket 16

DIN rail installation 17

Wall mounted via DIN bracket 17

Ceiling mounted via DIN bracket 18

Pole mounted via DIN bracket 18

Rail mounting adapter 19

5. Installation and configuration of the NTC-500 Series router 20

Powering the router 20

Powering the router 20

DC power via separately purchased DC power supply 20

DC power via field terminated power source 20

Installing the router 21

6. Advanced configuration 22

Initialization 22

Configure as a new device (create new passwords) 23
Logging In 24
7. Status 25
8. Networking 31
Cellular settings 32
SIM security 32
SIM switching 36
Network bands 37
Operator selection 38
Cell lock list 39
WAN profiles 40
5G Network slicing 45
Service assurance 49
LAN settings 50
LAN 50
DHCP 51
VLAN 53
Routing settings 55
Static routes 55
Firewall 57
DMZ 59
Port forwarding 59
Filtering 61
VRRP 64
RIP 67
VPN settings 68
IPSec 68
OpenVPN 72
GRE tunnelling 87
Pairpoint Secure VPN 89
Server Certificate 91
9. Services 93
Network time (NTP) 94
SMS messaging 95
Setup 95

Diagnostics 97
Inbox 110
Compose message 110
Outbox 111
Dynamic DNS 112
DNS server 113
Internet of Things 113
MQTT client 113
Cumulocity agent 117
Remote management 119
OMA-LWM2M 119
SNMP 122
TR-069 124
TR-369 126
Event configuration 129
Notifictaion configuration 129
Destination configuration 130
Event notification log 131
Email Settings 132
Low power mode 134
Percepxion 136
Configuration 136
Connection 1 138
Connection 2 139
10. System 140
Log 140
System log 141
System log settings 141
Diagnostic log 143
IPSec log 145
Watchdog 147
Periodic Ping 147
Periodic Reboot 148
System configuration 149
LDAP Settings 149

Restore factory defaults 150
Web server setting 151
Administration settings 152
Settings backup/restore 154
Site and location settings 155
Runtime configuration 156
SSH key management 156
LED operation mode 159
A/B system configuration 159
Firmware upgrade 160
Upgrading the router firmware 161
Access control 162
Reboot 163
Field test 164
Encrypted debuginfo 166
11. Help 167
Appendix A. Configuring Radio Access Technologies 168
Appendix B. NetComm Document History 169
Appendix C. Compliance Information 170
FCC Compliance 170
FCC Regulations 170
RF Exposure 171
External Antenna 171
IC regulations 171
RF Exposure Information (MPE) 172
External antenna 172
EU Declaration of Conformity 173
UK Declaration of Conformity 179

1. Overview

Introduction

This document provides you all the information you need to set up, configure, and use the Lantronix NTC-500 Series router.

Target audience

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

Prerequisites

Before continuing with the installation of your NTC-500 Series router, please confirm that you have the following:

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

Notation

The following symbols may be used in this document:

Note: *This note contains useful information.*

Important: *This is important information that may require your attention.*

Warning: *This is a warning that may require immediate action to avoid damage or injury.*

2. Product introduction

Product overview

The NTC-500 Series router is a high-end high-speed industrial-grade 5G router. Designed with critical and complex applications in mind, it provides ultra-reliable, high bandwidth throughput even in extremely harsh environments.

The NTC-500 Series router supports the latest 3GPP Release 16 5G features including 5G Non-standalone (NSA), 5G Standalone (SA) and 5G Slicing which enables complex end-to-end, on-demand quality of service solutions in partnership with leading carrier networks.

Perfect for connected smart building systems, vending and ticketing machines, digital signs, surveillance systems, traffic light control, and remote vehicle automation.

Product features

- 5G Standalone (SA)
- 5G Non-Standalone (NSA) with failover to 4G
- 2.5GbE Ethernet Port
- Robust ruggedized industrial-grade metal housing with multiple mounting options
- Wide operating temperature range
- Designed, assembled and tested for unmanned locations in extreme environments
- Easy and clear LED status display for connection status and network type as well as two user-customizable LEDs.
- Remote device configuration, management, and firmware upgrade.

Package contents

The Lantronix NTC-500 Series package contains:

- 1 x NTC-500 Series router
- 1 x Two-way terminal block connector
- 1 x 1.5m Ethernet cable
- 1 x DIN rail mounting bracket
- 1 x Welcome Card

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

3. Physical dimensions and indicators

Physical dimensions



Figure 3-1 NTC-500 Series router top and side views

Table 3-1 Router Dimensions

NTC-500 SERIES ROUTER DIMENSIONS	
Length	143.5 mm
Depth	110.5 mm
Height	30.0 mm
Weight	410 grams

Interfaces

The following interfaces are available on the NTC-500 Series router:

Table 3-2 Interfaces

ITEM	DESCRIPTION
Antenna sockets	SMA female connectors for cellular antennas.
SIM card tray	Insert SIM card here.
SIM Eject button	Press with a SIM removal tool to eject the SIM card tray.
Two-way terminal block connector	Connect power supply here. Power from a DC power supply may be terminated on terminal block connector and then insert the connector into the terminal block socket on the router. Refer to the diagram and table under the *Installation* section for correct wiring of the terminal block. Operates in the 8-40V DC range.
Factory reset button	Press and hold for less than 5 seconds to reboot to normal mode. The LEDs are green and extinguish in sequence to indicate that the router will reboot normally if the button is released during this period. Press and hold for 5 to 10 seconds to reboot to another partition for recovery purpose. The LEDs are amber and extinguish in sequence to indicate that the router will load the recovery image. Press and hold for 10 to 15 seconds to reset the router to factory default settings. The LEDs are red and extinguish in sequence to indicate that the router will reset to factory default settings if the button is released during this period.
2.5GbE RJ45 Ethernet port	Connect one or several devices via a network switch here.
USB-C port	Provides USB connectivity for debugging.

LED indicators

The NTC-500 Series router uses nine LEDs to display the current system and connection status.

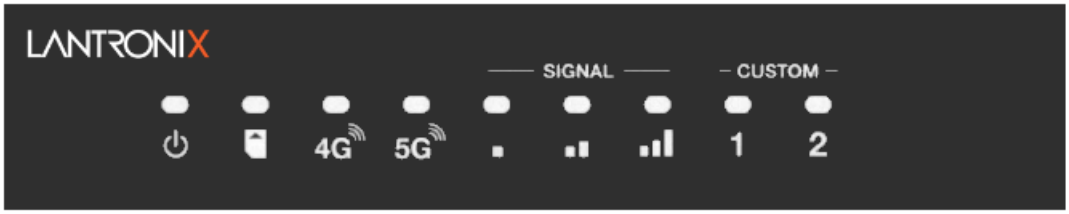


Figure 3-2 LED indicators

Table 3-3 LED indicators description

LED	NAME	COLOUR	STATE	DESCRIPTION
	Power		Off	Power off
			Blinking	Router starting up
			On	Power on
	SIM		Off	No SIM detected
			Blinking	SIM error
			On	SIM installed and working
4G	4G Network		Off	No 4G connection
			Blinking	Connecting to 4G network
			On	4G connected
5G	5G Network		Off	No 5G connection
			Blinking	Connecting to 5G network
			On	5G connected
SIGNAL	Signal Strength		Off	No signal
			One Lit	Poor signal
			Two Lit	Fair signal
			Three Lit	Good signal
CUSTOM	Custom 1	Customizable		Programmable LED for custom use
CUSTOM	Custom 2	Customizable		Programmable LED for custom use

Signal strength LEDs

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

Table 3-4 Signal strength of LED indicators

NUMBER OF LIT LEDS	SIGNAL STRENGTH
All LEDs unlit	No signal
1	> -90 dBm
2	-70 dBm to -90 dBm
3	< -70dBm

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-500 Series router has two LED indicators.

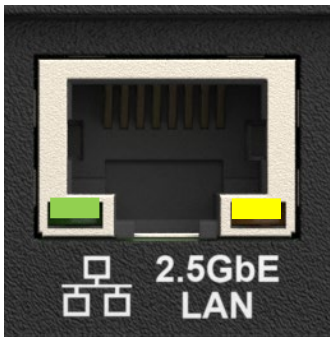


Figure 3-3 NTC-500 Series Ethernet port LED indicators

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

Table 3-5 Ethernet port LED indicators description

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

4. Placement of the router

Antenna installation

The router is fitted with four SMA female cellular antenna connectors. Attach antennas fitted with a SMA male connector by turning them in a clockwise direction.



Figure 4-1 NTC-500 Series router antenna installation

Connecting antennas to the device should provide optimum cellular 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.*

For best performance, position the antennas as shown in the following diagram.



Figure 4-2 NTC-500 Series router optimal antenna positioning

Mounting options

The NTC-500 Series router can be quickly and easily mounted in a variety of locations.

DIN rail mounting bracket

The DIN rail mounting bracket provides multiple ways to mount the router. Clip the router into the bracket as shown below.

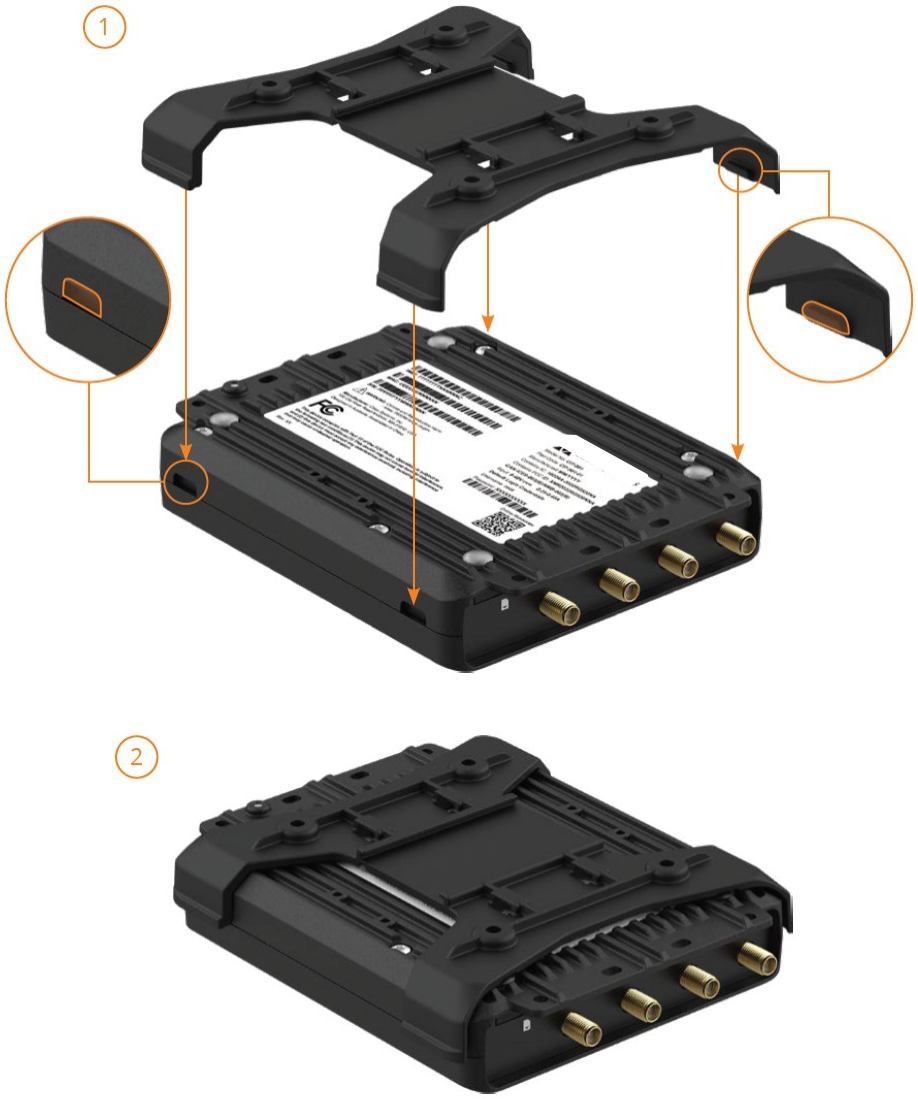


Figure 4-3 NTC-500 Series router DIN mounting bracket

DIN rail installation

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

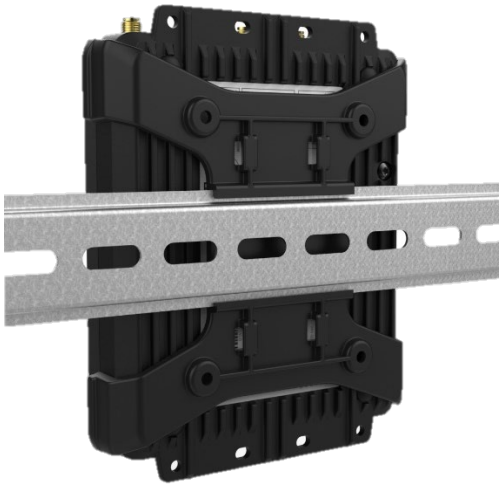


Figure 4-4 NTC-500 Series router DIN mounting bracket

Wall mounted via DIN bracket

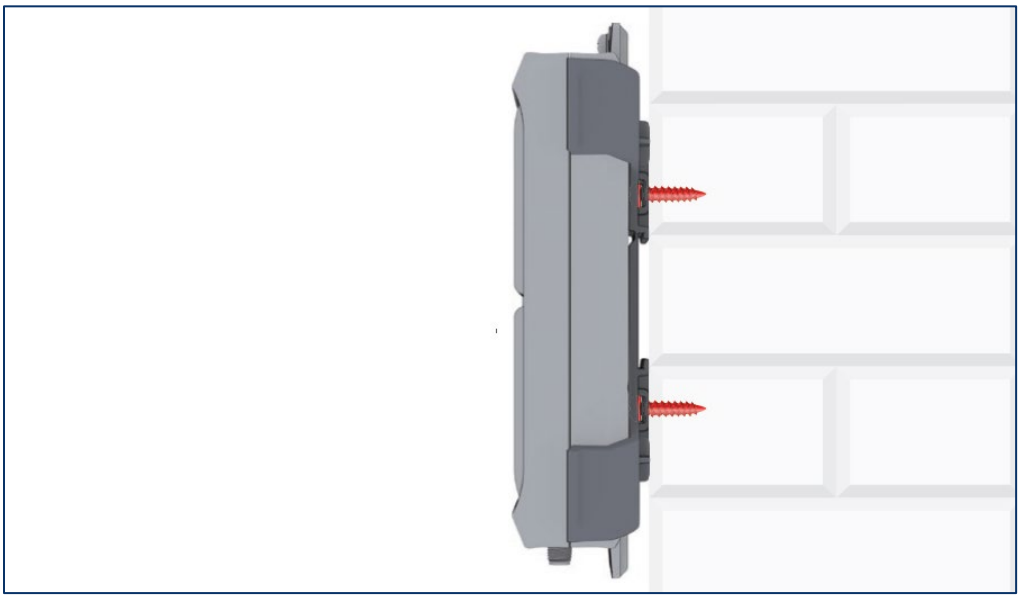


Figure 4-5 NTC-500 Series router wall mounted using DIN bracket

Ceiling mounted via DIN bracket

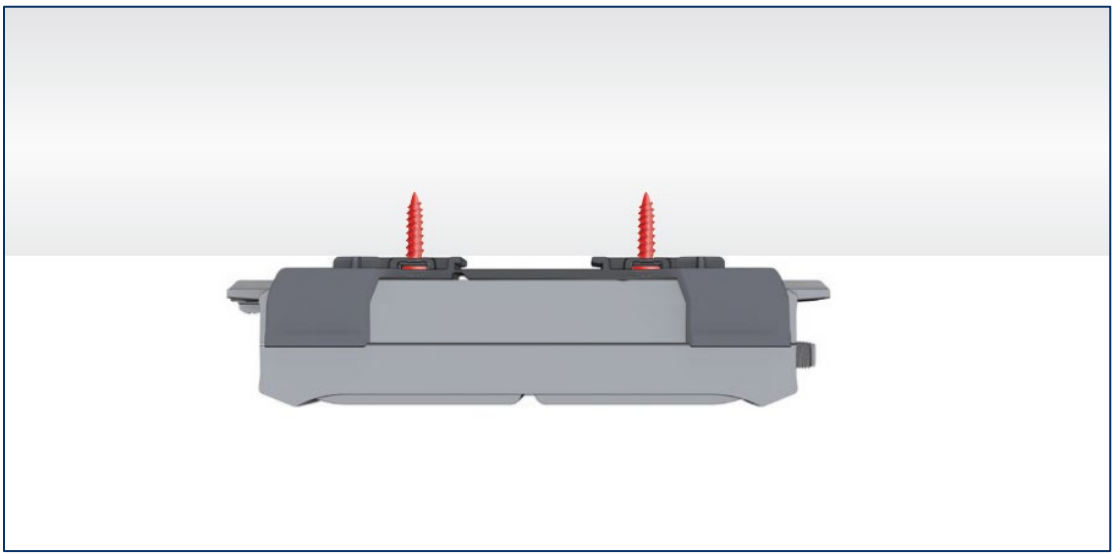


Figure 4-6 NTC-500 Series router ceiling mounted using DIN bracket

Pole mounted via DIN bracket

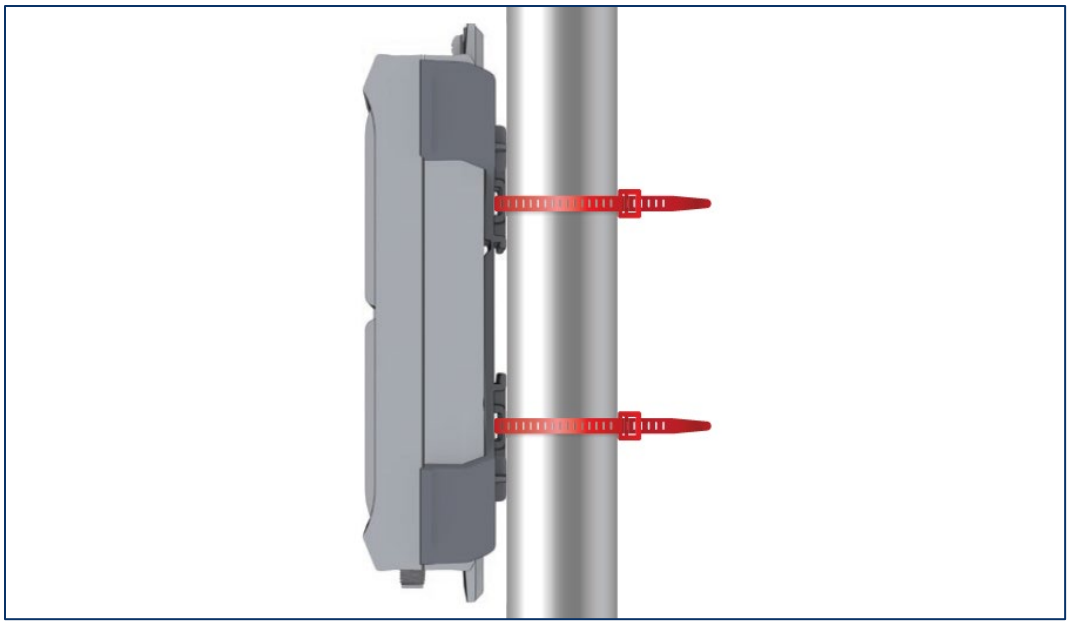


Figure 4-7 NTC-500 Series router pole mounted using DIN bracket

Rail mounting adapter

The NTC-500 Series router can also be mounted by using an optional rail mount adapter.



Figure 4-8 NTC-500 Series router rail mount adapter

5. Installation and configuration of the NTC-500 Series router

Powering the router

Powering the router

The NTC-502 router can be powered in one of two ways:

- DC power input via separately purchased DC power supply (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 separately purchased DC power supply

The positive and ground terminals on the 2-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 connector from the socket. 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 connector as shown below noting the polarity of the wires and then use a flathead screwdriver to raise the cage clamp to secure the wires. Insert the wired terminal block connector into the terminal block socket of the router and then connect the adapter to a wall socket.

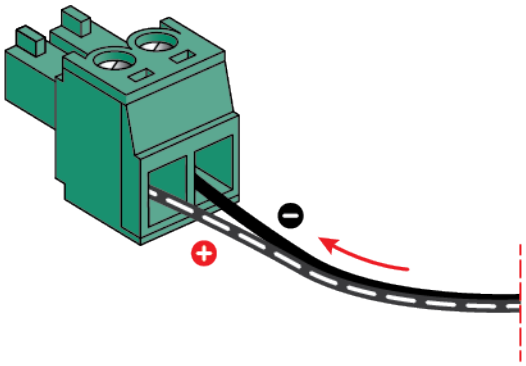


Figure 5-1 Terminal block wiring diagram



Figure 5-2 Terminal Block pinout

DC power via field terminated power source

If an existing 8-40 V DC power supply is available, you can insert the wires into the supplied terminal block connector to power your router. Use a flathead screwdriver to tighten the terminal block connector screws and

secure the power wires, making sure the polarity of the wires is correctly matched as shown above. You should avoid using DC cables greater than 2 metres in length.

Table 5-1 Locking power block pin outs

Terminal	Description
+	Positive wire for power.
–	Ground wire.

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-500 Series router. You can connect one device directly, or several devices using a network switch.
2. If you are attaching antennas, first remove the antenna socket caps from the Main and Auxiliary antenna sockets by turning them in an anti-clockwise direction, then screw the antennas onto the sockets by turning them in a clockwise direction.
3. If your router does not come with a SIM pre-installed, insert a SIM card into the SIM card slot by pressing the SIM Eject button to eject the SIM card tray. Place the SIM card in the tray and then insert the loaded tray into the SIM slot with the gold side facing up.
4. Ensure the external power source is switched on and wait 2 minutes for your NTC-500 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

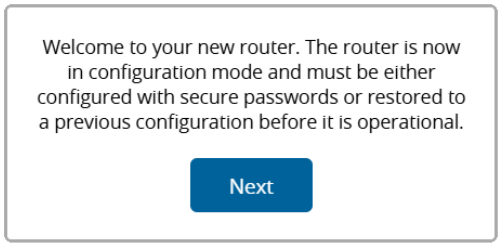
To access the web-based user interface, open a web browser (e.g. Mozilla Firefox or Google Chrome), type **https://192.168.1.1** into the address bar and press **Enter**.

The router's web user interface is displayed.

Important: *The HTTP protocol is disabled. Secure HTTP (HTTPS) is the default protocol.*

Initialization

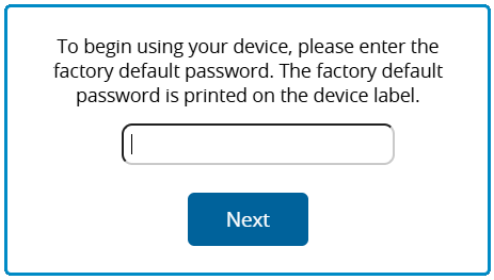
The first time the device is booted (or booted after a factory reset), the device enters Configuration mode. The below prompt displays.



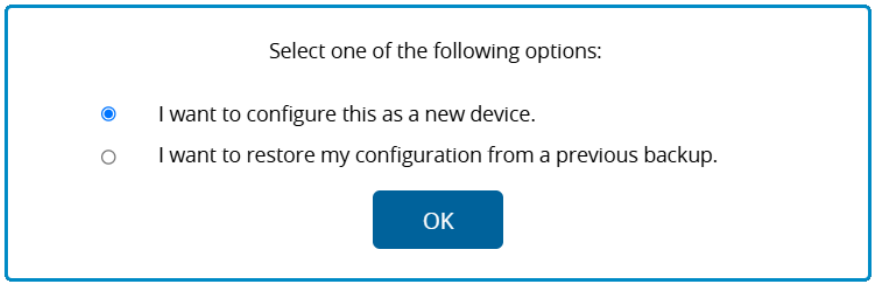
In Configuration mode, the router runs a setup wizard. Once you complete the setup wizard the router will boot into Live mode. This is a security feature which enables you to configure the router as a new device and set strong passwords for web root, web user, and Telnet/SSH access or restore configuration from a previous backup file.

To complete the setup:

1. Click the **Next** button in the configuration mode window. The below prompt displays.



2. Enter the factory default password printed on the device label and click **Next**, the below dialogue box displays.



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 **OK**.

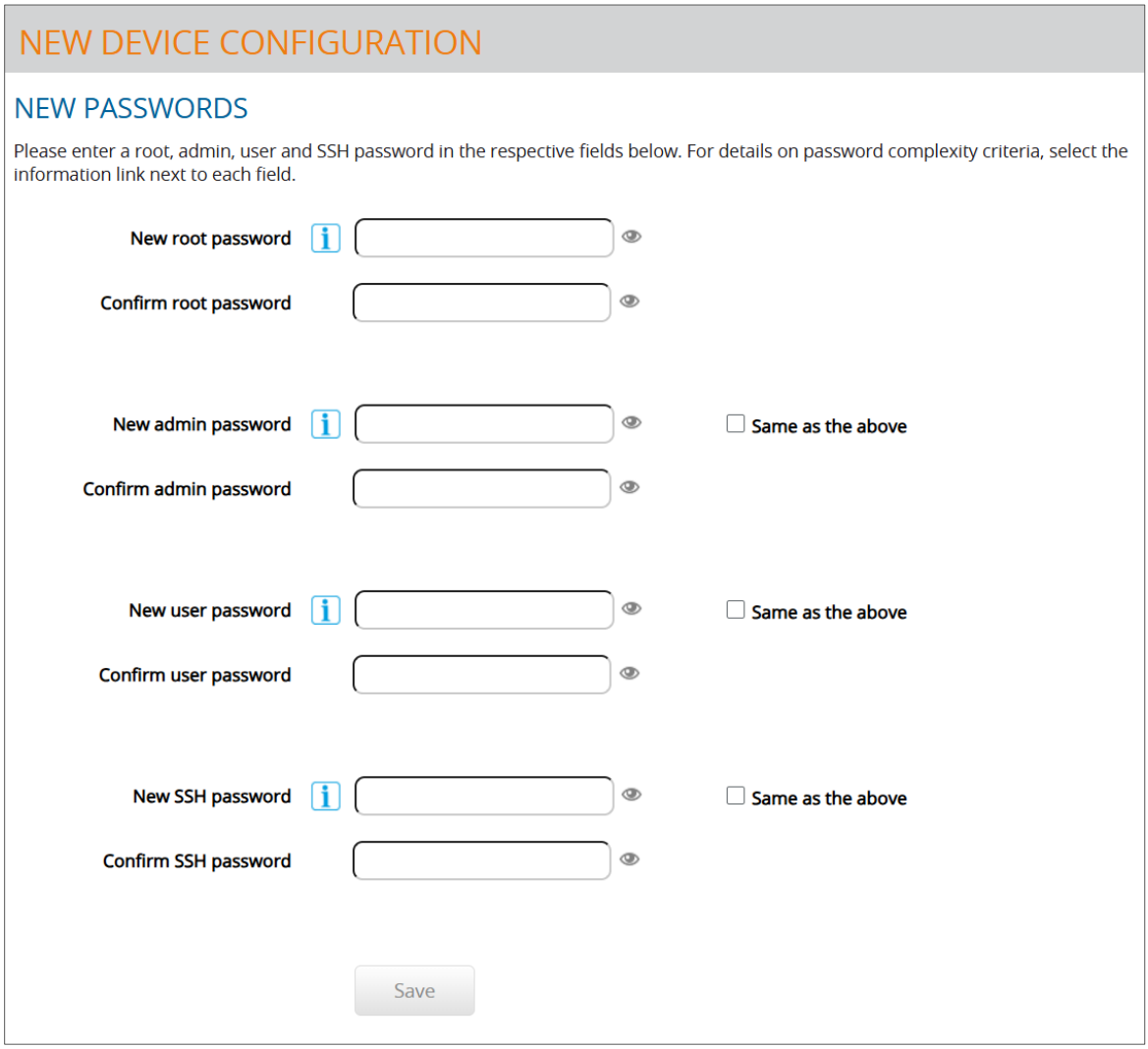


Figure 6-1 New device configuration

In the New Passwords section, enter a strong password in the **New root password** field and re-enter the password in the **Confirm root password** field. Similarly, configure passwords for the other users. You can click the **Same as above** checkbox for the password fields of a user to use the same passwords set for the above user. You may configure the same password for all accounts, but it must meet the following security requirements:

- The password must be a minimum of eight characters and no more than 128 characters in length.
- The password must contain at least one upper case, one lower case character, and one number.
- The password must contain at least one special character, such as: ` ~ ! @ # $ % ^ & * ( ) - _ = + [{] } \ | ; : ' " , < > / ?
    - Additionally, the password must satisfy an algorithm which analyses the characters as you type them, searching for commonly used patterns, passwords, names, and surnames according to US census data, popular English words from Wikipedia, US television, movies, and other common patterns such as dates, repeated characters (aaa), sequences (abcd), keyboard patterns (qwertyuiop), and substitution of numbers for letters.

  Click the ⓘ icon for each password field to display the password criteria.

When you have completed all password fields, click the **Save** button. If the passwords meet the security criteria, they are saved and the router reboots to Live mode automatically and the login page displays.

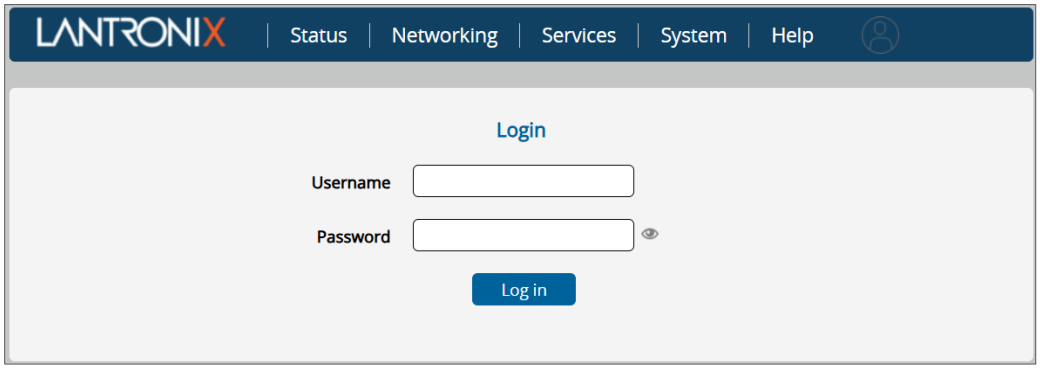


Figure 6-2 Login page for web-based user interface

Logging In

To log in to the router, enter the login username (root or user) and the corresponding password that you configured during the initialisation process.

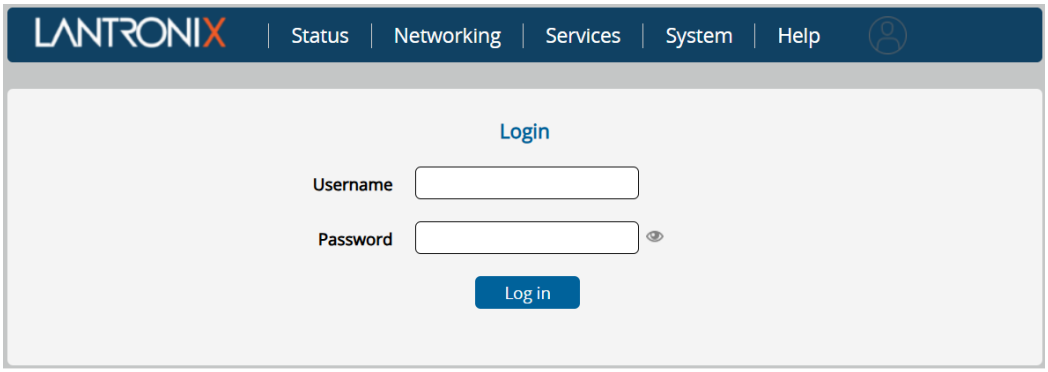


Figure 6-3 Login page for web-based user interface

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

7. Status

The Status page displays a summary of the currently configured details for the following:

- System Information
- LAN
- Cellular Connection Status
- WWAN Connections Status
- Advanced status
- 4G LTE Neighbouring Cell Information
- 5G NR Neighbouring Cell Information

The Status page is displayed when you log into the NTC-500 Series router web interface after initialization or reboot. When using the web interface, you can click **Status** tab on the top menu bar to access the Status page. On the Status page click each section tab to show or hide the details in that section. New sections are added to the Status page for additional software features when enabled (e.g. VPN connectivity).

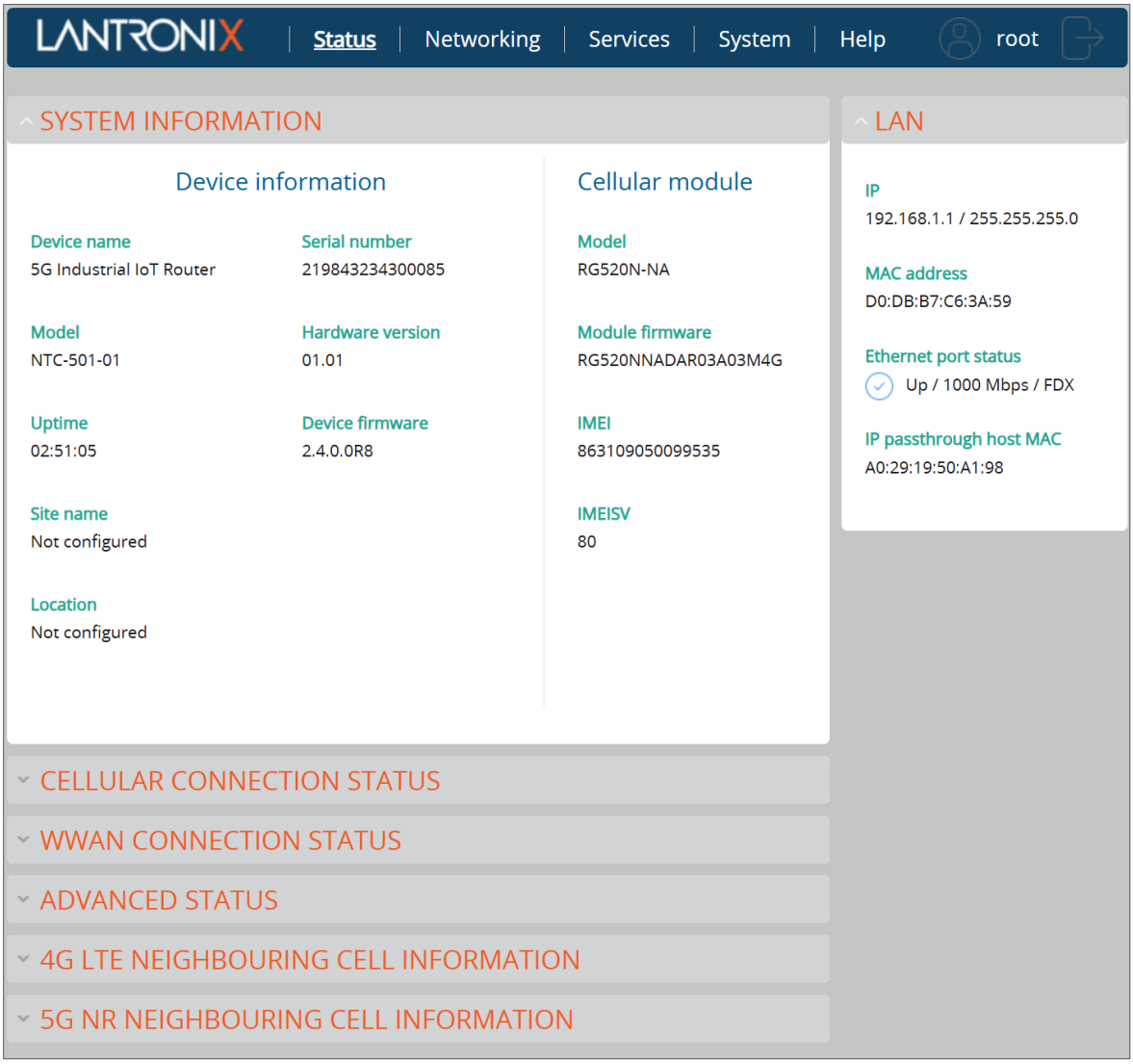


Figure 7-1 NTC-500 Series router status page

Table 7-1 Status page item details

Item	Definition
System information	
Device name	The device name of the NTC-500 Series router
Model	The commercial product name which helps to identify the available features of the router
Uptime	The current up time (the time since the router was last turned on) of the router
Site name	The configured site name
Location	The configured location
Serial number	The serial number of the router
Hardware version	The hardware version of the router
Device firmware	The current firmware version of the router
Model	The model of the cellular module
Module firmware	The current firmware version of the cellular module
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device
IMEISV	International Mobile Equipment Identity and Software Version. A 16-digit identifier that uniquely identifies the mobile device and its software version. Only two digits are displayed, which are the last two digits of the IMEISV and represent its software component
LAN	
IP	The IP address and subnet mask of the router
MAC address	The MAC address of the router
Ethernet Port Status	Displays the current status of the LAN port and its operating speed
IP passthrough host MAC	The MAC address associated with the passthrough host when IP passthrough is enabled
Cellular Connection Status	
SIM status	Displays the SIM status of the router. It shows if a SIM is inserted and whether it is active
Signal strength (dBm)	The current signal strength measured in dBm
Network registration status	It shows if the SIM is registered on the network

Item	Definition
Operator selection	The mode used to select an operator network
Provider	The operator of the network on which the device is currently registered
Roaming status	The roaming status of the current network in use
Enabled bands	The bands to which the NTC-500 Series router may connect
Current band	The band used by the NTC-500 Series router
Connection (RAT)	The Radio Access Technology in use
Coverage	The mobile network in use
Service options	The type of cellular service or radio technology currently in use
WWAN Connection Status	
Profile	The name of the active profile.
APN	The Access Point Name currently in use, if manually entered by you. **Auto-assigned** is displayed if the APN is assigned by the network
Connection uptime	The duration of the current mobile connection session
Default profile	Indicates whether the current profile in use is the default profile
IPv4 status	The IPv4 connection status of the active profile
IPv4 WWAN	The IPv4 address assigned by the mobile broadband carrier network
IPv4 DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection
IPv4 MTU	The current IPv4 Maximum Transmission Unit (MTU) of the WWAN connection
IPv6 status	The IPv6 connection status of the active profile
IPv6 WWAN	The IPv6 address assigned by the mobile broadband carrier network
IPv6 DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection
IPv6 MTU	The current IPv6 Maximum Transmission Unit of the WWAN connection
Advanced Status	
Mobile country code	The Mobile Country Code (MCC) of the NTC-500 Series router
Mobile network code	The Mobile Network Code (MNC) of the NTC-500 Series router
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the NTC-500 Series router, a unique number up to 19 digits in length
IMSI	The International Mobile Subscriber Identity, a unique identifier of the user of a cellular network

Item	Definition
Packet service status	Displays whether the packet service is attached or detached. When APN or username/password is changed, the device detaches and reattaches to the network
ECGI	E-UTRAN Cell Global Identifier. The globally unique identity of a cell in E-UTRA. The ECGI concatenates the PLMN-Id and the ECI (E-UTRAN Cell Identifier) The ECI concatenates the eNodeB ID and the Cell ID
eNodeB	Also known as the Evolved Node B, this is the hardware element in the LTE network that communicates directly with mobile devices
Cell ID	A unique code that identifies the base station from within the location area of the current mobile LTE network signal
PCI	Physical Cell ID of the LTE Cell
Channel number (EARFCN)	The channel number of the current cellular connection
Reference Signal Received Power (RSRP)	A cell-specific reference signal used to determine RSRP
Reference Signal Received Quality (RSRQ)	RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by N x RSRP / RSSI where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured
Signal to interference plus noise ratio (SINR)	The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise
CQI	Channel Quality Indicator. This is a value between 1 and 15 with 15 being the highest rating
NCGI	NR Cell Global Identifier. This concatenates the PLMN-Id (PLMN Identifier) and the 36bit NCI (NR Cell Identity). This information is not available when the device is operating in LTE or 5G Non-Standalone mode
gNodeB	The gNodeB (gNB) is the term given to network equipment that transmits and receives wireless communication between UE and a mobile network
gNB Cell ID	A unique code that identifies the base station from within the location area of the current mobile 5G network signal. This is not available when the device is operating in LTE or 5G Non-Standalone mode
gNB PCI	Physical Cell ID of the 5G NR Cell
Channel number (NR ARFCN)	The channel number of the current 5G cellular connection

Item	Definition
SSB Channel Number (SSB ARFCN)	The Synchronization Signal Block (SSB) channel number of the current 5G cellular connection
Subcarrier spacing (SCS)	The size of the current Subcarrier Spacing (SCS) expressed in KHz
Reference Signal Received Power (SS-RSRP)	Synchronization Signal Reference Signal Received Power (SS-RSRP). The linear average over the power contributions (in Watts) of the resource elements that carry Secondary Synchronization Signal (SSS)
Reference Signal Received Quality (SS-RSRQ)	Secondary Synchronization Signal Reference Signal Received Quality. SS-RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by N x SS-RSRP / NR carrier RSSI where N is the number of Physical Resources Blocks (PRBs) over which the NR RSSI is measured
Signal to interference plus noise ratio (SS-SINR)	Synchronization Signal – Signal to Interference plus Noise Ratio. The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise
NR CQI	The 5G NR Channel Quality Indicator (CQI)
Synchronization Signal Block (SSB) Index	This is a key part of beam management. It is a value comprising of Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS) and the Physical Broadcast Channel (PBCH).
4G LTE Neighbouring cell information	
PCI	The Physical Cell ID.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency
RSRP	Reference Signal Received Power (RSRP)
RSRQ	Reference Signal Received Quality (RSRQ)
RAT	The Radio Access Technology in use
5G NR Neighbouring Cell Information	
PCI	The Physical Cell ID
NR ARFCN	NR Absolute Radio Frequency Channel Number
SS-RSRP	Synchronization Signal Reference Signal Received Power
SS-RSRQ	Secondary Synchronization Signal Reference Signal Received Quality
Type	The type of neighbouring cell
Role	Displays the function of the neighbouring cell in relation to the current connection (for example, serving or neighbouring cell)

Item	Definition
SSB ARFCN	The Synchronization Signal Block Absolute Radio Frequency Channel Number of the current 5G cellular connection
RAT	The Radio Access Technology in use

8. Networking

The Networking page allows you to access and configure the following features:

- Cellular settings
- LAN settings
- Routing Settings
- VPN settings

To access the Networking page, click **Networking** tab on the top menu bar.

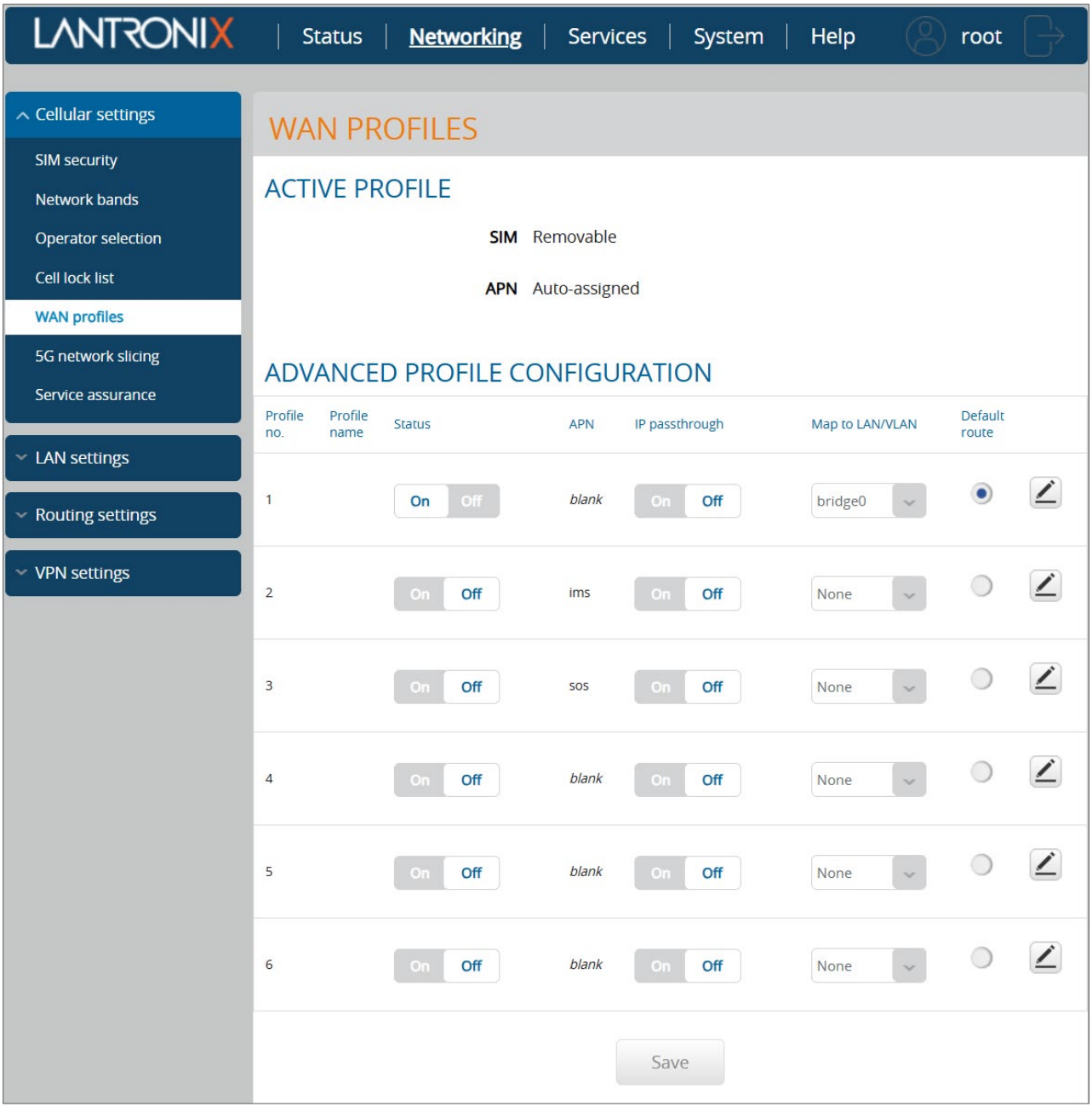


Figure 8-1 Networking page

Cellular settings

SIM security

SIM security allows you to manage the PIN settings of the of the SIM, if the SIM is PIN enabled. To access the SIM security page, navigate to **Networking > Wireless WAN > SIM security**.

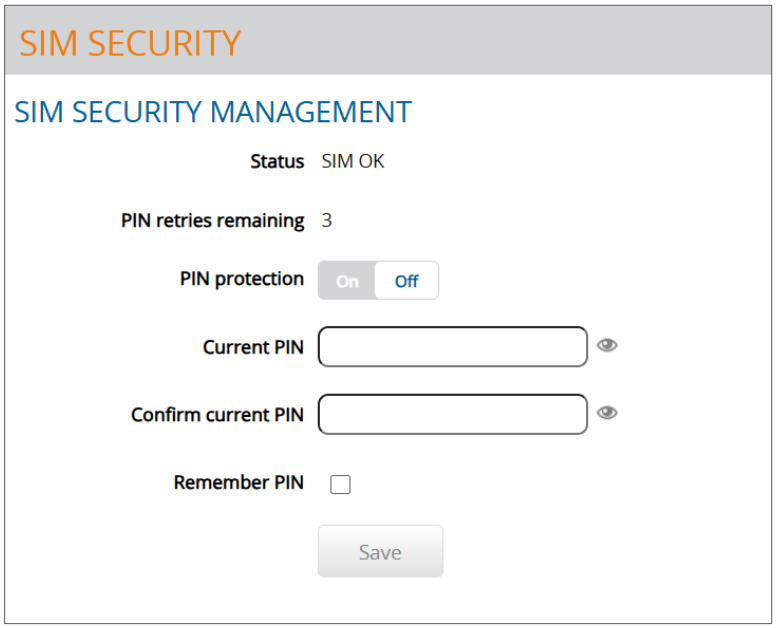


Figure 8-2 SIM security page

To enable PIN protection, set **PIN protection** to **ON**, enter the PIN in the **Current PIN** and **Confirm current PIN** fields and click **Save**. Once SIM protection is enabled the SIM security page displays with **Change PIN** button.

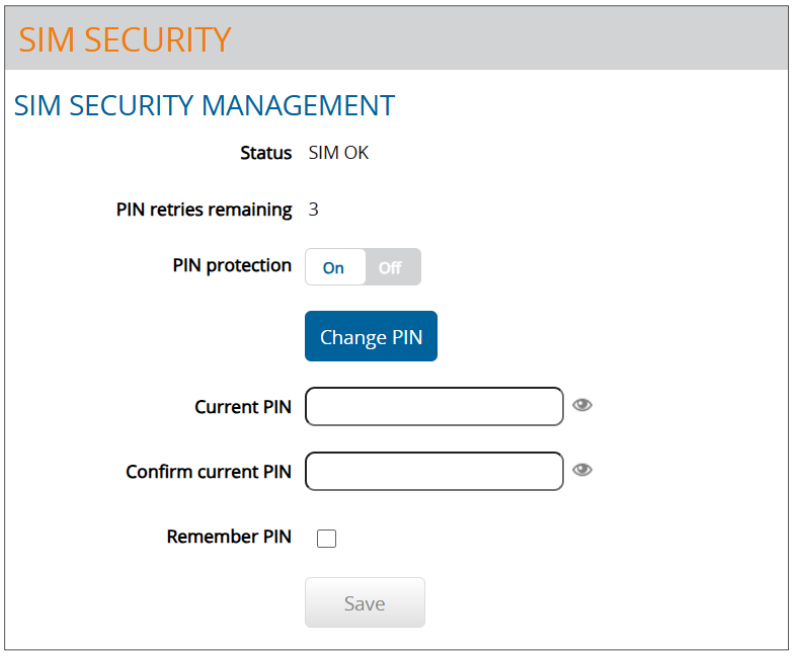


Figure 8-3 SIM security page after enabling PIN protection

When SIM protection is enabled, each time you log into the router after a reboot you will be directed to the SIM security page.

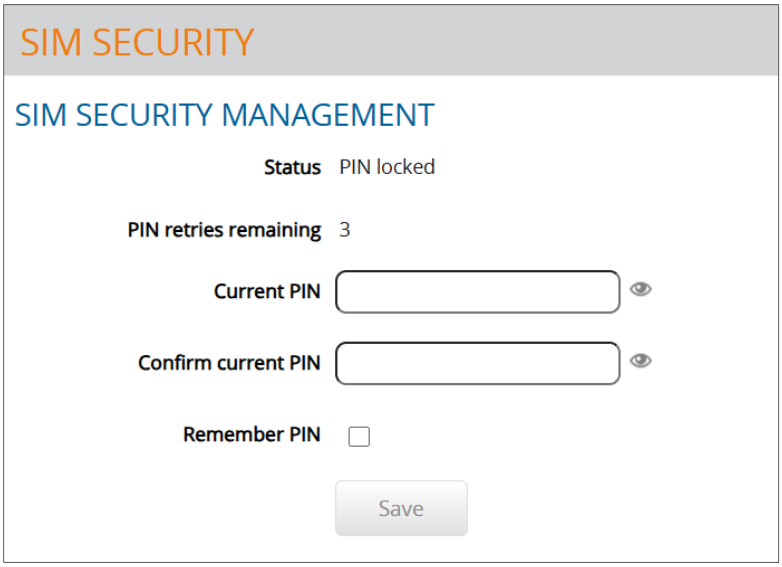


Figure 8-4 SIM security page when SIM is PIN locked

To unlock the SIM, enter the PIN in **Current PIN** and **Confirm Current PIN** fields and click **Save**. Once the SIM is successfully unlocked, click **OK** at the prompt and the Web UI login page displays as you are required to log in again. Enter the credentials and log into the router. The SIM security page displays.

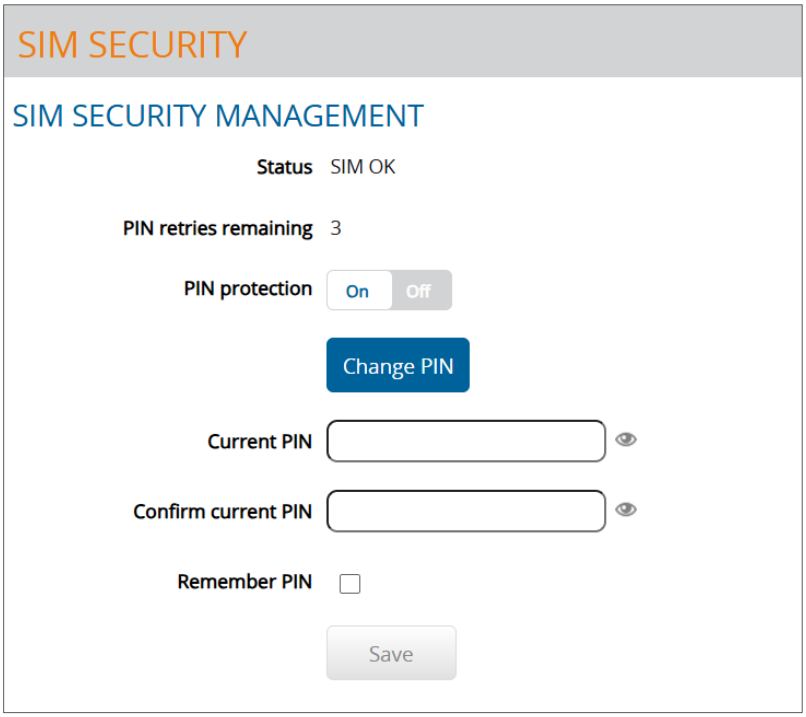


Figure 8-5 SIM security page after SIM is unlocked

Once unlocked, you can disable PIN protection, if you do not wish to have access locked by a PIN. To disable PIN protection set **PIN protection** to **OFF**, enter the PIN number in the **Current PIN** and **Confirm current PIN** fields and click **Save**.

If you are placing the router in a remote, unattended location, you can check **Remember PIN** option to enable it. 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 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.

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

SIM PUK Lock

If you enter the wrong PIN three times the SIM gets Personal Unblocking Key (PUK) locked.

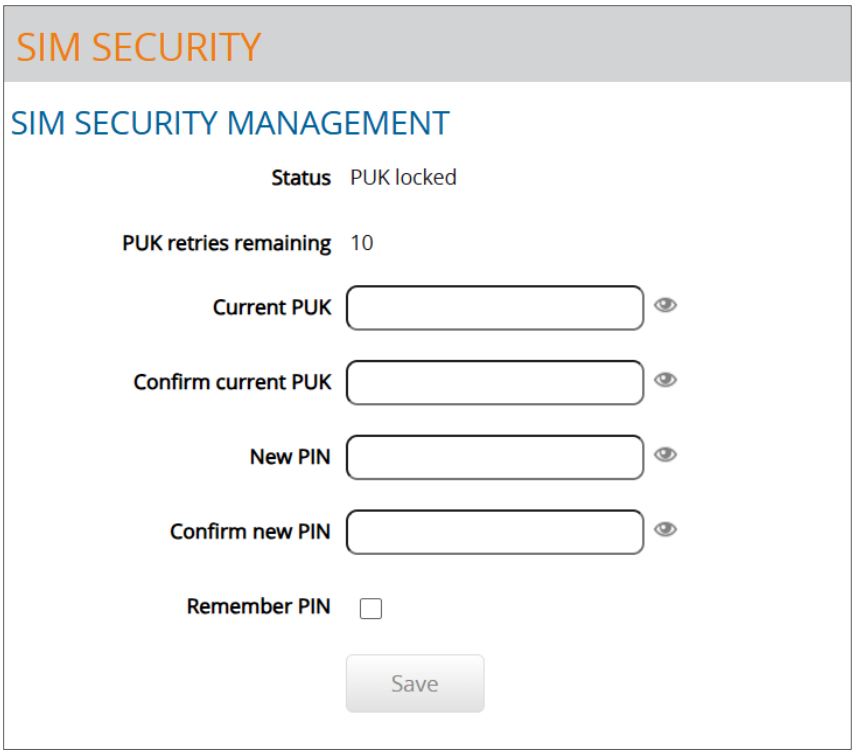


Figure 8-6 SIM security page when SIM is PUK locked

To unlock the PUK locked SIM, you have to request your service provider for a PUK code. Once you have the PUK code, enter it in the **Current PUK** and **Confirm current PUK** fields, enter a new PIN in the **New PIN** and **Confirm new PIN** fields, and then click **Save**. Once the SIM is successfully unlocked, click **OK** at the prompt and the Web UI login page displays as you are required to login again. Enter the credentials and log into the router. The SIM security page displays.

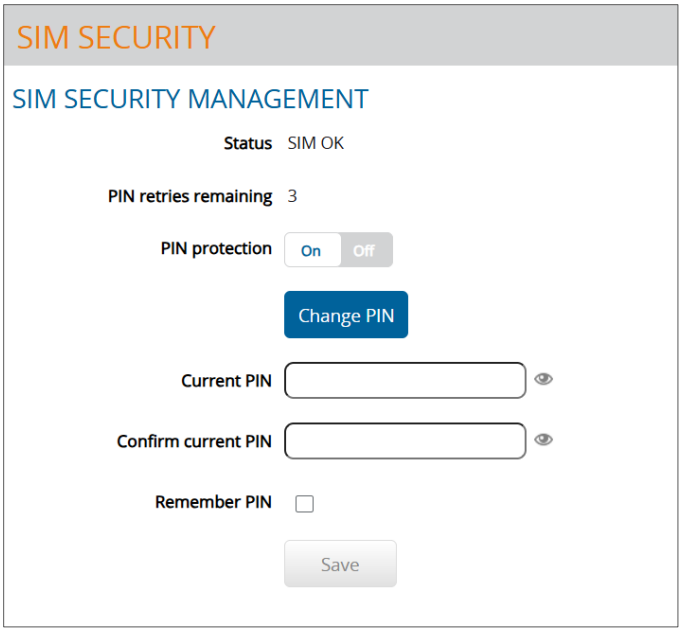


Figure 8-7 SIM security page when SIM is PUK unlocked

Changing SIM PIN

To change the PIN of the SIM:

1. Click **Change PIN**, the PIN settings page displays with **New PIN** and **Confirm new PIN** fields.

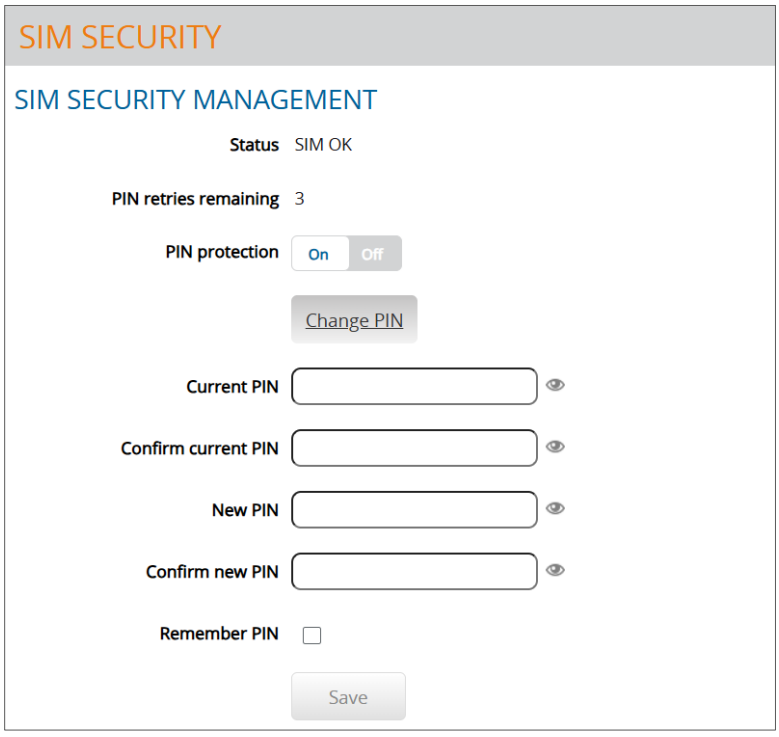


Figure 8-8 SIM security page when changing PIN

2. Enter the current PIN in **Current PIN** and **Confirm current PIN** fields.
3. Enter the new PIN in **New PIN** and **Confirm new PIN** fields.
4. Click **Save** to save and apply the settings.

SIM switching

Note: *SIM switching menu item is displayed in the Cellular settings section only when an internal (embedded) SIM is installed.*

The NTC-500 Series router is equipped with both a removable and an internal SIM. To configure and switch between the two SIMs, the SIM switching page is used. The SIM switching page also provides several failover options to switch between the SIM cards.

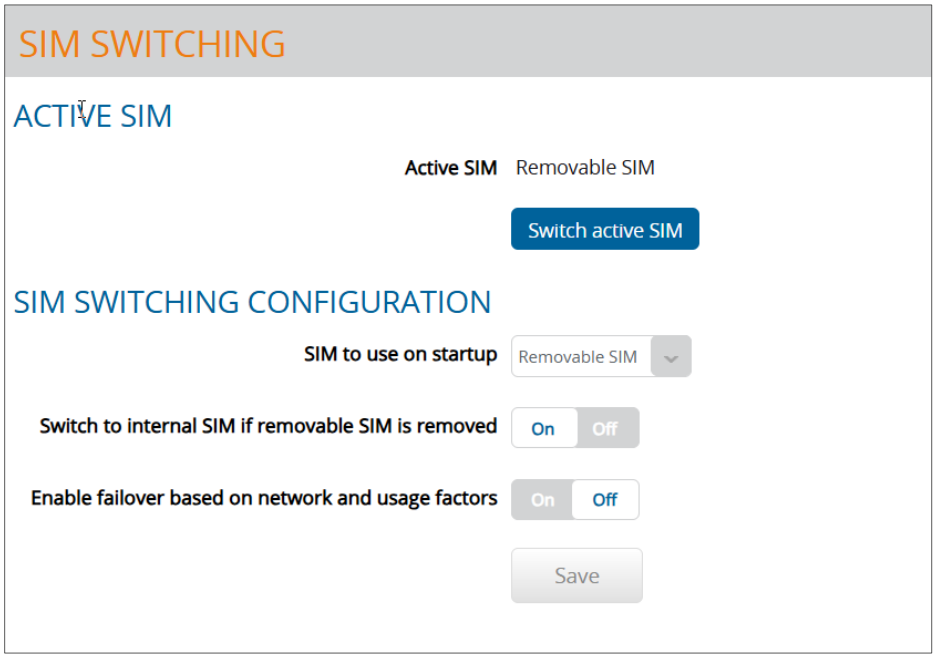


Figure 8-9 SIM switching page

Active SIM

Active SIM displays the SIM that is currently in use. To change the **Active SIM** from Internal SIM to Removable SIM or vice-versa click Switch active SIM and then click **Yes** at the prompt.

SIM Switching Configuration

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

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

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

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

Network bands

Network bands allows you to select individual bands from the following band groupings:

- 4G LTE
- 5G NR NSA
- 5G NR SA

To access Network bands page, navigate to **Networking > Cellular settings > Network bands**.

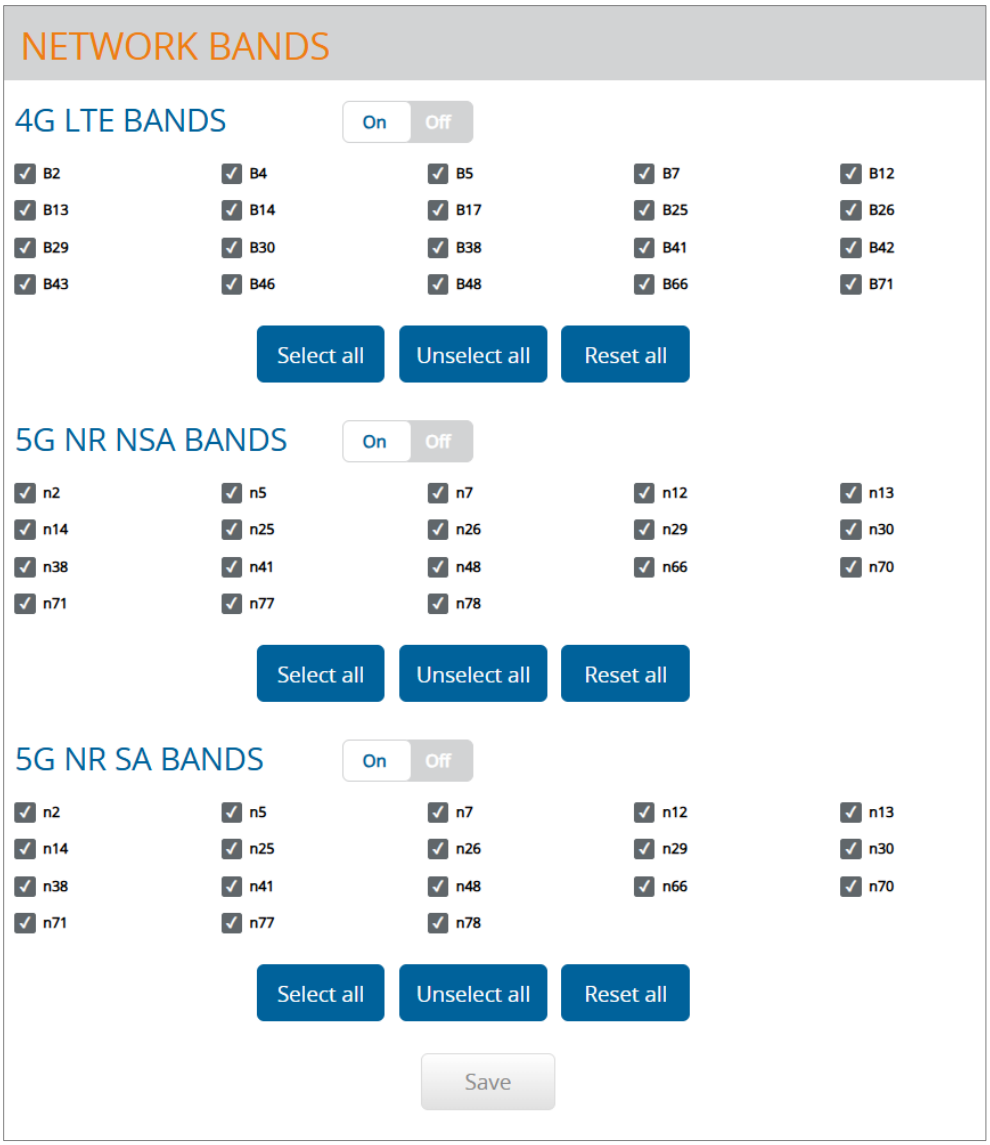


Figure 8-10 Network bands

To set a device up for different 4G LTE, 5G non-standalone (5G NR NSA) and 5G Standalone (5G NR SA) modes, refer to *Appendix A. Configuring Radio Access Technologies*.

Operator selection

Operator selection allows you to configure how the NTC-500 Series router selects the operator, whether automatically or manually. If you set it to manual, you can override and lock it to a particular carrier or access technology. The Operator selection page also contains roaming controls. To access Operator selection page, navigate to **Networking > Cellular settings > Operator selection**.

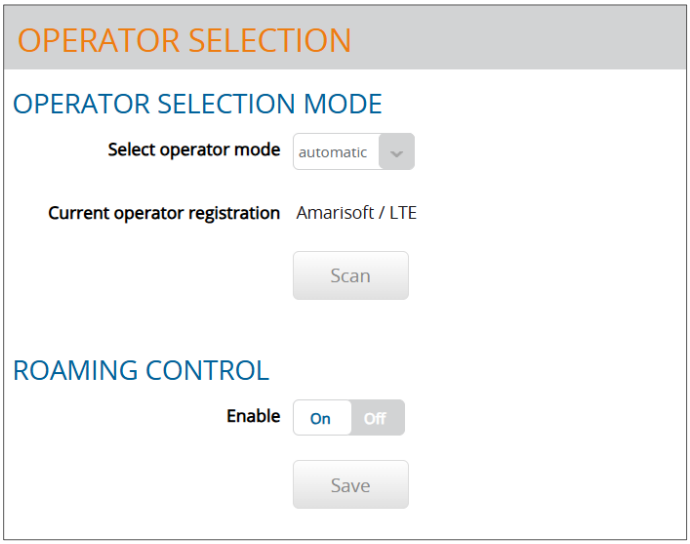


Figure 8-11 Operator selection page

Operator selection mode

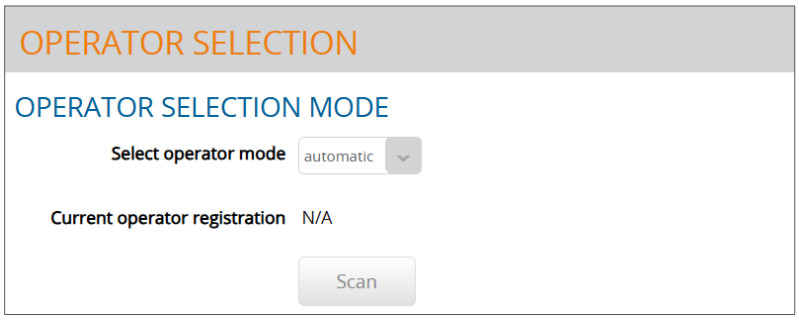


Figure 8-12 Operator selection mode

To scan for available networks, set the **Select operator mode** 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.

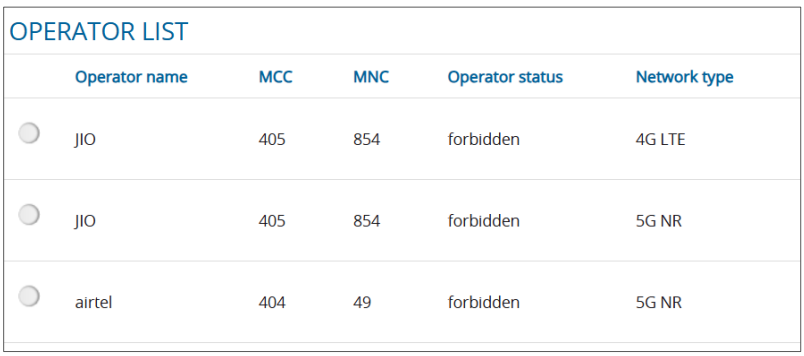


Figure 8-13 Operator list

Select the most appropriate service from the list shown and Click **Save** to connect to the service.

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

Roaming control

The roaming control function allows roaming to be enabled or disabled on the NTC-500 Series router. Enable roaming by setting the **Enable** toggle to **On**, then select **Save.**



Figure 8-14 Roaming control

Cell lock list

The Cell lock list allows you to specify a list of cells that the NTC-500 Series router will not deviate from. The cells are separated on the basis of LTE and NR5G networks. To access Cell lock list page, navigate to **Networking > Cellular settings > Cell lock list**.

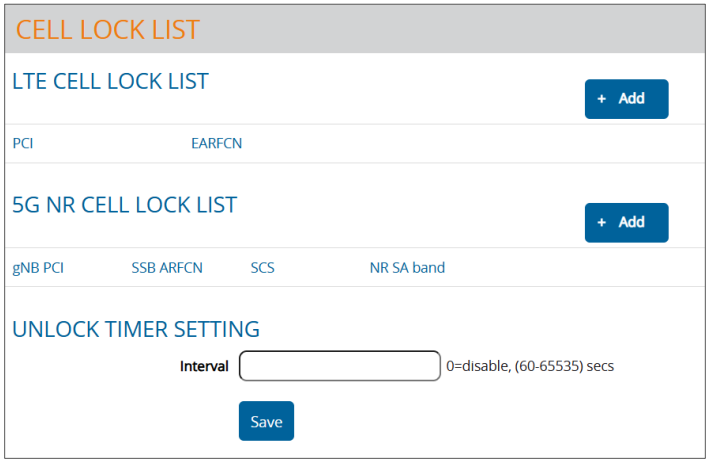


Figure 8-15 Cell lock list page

Adding a cell to LTE cell lock list

To add a cell to the LTE cell lock list:

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

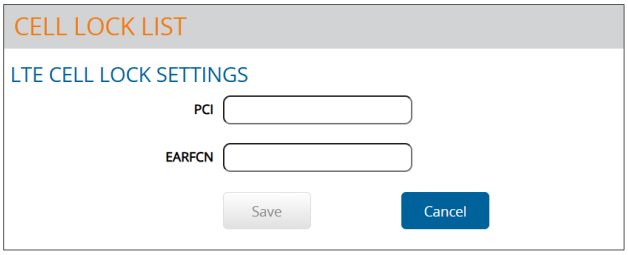


Figure 8-16 LTE cell lock settings

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

Adding a cell to NR cell lock list

To add a cell to NR cell lock list:

1. Click **Add** button, next to the **NR5G Cell Lock List**

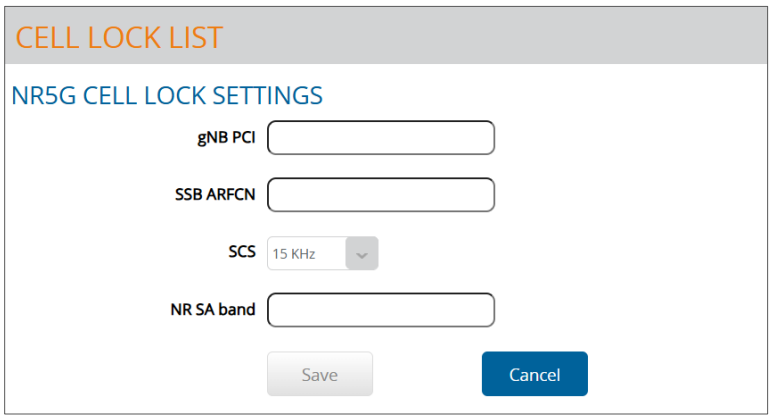


Figure 8-17 NR5G cell lock settings

2. Enter the **gNB PCI**, **SSB ARFCN** values, select **SCS** value, and enter **NR SA band** value for the NR5G cell that you want to lock to.
3. Click **Save** button. Repeat steps 1 to 3 for all the NR5G cells that you wish to add.

Unlock Timer Setting

In the **Interval** field, enter duration in seconds for which a locked cell remains restricted before it is automatically unlocked.

WAN profiles

WAN profiles displays the Active Profile and the Advanced Profile Configuration section. It allows you to configure and enable/disable connection profiles. To access WAN profiles page, navigate to **Networking > Cellular settings > WAN profiles**.

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

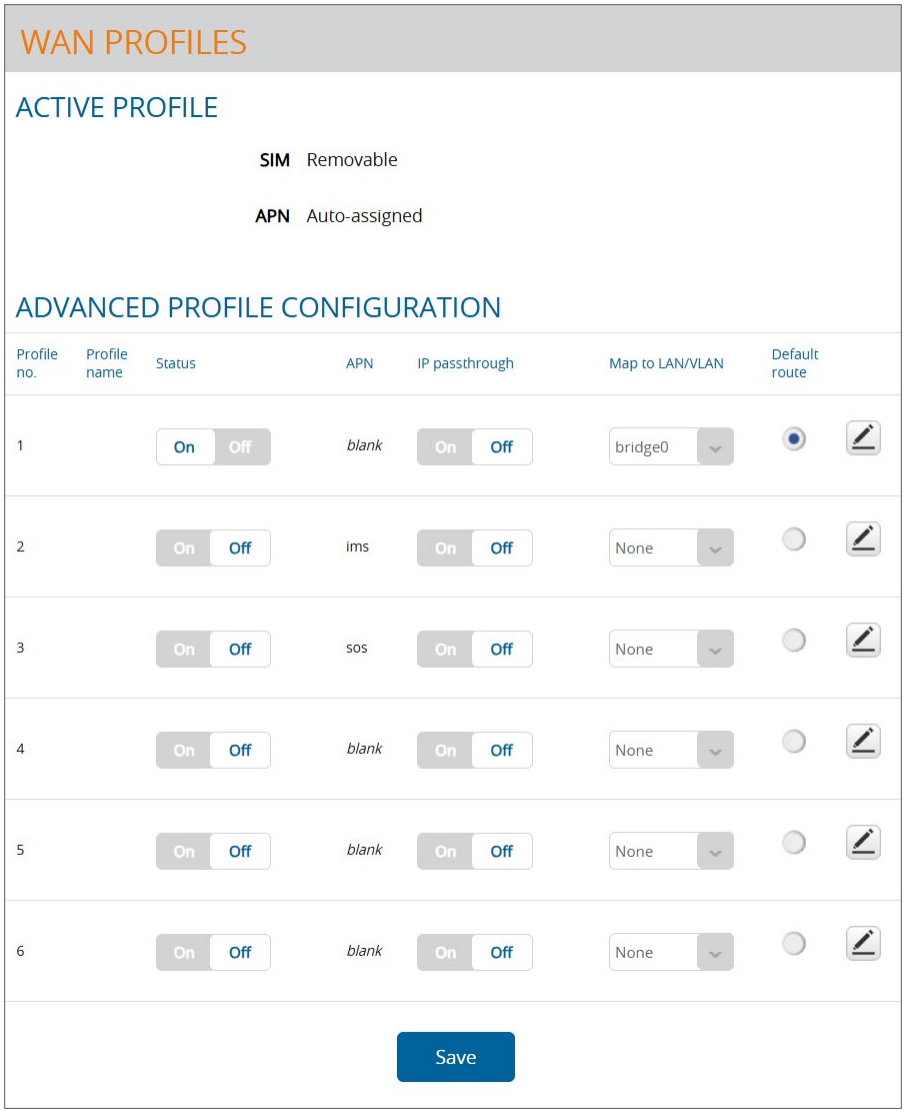


Figure 8-18 WAN profiles page

Table 8-1 Advanced profile configuration details

ITEM	DEFINITION
Profile no.	Number of the profile.
Profile name	Name of the profile.
Status	Toggles the corresponding profile to **On** or **Off**. Only one profile may be turned on at any time.
APN	The APN configured for the corresponding profile.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device. Internet traffic is still terminated at the gateway (NTC-500 Series router) and passed through to a downstream device, so the carrier is still able to connect to the gateway.

ITEM	DEFINITION
Map to LAN/VLAN	The LAN or VLAN that the profile is assigned to.
Default Route	Sets the profile as the default route for traffic.

Connecting to the mobile broadband network

The NTC-500 Series router supports the configuration of up to six APN profiles. These profiles allow you to configure the settings that the router will use to connect to the 5G/4G network and switch easily between different connection settings.

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

Manually configuring a connection profile

To manually configure a connection profile:

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

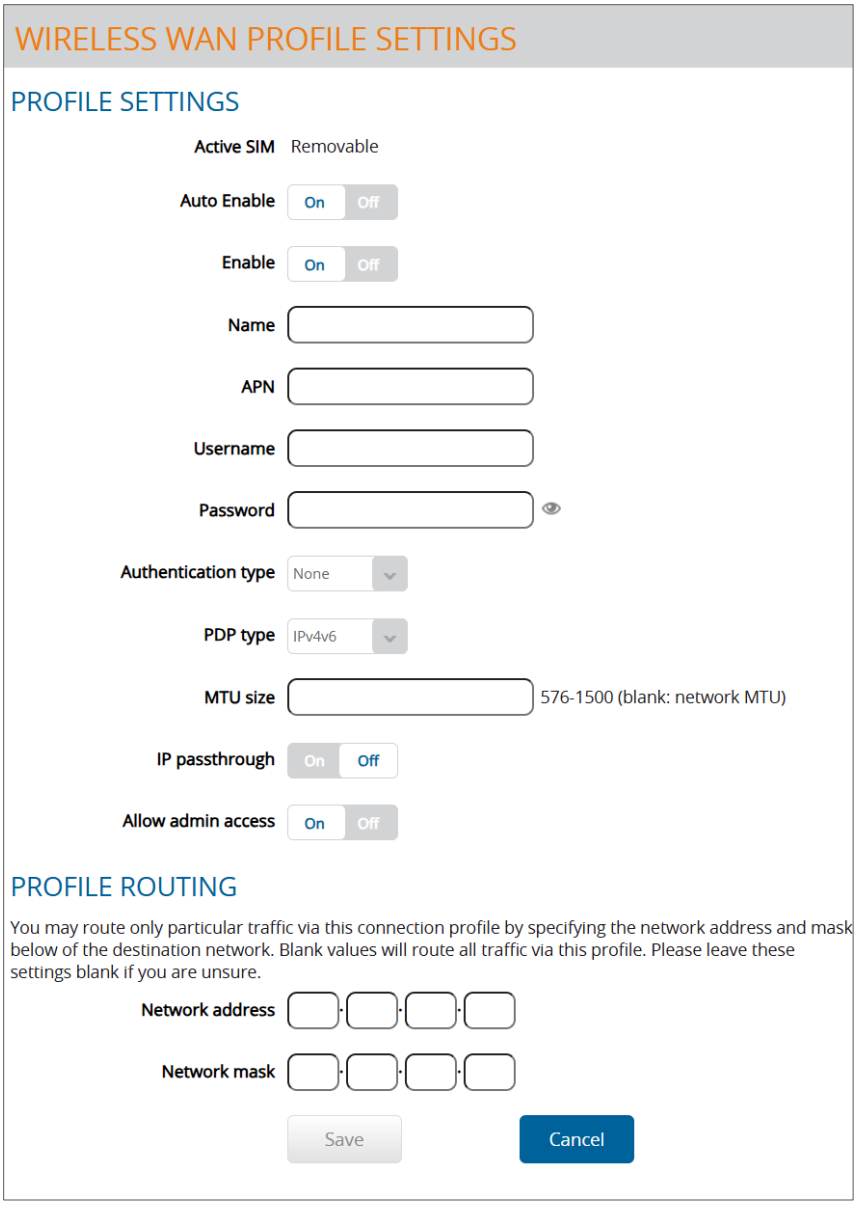


Figure 8-19 WWAN profile settings

Table 8-2 WWAN profile configuration details

Item	Definition
Active SIM	The SIM currently in use: • **Removable** (SIM inserted via SIM tray) • **Internal** (Embedded SIM)
Auto Enable	Set to **ON** to enable. It is enabled by default. When you boot the router for the first time or perform a factory reset, **Auto Enable** allows the router to automatically enable the default profile for the active SIM and connect to the network via that profile.

Item	Definition
	When **Auto Enable** is enabled for any one profile for a SIM, it is automatically enabled for all the profiles for that SIM.
Enable	Set to **On** to enable the profile.
Name	The name of the APN for easy identification on the Wireless WAN profile page. This name is only used to identify the profile on the NTC-500 Series router.
APN	Enter the APN (Access Point Name) configured for the corresponding profile.
Username	The username for the corresponding APN (if required).
Password	The password for the corresponding APN (if required).
Authentication type	The authentication type required by your provider. This can be set to: **None**, **PAP** or **CHAP**
PDP Type	Select the **PDP type** (IP protocol) to use for the connection. ⊙ **IPv4** – Sets a single stack IPv4 connection through which the NTC-500 Series router receives only IPV4 network and DNS addresses. ⊙ **IPv6** – Sets a single stack IPv6 connection through which the NTC-500 Series router receives only IPV6 network and DNS addresses. ***Note:*** *Before selecting this PDP type, check with your carrier to confirm that single stack IPV6 connectivity is supported.* ⊙ **IPv4v6** – Sets a dual stack connection allowing simultaneous IPV4 and IPV6 network connectivity. The NTC-500 Series router receives both IPv4 and IPV6 network and DNS addresses. This is the default **PDP type.**
MTU size	Sets the Maximum Transmission Unit size. This may be from 576 to 1500 bytes.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device.

Item	Definition
	Internet traffic is still terminated at the gateway (NTC-500 Series router) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Allow Admin Access	Set to enable, to allow SSH, TR-069 or Web GUI access to the device via this Wireless WAN Profile. ***Note:*** *SSH /HTTPS can be individually restricted in the* ***Access Control*** *menu. It will automatically be enabled if the profile is selected in the* ***TR-069 settings*** *menu.*
Profile Routing (See the **Profile Routing** section below)	
Network address	Enter network address of the remote network.
Network mask	Enter the network mask of the remote network.

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

Profile routing

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 section, enter the **Network address** and **Network mask** of the remote network. If you do not want to use this feature, or are unsure, please leave these fields blank. This will not designate any particular traffic to be routed via this profile.

5G Network slicing

5G Network Slicing allows you to perform network slice configuration. To access 5G Network slicing page, navigate to **Networking > Cellular settings > 5G network slicing**.

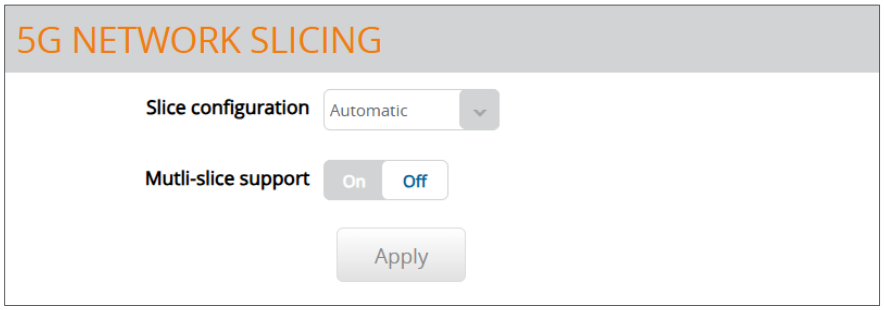


Figure 8-20 5G network slicing page

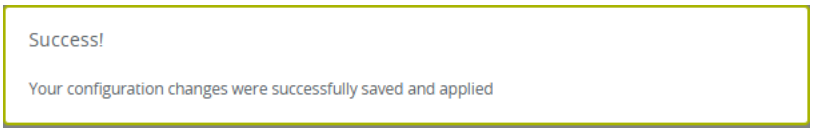
You can perform automatic or manual network slice configuration.

Automatic Network Slice Configuration

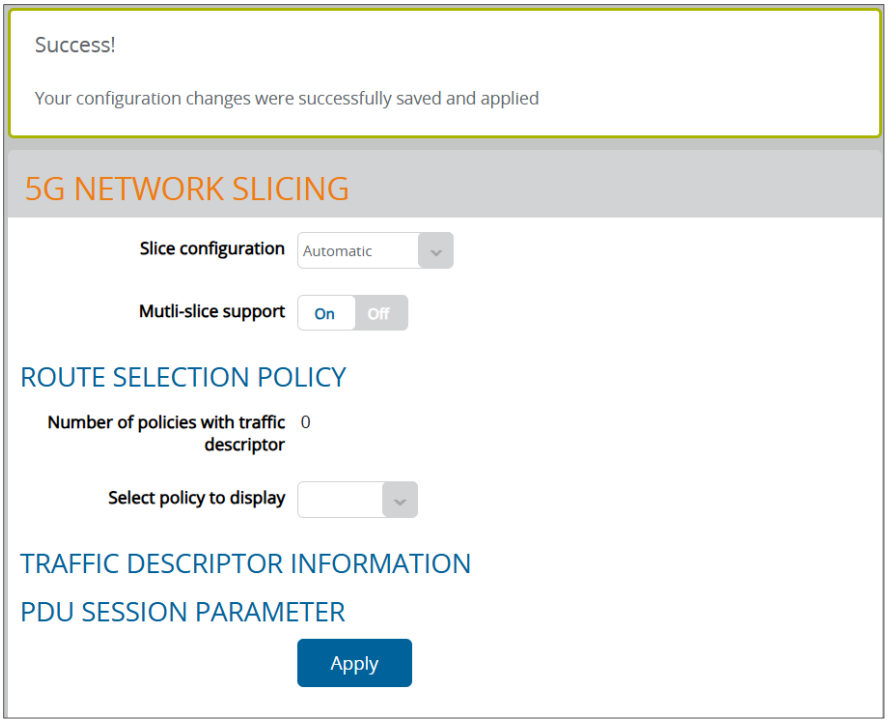
To perform automatic network slice configuration:

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

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



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



Manual Network Slice configuration

To perform manual network slice configuration:

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

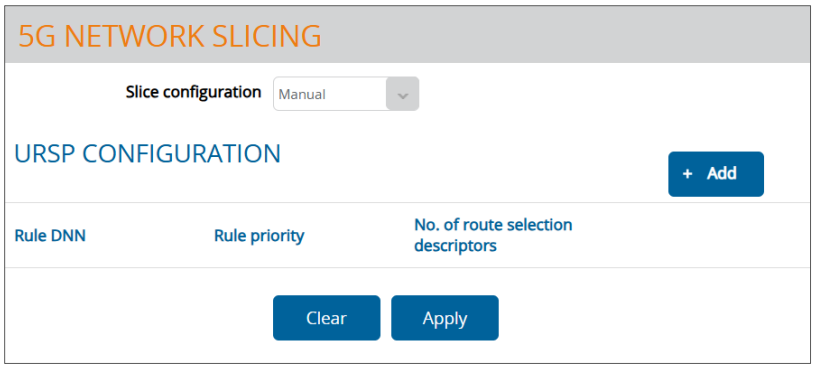


Figure 8-21 Manual Network Slicing

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

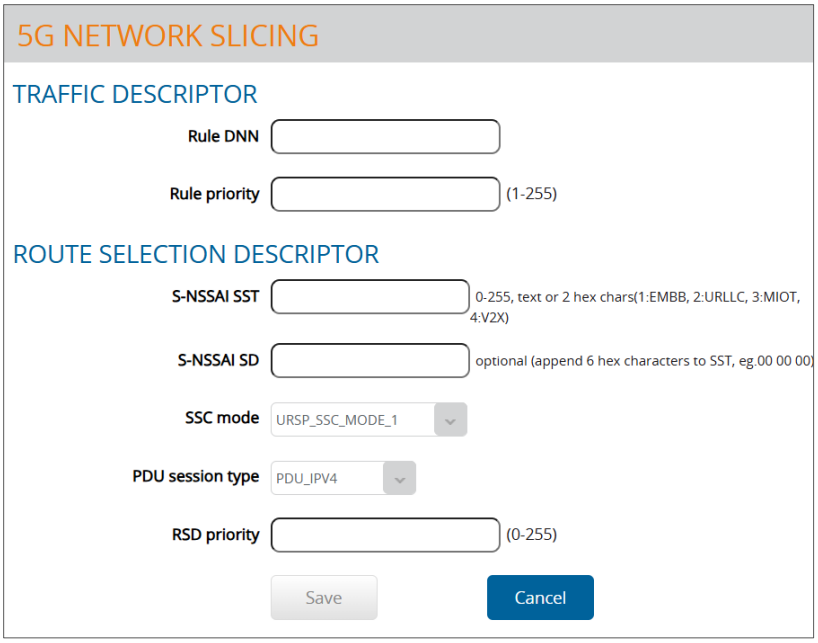


Figure 8-22 Manual Network Slicing settings

Table 8-3 Manual Network Slicing Configuration Details

Item	Definition
Traffic Descriptor	
Rule DNN	Enter the Data Network Name. It identifies the external data network (e.g., "internet" or an enterprise APN) that a PDU session should connect to.
Rule priority	Enter a number from 1 to 255. It Determines the order in which URSP rules are evaluated (lower number = higher priority)
Route Selection Descriptor	
S-NSSAI SST	Enter the required value. Single-Network Slice Selection Assistance Information SST (Slice/Service Type) indicates the category or type of service the slice is intended to provide.
S-NSSAI SD	Enter the required value. Single-Network Slice Selection Assistance Information SD (Slice Differentiator) complements the mandatory SST (Slice/Service Type) to further differentiate between multiple network slices that share the same SST value.
SSC mode	Select a mode. Options are: • **URSP_SSC_MODE_1**: The network preserves the UE's connectivity and retains the same IP address throughout the session. • **URSP_SSC_MODE_2**: The network may release the PDU session and re-establish a new session, possibly assigning a new IP address. • **URSP_SSC_MODE_3**: The network allows the PDU Session Anchor (PSA) to be relocated while the session remains active, which can result in the IP address being changed.

Item	Definition
PDU session type	Select an option. It specifies the kind of data connectivity established between a user device (UE) and the data network (DN) for a given PDU (Packet Data Unit) session. Options are: • **PDU_IPV4** • **PDU_IPV6** • **PDU_IPV4V6**
RSD priority	Enter a number from 0 to 255. It refers to the order in which Route Selection Descriptors (RSDs) are evaluated within a UE Route Selection Policy (URSP) rule.

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

Service assurance

Service assurance allows you to run tests to confirm connectivity on different WWAN profiles. To access the Service assurance page, navigate to **Networking > Cellular settings > Service assurance**.

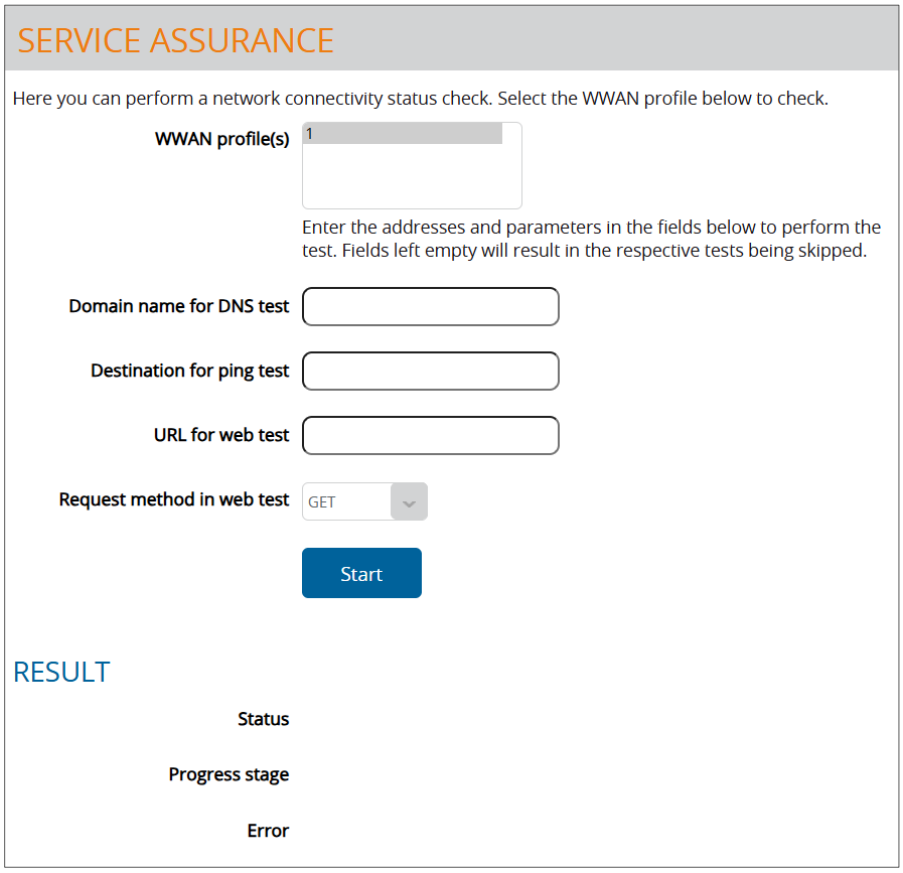


Figure 8-23 Service assurance page

To run a service assurance test:

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

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

LAN settings

LAN

LAN allows you to configure the LAN settings of the NTC-500 Series router. To access the LAN page, navigate to **Networking > LAN settings > LAN**.

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

Note: *If you change the IP address, remember to refresh the Ethernet interface of your device, or set an appropriate IP address range, then enter the new IP address into your browser address bar to access the NTC-500 Series router.*

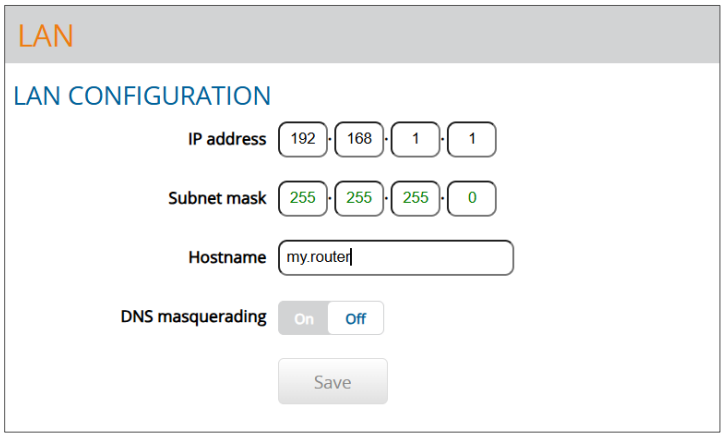


Figure 8-24 LAN page

DNS masquerading

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

The DNS masquerading toggle key is Off by default.

With DNS masquerading **Off**, the DHCP server hands out the upstream cellular DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the NTC-500 Series router.

With DNS masquerading **On**, the DHCP server embedded in the NTC-500 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-500 Series router, which proxies them to the upstream DNS servers.

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

DHCP

DHCP allows you to configure the DHCP settings of the NTC-500 Series router. To access the DHCP page, go to **Networking > LAN settings > DHCP**.

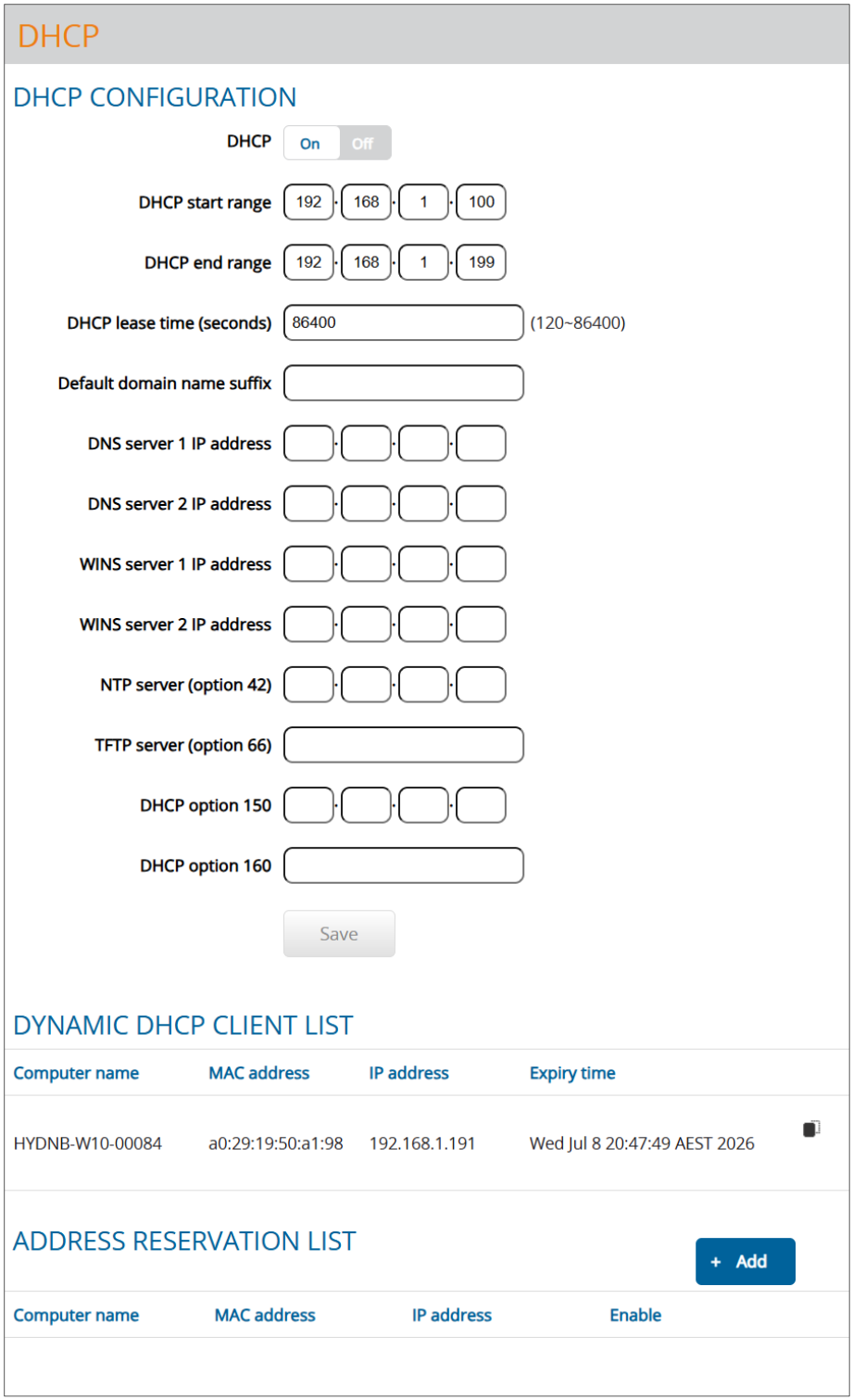


Figure 8-25 DHCP page

Table 8-4 DHCP configuration details

Option	Description
DHCP	Set to **On** to enable DHCP
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 IP address 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.

Click **Save** to save and apply 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, select the **Clone** icon and the details will be copied to the address reservation list fields.

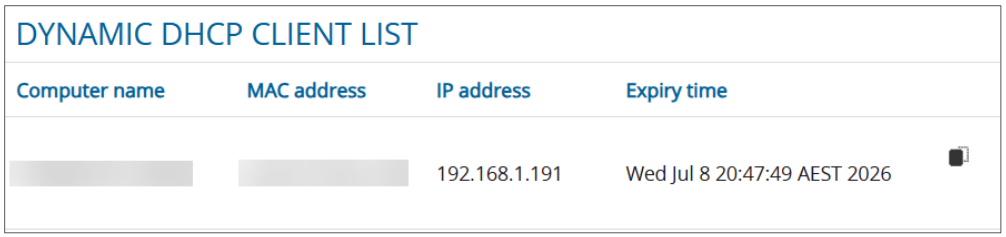


Figure 8-26 Dynamic DHCP client list

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 8-27 Address reservation list

To add a device to the address reservation list:

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

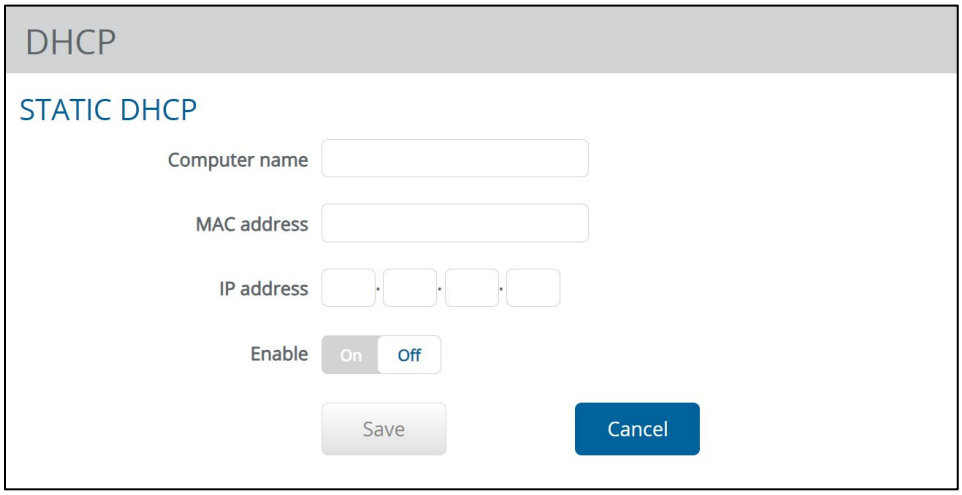


Figure 8-28 Static DHCP settings

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

Click icon to edit the details of that device and click icon to delete that device from the Address Reservation List.

VLAN

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

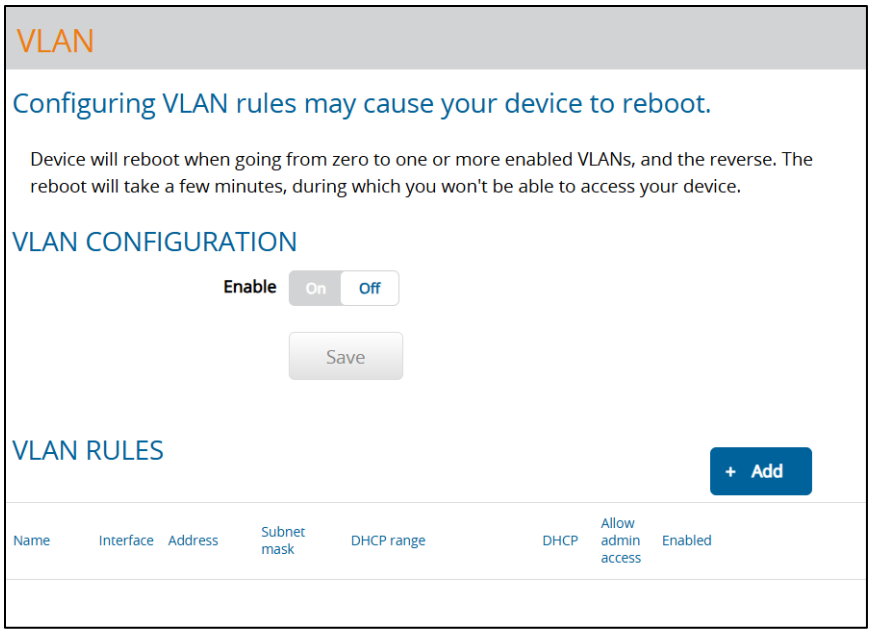


Figure 8-29 VLAN page

VLAN Settings

To create a VLAN:

1. Set the **Enable** toggle to the **On** position.
2. Select on the **+Add** button on the VLAN page, the VLAN Settings display.

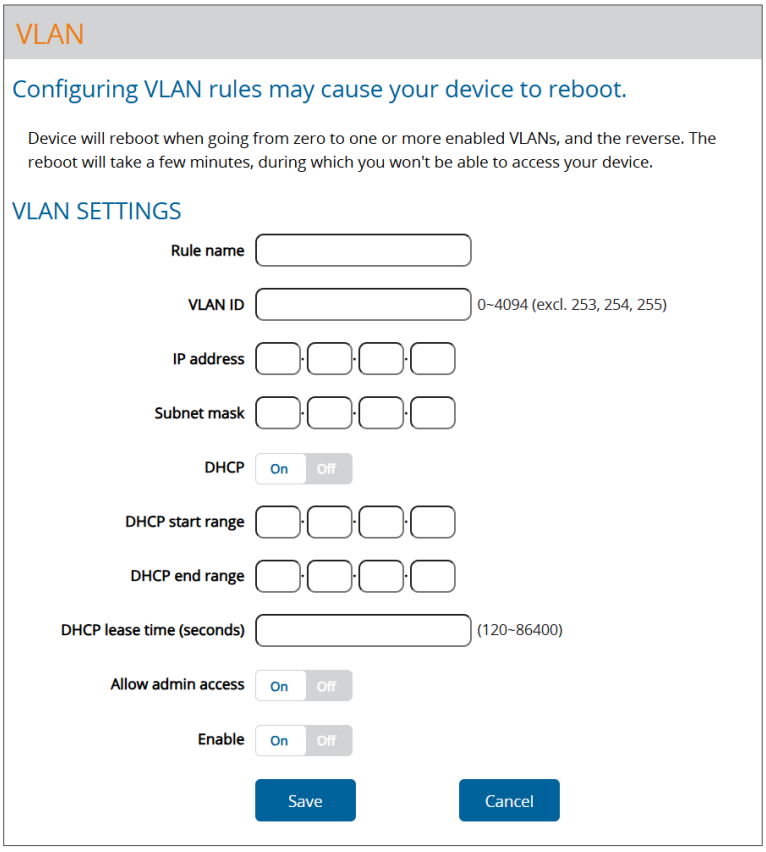


Figure 8-30 VLAN settings

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

Routing settings

Static routes

Static routing is the alternative to dynamic routing, used in more complex network scenarios and 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 routes page, navigate to **Networking > Routing settings > Static routes**.

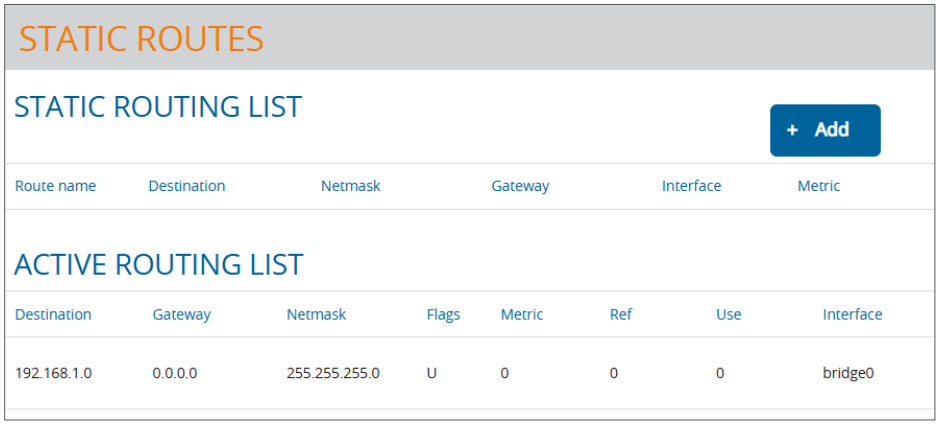


Figure 8-31 Static routes page

Adding Static Routes

To add a new route to the static routing list:

1. Select the **+Add** button. The Route Configuration settings display.

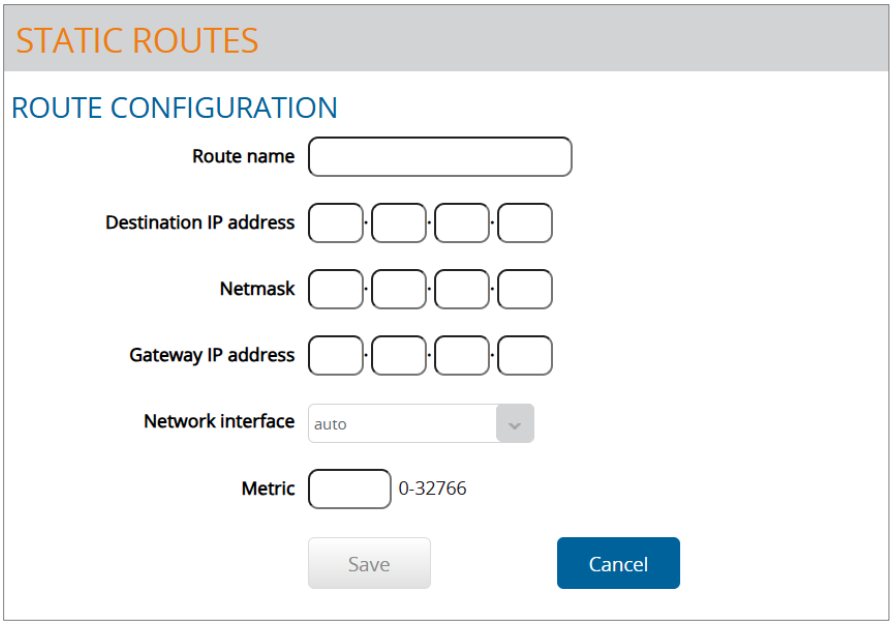


Figure 8-32 Static route configuration settings

2. In the **Route name** field, type a name for the route so that it can be identified in the static routing list.
3. In the **Destination IP address** field, enter the IP address of the destination of the route.
4. In the **Netmask** 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. From the **Network interface** drop-down list, select the interface for which you would like to create a static route.
7. In the **Metric** field enter the metric for the route. The metric value is used by the router to prioritize routes. The lower the value, the higher the priority. To give the route the highest priority, set it to 0.
8. Select the **Save** button to save and apply your settings. The route is added to the Static Routing List.

Static Routing List

The static routes added by you are displayed in the Static Routing List. If the route is valid it is displayed in the Active Routing List.

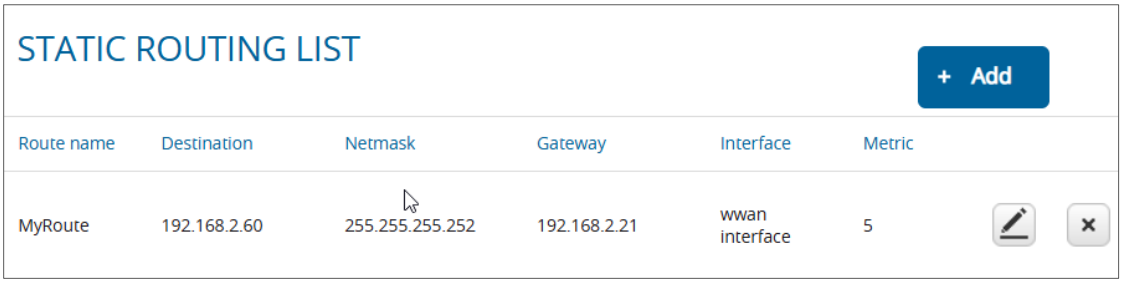


Figure 8-33 Static routing list

Click icon to edit the details of the route and click icon to delete the route.

Active Routing List

All the active routes are displayed in the Active Routing List.

ACTIVE ROUTING LIST

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	192.168.2.21	0.0.0.0	UG	0	0	0	rmnet_data0
8.8.8.8	0.0.0.0	255.255.255.255	UH	10	0	0	rmnet_data0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	bridge0
192.168.2.20	0.0.0.0	255.255.255.252	U	0	0	0	rmnet_data0
192.168.2.60	192.168.2.21	255.255.255.252	UG	5	0	0	rmnet_data0

Figure 8-34 Active routing list

Firewall

The Firewall on the NTC-500 Series router implements an Intrusion Prevention System (IPS). The IPS works together with, but in a different manner than, system firewalls to prevent unauthorised access to your network and potentially malicious attacks. It provides a few more levels of security protection for your system from external threats.

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

IPS filters are interposed between the firewall and the other NTC-500 Series router functionality. It uses a variety of sophisticated techniques to monitor traffic flows and analyse inbound packets to determine whether they constitute network threats and, if so, to deny them access. The IPS firewall allows different levels of protection to be selectively applied, to thwart a threat specifically identified.

To access the Firewall page, navigate to **Networking > Routing settings > Firewall**.

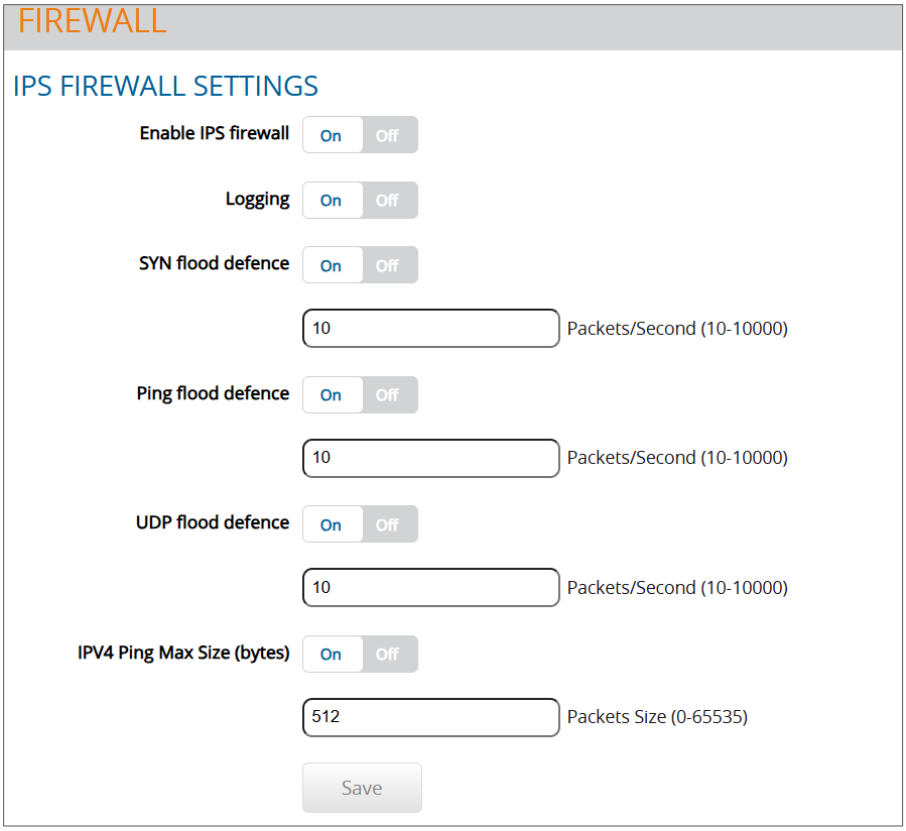


Figure 8-35 Firewall page

Table 8-5 IPS Firewall configuration details

Item	Description
Enable IPS Firewall	Enables or disables IPS Firewall
Logging	Enables or disables logging of network activity.
SYN flood defense	Enables or disables SYN flood defense which restricts the number of SYN requests processed by the router during a given time frame. When enabled enter the number of packets/second. Default value is 10, range (10-10000)
Ping flood defense	Enables or disables Ping flood defense. When enabled enter the number of packets/second accepted. Default value is 10, range (10-10000)
UDP flood defense	Enables or disables UDP flood defense. When enabled enter the number of packets/second allowed from a single source. Default value is 10, range (10-10000)
IPV4 Ping Max Size (bytes)	Enables or disables IPV4 Ping Max Size which allows you to set maximum size for an IPv4 packet. When enabled enter the maximum packet size. Default value is 512, range (0-65535)

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

DMZ

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

To access the DMZ page, navigate to **Networking > Routing settings > DMZ**.

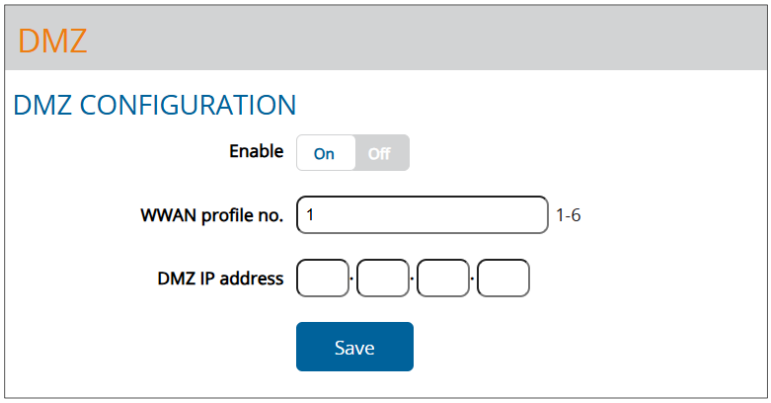


Figure 8-36 DMZ page

Configuring the DMZ

To enable and configure the DMZ:

1. Set Enable to **On**.
2. In the **WWAN profile no.** field, enter the WWAN profile number that you wish to associate the DMZ configuration with.
3. Enter the IP Address of the device to be the DMZ host into the **DMZ IP Address** field.
4. Select the **Save** button to save and apply your settings.

Port forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the NTC-500 Series router. To access the Port forwarding page, navigate to **Networking > Routing settings > Port forwarding**.

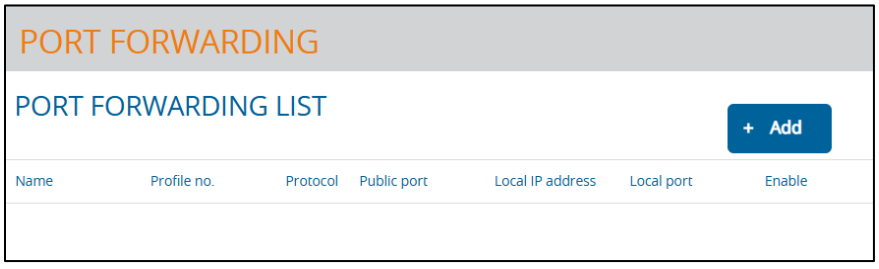


Figure 8-37 Port forwarding

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

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

Adding a port forwarding rule

To create a new port forwarding rule:

1. From the **Port forwarding list**, click the **+Add** button. The port forwarding settings screen is displayed.

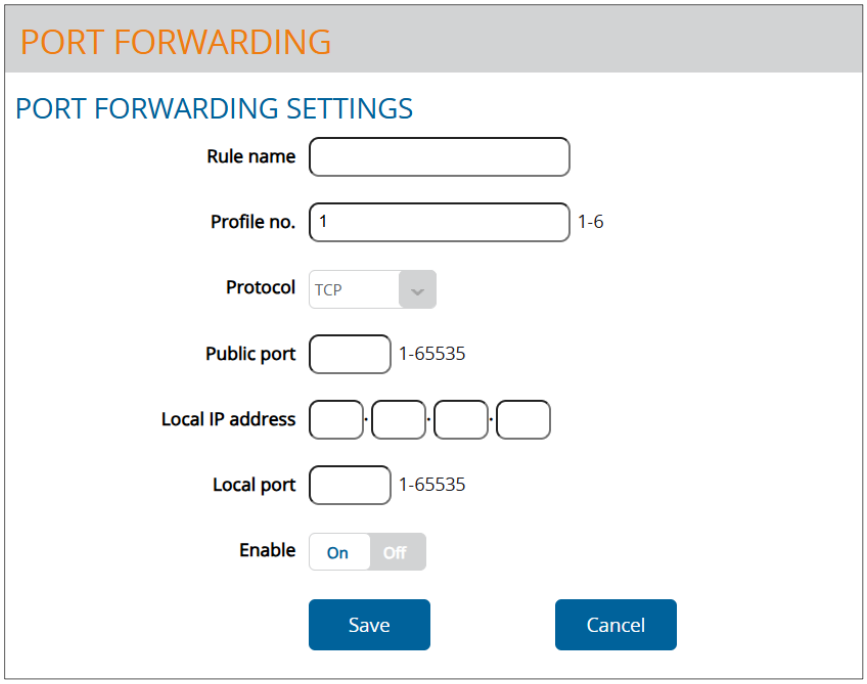


Figure 8-38 Port Forwarding Settings

1. In the **Rule name** field, enter a name for the rule so that it can be easily identified.
2. In the **Profile no.** field, enter a number that corresponds to the Wireless WAN Profile that you want to use for the rule.
3. Use the **Protocol** drop-down list to select the type of protocol you want to use for the rule. The protocols selections available are **TCP**, **UDP** and **TCP/UDP**.
4. In the **Public port** field, enter a number between 1 and 65535 to use for the communication port from the NTC-500 Series router out to the mobile network.
5. In the **Local IP Address** field, enter the IP address of LAN equipment to which traffic should be routed or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the traffic.
6. In the **Local port** field, enter a port number to use for traffic to the local device. This may be an integer between 1 and 65535.
7. Ensure that the **Enable** toggle button is set to the **ON** position.
8. Select the **Save** button to save and apply your settings. The new rule is added to the Port Forwarding List

To delete a port forwarding rule, select the × button on the **Port forwarding list** for the corresponding rule that you would like to delete. To edit an existing rule, select on the ✎ button.

Filtering

Filtering allows you to restrict devices that are allowed to connect to the NTC-500 Series router by their MAC address. To access the Filtering page, navigate to **Networking > Routing settings > Filtering**.

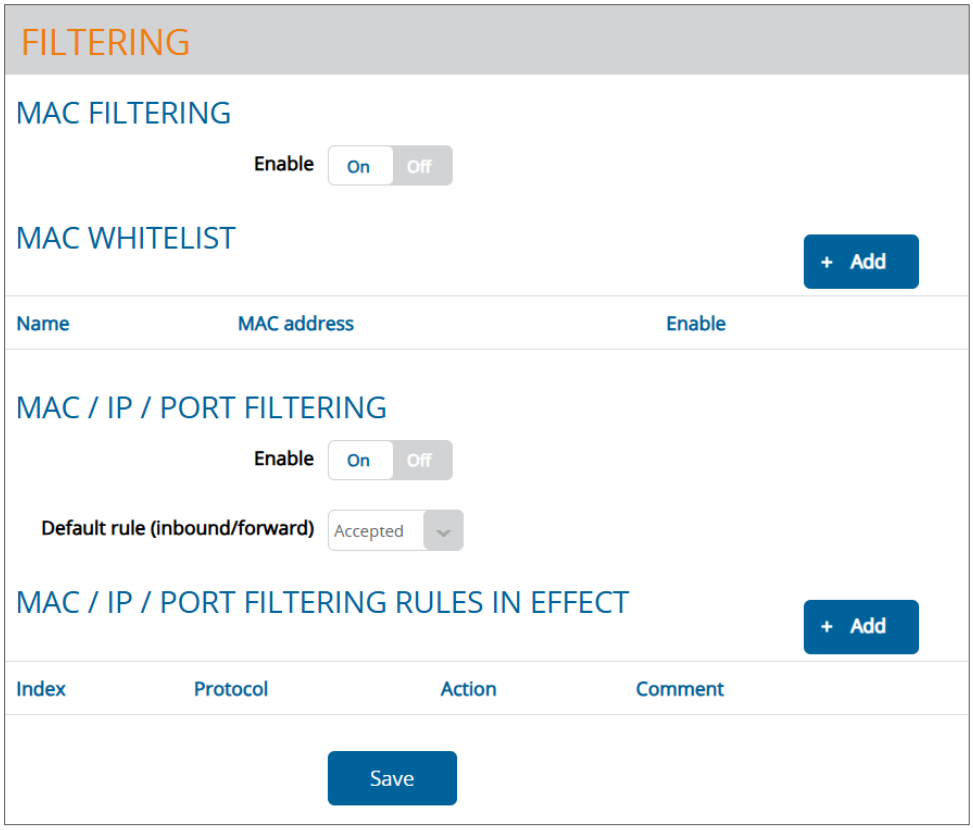


Figure 8-39 Filtering page

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

MAC whitelist

To add a device to the MAC whitelist:

1. Click the **+Add** button. The **MAC whitelist settings** page appears.

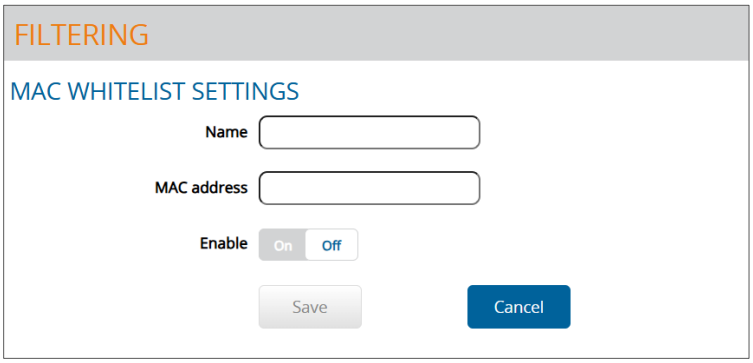


Figure 8-40 MAC whitelist settings

2. In the **Name** field, enter a name to identify the device.
3. In the **MAC address** field, enter the MAC address of the device.

4. Set the Enable toggle to **On.**
5. Select the **Save** button.
6. The device appears in the **MAC Whitelist** section.

To remove a device, select the button for the device in the MAC Whitelist. To edit the device or temporarily disable it, select the button.

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.

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

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

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

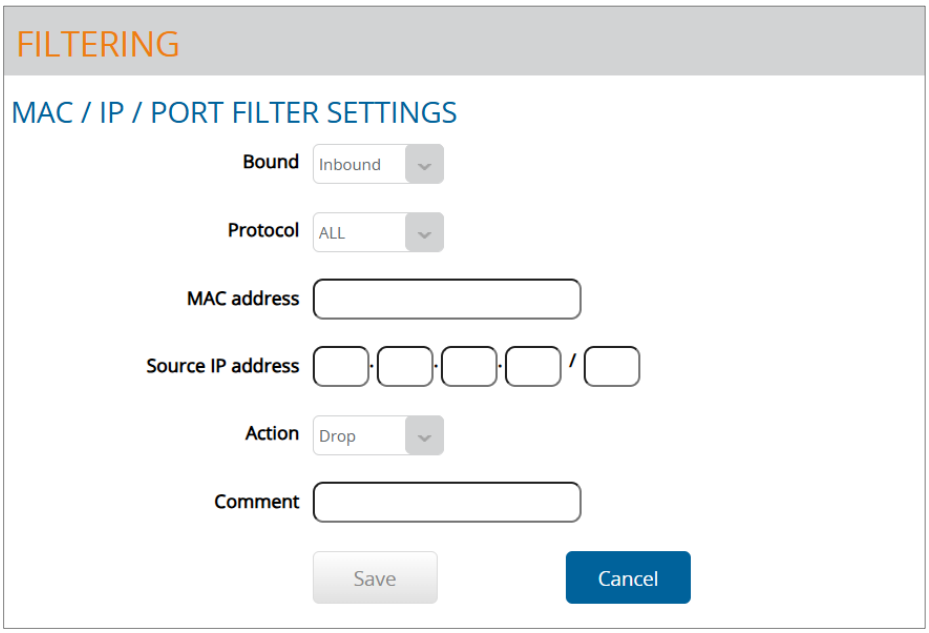


Figure 8-41 MAC/IP/Port Filter Settings

Table 8-6 MAC/IP/Port Filter Configuration Details

Item	Description
Bound	Select the direction of traffic. The options available are: • **Inbound** • **Outbound** • **Forward**
Protocol	Select the protocol of the traffic. The options available are: • **All** • **UDP/TCP** • **UDP** • **TCP** • **ICMP**
MAC Address	Enter MAC Address of the source device.
Source IP address	Enter IP address of the source device.
Action	Select the action to be taken. The options available are: • **Drop** • **Accept**
Comment	Add comments for the rule

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

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

VRRP

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

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

To access the VRRP page, navigate to **Networking > Routing settings > VRRP**.

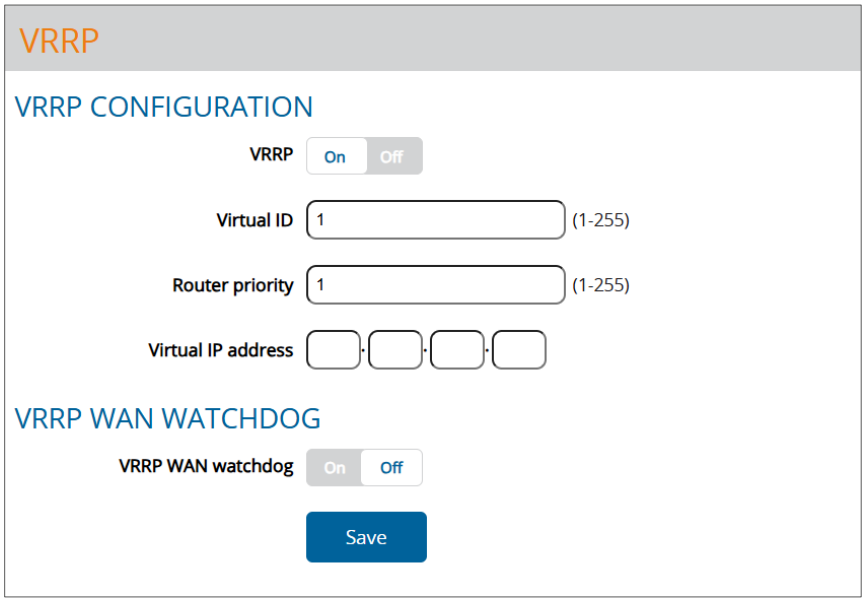


Figure 8-42 VRRP page

Configuring VRRP

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

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

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

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

Configuring the VRRP WAN watchdog

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

To configure the VRRP WAN Watchdog, set **VRRP WAN watchdog** to **On**. The configuration settings display.

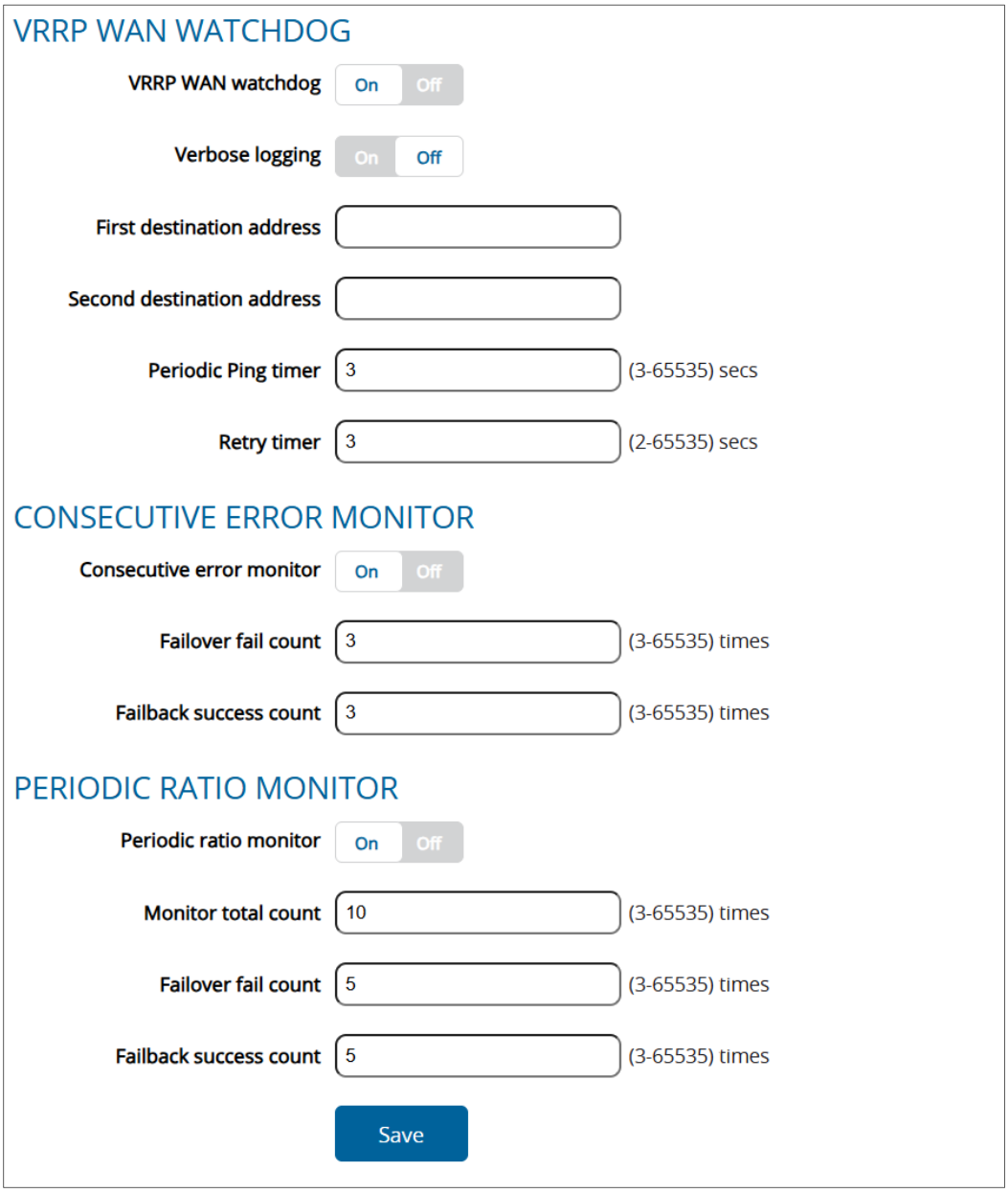


Figure 8-43 VRRP WAN watchdog settings

Table 8-7 VRVP WAN Watchdog configuration details

Parameter	Description
VRRP WAN Watchdog	Set the VRRP WAN Watchdog to **On** to enable the watchdog.
Verbose logging	Set to **On** to enable. When enabled verbose comments are logged in the system log related to the failover monitoring.
First destination address	The first address 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 that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	The time in seconds between ping attempts.
Retry timer	The time in seconds between attempts when a ping failure occurs.
Consecutive error monitor	
Consecutive Error Monitor	Set to **On** to enable the consecutive error monitor. Using this method, the router will determine the availability of an interface based on a set number of consecutive ping instance responses.
Failover fail count	The number of failed pings that must occur before the monitor fails the connection over to the next interface.
Failback success count	The number of successful pings that must occur before the monitor fails the connection back to the higher priority interface.
Periodic ratio monitor	
Periodic ratio monitor	Set to **On** to enable the Periodic ratio monitor. Using this method, the router will determine the availability of an interface based on a set ratio of ping instance successes or failures to the number of attempts.
Monitor total count	This field specifies a series of pings to consider when calculating whether to fail over or fail back. When the Series is completed, the router repeats the ping test and resets the Failover fail count/Failback success count, therefore, 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.

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

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

RIP

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

To access the RIP page, navigate to **Networking > Routing settings > RIP**.

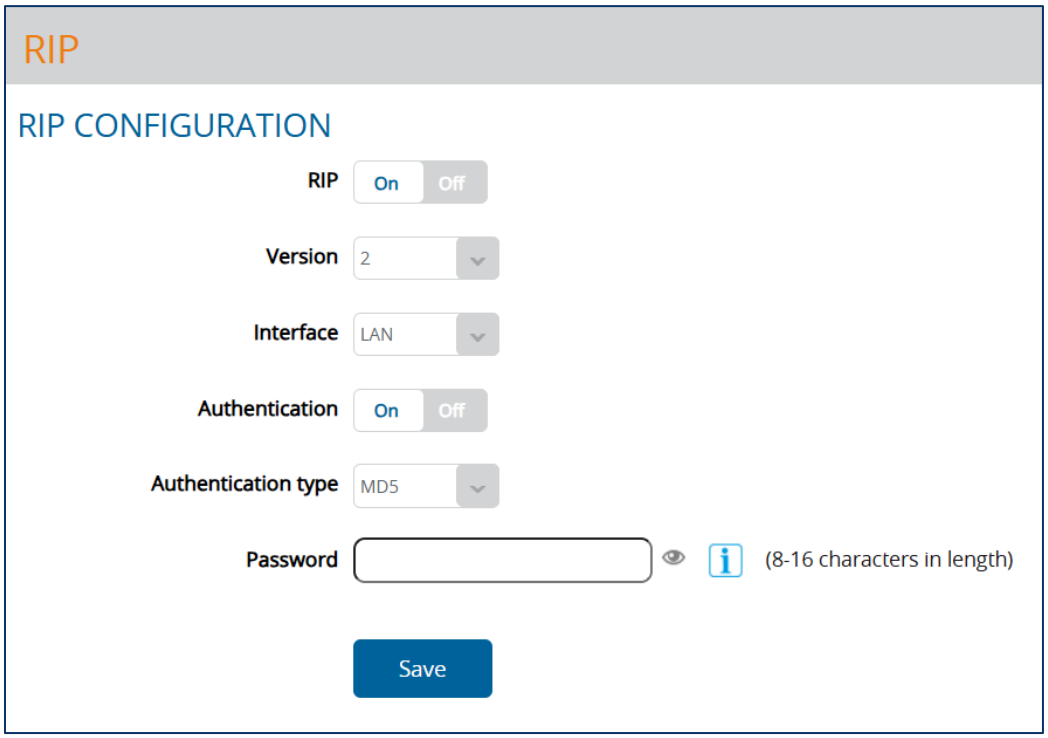


Figure 8-44 RIP page

Note: *Other routers may ignore RIP.*

To enable RIP:

1. Set the **RIP** toggle to **On** to enable RIP.
2. Using the **Version** drop-down list, select the version of RIP that you would like to use.
3. Select the **Interface** that RIP should apply on. Options are **LAN**, **WWAN** 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. Select the **Save** button to confirm your settings.

VPN settings

IPSec

IPSec operates on Layer 3 of the OSI model and can protect higher layered protocols. IPSec is used for both site-to-site VPN and Remote Access VPN. The NTC-500 Series router supports IPsec end points and can be configured with site-to-site VPN tunnels for third party VPN routers.

To access the IPSec page, navigate to **Networking > VPN settings > IPSec**.

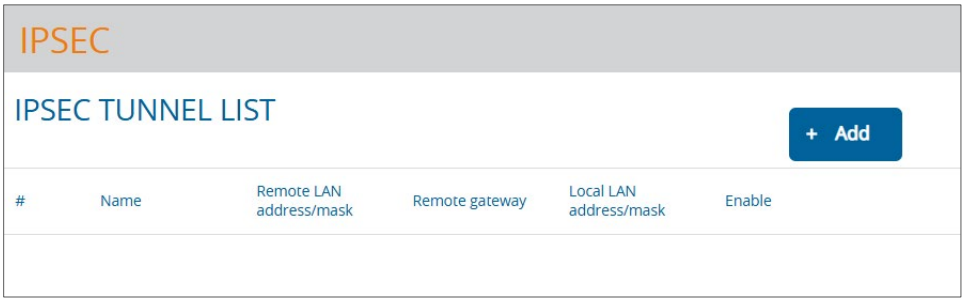


Figure 8-45 IPSec page

Configuring an IPSec VPN

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

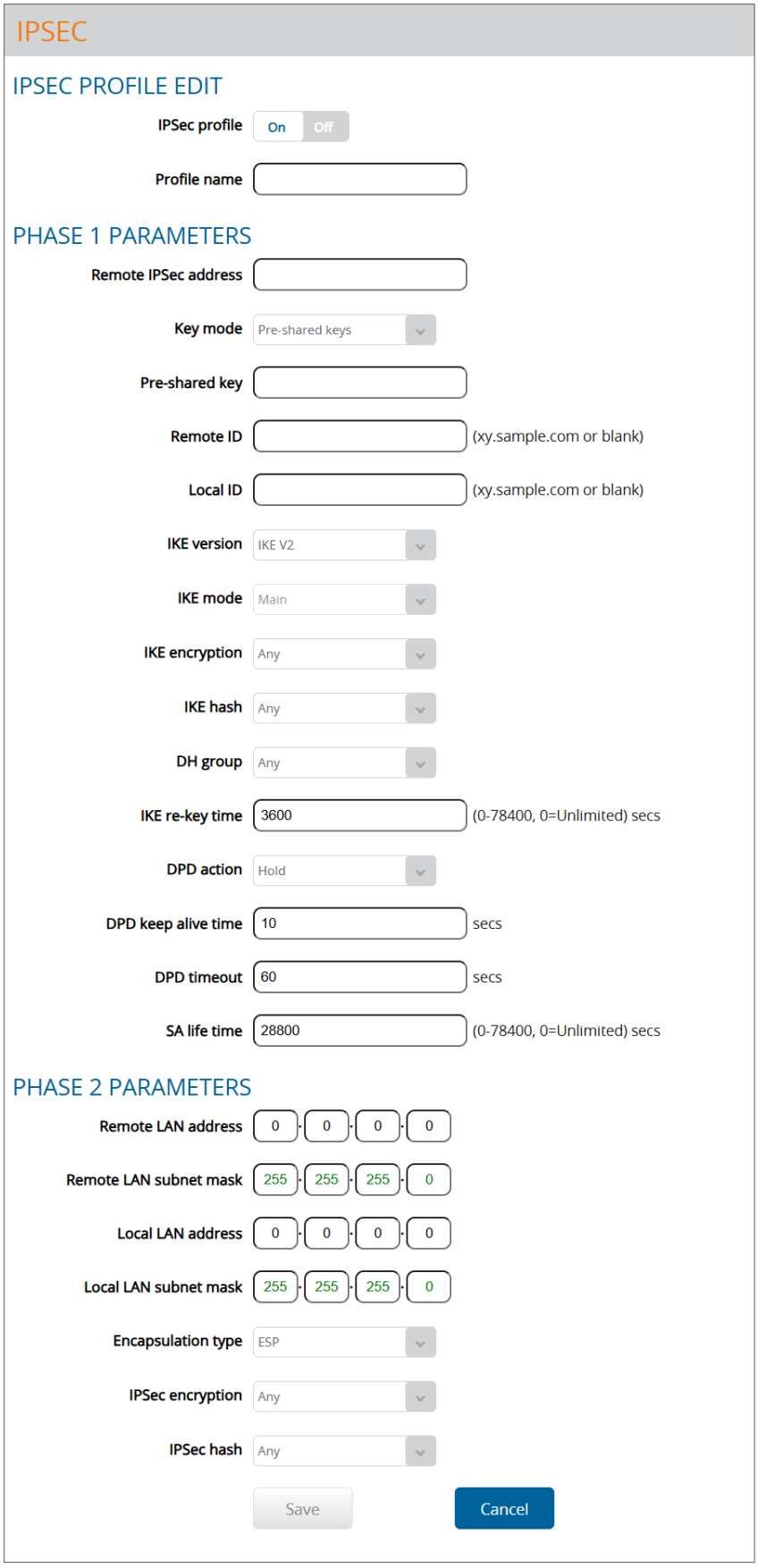


Figure 8-46 IPSec configuration settings

Table 8-8 IPSec configuration details

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

Parameter	Description
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 required Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.
DPD keep alive time	Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.
DPD timeout	Enter the time in seconds of no response from a peer before Dead Peer Detection times out.
SA life time	Enter the time in seconds for the security association lifetime.
Phase 2 parameters	
Remote LAN address	Enter the IP address of the remote network for use on the VPN connection.
Remote LAN subnet mask	Enter the subnet mask in use on the remote network.
Local LAN address	Enter the IP address of the local network for use on the VPN connection.
Local LAN subnet mask	Enter the subnet mask in use on the local network.
Encapsulation type	Select the encapsulation protocol to use with the VPN connection. You can choose **ESP**, **AH** or **Any**.
IPSec encryption	Select the IPSec encryption type to use with the VPN connection.
IPSec hash	Select the IPSec hash type to use for the VPN connection. The hash is used for authentication of packets for the VPN connection.

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

OpenVPN

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

To access the OpenVPN page, navigate to **Networking > VPN settings > OpenVPN**.

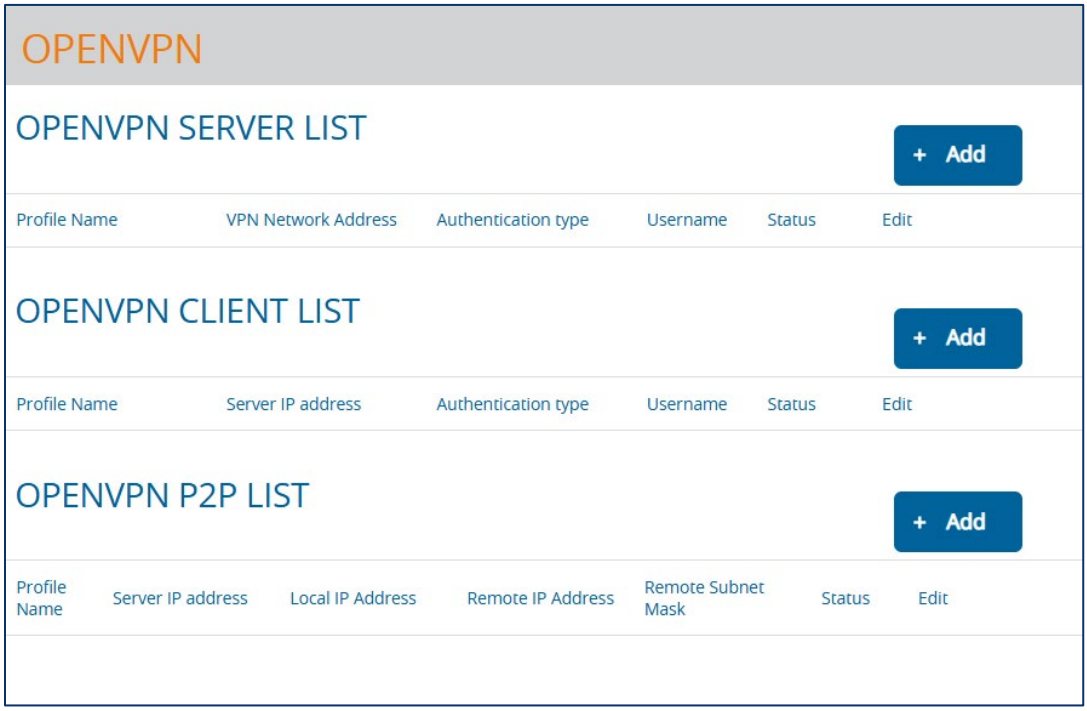
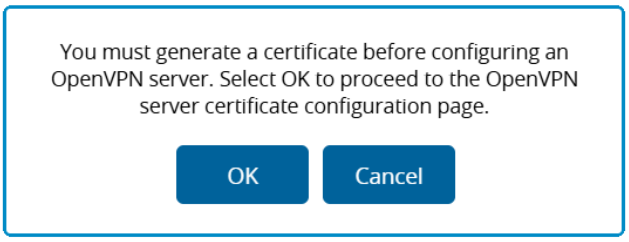


Figure 8-47 OpenVPN page

Configuring an OpenVPN Server

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



Select 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 to continue the setup.

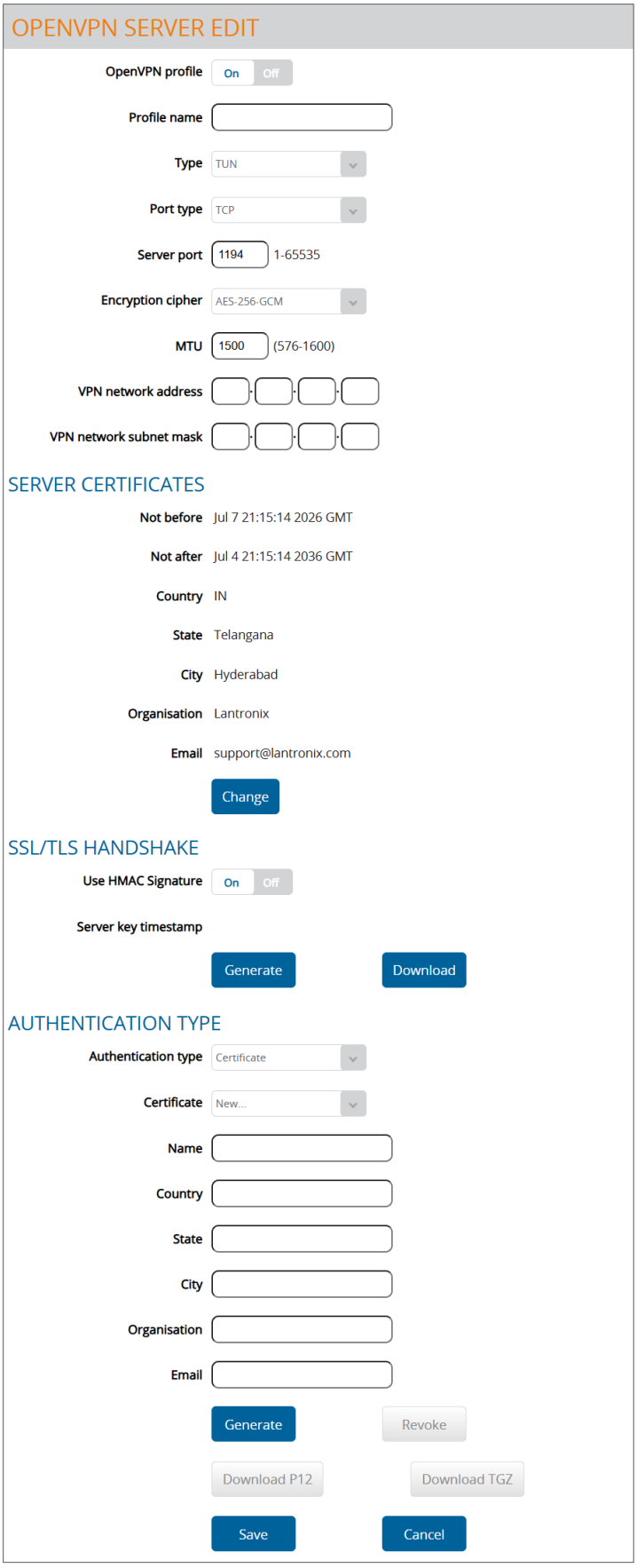


Figure 8-48 OpenVPN server settings

To configure an OpenVPN server:

1. Set the **OpenVPN profile** toggle key to **On** position.
2. In the **Profile name** field, enter a name for the OpenVPN server profile you are creating.
3. In the **Type** field, select the OpenVPN connection type (**TUN/TAP**). Default is **TUN**.
4. In the **Port type** field, select a packet type to use for your OpenVPN Server and in the **Server port** field, enter a port number. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **Encryption cipher** field, select the encryption type for the connection. The default is **AES-256-GCM** as this is the strongest encryption level.
6. Enter a maximum transmission unit value into the **MTU** field. The default is 1500.
7. In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
8. The Server certificates section displays the details of the certificate. If you wish to change the certificate, click the **Change** button.
9. HMAC or Hash-based Message Authentication Code is a means for calculating a message authentication code using a cryptographic hash function and a cryptographic key. If you wish to use the HMAC signature as an additional key and level of security, under the SSL/TLS handshake section, set the **Use HMAC Signature** toggle key to **On** position, then click the **Generate** button so that the router can randomly generate the key. The **Server key timestamp** field is updated with the time that the key was generated. Click the **Download** button to download the key file so that it can be uploaded on the client.
10. Select an **Authentication type**. Authentication may be done using a Certificate or Username / Password or Certificate and Username / Password. See the below sections for information on each of the certificate types.

Certificate authentication

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

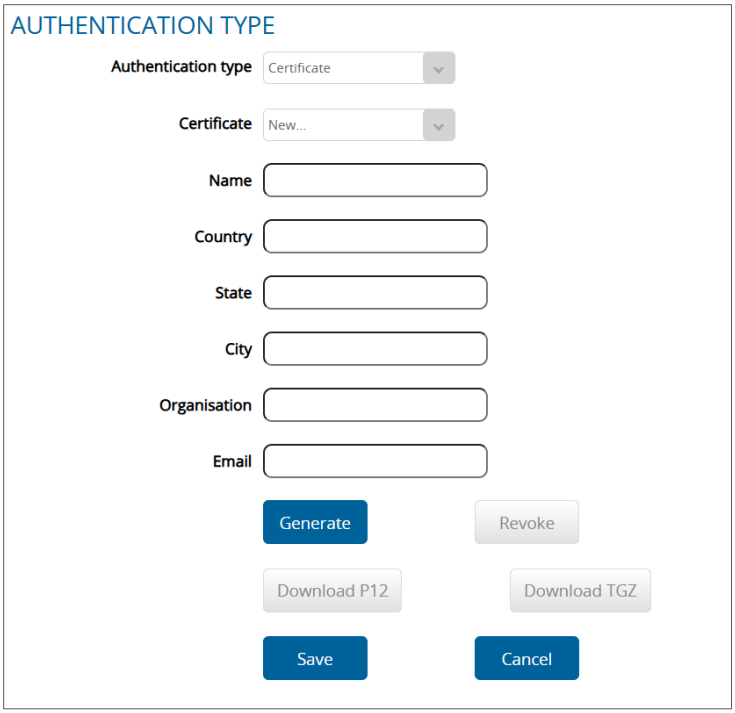


Figure 8-49 OpenVPN server Certificate authentication settings

Once the certificate is generated, click **Download P12 button** or **Download TGZ button** to save the certificate file, depending on which format you would like. If for some reason the integrity of your network has been compromised, return to this screen, use the **Certificate** drop-down list to select the certificate and then select the **Revoke** button to make the certificate invalid. Click **Save** to save the 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 t**he Download CA TGZ** or **Download CA certificate** depending on file format to save the ca.crt file. This file will need to be provided to the client.

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

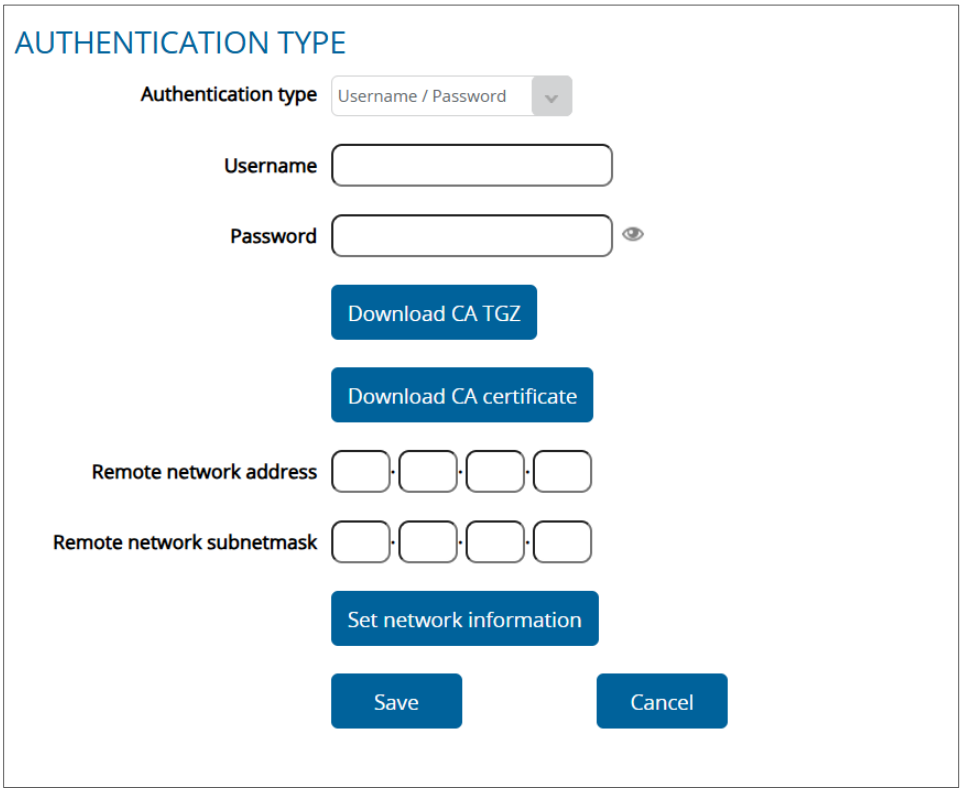


Figure 8-50 OpenVPN server Username/Password authentication settings

Optional: Enter values for **Remote network address** and **Remote network subnetmask** and click **Set Network Information** to allow the OpenVPN server to route traffic to the network behind the client.

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

Certificate and Username / Password Authentication

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

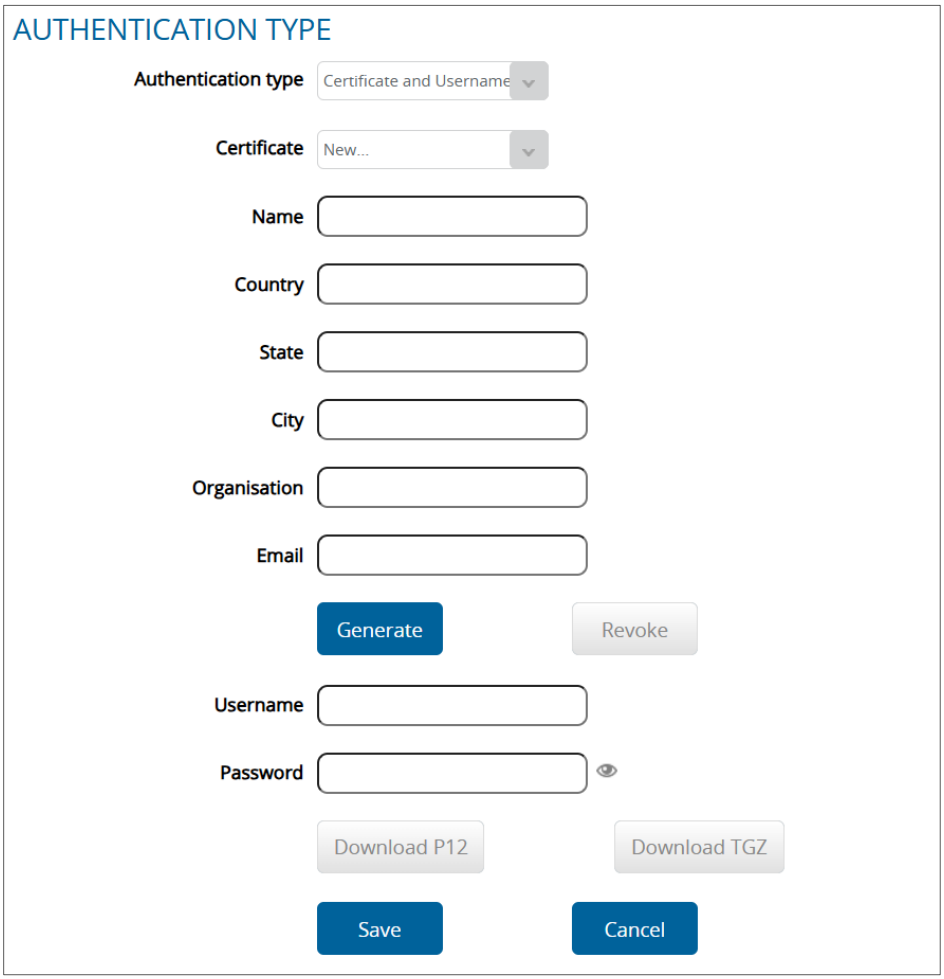


Figure 8-51 OpenVPN server Certificate and Username/Password authentication settings

Configuring an OpenVPN client

To configure and OpenVPN client:

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

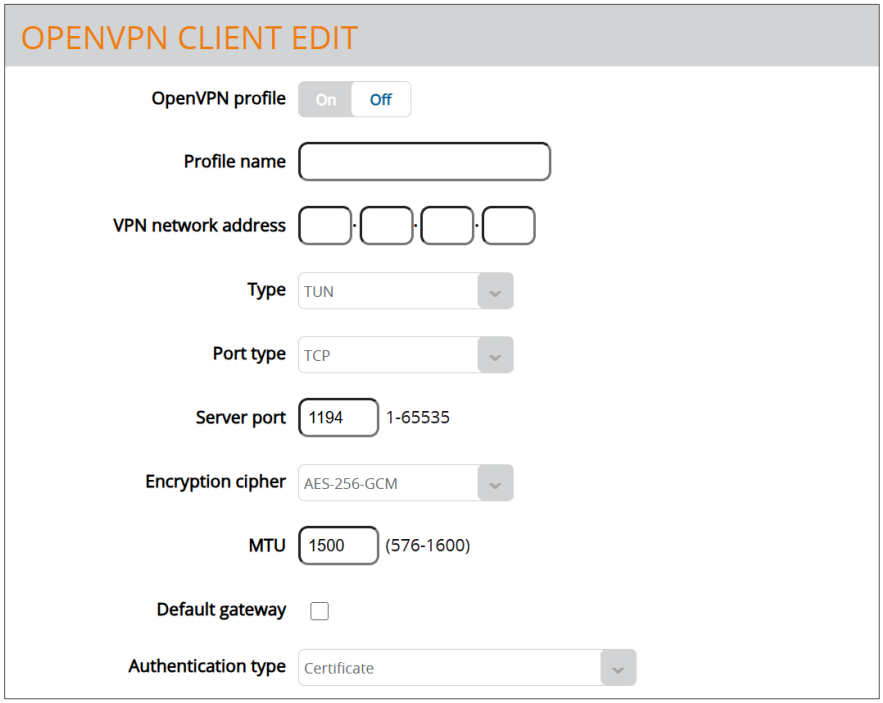


Figure 8-52 OpenVPN client settings

2. Set the **OpenVPN profile** toggle key to the **On** position.
3. In the **Profile name** field, enter a name for the OpenVPN client profile you are creating.
4. In the **VPN network address** field, enter the WAN IP address / host domain name of the OpenVPN server.
5. Select **Type** (**TUN/TAP**). Default is **TUN**.
6. In the **Port type** field, select a packet type to use for your OpenVPN Server and in the **Server port** field, enter a port number. The default OpenVPN port is 1194 and default packet type is UDP.
7. In the **Encryption cipher** field, select the encryption type for the connection. The default is **AES-256** as this is the strongest encryption level.
8. Enter a maximum transmission unit value in the **MTU** field.
9. 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.
10. Select the **Authentication type** to use for the OpenVPN client. The available options are Certificate, Username and Password, and Certificate and Username / Password. See the below sections to understand the different authentication types.

Certificate Authentication

In the OpenVPN client edit section, if the **Authentication type** is selected as **Certificate**, the below sections display.

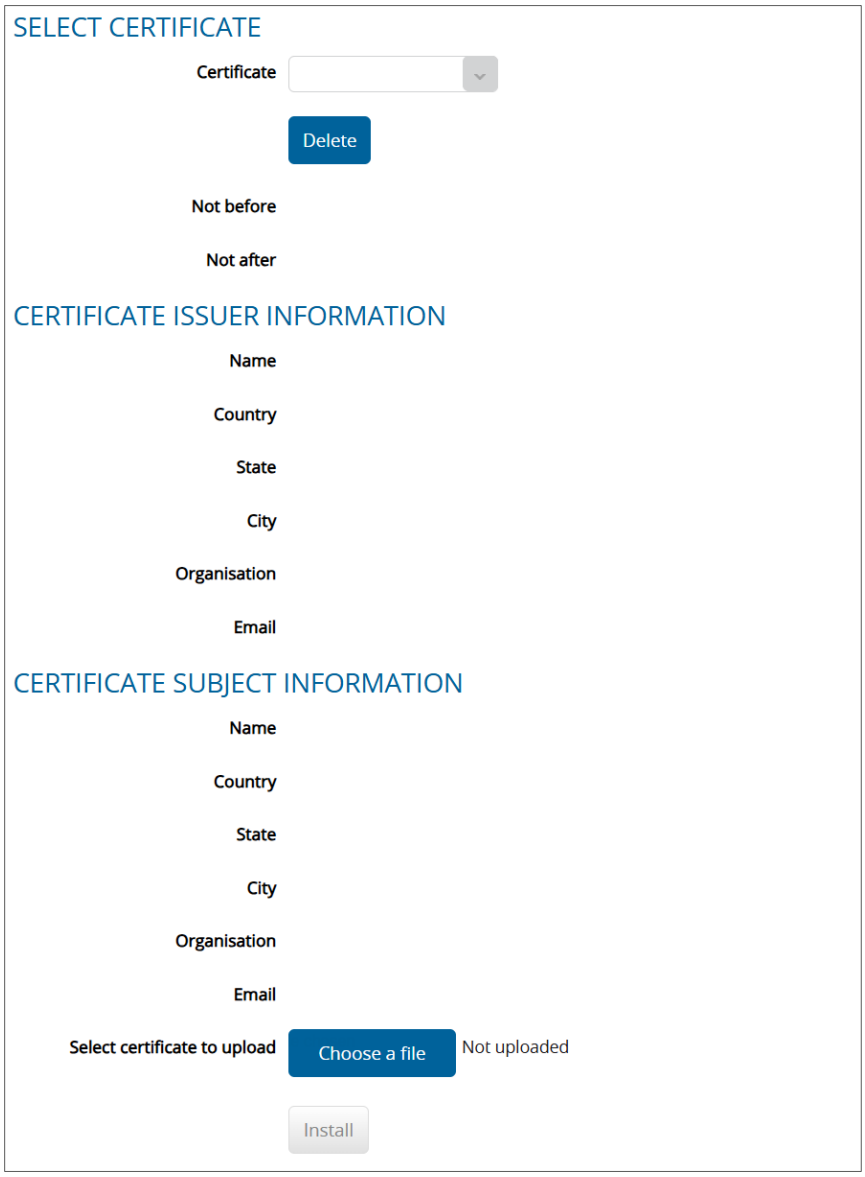


Figure 8-53 OpenVPN client Certificate authentication

In the **Select certificate to upload** field at the bottom of the screen, click **Choose a file**, locate and select the certificate file saved during OpenVPN server configuration. Click **Upload** to upload it to the router, all the certificate related fields are populated accordingly.

Use the **Certificate** field to select the required certificate from the drop-down when you have multiple certificates.

If you want to delete an existing certificate, use the Certificate field to select the certificate and then click **Delete**.

Username / Password Authentication

In the OpenVPN client edit section, if the **Authentication type** is selected as **Username / Password**, the below sections display.

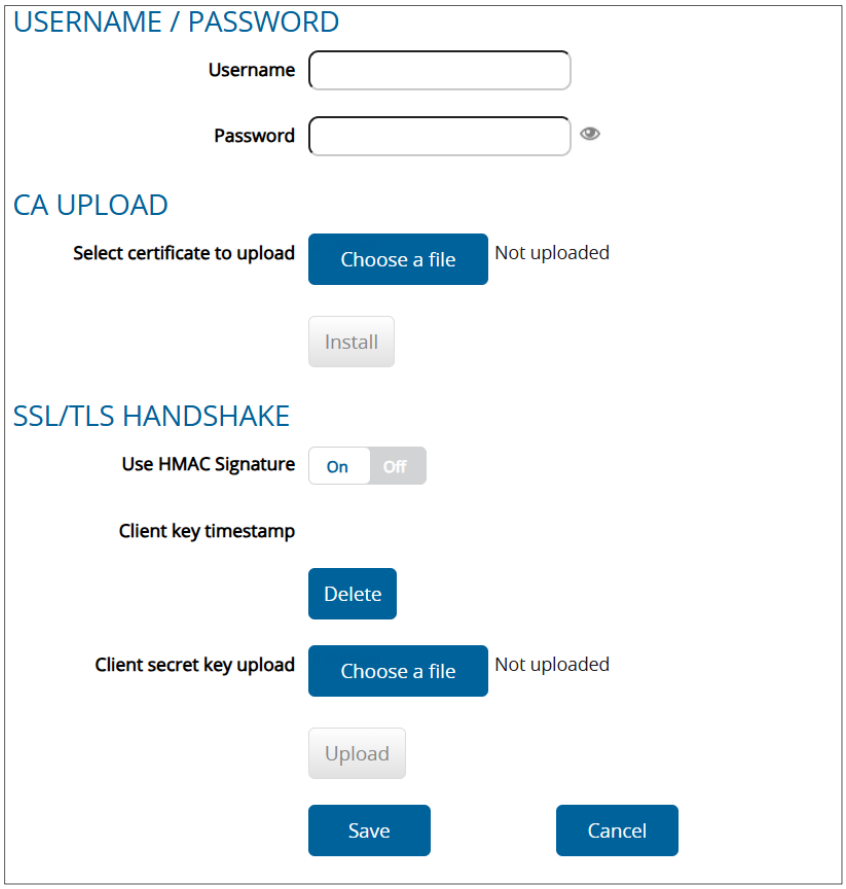


Figure 8-54 OpenVPN client Username/Password authentication

To configure Username / Password authentication:

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

Certificate and Username / Password authentication

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

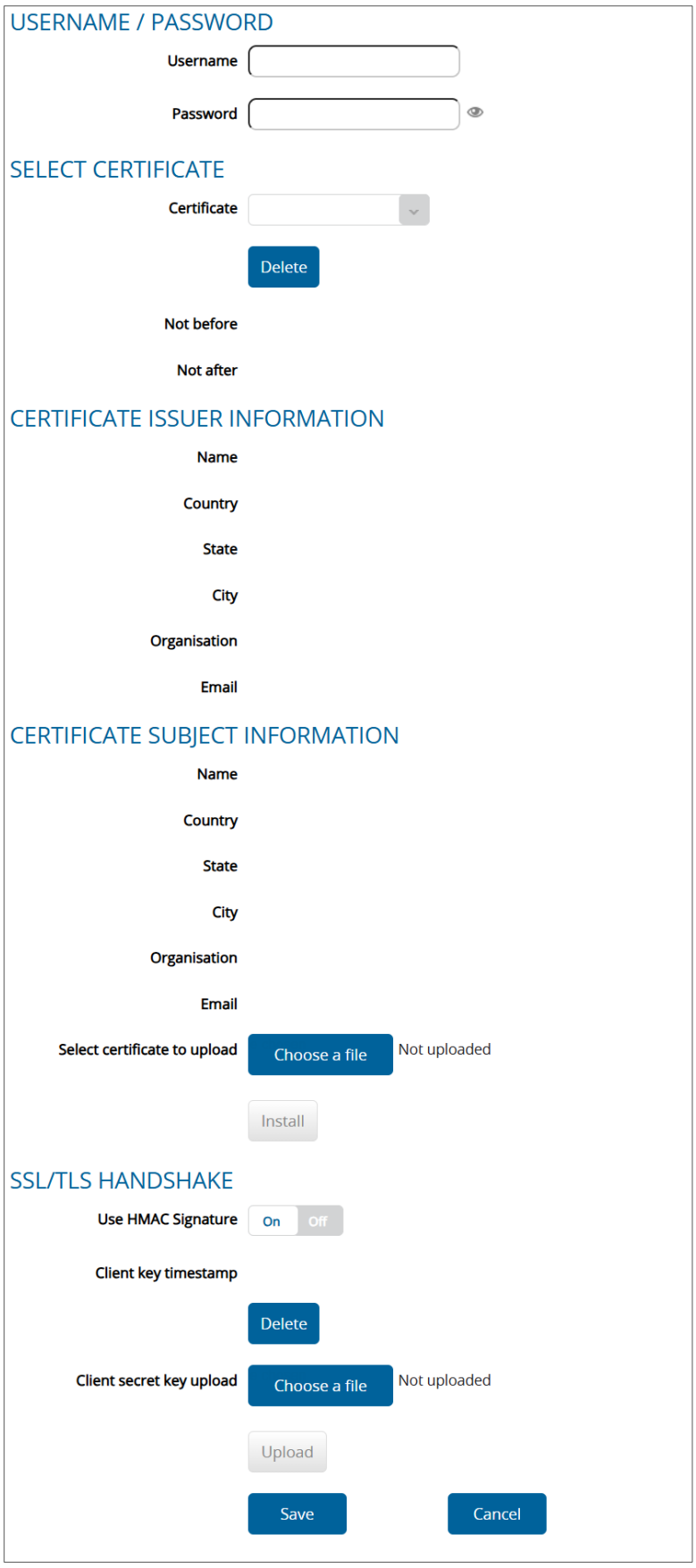


Figure 8-55 OpenVPN client Certificate and Username/Password authentication settings

Configuring an OpenVPN P2P Connection

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

To configure an Open VPN P2P profile, click **+Add** button for the OpenVPN P2P list, the OpenVPN Peer Edit page displays.

OpenVPN P2P server configuration

In the OpenVPN Peer Edit page, for **Peer type** field select **server**, the OpenVPN P2P server configuration settings display.

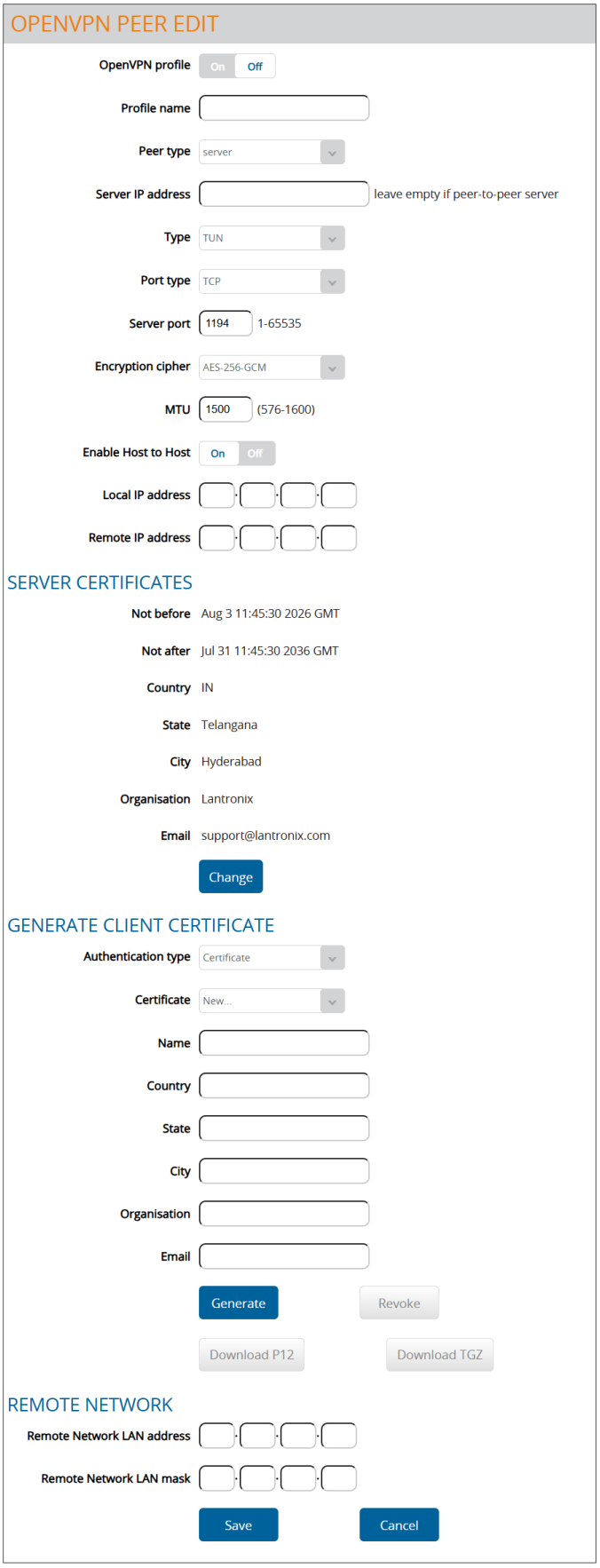


Figure 8-56 OpenVPN P2P server settings

Table 8-9 OpenVPN P2P server configuration details

Parameter	Description
OpenVPN profile	Set to **On** to enable.
Profile name	Enter a name for OpenVPN P2P profile.
Peer type	Select **server** to configure the router to operate as an OpenVPN server and accept connection requests from the remote OpenVPN client.
Server IP address	Leave the field blank when **Peer type** is set to **sever**.
Type	Enter the type of virtual network interface to create: • **TUN** • **TAP**
Port type	Select a packet type to use: • **TCP** • **UDP** The default packet type is **UDP**.
Server port	Enter the port number to use. The default OpenVPN port is **1194**.
Encryption cipher	Select the Encryption cipher to use: • **AES-256-GCM** • **AES-128-GCM** • **CHACHA20-POLY1305** • **None**
MTU	Enter the Maximum Transmission Unit (MTU) size. It specifies the maximum size (in bytes) of a data packet that can be transmitted through the VPN tunnel without fragmentation.
Enable Host to Host	Set to **On** to enable ad **Off** to disable. When enabled, it allows direct communication between the local and remote VPN endpoint devices over the tunnel. When disabled, only traffic between the connected networks is permitted.
Local IP address	Enter the Local IP address of the VPN tunnel.
Remote IP address	Enter the Remote IP address of the VPN tunnel.
Server Certificates	
Displays the details of the Server certificate used. Click **Change** to add a different certificate. You will be redirected to OpenVPN Sever Certificate page.	
Generate Client Certificate	
For **Authentication type** field, select **Certificate**. For **Certificate** field, select **New** and enter the required values for all the fields. Click **Generate** to generate the certificate. Once the certificate is generated, click **Download P12** or **Download TGZ** to save the certificate file in the corresponding format. If for some reason	

Parameter	Description
the integrity of your network has been compromised, return to this screen, use the Certificate drop-down list to select the certificate and then click **Revoke** to make the certificate invalid.	
Remote Network	
Remote Network LAN address	Enter the network address of the remote LAN network on the VPN client side.
Remote Network LAN mask	Enter the subnet mask of the remote LAN network.

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

OpenVPN P2P client configuration

In the OpenVPN Peer Edit page, for **Peer type** field select **client**, the OpenVPN P2P client configuration settings display.

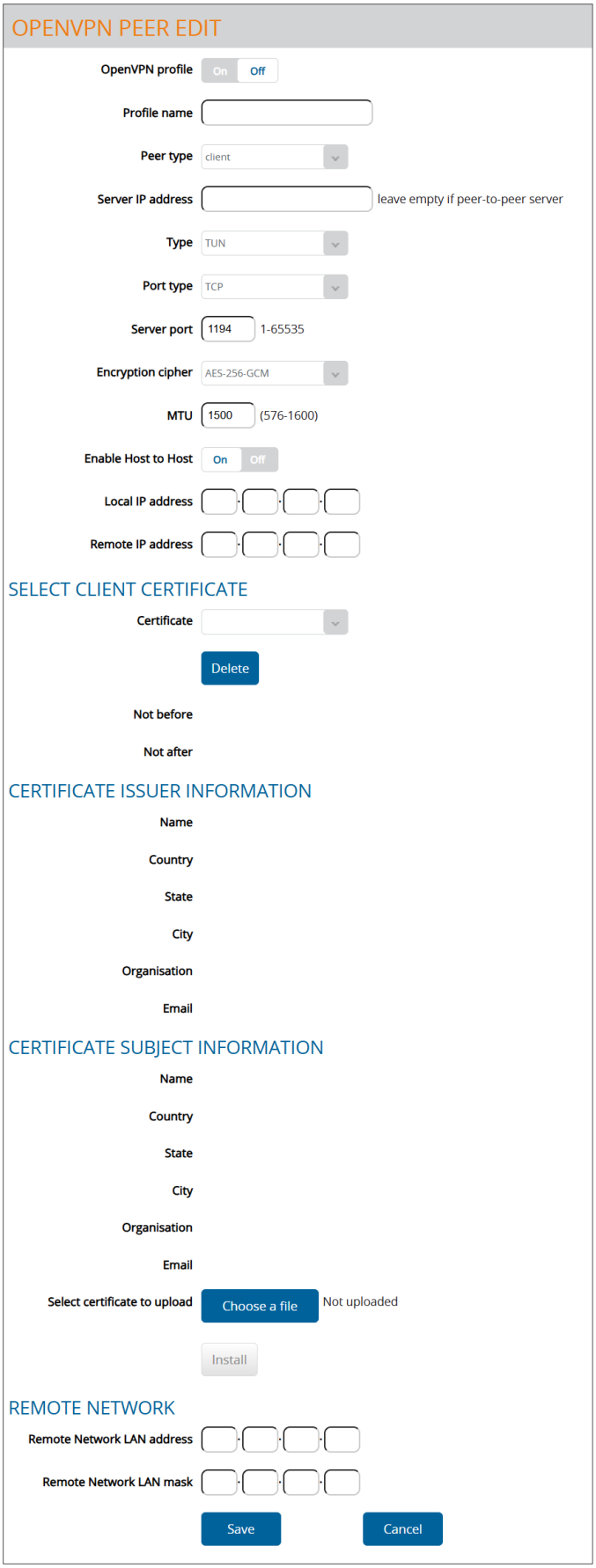


Figure 8-57 OpenVPN P2P client setings

Table 8-10 OpenVPN P2P client configuration details

Parameter	Description
OpenVPN profile	Set to **On** to enable.
Profile name	Enter a name for OpenVPN P2P profile.
Peer type	Select **client**, to configure the router to operate as an OpenVPN client and initiate a connection to the remote OpenVPN server.
Server IP address	Applicable when **Peer type** is set to **client**. Enter the IP address or hostname of the remote Open VPN server.
Type	Enter the type of virtual network interface to create: • **TUN** • **TAP**
Port type	Select a packet type to use: • **TCP** • **UDP** The default packet type is **UDP**.
Server port	Enter the port number to use. The default OpenVPN port is **1194**.
Encryption cipher	Select the Encryption cipher to use: • **AES-256-GCM** • **AES-128-GCM** • **CHACHA20-POLY1305** • **None**
MTU	Enter the Maximum Transmission Unit (MTU) size. It specifies the maximum size (in bytes) of a data packet that can be transmitted through the VPN tunnel without fragmentation.
Enable Host to Host	Set to **On** to enable ad **Off** to disable. When enabled, it allows direct communication between the local and remote VPN endpoint devices over the tunnel. When disabled, only traffic between the connected networks is permitted.
Local IP address	Enter the Local IP address of the VPN tunnel.
Remote IP address	Enter the Remote IP address of the VPN tunnel.
Select Client Certificate	
For the **Certificate** field, select the client certificate generated during the OpenVPN P2P server configuration. The other fields are populated accordingly.	
Certificate Issuer Information	

Parameter	Description
Click **Choose a file**, locate and select the client certificate. Click **Install** to upload the certificate. The other fields are populated accordingly.	
Certificate Subject Information	
Click **Choose a file**, locate and select the client certificate. Click **Install** to upload the certificate. The other fields are populated accordingly.	
Remote Network	
Remote Network LAN address	Enter the network address of the remote LAN network on the VPN server side.
Remote Network LAN mask	Enter the subnet mask of the remote LAN network.

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

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.

To access GRE Tunnelling page, navigate to **Networking > VPN settings > GRE tunnelling**.

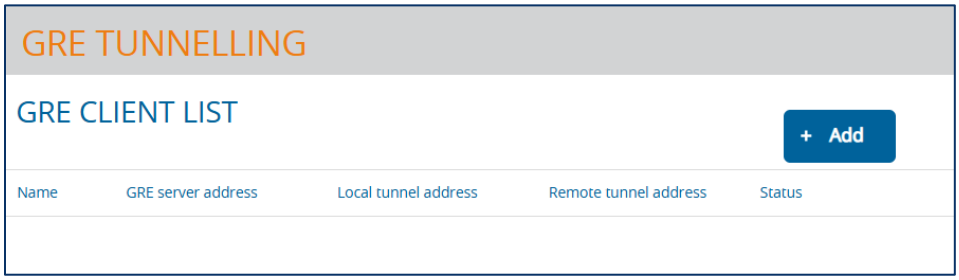


Figure 8-58 GRE tunnelling page

Configuring GRE tunnelling

To configure GRE tunnelling:

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

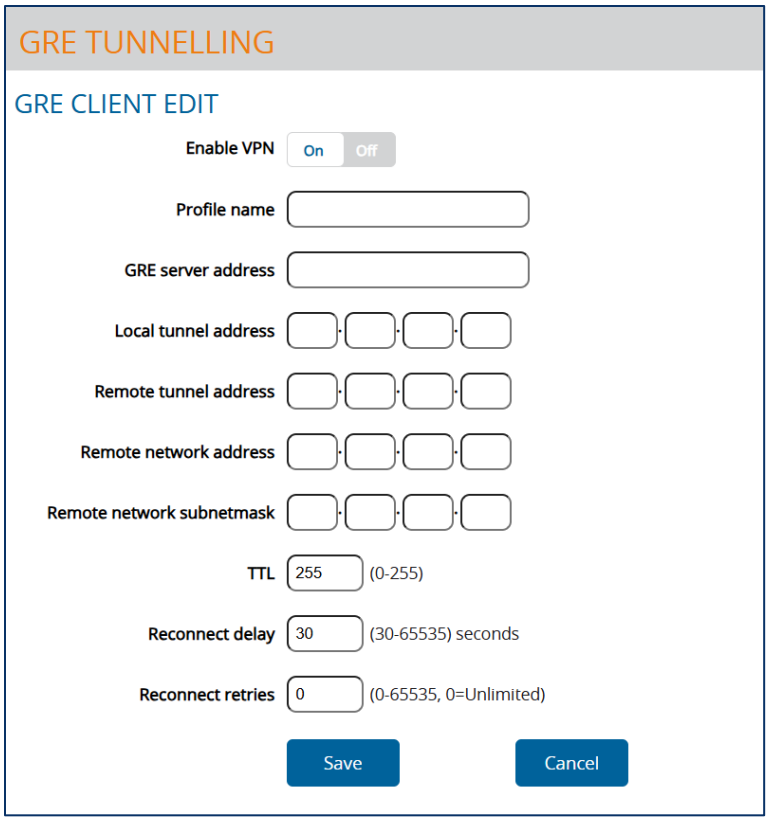


Figure 8-59 GRE client edit settings

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

Pairpoint Secure VPN

Pairpoint Secure VPN is a quantum-safe VPN client for the NTC-500 Series router. It establishes an OpenVPN tunnel secured with TLS-PSK (pre-shared key) authentication, where the pre-shared key is derived from the device SIM using the 3GPP Bootstrapping Security Function (BSF). Since the key is generated from the SIM on demand, no key material is stored on the router or shipped in the firmware image.

The VPN service can be managed from:

- Device Web UI
- Device CLI (pps-vpn-manager, the primary management interface over SSH)
- Percepxion cloud platform (for remote management at scale)

Configuring Pairpoint Secure VPN using Web UI

To access Pairpoint Secure VPN page, navigate to **Networking > VPN settings > Pairpoint Secure VPN**.

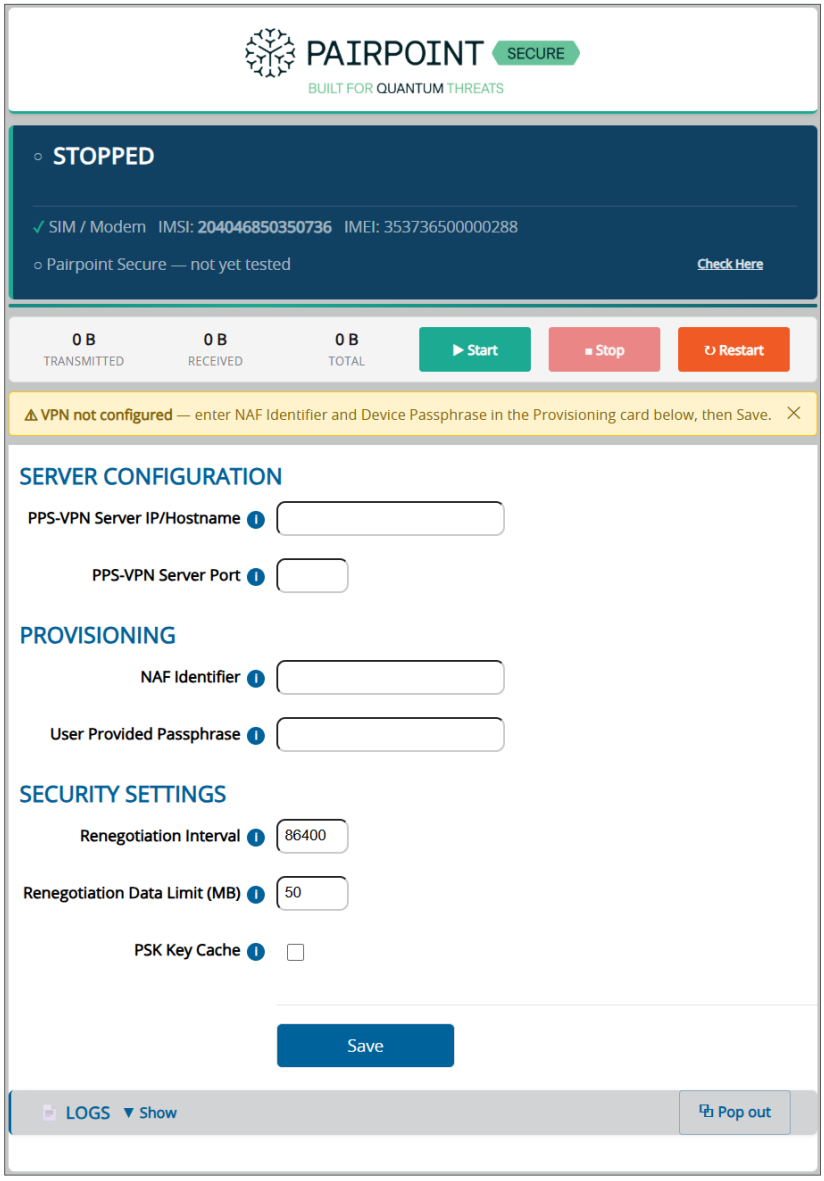


Figure 8-60 Pairpoint Secure VPN page

The Pairpoint Secure VPN page displays:

- Status of the VPN connection – **CONNECTED**, **CHECKING**, **STOPPED**, or **NOT CONFIGURED**
- Connected server, uptime, SIM/modem details, and diagnostic result when VPN is running
- Data transferred over the tunnel interface when VPN is running
- VPN controls (**Start**, **Stop**, and **Restart** buttons)
- VPN configuration settings
- Logs

To establish a Pairpoint Secure VPN connection:

1. Enter the required values for all the fields in VPN configuration settings (see Table 8-11) and click **Save**.

   Note: *The configuration settings are editable only when the VPN is stopped.*

   Table 8-11 Pairpoint Secure VPN configuration details

Parameter	Description
SERVER CONFIGURATION	
PPS-VPN Server IP/Hostname	Enter the IP address or hostname of the Pairpoint Secure VPN server.
PPS-VPN Server Port	Enter the server port. Default port is 1194.
PROVISIONING	
NAF Identifier	Enter the Network Application Function (NAF) identifier used to provision the device for Pairpoint Secure VPN.
User Provided Passphrase	Enter the passphrase used to create your own VPN keys.
SECURITY SETTINGS	
Renegotiation Interval	Enter the interval, in seconds, after which the VPN session renegotiates or refreshes its security parameters. Default value is 86400.
Renegotiation Data Limit (MB)	Enter the maximum amount of data, in MB, after which the VPN session renegotiates its security parameters. Default value is 50 MB.
PSK Key Cache	Select to cache and reuse PSK key material, for faster reconnection. Disabled by default.

2. Click **Start**, the device attempts to establish a VPN connection.
3. Upon successful connection, **CONNECTED** status displays with uptime and data transferred.

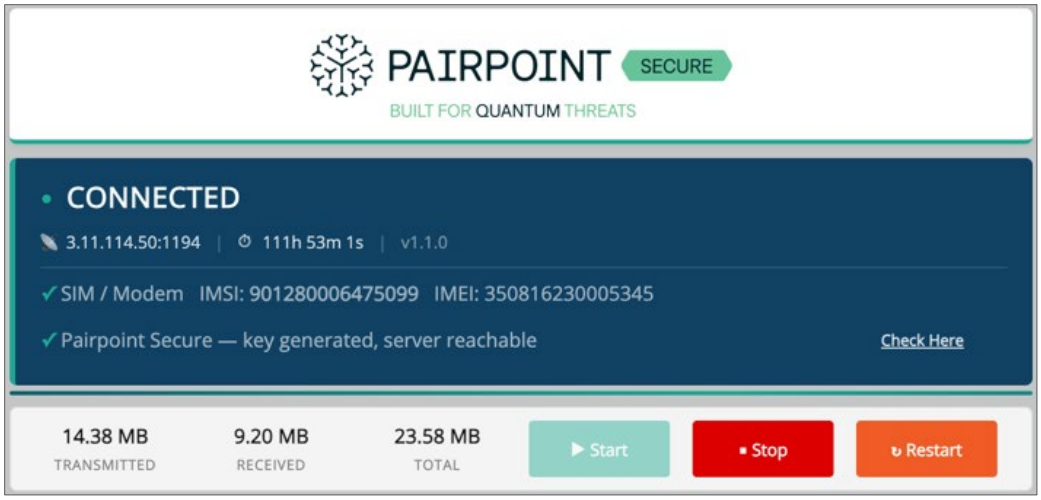


Figure 8-61 Pairpoint Secure VPN Connected Status

Click **LOGS** to show or hide the log information for the VPN session. The LOGS section displays the logs for VPN client activity during a connection attempt. It reports connection progress, authentication status, events, and errors that affect the session. You can use the logs to troubleshoot the errors in case a connection attempt fails.

Server Certificate

Server Certificate allows you to generate a certificate to use with OpenVPN. To access the Server certificate page, navigate to **Networking > VPN settings > Server certificate**.

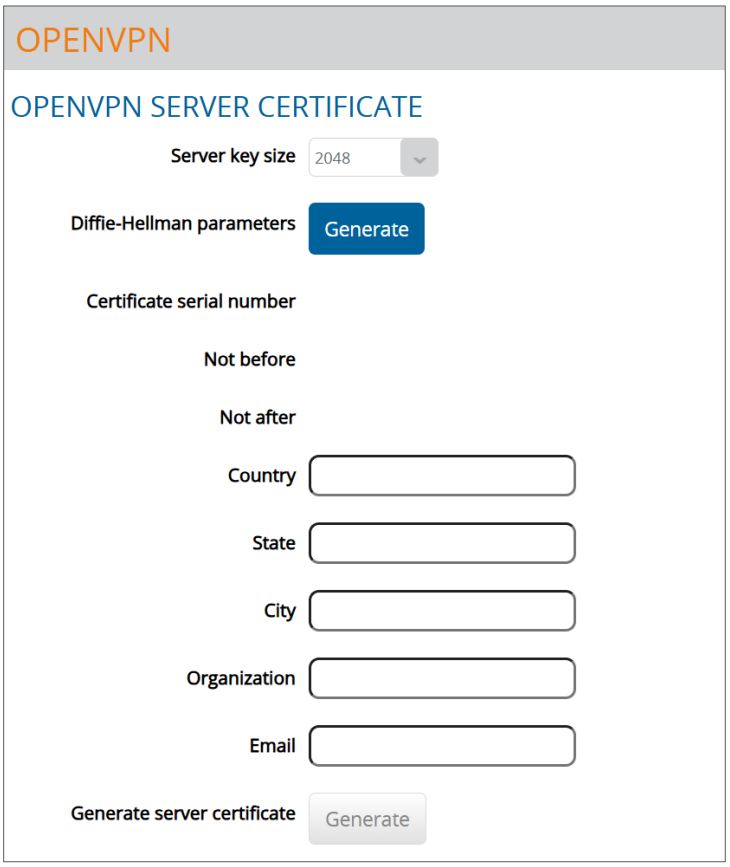
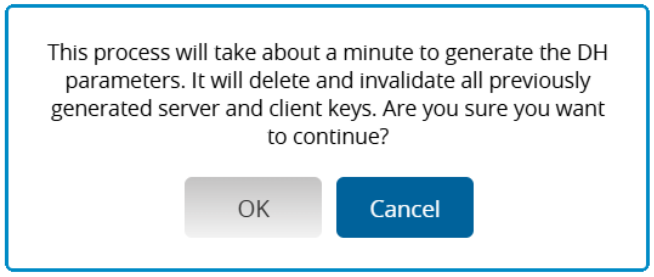


Figure 8-62 Server certificate page

To proceed with generating the certificate, the Diffie-Hellman parameters must be generated. Click **Generate** for the **Diffie-Hellman parameters field.** The following prompt displays.



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



The Server Certificate can now be generated.

Generating the OpenVPN Server Certificate

To generate an OpenVPN Server Certificate:

1. In the **Country** field, enter the SSL Country code for the country the certificate is issued for.
2. In the **State** field, enter the state the certificate is issued for.
3. In the **City** field, enter the city the certificate is issued for.
4. In the **Organization** field, enter the name of the organization for the certificate.
5. In the **Email** field, enter a contact email for the certificate.
6. For the **Generate Server Certificate** field click **Generate** to generate the certificate. Once the certificate is successfully generated, the Certificate serial number and validity dates are shown in **Certificate serial number**, **Not before** and **Not after fields**.

9. Services

The Services page allows you to access and configure the following features:

- Network Time (NTP)
- SMS messaging
- Dynamic DNS
- DNS server
- Internet of Things
- Remote management
- Event configuration
- Email settings
- Low power mode
- Percepxion

To access the Services page, click **Services** tab on the top menu bar.

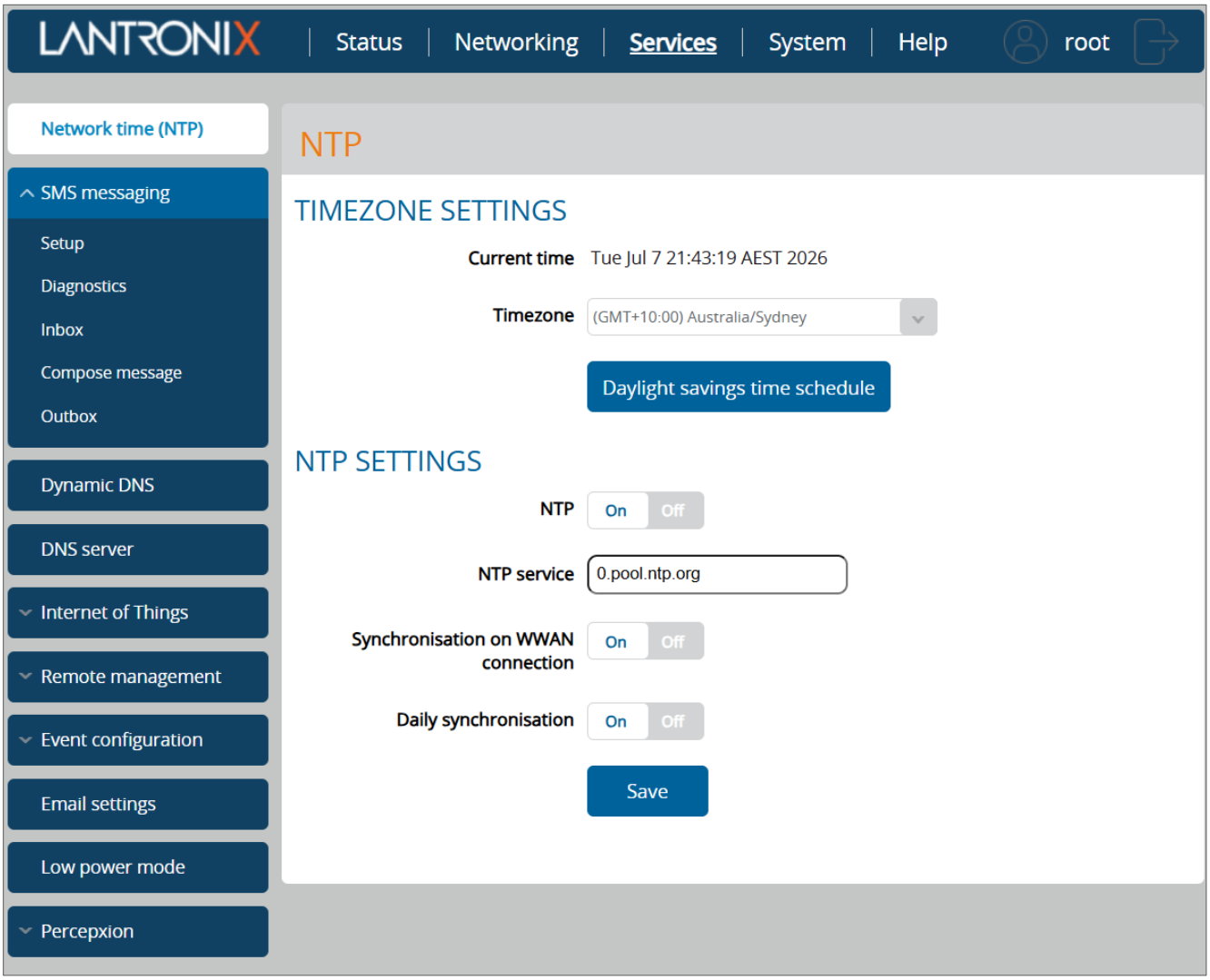


Figure 9-1 Services page

Network time (NTP)

Network Time Protocol (NTP) allows you to configure the NTC-500 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.

To access the Network time (NTP page), navigate to **Services > Network time (NTP)**.

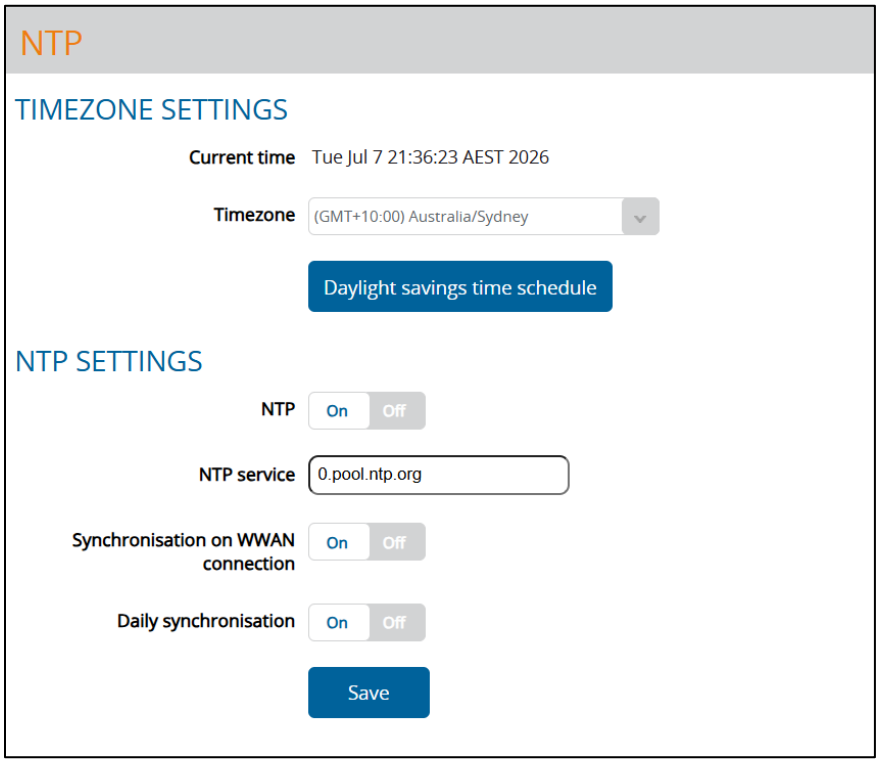


Figure 9-2 Network time (NTP) page

Table 9-1 Network time (NTP) configuration details

Parameter	Description
Timezone settings	
Current time	Displays the date and time configured on the router.
Timezone	Select the required time zone for the router.
Daylight savings time schedule	Click to display the start and end times for daylight savings, if the above selected time zone observes daylight savings.
NTP settings	
Network Time (NTP)	Set to **ON** to enable.
NTP service	Enter the IP address or hostname of the NTP server you want to use.
Synchronization on WWAN connection	Set to **ON** to enable the router to perform time synchronization each time a mobile broadband connection is established.

Parameter	Description
Daily synchronization	Set to **ON** to enable the router to perform time synchronization daily

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

SMS messaging

The NTC-500 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-500 Series router to download and install a firmware upgrade.
- Ability to trigger the NTC-500 Series router to download and apply a configuration file.

Setup

Setup allows you to configure SMS and SMS forwarding features the router. SMS messaging is enabled by default. To access the Setup page, navigate to **Services > SMS messaging > Setup**.

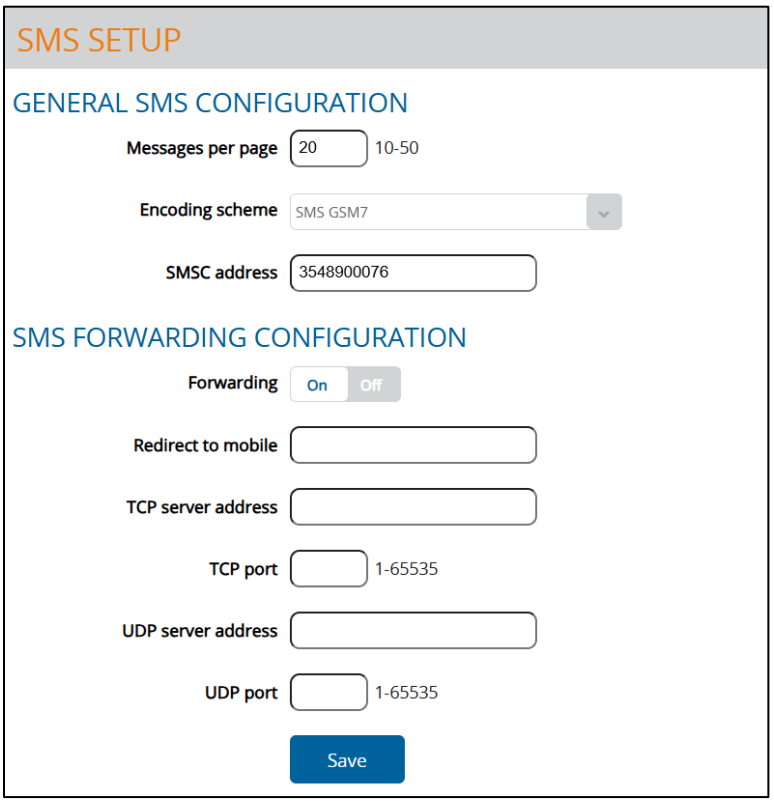


Figure 9-3 SMS setup page

Table 9-2 SMS setup configuration details

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

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 select the Save button.

Diagnostics

Diagnostics allows you 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, navigate to **Services > SMS messaging > Diagnostics**.

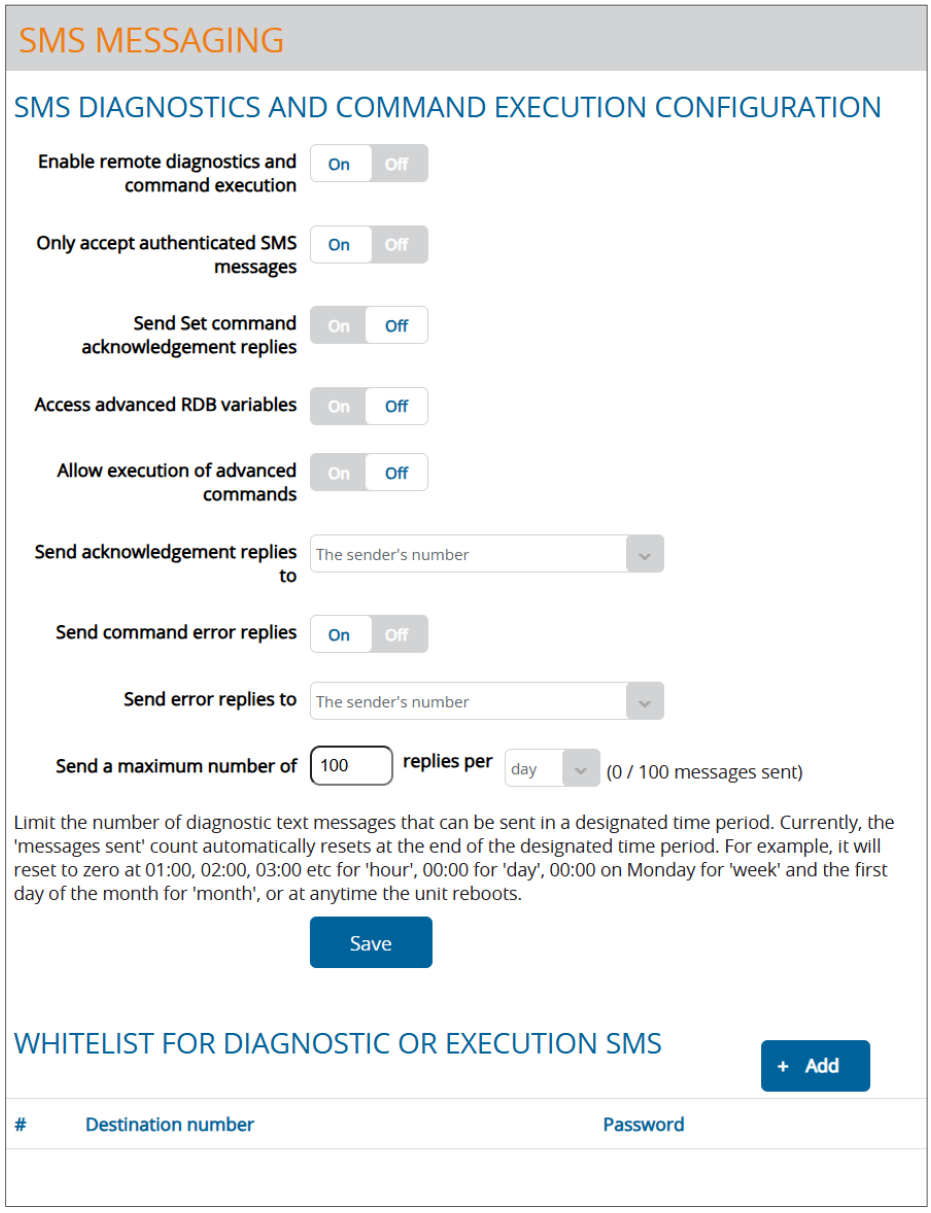


Figure 9-4 SMS diagnostics page

Table 9-3 SMS diagnostics and command execution configuration details

Item	Description
SMS Diagnostics and Command Execution Configuration	
Enable remote diagnostics and command execution	Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands. If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox. ***Note:*** *It is possible to adjust settings and prevent your router from functioning correctly using remote diagnostics. If this occurs, you will need to perform a factory reset to restore normal operation.*
Only accept authenticated SMS messages	Enables or disables checking the sender's phone number against the allowed sender whitelist for incoming diagnostics and command execution SMS messages. If authentication is enabled, the router will check if the sender's number exists in the whitelist. If it exists, the router then checks the password (if configured) in the incoming message against the password in the whitelist for the corresponding sending number. If they match, the diagnostic or command is executed. If the number does not exist in the whitelist or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message. This is enabled by default, and it is strongly advised that you leave this feature enabled to maintain security. ***Important:*** *We highly recommended that you use the whitelist and a password when utilising this feature to prevent unauthorised access. See the Whitelist description for more information.*
Send Set command acknowledgement replies	The NTC-500 Series router will automatically reply to certain types of commands received, such as get commands, or execute commands. However, acknowledgement replies from the NTC-500 Series router are optional with set commands and the Wakeup command. This option enables or disables sending an acknowledgment message after execution of a set command or SMS Wakeup command. If disabled, the router does not send any acknowledgement after execution of a set command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they

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

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

Whitelist for Diagnostic or Execution SMS details

The whitelist 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 whitelist to determine whether the diagnostic or command should be executed. You must configure a password for each number added to the whitelist to give an additional level of security.

The Whitelist for Diagnostic or Execution SMS displays the list of mobile numbers added to whit list and their details.

To configure a Whitelist for Diagnostic or Execution SMS:

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

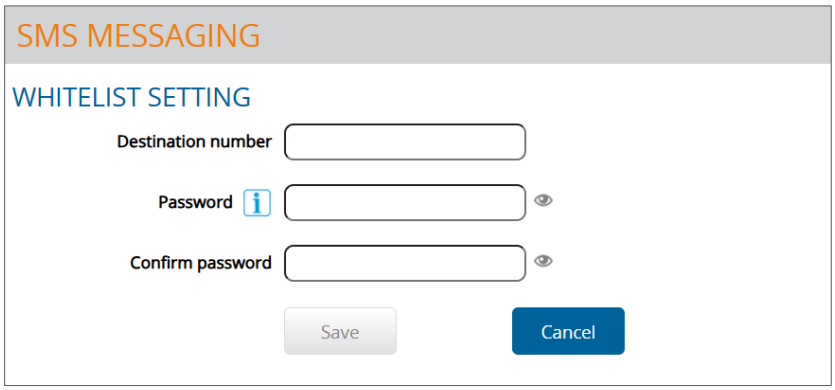


Figure 9-5 Whitelist setting

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

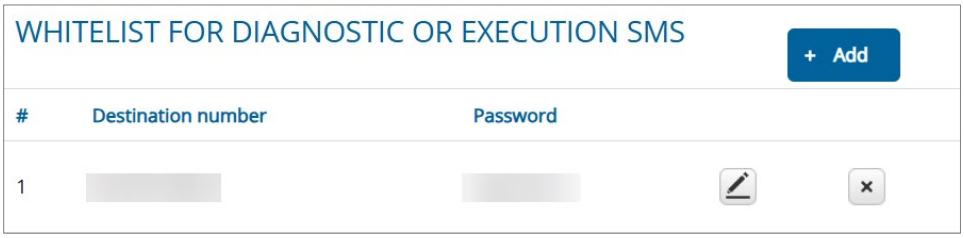


Figure 9-6 Whitelist for Diagnostic or Execution SMS

Table 9-4 Whitelist for Diagnostic or Execution SMS details

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

Types of SMS diagnostic commands

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

- execute COMMAND
- get VARIABLE
- set VARIABLE=VALUE

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

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

The following are some examples of SMS diagnostic commands:

- **password6657 execute reboot**
- **get rssi**
- **set apn1=testAPNvalue**

SMS acknowledgement replies

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

SMS command format

Generic Format for reading variables:

```
get VARIABLE
PASSWORD get VARIABLE
```

Generic Format for writing to variables:

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

Generic Format for executing a command:

```
Execute COMMAND
PASSWORD execute COMMAND
```

Replies

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

Table 9-5 SMS diagnostics command syntax

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

Type	SMS Contents	Notes
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 whitelist 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 9-6 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 whitelist 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
10	**ssh.genkey**s	Instructs the router to generate new public SSH keys.

Item	Command	Definition
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 9-7 List of get/set commands

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

Command name	Example	Description
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 9-8 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"

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

Network scan and manual network selection by SMS

Performing a network scan:

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

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

- MCC
- MNC
- Network Type (LTE, 5G)
- Provider's Name
- Operator Status (available, forbidden, current)

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

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

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

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

Note:

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

Setting the router to connect to a network

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

The command format for the set forceplmn command is:

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

For example:

```
set forceplmn=0
```

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

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

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

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

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

Table 9-10 Mobile Network Provider codes (Australia)

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

Confirming the currently configured operator and network type

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

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

```
Automatic,505,1
```

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

SMS diagnostics examples

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

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

If authentication required:

```
PASSWORD set username= ”CasaSystems”
```

If authentication not required:

```
set username=’CasaSystems’
```

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

Table 9-11 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`

Description	Input Command (without PASSWORD prefix)
Send SMS to check the current band	**get band**
Send SMS to Disconnect (if connected) and reconnect the data connection	**execute pdpcycle**
Send SMS to disconnect the data connection	**execute pdpdown**
Send SMS to connect the data connection	**execute pdpup**
Send multiple get command	**get wanip; get rssi**
Send multiple set command	**set ssh.genkeys=1; set username=test; set auth=pap**
Send SMS to reset to factory default settings	**execute factorydefaults**
Send SMS to retrieve status of router	**get status**
Send SMS to retrieve the history of the session, including start time, end time and total data usage	**get sessionhistory**
Send SMS to configure the router to send syslog to a remote syslog server	**set syslogserver=123.209.56.78**
Send SMS to perform firmware upgrade when firmware is located on HTTP server	**execute download http://download.com:8080/firmware_image.cdi** **execute download http://download.com:8080/firmware_image_r.cdi**
Send SMS to perform firmware upgrade when firmware is located on FTP server	**execute download ftp://username:password@download.com/firmware_image.cdi** **execute download ftp://username:password@ download.com/firmware_image_r.cdi**
Send SMS to download and install IPK package located on HTTP server	**execute download http://download.com:8080/package.ipk**
Send SMS to download and install IPK package located on FTP server	**execute download ftp://username:password@ download.com:8080/package.ipk**
Send SMS to set the LED mode timeout to 10 minutes	**set ledmode=10**
Send SMS to retrieve the current LED mode	**get ledmode**
Retrieve current SSH protocol	**get ssh.proto**
Select SSH protocol	**set ssh.proto=1**
Retrieve password authentication status	**get ssh.passauth**
Enable/disable password authentication on host	**set ssh.passauth=1 or set ssh.passauth=0**

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

Inbox

Inbox displays all received messages that are stored on the router. To access Inbox, navigate to **Services > SMS messaging > Inbox**.

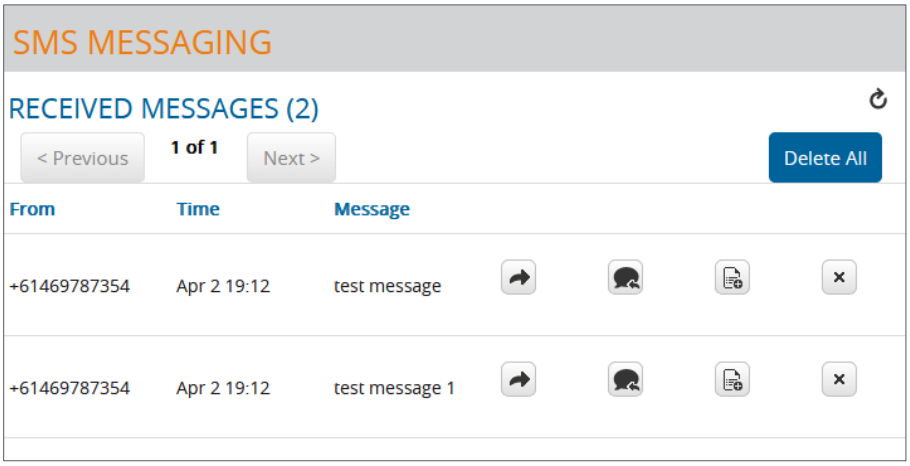


Figure 9-7 Inbox

Table 9-12 Inbox details

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

Compose message

Compose message allows you to send SMS text messages to a single or multiple recipients. To access the Compose message page, navigate to **Services > SMS messaging > Compose message**.

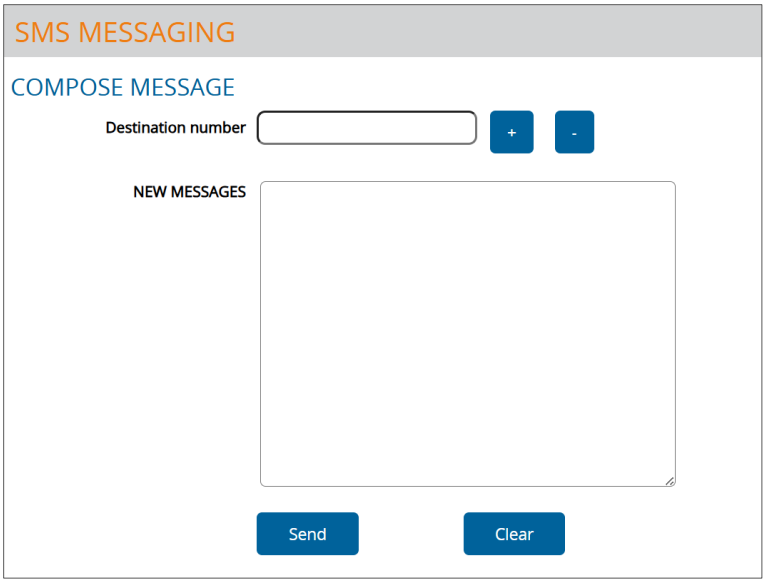


Figure 9-8 Compose message

A new SMS message can be sent to a maximum of 9 recipients at the same time. After sending the message, the result is displayed next to the destination number as "Success" or "Failure". By default, only one destination number field is displayed. Additional destination numbers may be added one at a time after entering a valid number for the current destination number field. To add a destination number, select the + button and to remove the last destination in the list, select the - button.

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

For example:

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

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

Outbox

The Outbox displays all sent messages. To access Outbox, navigate to **Services > SMS messaging > Outbox**.

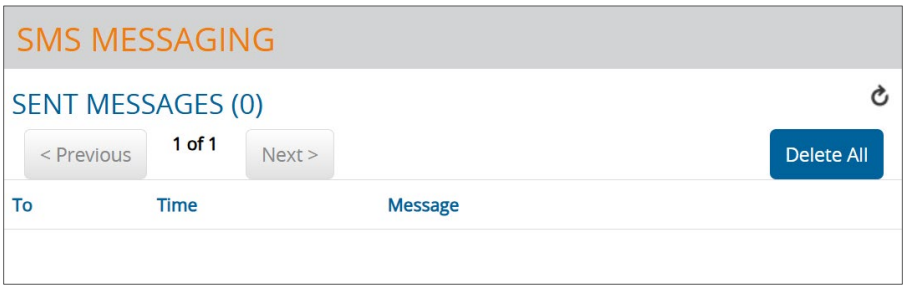


Figure 9-9 Outbox

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

Dynamic DNS

Dynamic DNS (DDNS) allows your NTC-500 Series router to associate an easy-to-remember domain name, such as **[yourdomainname].com** with the regularly changing IP address assigned by your carrier. This feature allows you to connect to the NTC-500 Series router and its internal network more easily for maintenance. To access the Dynamic DNS page, navigate to **Services > Dynamic DNS**.

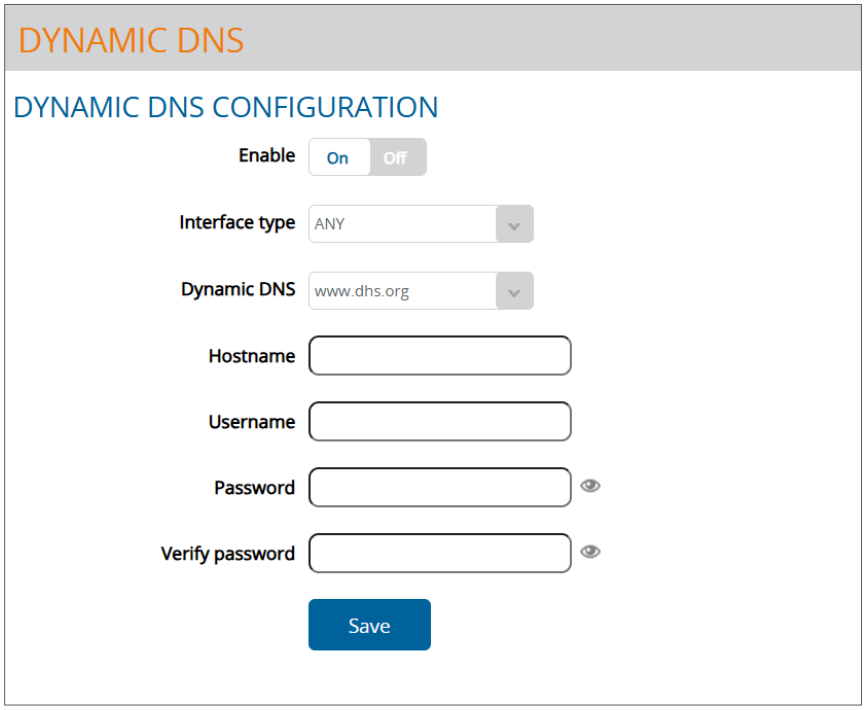


Figure 9-10 Dynamic DNS page

To use DDNS, you will need to sign up for a DDNS provider which is supported by the NTC-500 Series router. The supported providers are:

- www.dhs.org
- www.dydns.org
- www.easydns.com
- www.no-ip.com
- www.zoneedit.com

To configure DDNS on the NTC-500 Series router you will require your unique hostname from the provider, as well as your username and password which you used to sign up to the provider.

To configure DDNS:

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

DNS server

DNS server allows you to configure custom DNS servers for your NTC-500 Series router. To access the DNS server page, navigate to **Services > DNS server**.

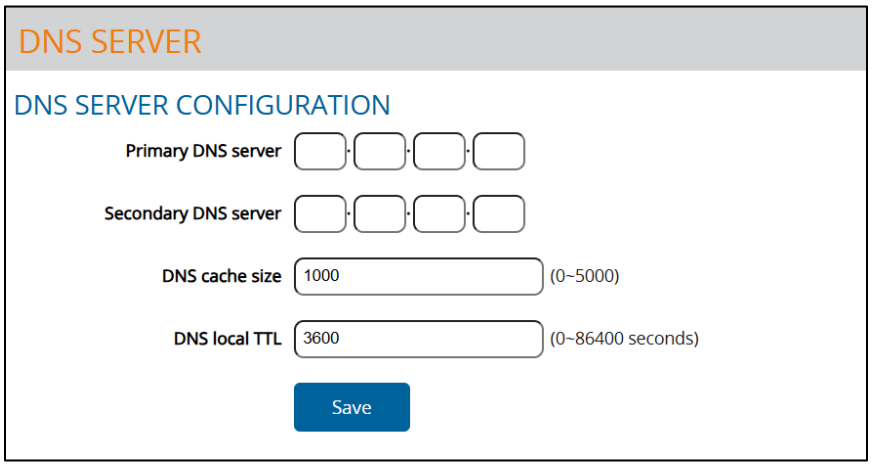


Figure 9-11 DNS server page

To configure the DNS servers:

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

Internet of Things

MQTT client

MQTT is a standards-based messaging protocol used for machine-to-machine communication. Information is sent to clients in the form of a 'topic'. The NTC-500 Series router can be configured to send device information and neighbouring cells as a topic to common IoT monitoring applications, such as Microsoft Azure IoT Hub and Amazon IoT, using MQTT. The MQTT client page is used to configure the NTC-500 Series router to use the MQTT protocol.

To access the MQTT client page, navigate to **Services > Internet of Things > MQTT client**.

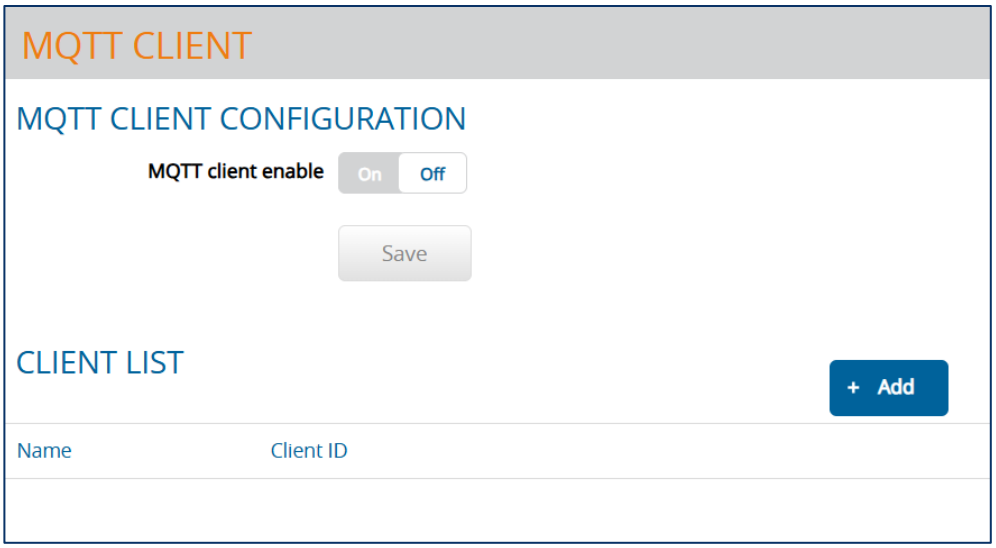


Figure 9-12 MQTT client page

Configuring MQTT

Prerequisites

To configure MQTT on the NTC-500 Series router, you need to create the device on your external MQTT client provider, and generate certificates and keys as required for secure authentication. Refer to your external MQTT provider's documentation for the required authentication configuration.

To configure MQTT:

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

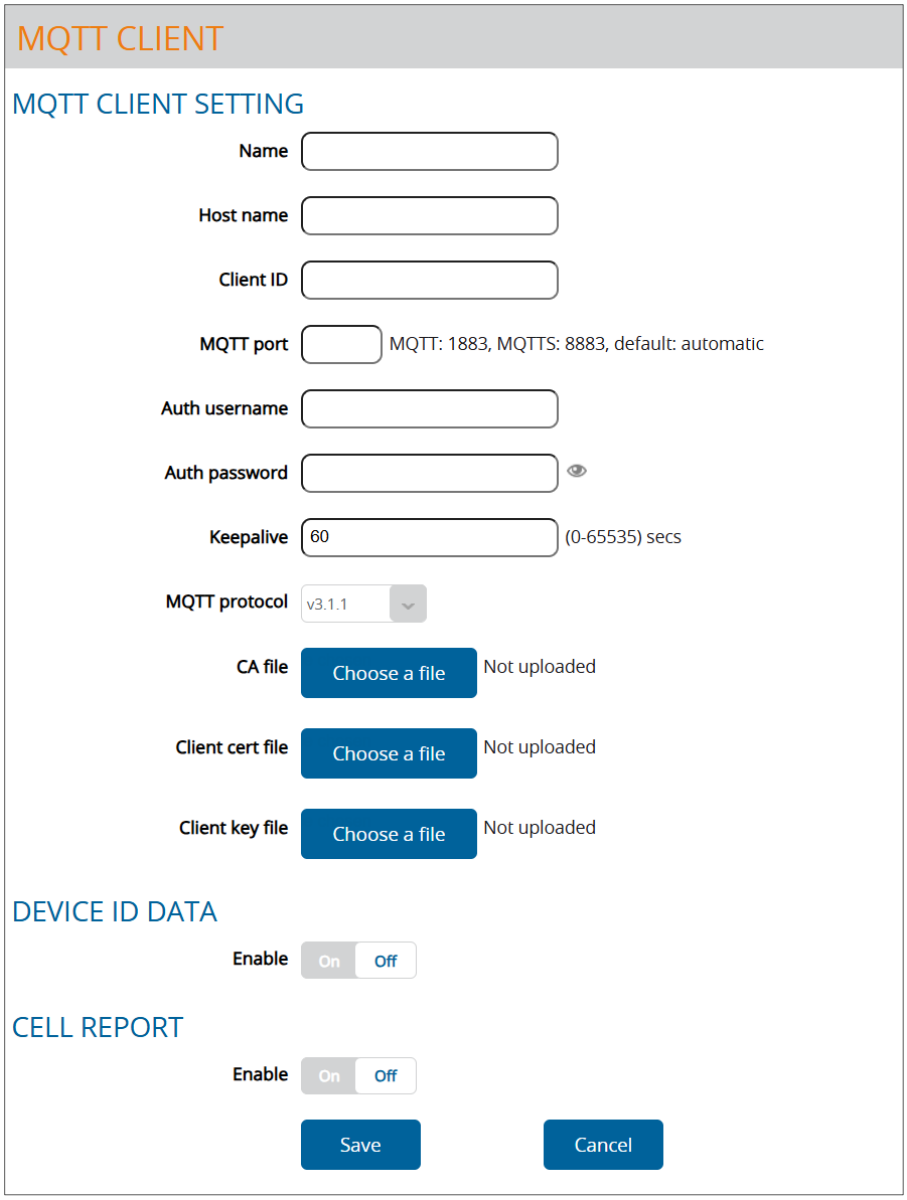


Figure 9-13 MQTT Client settings

Table 9-13 MQTT client configuration details

Item	Description
Name	Enter the name of the client to identify the client on the NTC-500 Series router
Host name	Enter the Hostname of your client
Client ID	Enter Client Id of the client. The Client Id may match the name of your client provider, for example, the name of your AWS IoT 'Thing'.
MQTT port	Enter the port MQTT should be initiated over.
Auth username	Enter the username of the connection.
Auth password	Enter the password of the connection.

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

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

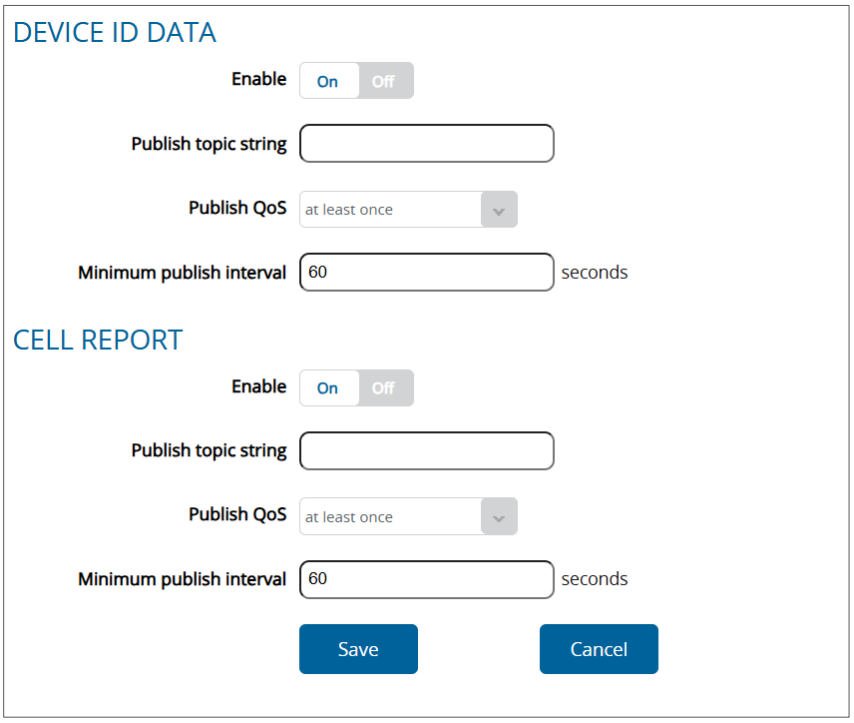


Figure 9-14 MQTT client topics

Table 9-14 MQTT client topics configuration details

Item	Description
Device ID Data	
Enable	Set to **On** to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • **At most once** • **At least once**

Item	Description
	• **Exactly once** At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish interval in seconds. This is the amount of time the NTC-500 Series router will wait before attempting to publish a message.
Cell Report	
Enable	Set to **On** to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • **At most once** • **At least once** • **Exactly once** At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish interval in seconds. This is the amount of time the NTC-500 Series router will wait before attempting to publish a message.

5. Click **Save** to create the client. The client displays in the MQTT client list.
6. Click icon to edit the client and click con to delete the client.

Cumulocity agent

Cumulocity agent allows you to configure a cumulocity agent on the NTC-500 Series router which facilitates communication and data exchange between the router and the Cumulocity IoT platform. It enables centralized management and monitoring of devices.

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

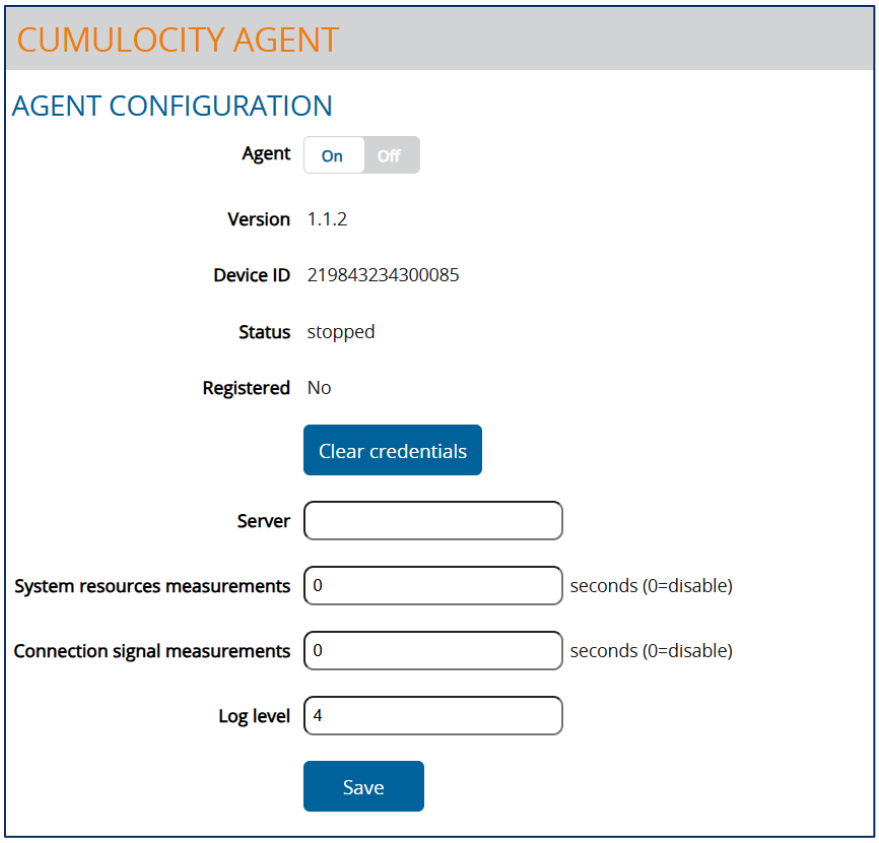


Figure 9-15 Cumulocity agent page

Table 9-15 Cumulocity agent configuration details

Item	Description
Agent	Set toggle to **On** to enable the agent.
Version	Version of the Cumulocity platform.
Device ID	Router's serial number. A unique identifier for the router in Cumulocity.
Status	Status of the agent.
Registered	Displays if the device is registered with the Cumulocity platform.
Clear credentials button	Click to clear credentials related to an existing cumulocity configuration.
Server	Enter the URL of the Cumulocity platform.
System resources measurements	Enter the time interval at which system resource measurements such as CPU usage, memory consumption, disk, and network I/Oare communicated.
Connection signal measurements	Enter the interval at which the cellular signal measurements are communicated.
Log level	Enter the log level to be communicated. The available log levels are: • **1 – dmesg**

Item	Description
	• **2 – ipsec** • **3 – logread** • **4 – ntcagent**

Remote management

OMA-LWM2M

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

It provides:

- Firmware upgrades
- Device monitoring and configuration
- Server provisioning

To access the OMA-LWM2M page, navigate to **Services > Remote management > OMA-LWM2M**.

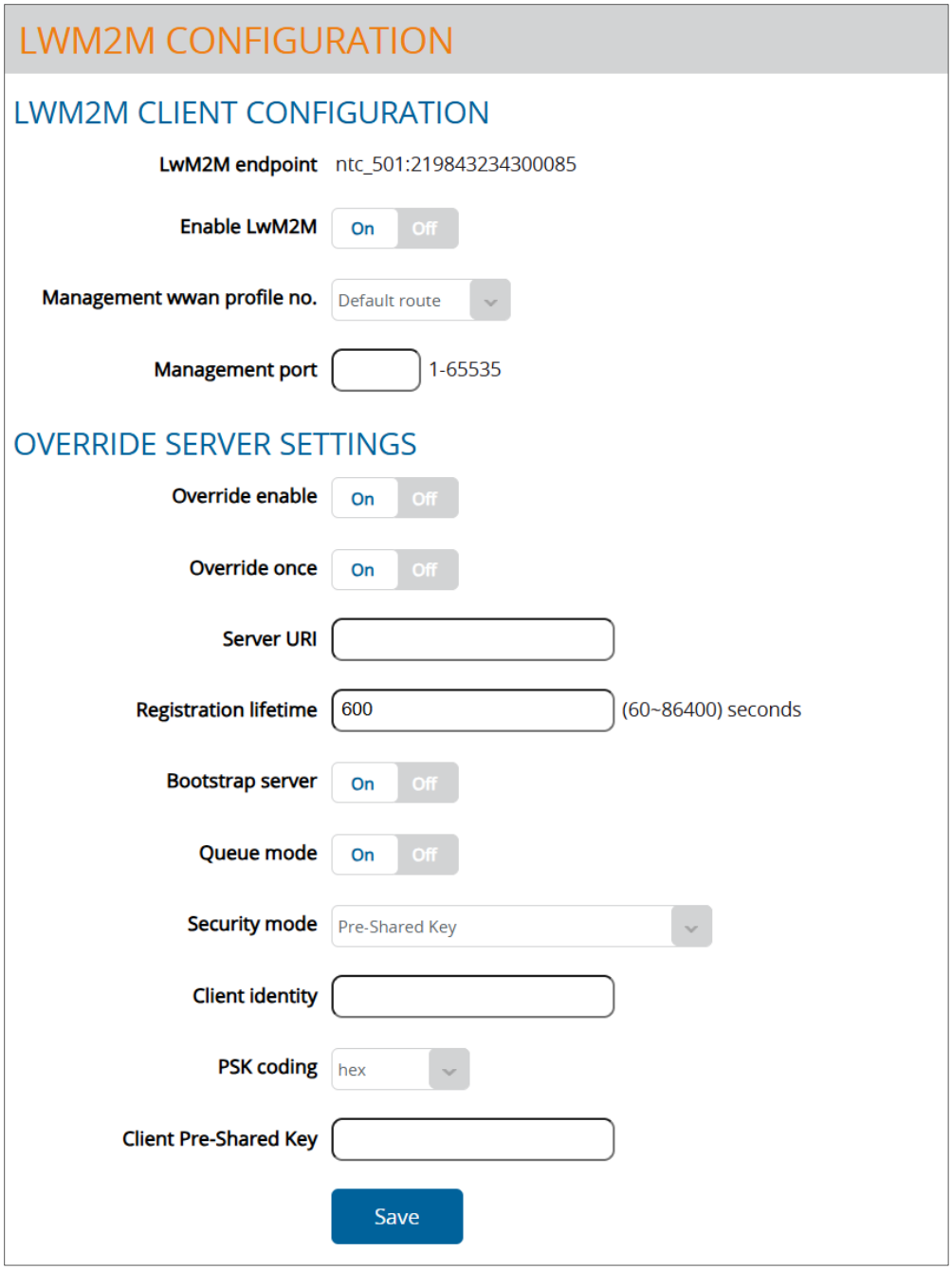


Figure 9-16 OMA-LWM2M page

The table below lists the LWM2M Configuration details.

Table 9-16 LWM2M Configuration details

Item	Description
LWM2M Client Configuration	
LwM2M Endpoint Name	This is the unique ID the device will use to identify itself with LwM2M servers.
Enable LwM2M	Set to **On** to enable LwM2M. The configuration settings display.

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

Supported LWM2M objects

The table below lists the supported object IDs on the NTC-500 Series router. For further information on the objects, refer to the Open Mobile Alliance LWM2M registry.

Table 9-17 LWM2M supported objects

Object	Object ID	Note
LWM2M Server	1	

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

Timeouts

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

SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NTC-500 Series router (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

To access the SNMP page, navigate to **Services > Remote Management > SNMP**.

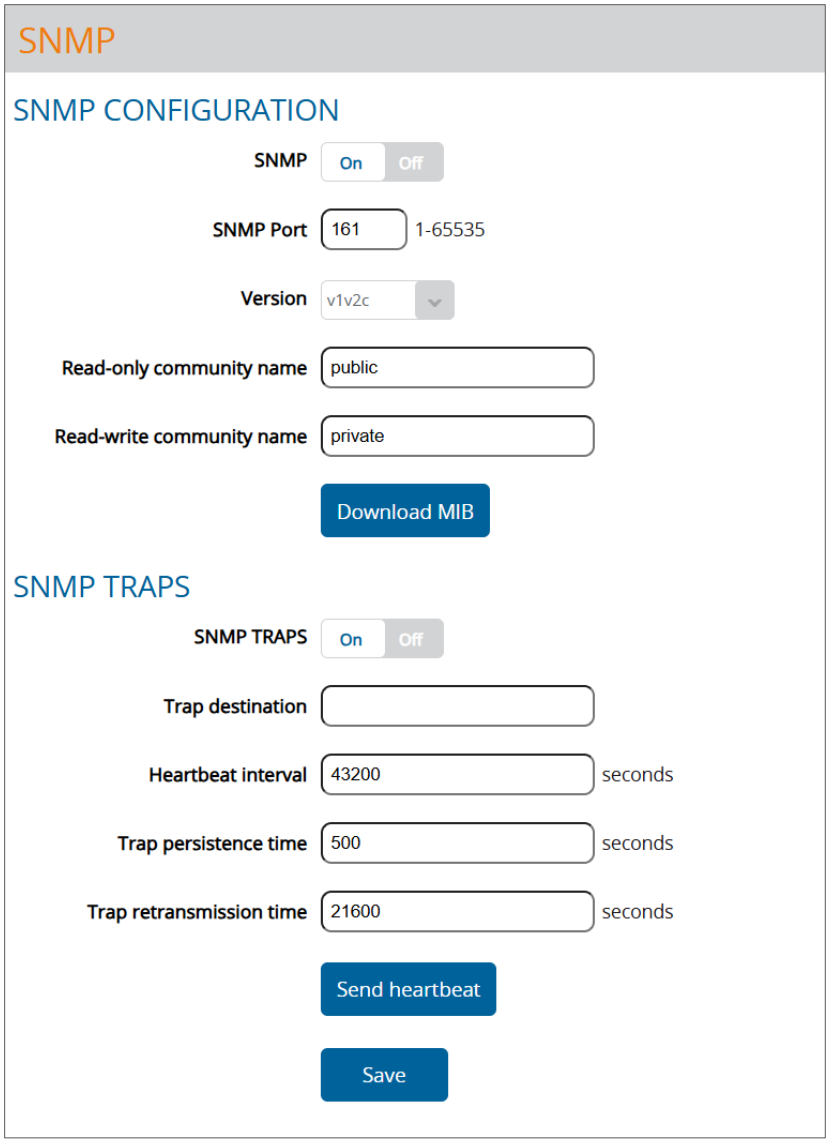


Figure 9-17 SNMP page

Configuring SNMP

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

Configuring SNMP traps

The NTC-500 Series router can be configured to send SNMP traps to a central SNMP Network Management System (NMS) when certain events occur. To configure the SNMP traps:

1. Set the **SNMP Traps** toggle to **On**.
2. In the **Trap Destination** field, enter the address of the SNMP NMS.
3. In the **Heartbeat interval** field, enter the interval in seconds which the NTC-500 Series router should send a heartbeat.

4. In the **Trap persistence time** field, enter the interval in seconds that the NTC-500 Series router should attempt to send a specific trap after the initial occurrence that triggered the trap.
5. In the **Trap retransmission time** field, enter the interval in seconds that the NTC-500 Series router should wait before retransmitting the trap.
6. Use the **Send heartbeat** button to send a test heartbeat.
7. Click **Save** to save and apply the settings.

TR-069

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

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

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

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

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

The NTC-500 Series router sends “inform” messages periodically to alert the ACS server that it is ready. These inform messages can also be configured to accept a connection request from the ACS server. When a connection is established, any tasks queued on the ACS server are executed. These tasks may be value retrieval or changes and firmware upgrades.

To access the TR-069 configuration page, navigate to **Services > Remote management > TR-069**.

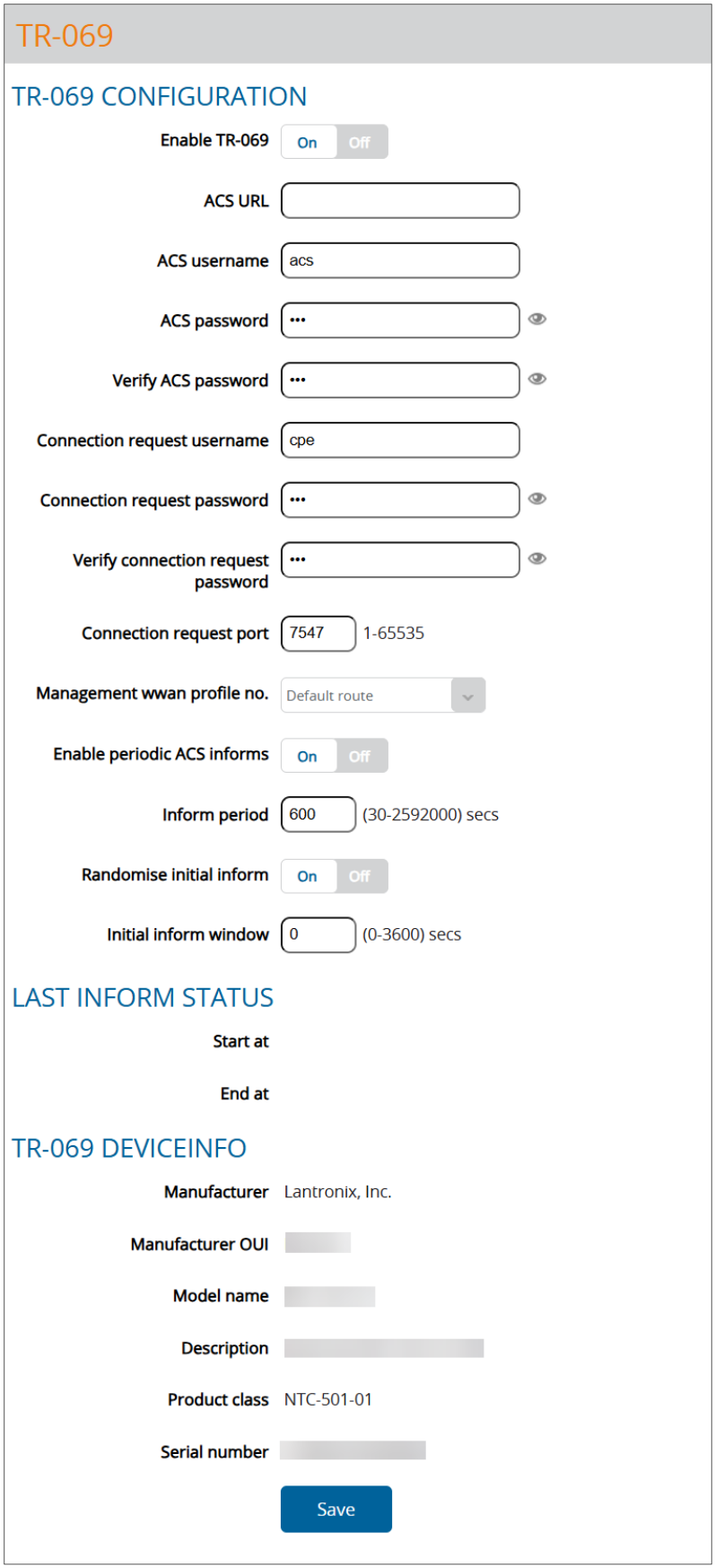


Figure 9-18 TR069 page

To configure TR-069:

1. Set **Enable TR-069** toggle key **On** position.
2. In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.
3. In the **ACS username** field, 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 connection request password** fields, enter the password that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
7. In the **Connection request port** field, enter the port that the request should connect to.
8. In the **Management wwan profile no.** field, enter the WAN profile that should handle the request.
9. Select **Enable periodic ACS informs** toggle key to **On** to turn on the periodic ACS inform messages. The inform message acts as a beacon to inform the ACS of the existence of the router.
10. In the **Inform Period** field, enter the number of seconds between the inform messages.
11. Set the **Randomise Initial inform** to **On** to enable it. This allows the CPE to wait for a random delay within a configured time window before sending the first Inform. It is helpful where many CPE devices contact the AC at the exact same time after reboot or power-up.
12. In the **Initial inform window** field, enter the number of seconds for initial inform window.
13. Select the **Save** to save the settings.

TR-369

TR-369 (User Services Platform – USP) is a device management protocol that allows you to remotely monitor, configure, and control connected devices such as routers, gateways, and IOT devices. It uses a USP controller-USP agent architecture, where a USP controller (central management system) communicates with a USP agent running on the device.

TR-369 supports secure, real-time, and bidirectional communication over multiple transport protocols such as MQTT, WebSockets, etc. NTC-500 Series router uses MQTT protocol for remote management with TR-369 (USP).

To access the TR-369 page, navigate to **Services > Remote management > TR-369**.

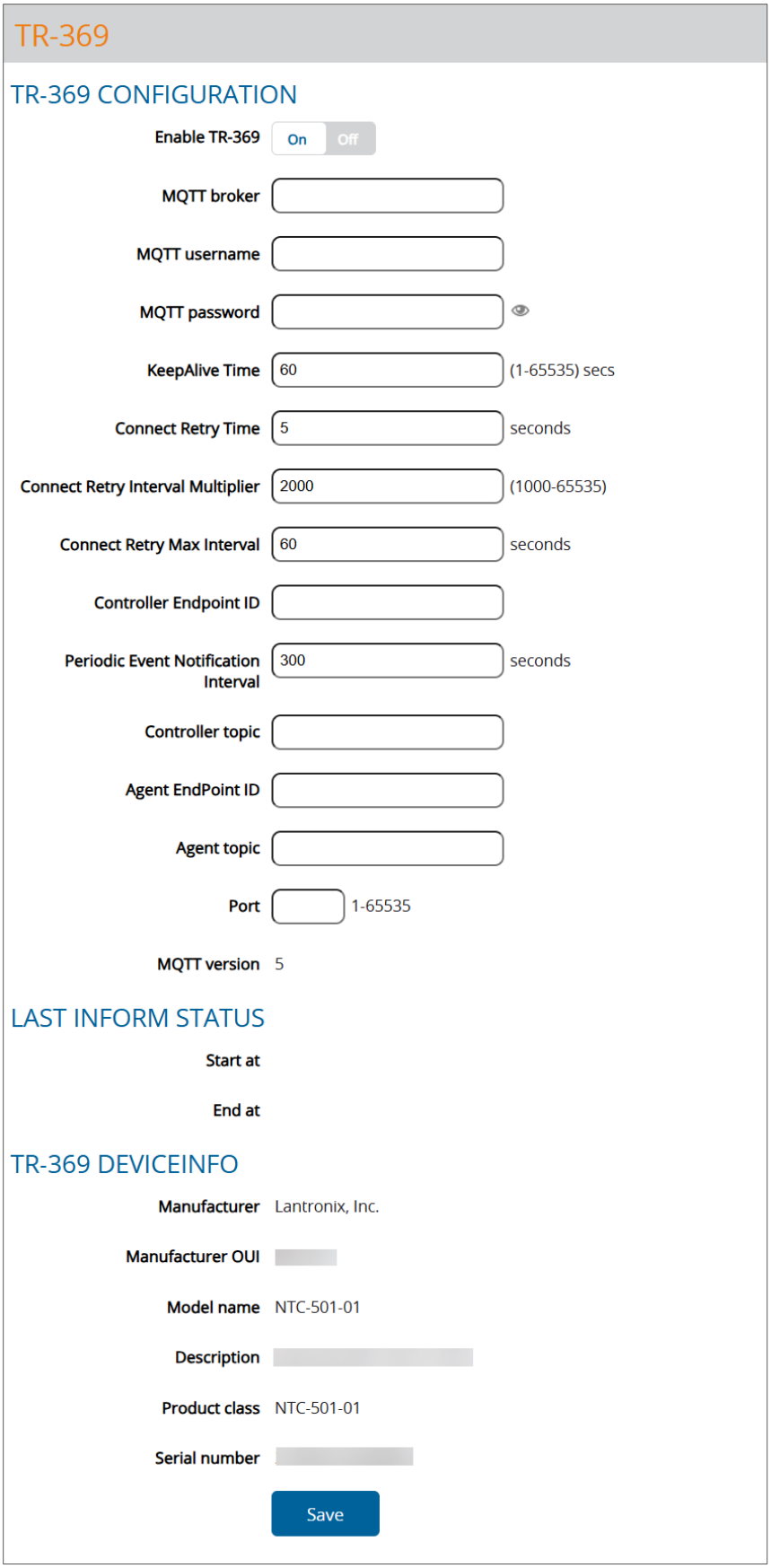


Figure 9-19 TR-369 page

Table 9-18 TR-369 configuration details

Item	Description
TR-369 Configuration	
Enable TR-369	Set to **On** to enable TR-369.
MQTT broker	Enter the hostname or IP address of the MQTT broker to which USP agent connects. This broker acts as the message exchange point between the USP controller and the USP agent.
MQTT username	Enter the username used by the USP agent to authenticate with MQTT broker.
MQTT password	Enter the password for the MQTT username for secure authentication with the MQTT broker.
KeepAlive Time	Enter the time interval in seconds between keepalive messages sent by the USP agent to the MQTT broker to ensure the connection remains active.
Connect Retry Time	Enter the initial delay in seconds before the USP agent attempts to reconnect to the MQTT broker after a connection failure.
Connect Retry Interval Multiplier	Enter the factor by which the retry interval increases after each failed connection attempt.
Connect Retry Max Interval	Enter the maximum time interval in seconds between reconnection attempts.
Controller Endpoint ID	Enter a unique ID for the USP controller. It is used by agent to route messages to the correct controller.
Periodic Event Notification Interval	Enter the time interval in seconds at which the USP agent sends periodic event notifications to the controller.
Controller topic	Enter the MQTT topic on which the USP controller listens for messages from the agent. The agent publishes messages to this topic.
Agent EndPoint ID	Enter a unique identifier for the USP agent. It is used by the controller to identify the agent.
Agent topic	Enter the MQTT topic on which the USP agent listens for messages from the controller. The controller publishes messages to this topic.
Port	Enter the port used to connect to the MQTT broker.
MQTT version	Specifies the version of the MQTT protocol used. The version must be supported by the MQTT broker and the USP agent.

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

Event configuration

Notifictaion configuration

The NTC-500 Series router can be programmed to send notifications when certain events occur on the router. These notifications can be used for proactive monitoring of events such as unit reboots and Ethernet link changes.

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

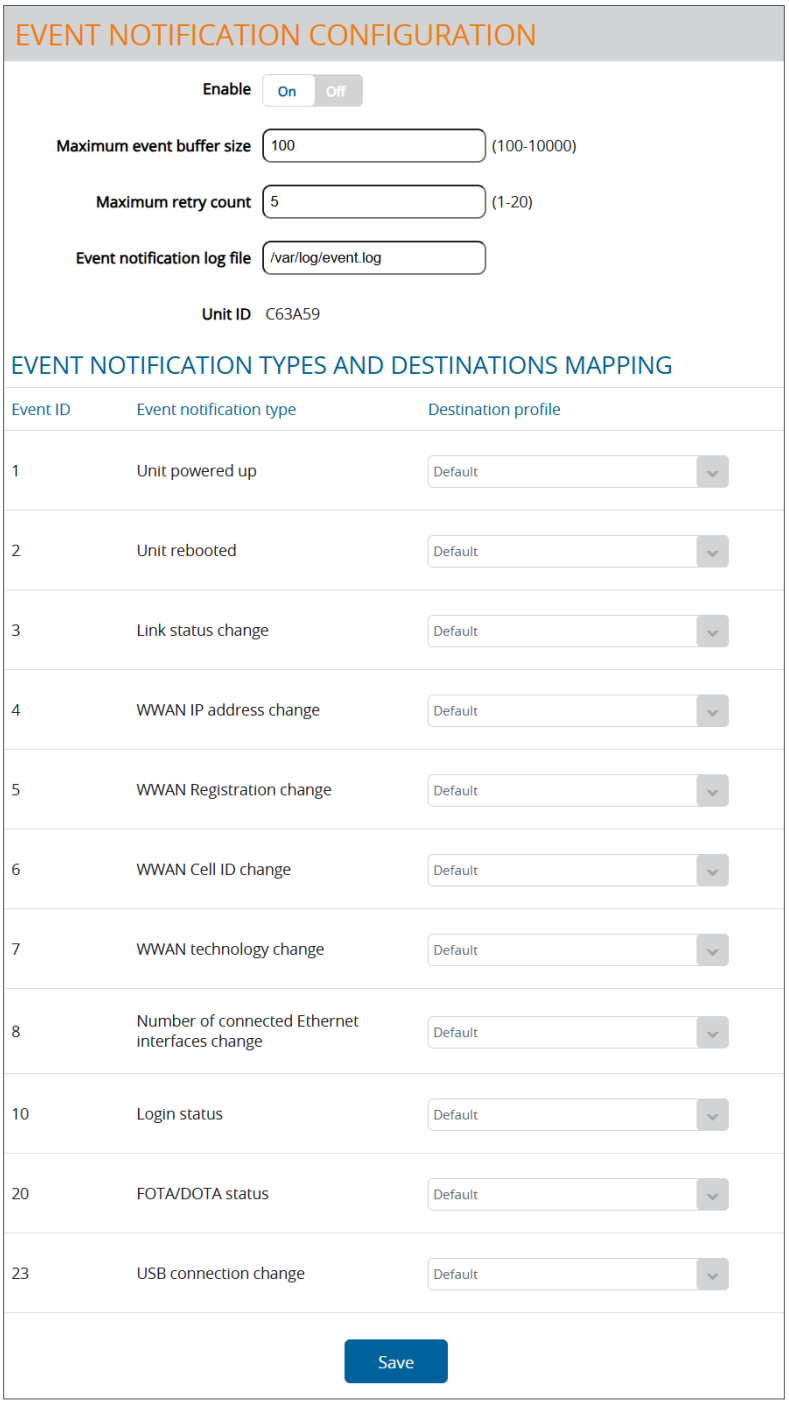


Figure 9-20 Notification configuration page

To configure Notification configuration:

1. Set **Enable** toggle to **On.**
2. In the **Maximum buffer event size** field, specify the buffer size for event notifications which failed to be delivered or are yet to be sent.
3. In the **Maximum retry count** field, enter the number of times the NTC-500 Series router should attempt to deliver the notification in the event of a delivery failure.
4. If required, adjust the output location of the **Event notification log file.**
5. For each **Event notification type** select the **Destination profile** which should send the notification when the notification is triggered. For details on how to configure the Destination Profiles, view the *Destination configuration* section.
6. Select the **Save** button to apply the configuration.

Destination configuration

Destination configuration allows you to configure of the Event Destination profile, which specifies where notifications should be sent when they are triggered.

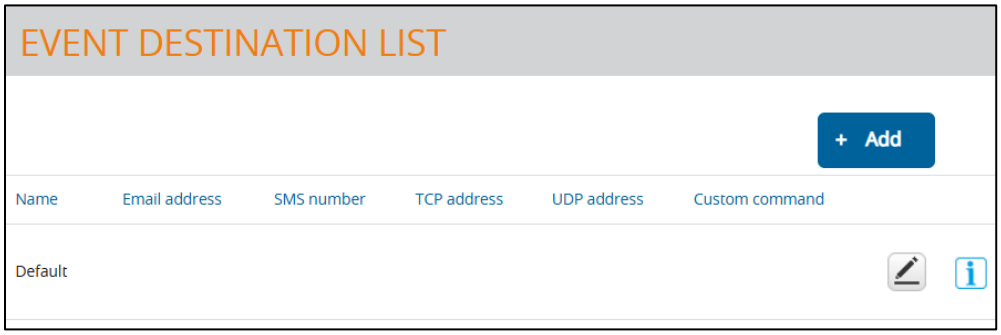


Figure 9-21 Destination configuration page

Configuring a destination

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

To configure an event destination profile:

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

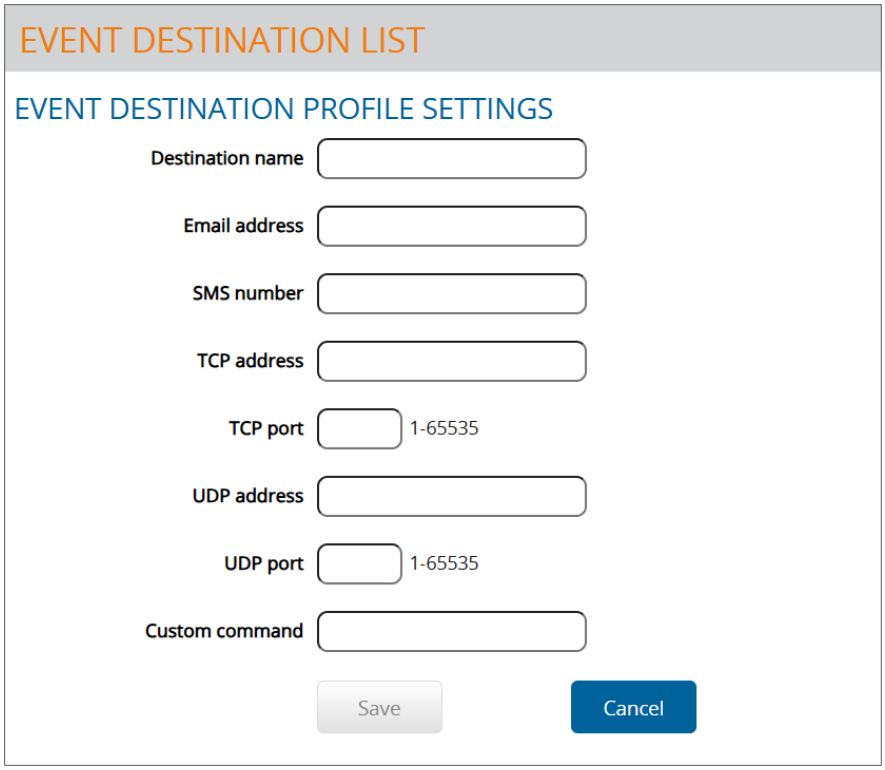


Figure 9-22 Event Destination Profile settings

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

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

3. In the **Email address** field, enter an email address to receive the notification.
4. In the **SMS number** field, enter a phone number to receive the notification as an SMS.
5. In the **TCP address** and **TCP port** fields, enter a TCP address and TCP port to receive the notification over TCP.
6. In the **UDP address** and **UDP port** fields, enter a UDP address and UDP port to receive the notification over UDP.
7. In the **Custom command** field, enter a custom command to execute when the notification is triggered. The command should be a bash compatible command.
8. Select the **Save** button to save the destination profile.

Event notification log

The Event Notification Log displays a log of events which have been triggered.

To access the Event notification log page, navigate to **Services > Event configuration > Event notification log**.

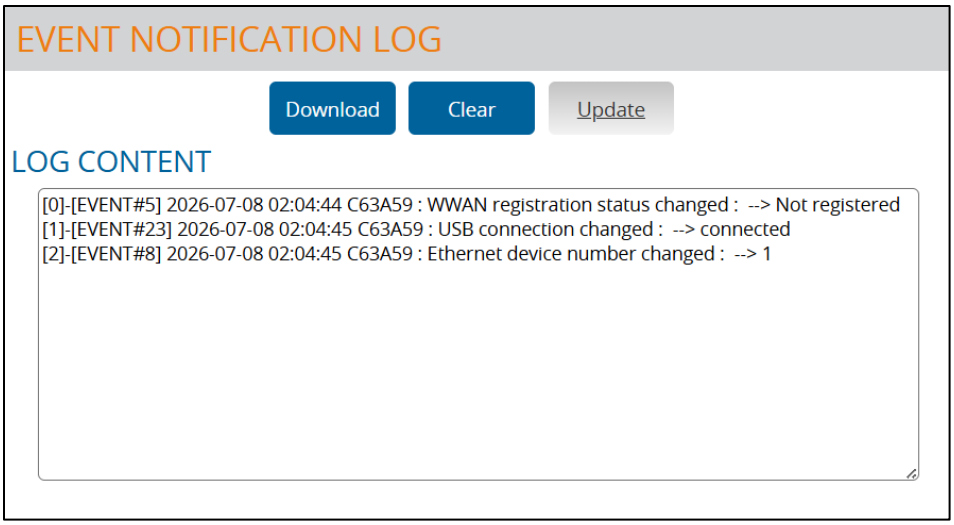


Figure 9-23 Event notification log page

Select the **Update** button to refresh the content in the **Log Content** window. Select the **Download** button to download a log file for review in an external application. Select the **Clear** button to clear the log.

Email Settings

Email settings allows you to configure the SMTP server to be used to deliver Event Notifications (configured in the Event notification configuration section).

To access the Email settings page, navigate to **Services > Email settings**.

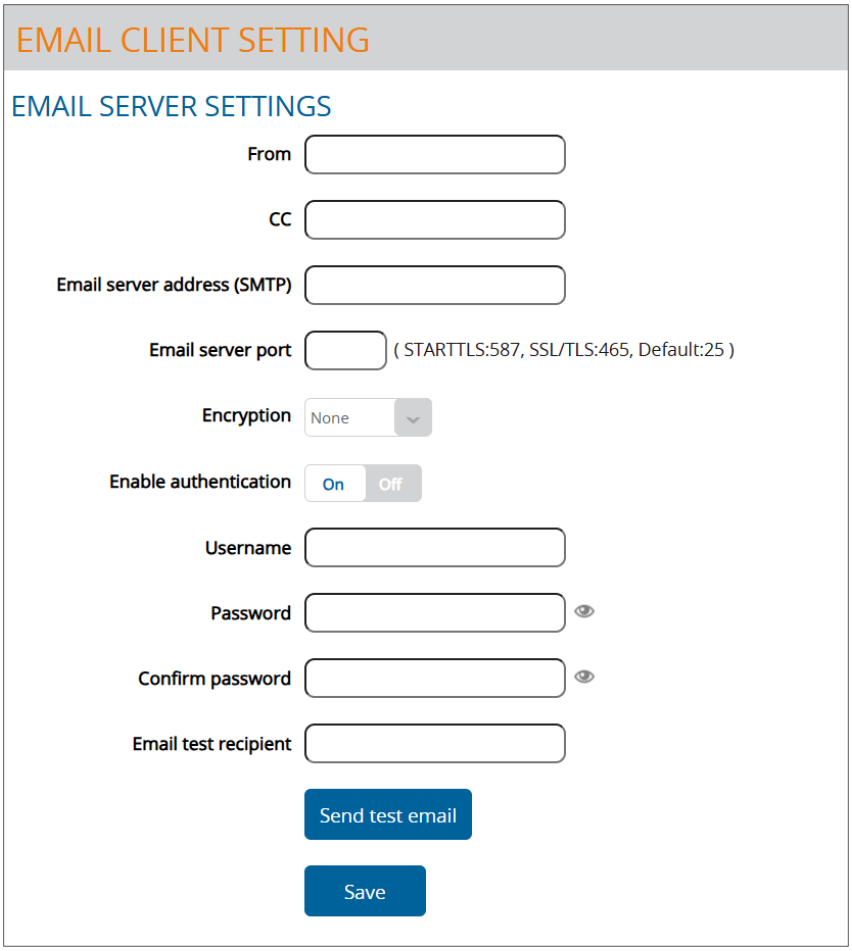


Figure 9-24 Email settings page

Table 9-19 Email configuration details

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

Parameter	Description
Confirm password	Re-enter the password to authenticate with the SMTP server.
Email test recipient	Enter an email address here after completing the previous details to test the SMTP configuration.
Send test email button	Select this button to send the test email to the address configured in the **Email test recipient** field.
Save button	Click to save and apply the settings

Low power mode

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

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

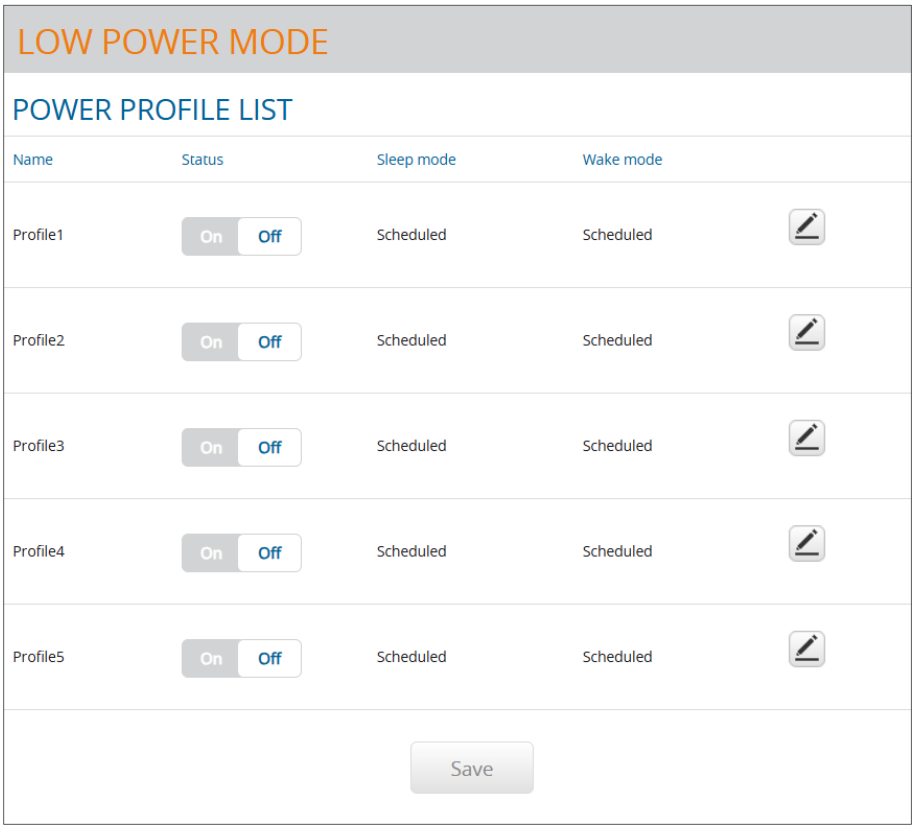


Figure 9-25 Low power mode page

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

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

Click icon to edit that profile.

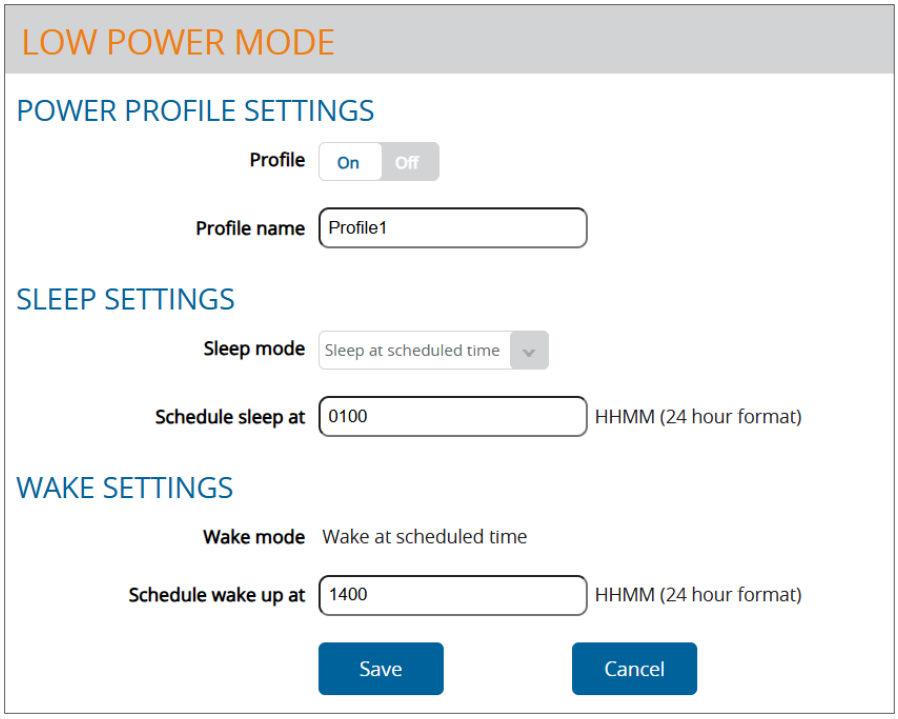


Figure 9-26 Low power mode profile settings

The table below lists the Low Power Mode configuration details.

Table 9-20 Low power mode profile configuration details

Item	Description
Power Profile Settings	
Profile	Set to **On** to activate the profile
Profile name	Enter a name for the profile.
Sleep Settings	
Sleep mode	The Sleep mode selects the condition for the router to enter sleep mode. Select Sleep mode from the following options: • **Sleep after timer** • **Sleep at scheduled time**
Sleep after	Enter the duration after which the router should go to sleep mode, when Sleep mode is selected as **Sleep after timer**.
Schedule sleep at	Enter the time when the router should go to sleep mode, when Sleep mode is selected as **Sleep at schedule time**.
Wake Settings	
Wake mode	**Wake at scheduled time** is the only Wake mode available
Schedule wake up at	Enter the time when the router should wake up

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

Percepxion

The NTC-500 series router comes integrated with Percepxion cloud platform to allow for remote management of devices.

Configuration

Configuration allows you to configure the Percepxion client settings. To access the configuration page, navigate to **Services > Percepxion > Configuration**.

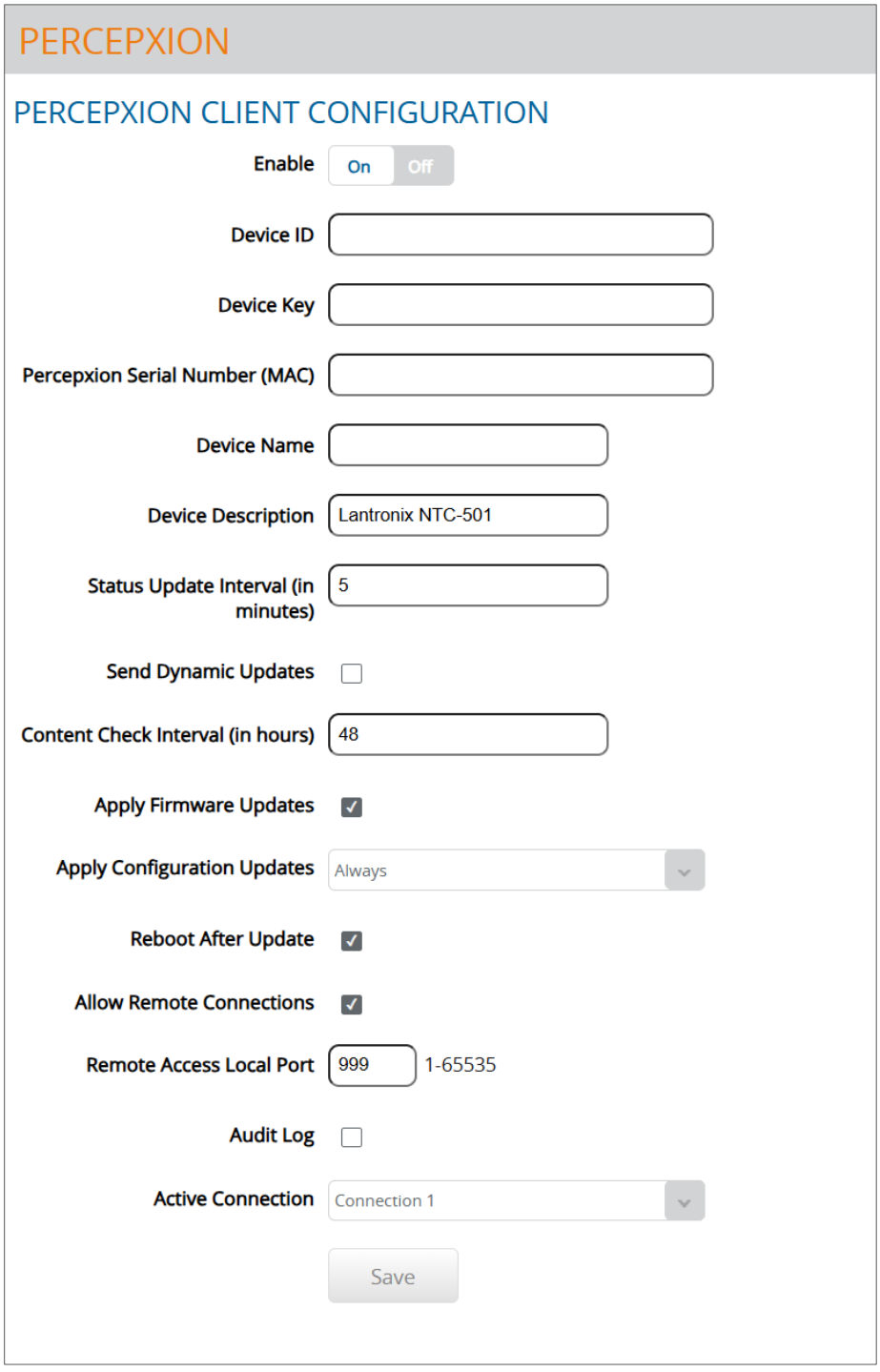


Figure 9-27 Percepxion Configuration page

Table 9-21 Percepxion configuration details

Item	Description
Enable	Set to **ON** to enable Percepxion client.
Device ID	Displays the Device ID. Read only.
Device Key	Displays <Configured>. Read only.
Percepxion Serial Number (MAC)	Device MAC address. Read only.
Device Name	Displays the Percepxion Device name. You can modify this value as required.
Device Description	Displays the Percepxion Device description. You can modify this value as required.
Status Update Interval (in minutes)	Enter the time interval in minutes at which the gateway updates the device status to Percepxion
Send Dynamic Updates	Set to **ON** to enable. If enabled, the device will send updates for RSSI and temperature. The fields will be dynamically updated on Percepxion.
Content Check Interval (in hours)	Enter the time interval in hours at which the device checks Percepxion for updates to configuration or firmware.
Apply Firmware Updates	Check the box to allow firmware updates to be applied via Percepxion.
Apply Configuration Updates	Select when to apply configuration updates. Options are: • **Always:** Always apply configuration updates. • **Never:** Never apply configuration updates.
Reboot After Update	Check the box to automatically reboot the device after configuration update.
Allow Remote Connections	Check the box to allow remote connections.
Remote Access Local Port	Enter the local port for remote access connection.
Audit Log	Check the box to enbale. If enabled, the device will send audit events such as user login, firmware update, configuration update, and CLI access to Percepxion server.
Active Connection	Select the connection instance to use when connecting to Percepxion. Options are: • **Connection 1** • **Connection 2** You can configure two connection instances.

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

Connection 1

Connection 1 allows you configure the settings for Percepxion connection instance **Connection 1**. To access Connection 1 page, navigate to **Services > Percepxion > Connection 1**.

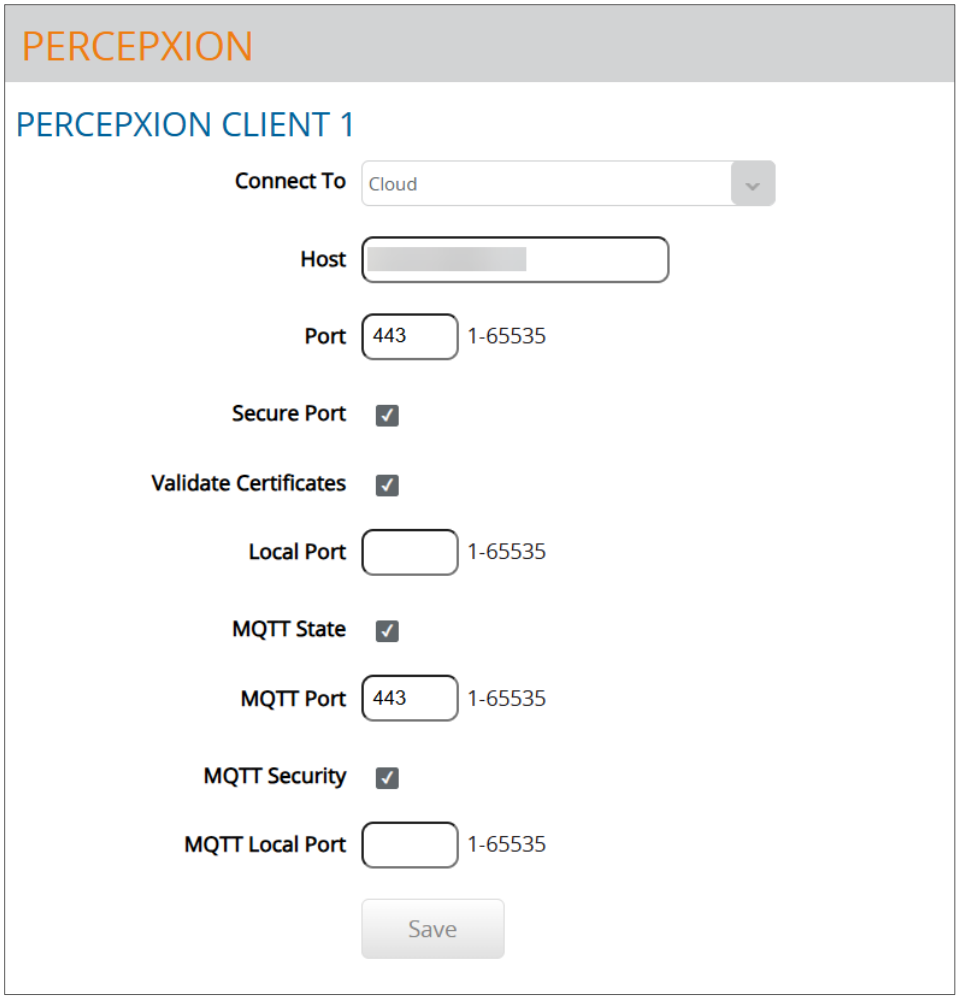


Figure 9-28 Percepxion Connection 1 page

Table 9-22 Percepxion connection1/connection2 configuration details

Item	Description
Connect To	Select the type of Percepxion connection. Options are: • **Cloud** • **Premise**
Host	Enter the host name or IP address of the Percepxion server, used to register the device.
Port	Enter the Percepxion port. Default port is 443.
Secure Port	Check the box to enable the Percepxion client secure port 443.

Validate Certificates	Check the box to enable the validation of the Percepxion server certificates. To validate certificates, both MQTT Security and Secure Port must be enabled.
Local Port	Enter local port for the Percepxion client. When configured, a total of 32 consecutive ports will be reserved.
MQTT State	Check the box to enable MQTT.
MQTT Port	Enter the port number of the Percepxion MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Check the box to enable SSL for MQTT.
MQTT Local Port	Enter the local port for Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.

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

Connection 2

Connection 2 allows you configure the settings for Percepxion connection instance **Connection 2**. To access Connection 2 page, navigate to **Services > Percepxion > Connection 2**.

See Table 9-22 for configuration details.

10. System

The System page allows you to access and configure the following features:

- Log
- Watchdog
- System configuration
- Firmware upgrade
- Access control
- Reboot
- Field test
- Encrypted debuginfo

To access the System page, click **System** tab on the top menu bar.

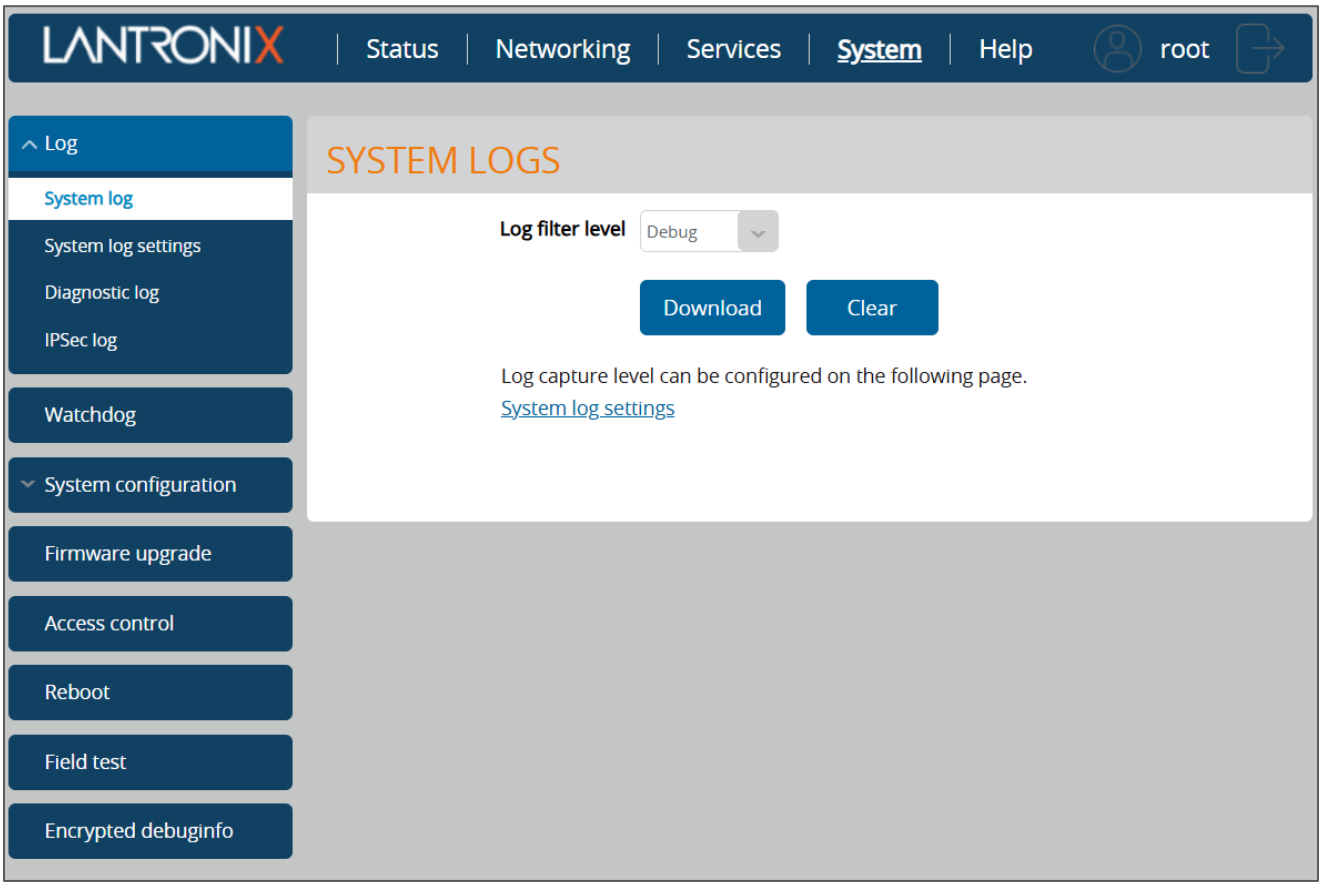


Figure 10-1 System page

Log

Log section provides the different types logs generated by the router allows you to configure the System log settings.

System log

System log allows you to set the log filter level and download the required logs. You can use these logs to troubleshoot any issues that you experience with your NTC-502 router. To access the System log page, navigate to **System > Log > System log**.

The **Log filter level** field allows you to set the level of logs to download. When set to a certain level, the logs corresponding to that level and all the lower levels are downloaded if you click **Download**, provided the Log capture level in System log settings is set to the same or higher level.

Table 10-1 System log filter 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.

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++).

Click **System log settings** to access the System log settings page.

System log settings

System log settings allows you to set the level of logs to be captured and how to save the log data. Log data is stored in RAM and therefore when the unit loses power or is rebooted, any log information stored in the RAM is lost. To ensure that log information is saved between reboots of the router, you can save the logs to no-volatile memory or on a remote syslog server.

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

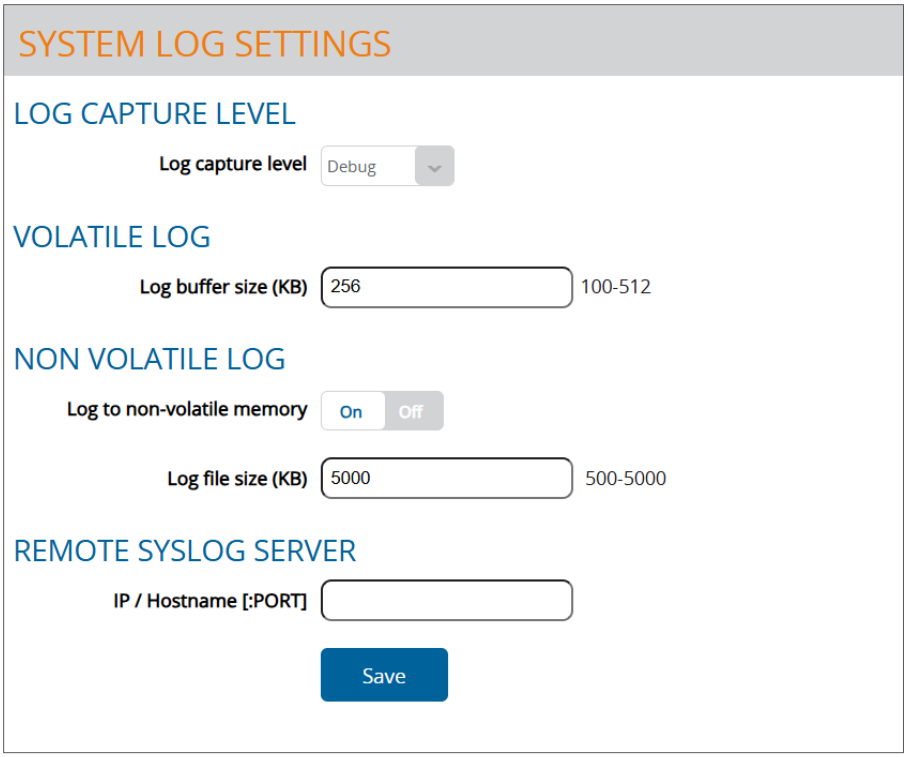


Figure 10-2 System log settings page

Log capture level

The **log capture level** field allows you to define the level of detail that the system log stores. When set to a certain level, the logs corresponding to that level and all the lower levels are captured.

Table 10-2 System log level details

Level	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.

Volatile Log

The size of the volatile log buffer can be configured to store larger logs if required. Enter the required size in KB, in the **Log buffer size (KB)** field. The default is 256KB.

Non-volatile Log

When **Log to non-volatile memory** is set to **On**, the log data is stored in flash memory, making it accessible after a reboot of the router. In the **Log file size (KB)** field enter the size of the log file in KB. 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-500 Series router to output log data to a remote syslog server enter IP address or hostname of the syslog server with port number in the **IP / Hostname [:PORT] field** in Remote Syslog Server section. If you do not specify a port number, the router will use the default UDP port 514.

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

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

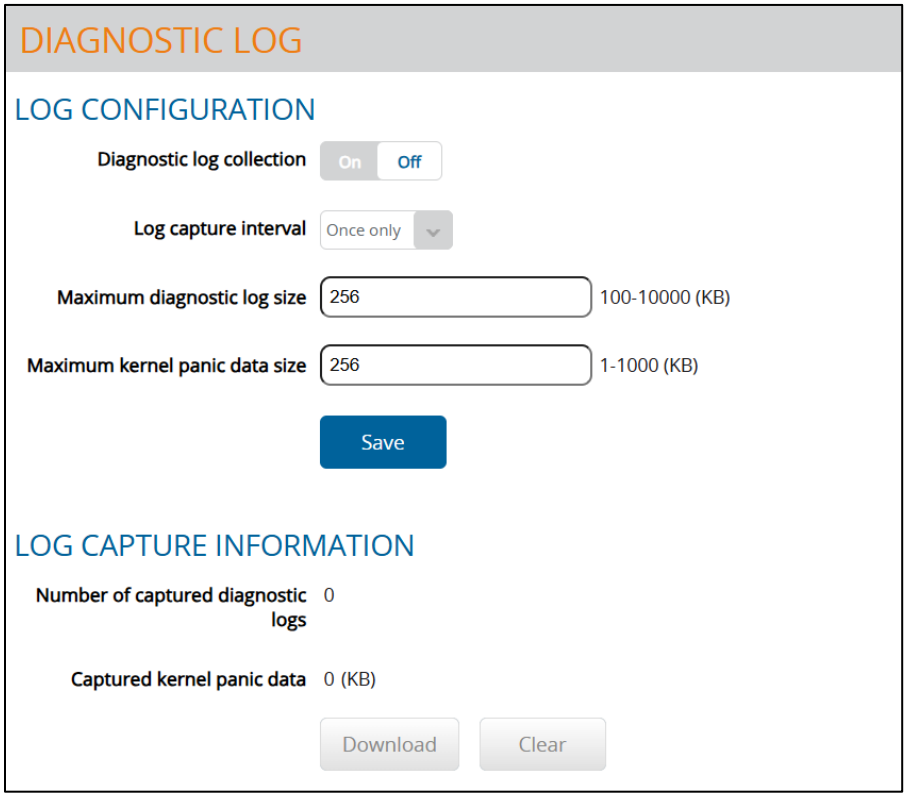


Figure 10-3 Log – Diagnostic log page

Table 10-3 Diagnostic log configuration details

Item	Description
Log Configurarion	
Diagnostic log collection	Set to **On** to enable diagnostic log collection.
Log capture interval	Enter the time interval at which the router should collect diagnostic log data.
Maximum periodic log size (KB)	Enter the maximum size of the log file in KB.
Maximum kernel panic data size (KB)	Enter the maximum size of the kernel panic data file in KB.
Save button	Click to save and apply the details
Log Capture Information	
Number of captured diagnostic logs	Displays the number of captured periodic logs.
Captured kernel panic data (KB)	Displays the total size of captured kernel panic data in kilobytes.
Download button	Click to download all captured logs.
Clear button	Click clear all captured logs.

IPSec log

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

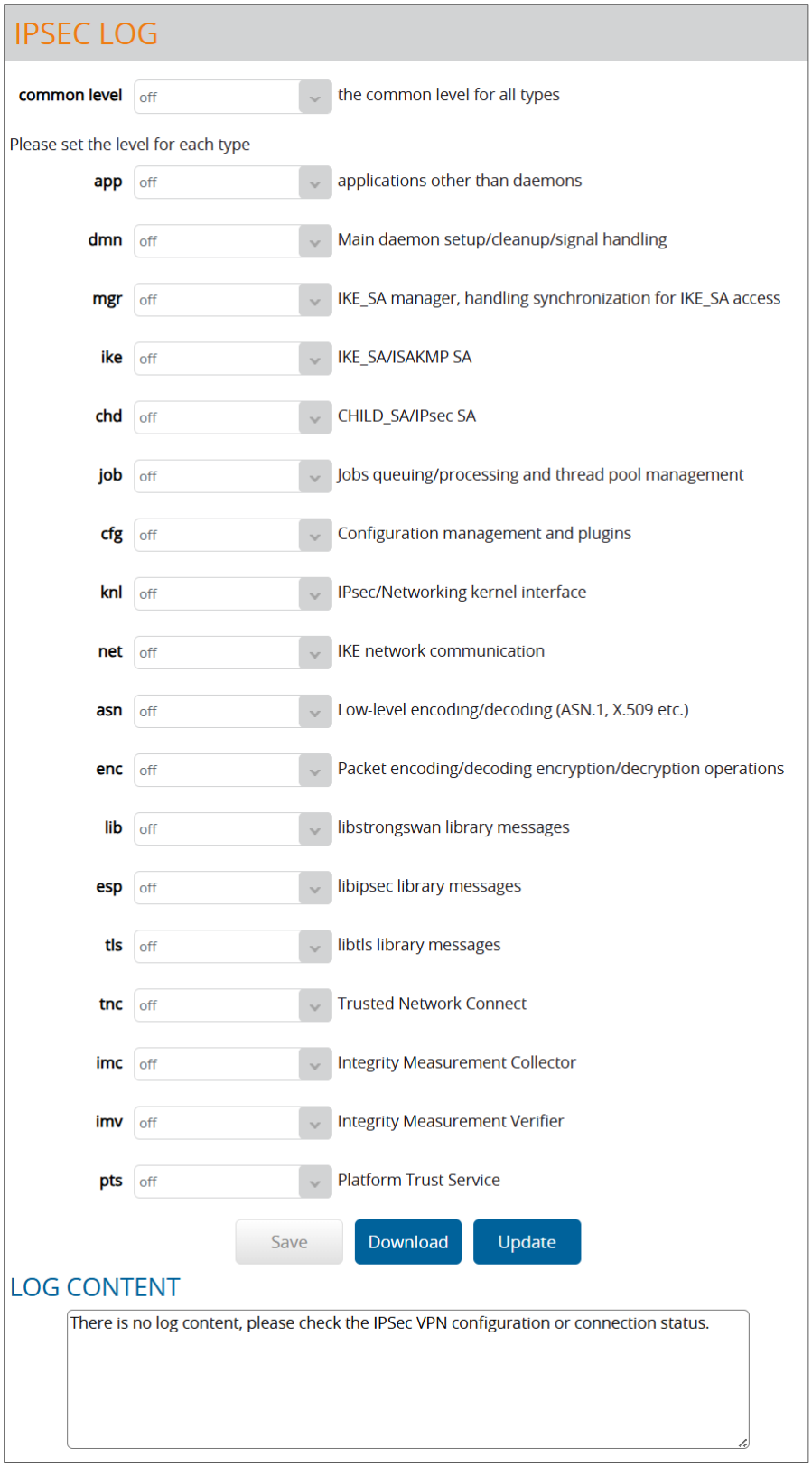


Figure 10-4 IPSec log page

To use the IPsec log, set the **common level** for each type of log that should be captured. The table below lists the available log levels.

Table 10-4 Common level log levels

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

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

You can also set the level for individual log types as required. This will override the common level for that log type.

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

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

Watchdog

Watchdog allows you to configure Periodic Ping and Periodic Reboot features. To access the Watchdog page, navigate to **System > Watchdog**.

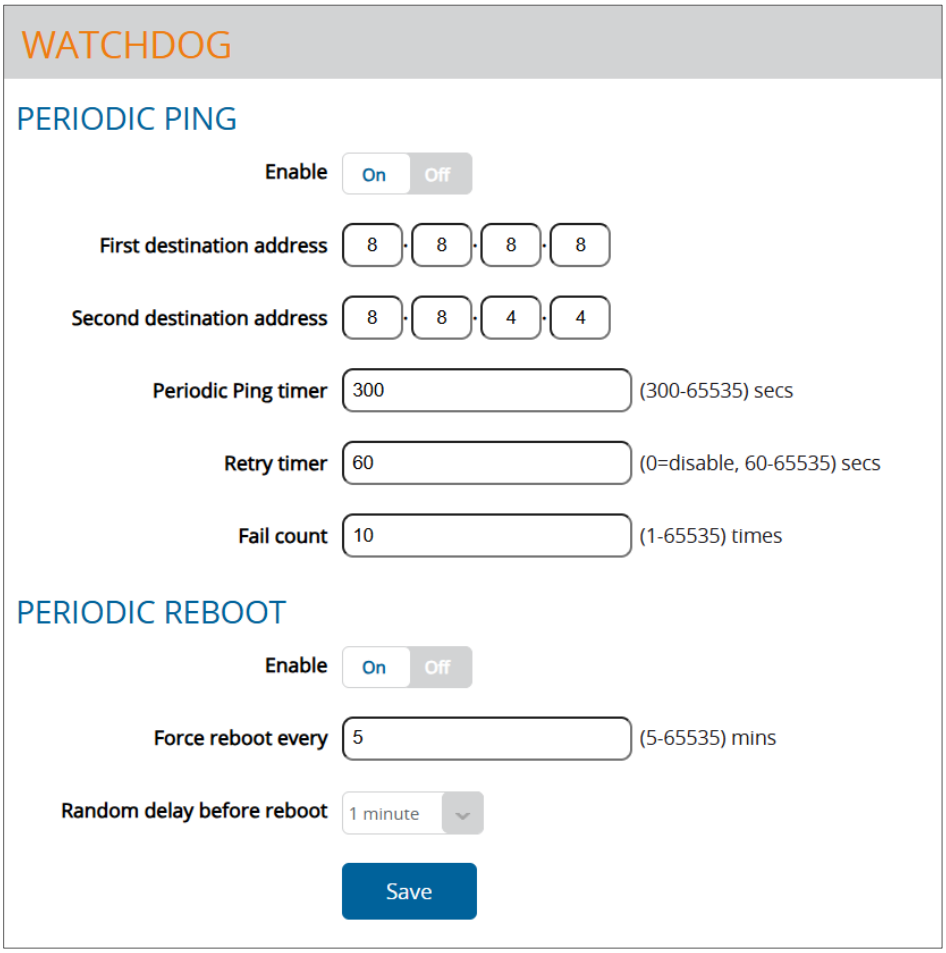


Figure 10-5 Watchdog page

Periodic Ping

Periodic ping allows you to configure the behaviour of the Periodic Ping monitor function.

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

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

The ping watchdog being a last resort standalone backup mechanism 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. 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 the number of times configured in “Fail count”, the router reboots.
5. If any ping succeeds, the router returns to step A and does not reboot.

Configuring Periodic Ping

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 Periodic Ping:

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

Periodic Reboot

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

To configure Periodic Reboot:

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



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

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

System configuration

LDAP Settings

LDAP Settings allows you to configure a Lightweight Directory Access Protocol (LDAP) on the NTC-500 Series router. LDAP allows the router to use a centralized directory service for user authentication and authorization.

To access the LDAP settings page, navigate to **System > System Configuration > LDAP settings**.

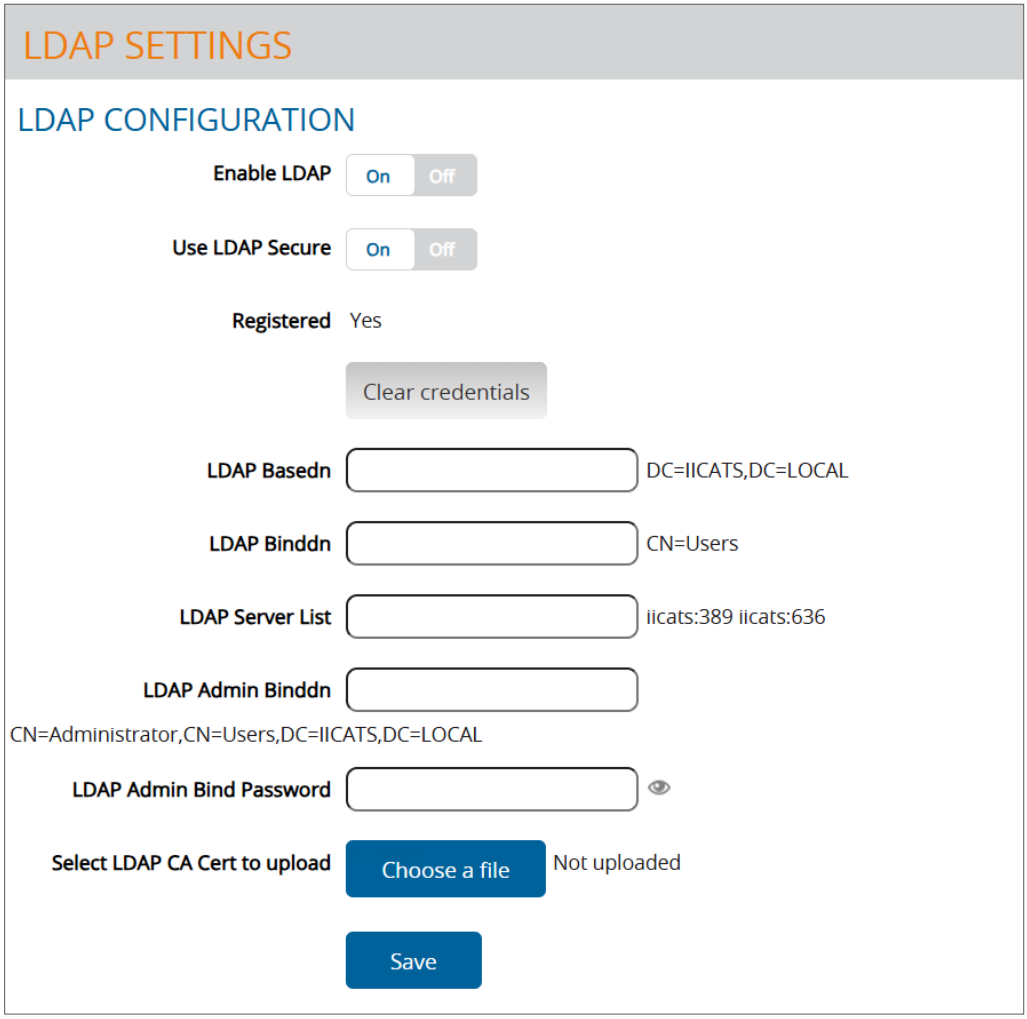


Figure 10-6 LDAP settings page

Table 10-5 LDAP configuration details

Item	Description
Enable LDAP	Set to **On** to enable LDAP
Use LDAP Secure	Set to **On** to enable use of LDAP over SSL/TLS, a secure version of LDAP.
Registered	Displays whether the LDAP server is registered on the router.
Clear Credentials button	Click to clear credentials related to an existing LDAP configuration.

Item	Description
LDAP Basedn	Enter the LDAP Base Distinguished Name. It specifies the starting point within the LDAP directory tree from which searches will be performed.
LDAP Binddn	Enter the LDAP Bind Distinguished Name of the LDAP entry used to authenticate (bind) to the LDAP server.
LDAP Server List	Enter the IP address or Hostname of the LDAP server and port number. (IP address/Hostname:Port)
LDAP Admin Binddn	Enter the LDAP Admin Bind Distinguished Name, which refers to a special Bind DN with administrative privileges in the LDAP directory.
LDAP Admin Bind Password	Enter the password for the LDAP Admin Bind DN used.
Select LDAP CA Cert to upload	Displays if **Use LDAP Secure** is enabled. Click **Choose a file**, then select the required file and upload it.
Save button	Click to save and apply the settings.

Restore factory defaults

Restoring factory defaults will reset the NTC-500 Series router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-500 Series router.

To access the Restore factory defaults page, navigate to **Services > System configuration > Restore factory defaults**.

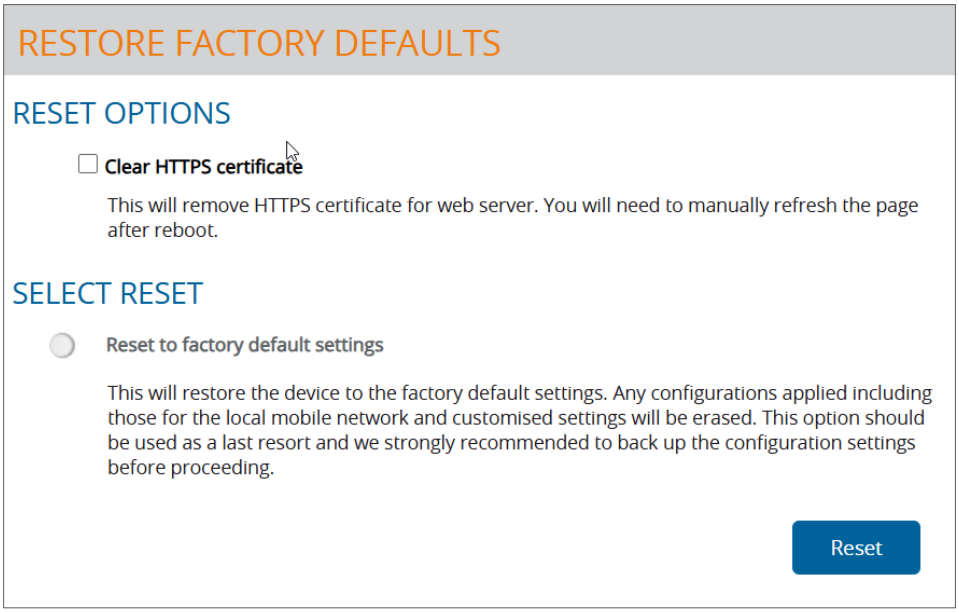


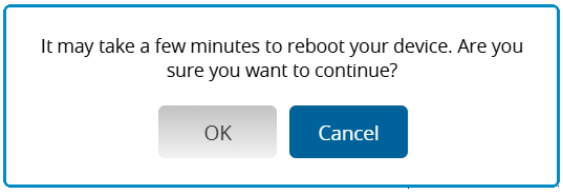
Figure 10-7 Restore factory defaults page

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

Important: *The full factory reset will require the NTC-500 Series router to be completely reconfigured.*

To perform a factory reset:

1. Click the **Clear HTTPS certificate** checkbox if you want to clear the HTTPS certificate.
2. Select **Reset to factory default settings**.
3. Click **Reset**. You will be prompted to confirm. Click **OK** to proceed with the reset.



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

Web server setting

Web server setting allows you to configure and generate a Web Server certificate and also upload an existing Web Server certificate.

To access the Web server setting page, navigate to **System > System configuration > Web server setting**.

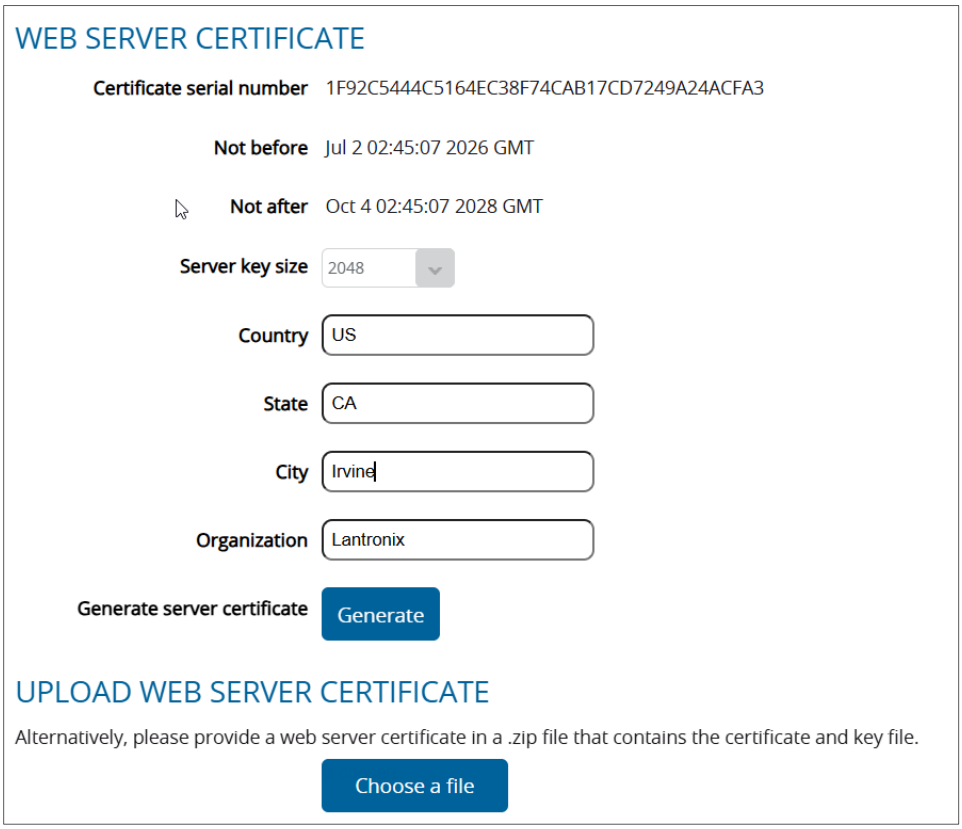


Figure 10-8 Web server setting page

To generate a Web Server certificate, select required **Server Key size** and enter required values for all the fields in the Web Server Certificate section. Then click **Generate**.

To upload a Web Server certificate, click **Choose a file**, locate and select the certificate.

Administration settings

Administration settings allows you to configure Web UI credentials, Web UI login limits, and SSH credentials.

To access the Administration settings page, navigate to **System > System configuration > Administration settings**.

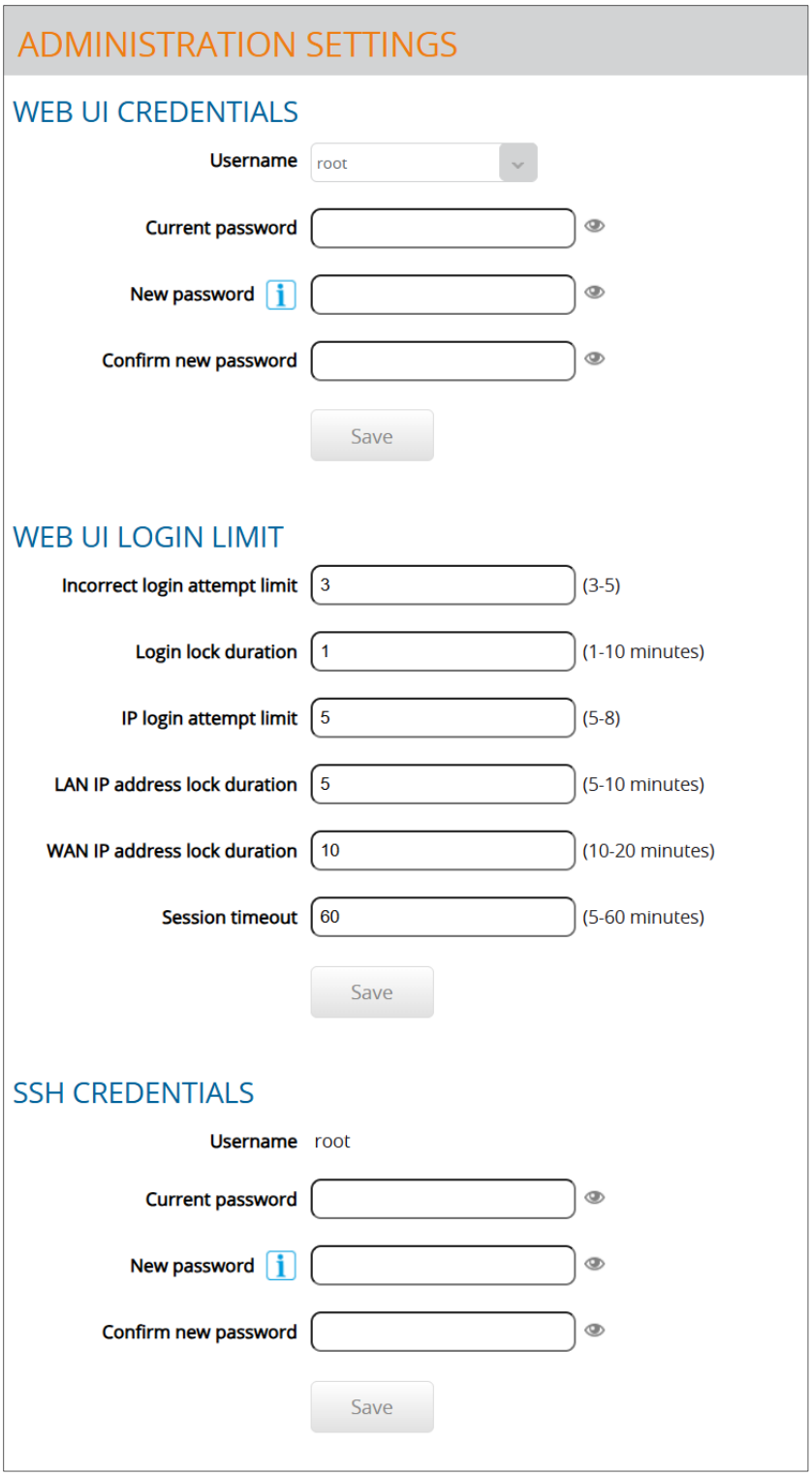


Figure 10-9 Administration settings page

Web UI credentials

Web UI credentials allows you to update the password for the different users that have access to the NTC-500 Series router via the web interface.

Table 10-6 Web UI credentials configuration details

Item	Description
Username	Select the user whose password needs to be updated.
Current password	Enter the current password for that user.
New password	Enter the new password.
Confirm new password	Re-enter the above password.
Save button	Click to save and apply the settings.

Web UI login limits

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

Table 10-7 WebUI login limits configuration details

Item	Description
Incorrect login attempt limit	Enter the number of times an incorrect password can be entered into the web interface before it locks access and does not allow any further attempts.
Login lock duration	Enter the amount of time the login lock lasts.
IP login attempt limit	Enter the number of logins that can be attempted from one IP before any further attempts are locked out.
LAN IP address lock duration	Enter the amount of time an IP attempting to log in from the LAN is forbidden from trying to login.
WAN IP address lock duration	Enter the duration of time an IP attempting to log in from the WAN is forbidden from trying to login.
Session timeout	The duration of time in minutes that a logged in session lasts on the web interface without any activity. The web interface will log out the current user after the configured time.
Save button	Click to save and apply the settings

SSH credentials

SSH credentials allows you to update the password for SSH access to the NTC-500 Series router. The default SSH username is root.

Adding new users

The NTC-500 Series router allows you to add new users that can access Web UI and access the router via ssh. You can add the following types of users:

- **Root-privileged user**
  - The user has privileges similar to root user
  - The user can access the Web UI and access the router via ssh
  - The user is authenticated locally, not via LDAP
  - The password for the user cannot be updated via Web UI
- **Read only user**
  - The user has read-only privileges
  - The user can access only the Web UI
  - The user is authenticated locally, not via LDAP
  - The password for the user cannot be updated via Web UI

To add a root-privileged user:

1. Log in to the router as root user via ssh.
2. Execute the command:

```
add_user.sh -a add -u <user> -p <pass> -g root
```

<user> - Username for new user

<pass> - Password for new user

To add a read-only user:

1. Log in to the router as root user via ssh.
2. Execute the command:

```
manage_viewer.sh add <user> <password>
```

<user> - Username for new user

<pass> - Password for new user

Note:

- Do not use **root**, **admin**, and **user** as usernames for the new users.
- *If you perform a factory reset and choose to configure the router as new device, the new users will be deleted.*

Settings backup/restore

Settings Backup and Restore allows you to backup or restore the router's configuration. To access this page, you must be logged in to the web user interface as root or admin. The backup/restore functions can be used to easily configure many NTC-500 Series routers by configuring one router with your desired settings, backing them up to a file and then uploading that file to multiple N routers.

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

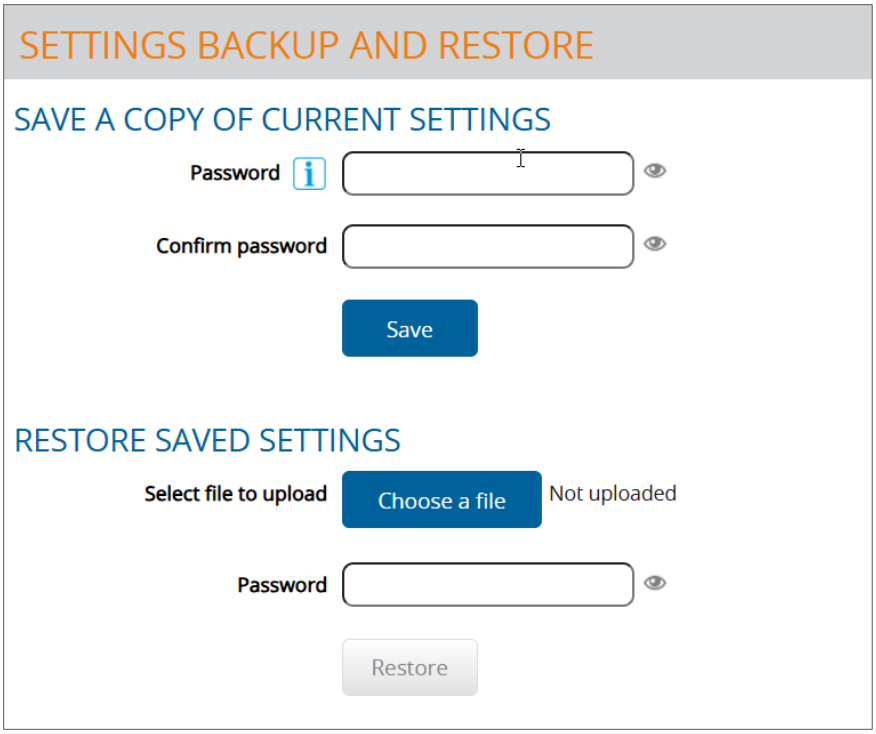


Figure 10-10 Settings backup/restore page

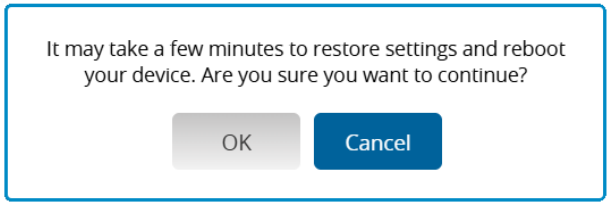
Creating a settings backup

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

Restoring a settings backup

To restore a settings backup:

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



Site and location settings

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

To access the Site and location settings page, navigate to **System > System configuration > Site and location settings**.

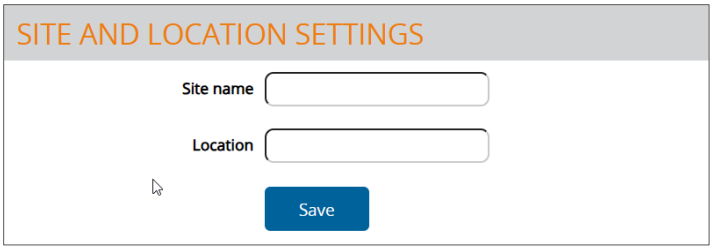


Figure 10-11 Site and location settings

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

Runtime configuration

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

To access the Runtime configuration page, navigate to **System > System configuration > Runtime configuration**.

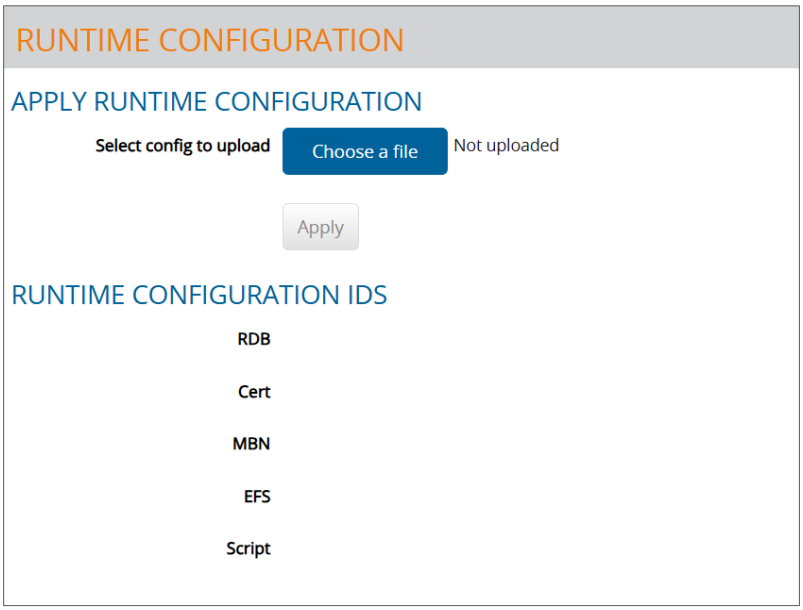


Figure 10-12 Runtime configuration

To apply runtime configuration:

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

SSH key management

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

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

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

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

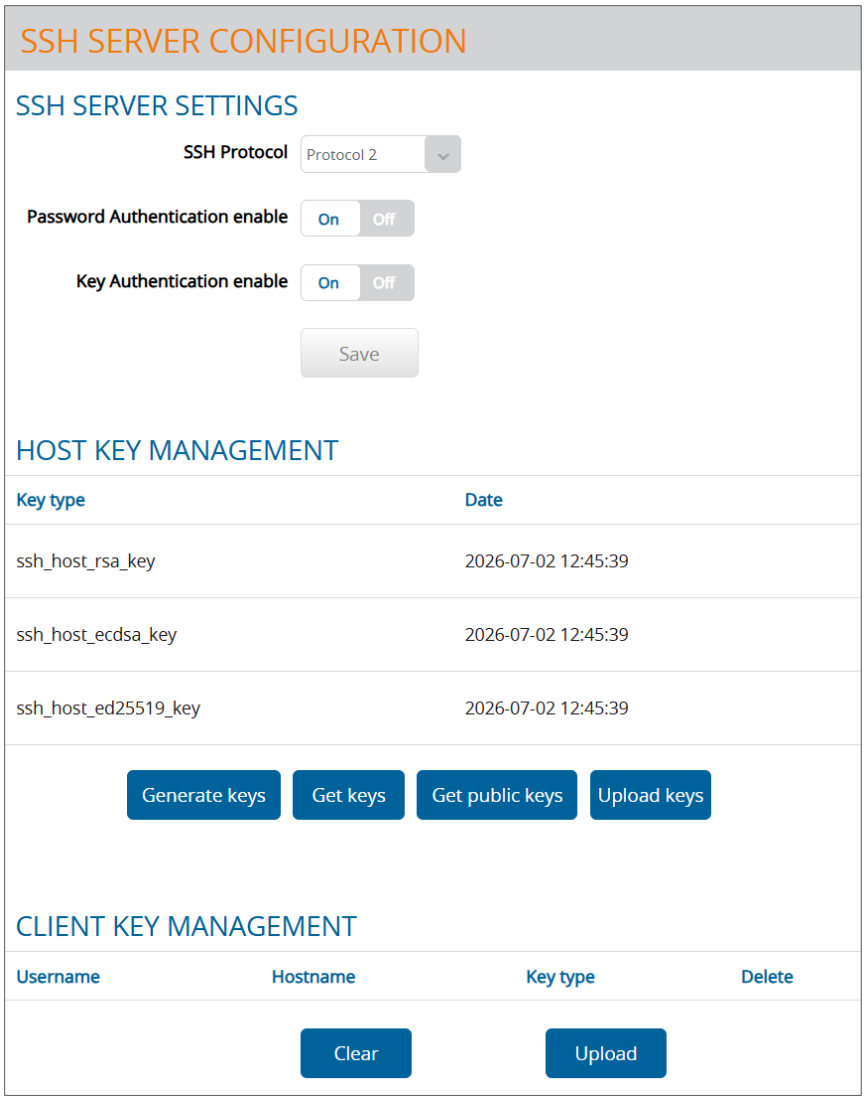


Figure 10-13 SSH server configuration

SSH server configuration

To configure the SSH server settings:

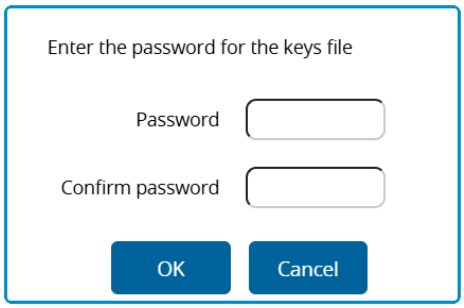
1. Select the **SSH Protocol** to use. Protocol 2 is more recent and is considered more secure.
2. Select the type of authentication you want to use by setting **Password Authentication enable** and **Key Authentication enable** toggle keys to **On**. Note that you may have both authentication methods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

Host key management

The Host key management section allows you to manage the SSH keys on the NTC-500 Series router.

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

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



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

Click the **Get public keys** to download the public keys.

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

Client key management

The Client key management section allows you to upload client keys to the NTC-500 Series router, allowing key based SSH access to the NTC-500 Series router. Select the **Upload** button to upload the public key of your SSH client. The key displays in **Client key management** section. Click ✕ icon in the **Delete** column to remove that key. Click **Clear** to clear all the uploaded keys.

LED operation mode

LED operation mode allows you to control the operation of the LED indicator lights on the NTC-500 Series router. There are two modes available, **Always on** and **Turn off after timeout.** Setting the mode to **Always on** sets the indicator LEDs to be lit when the device is on. Setting the mode to **Turn off after timeout** sets the indicator LEDs to turn off after the timer has expired.

To access LED operation mode page, navigate to **System > System configuration > LED operation mode**.

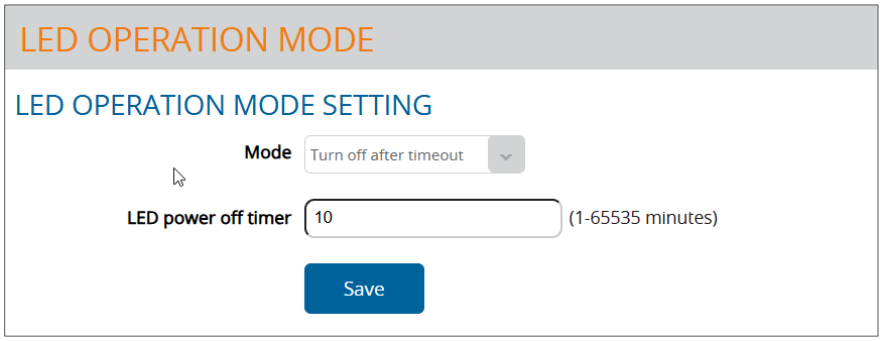


Figure 10-14 LED operation mode

Setting the LED operation mode

To set the LED operation mode:

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

A/B system configuration

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

To access the A/B system page, navigate to **System > System configuration > A/B system**.

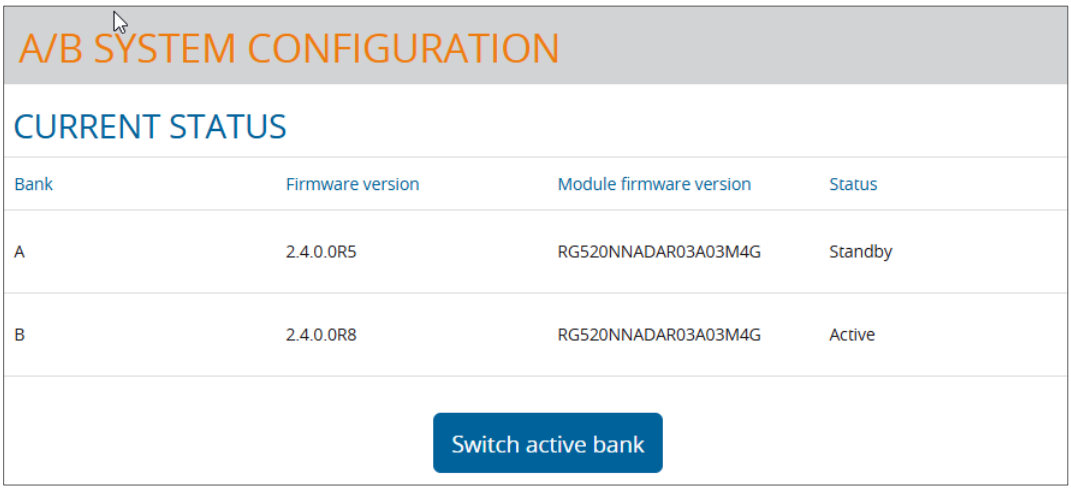
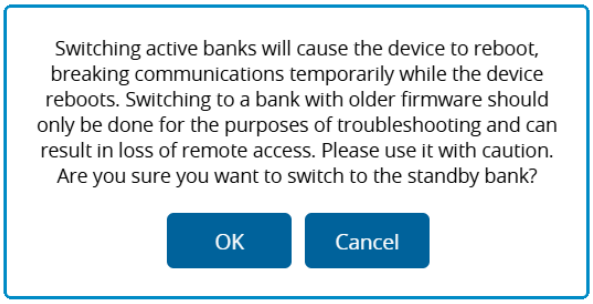


Figure 10-15 A/B System configuration page

To switch the active bank, click the **Switch active bank** button. You will be prompted to accept the following message:



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

Firmware upgrade

Firmware upgrade allows you to upload firmware files to the NTC-500 Series router and perform a Firmware Upgrade. The firmware upgrade will be applied to the Standby bank, to ensure the current firmware can be restored in the event of an issue. Once the Firmware is successfully upgraded and the device reboots, the Standby bank becomes Active bank.

To access the Firmware upgrade page, navigate to **System > Firmware Upgrade**.

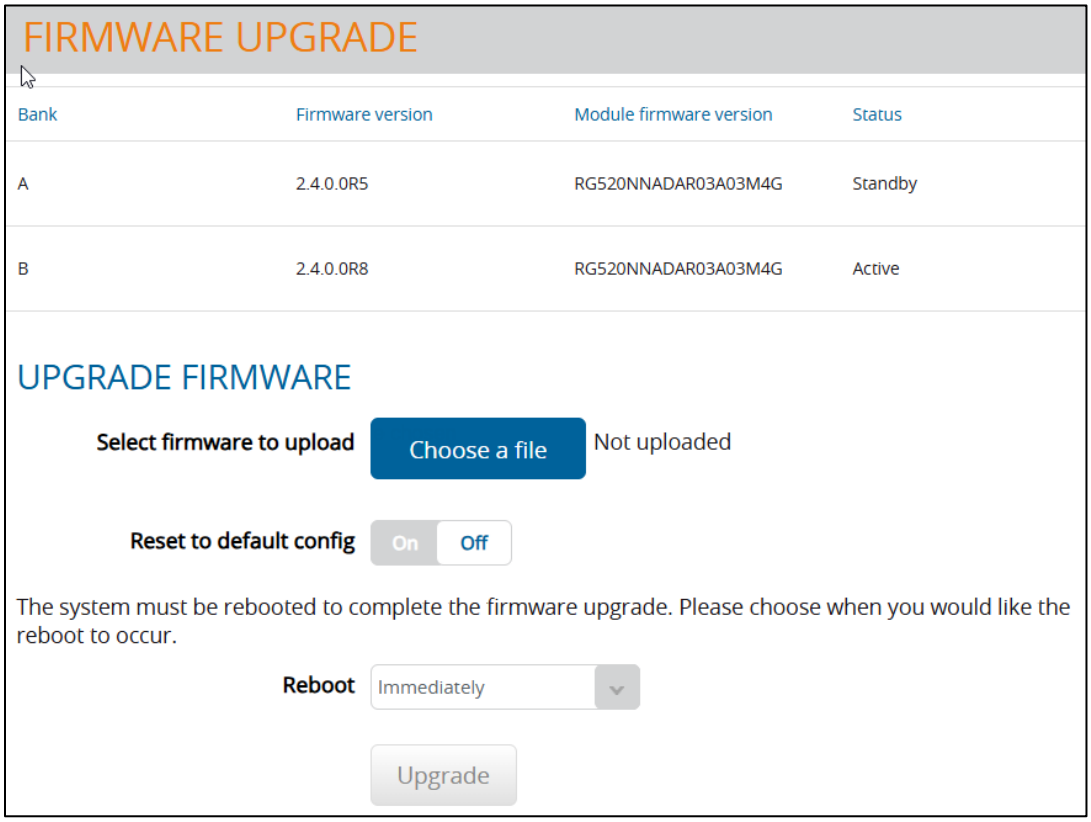


Figure 10-16 Firmware upgrade page

Upgrading the router firmware

To upgrade the NTC-500 Series router's firmware:

1. In the Upgrade Firmware section, click **Choose a file**. Locate the firmware image file on your computer and select **Open**.
2. If required set the **Reset to default config** toggle to **On** to reset the NTC-500 Series router to the default configuration.
3. Select an option for Reboot field. The options are **Immediately** and **Scheduled**. If you select **Scheduled** option, the **Date** and Time **settings** display.

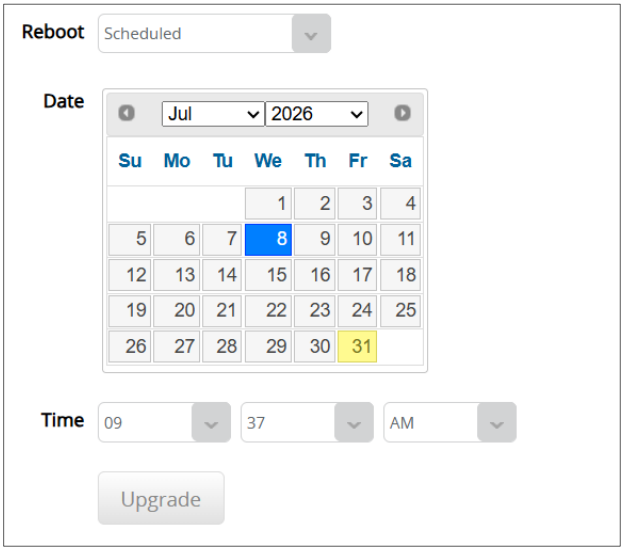


Figure 10-17 Scheduled firmware upgrade

4. Set the required **Date** and **Time**.
5. Click **Upgrade** button to upgrade the firmware.

Access control

Access control allows you to configure the remote and local access protocols to access the router.

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

To access the Access control page, navigate to **Services > Access control**.

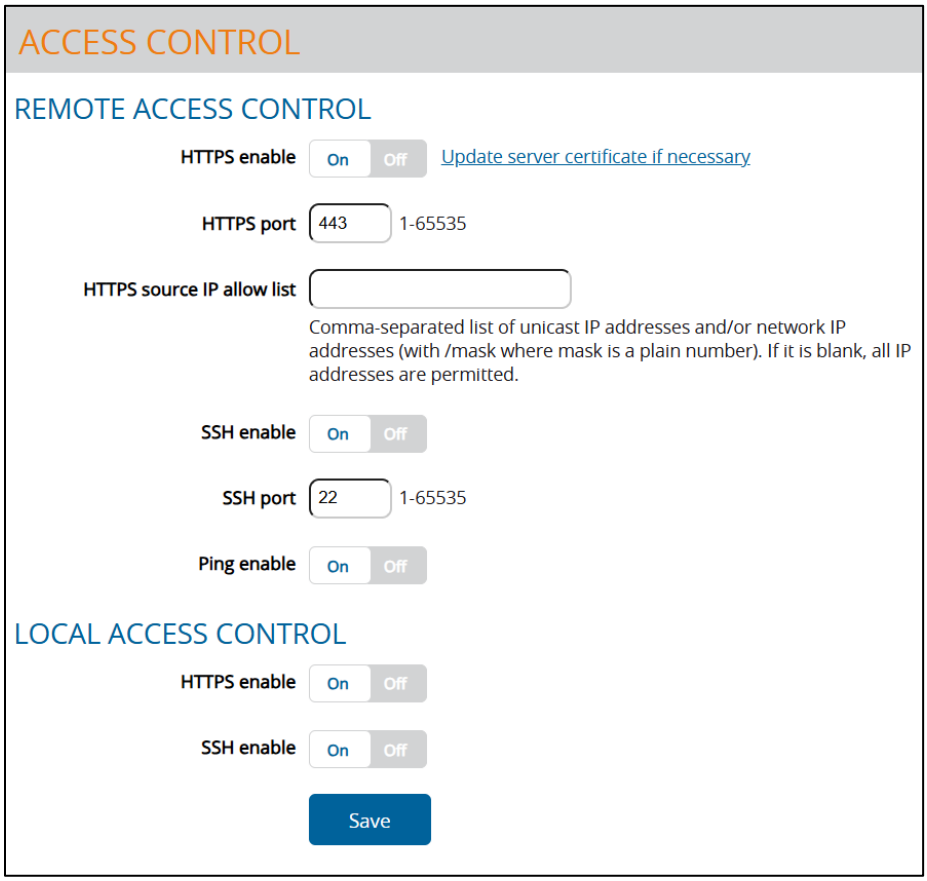


Figure 10-18 Access control page

Table 10-8 Access control configuration details

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

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

Reboot

Reboot provides allows you to perform a soft reboot of the device. This can be useful if you have made configuration changes you want to implement.

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

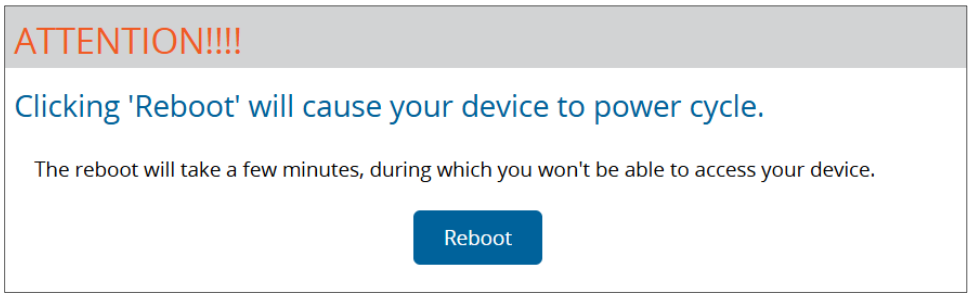
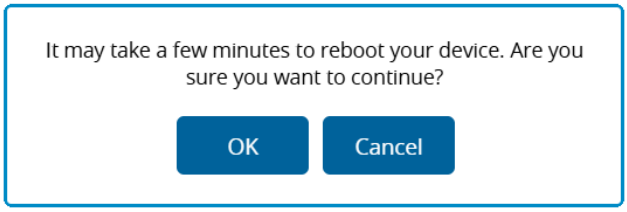


Figure 10-19 Reboot

To reboot the NTC-500 Series router:

1. Click **Reboot**. The below prompt is displayed.



2. If you wish to proceed, click **OK** button.

Field test

Field test displays the following information which may be useful when troubleshooting signal strength issues.

- LTE PCELL Information
- LTE SCELL Information
- 5G NR Serving Cell Information
- 5G NR Extended Information

To access the Field test page, navigate to **System > Field test**.

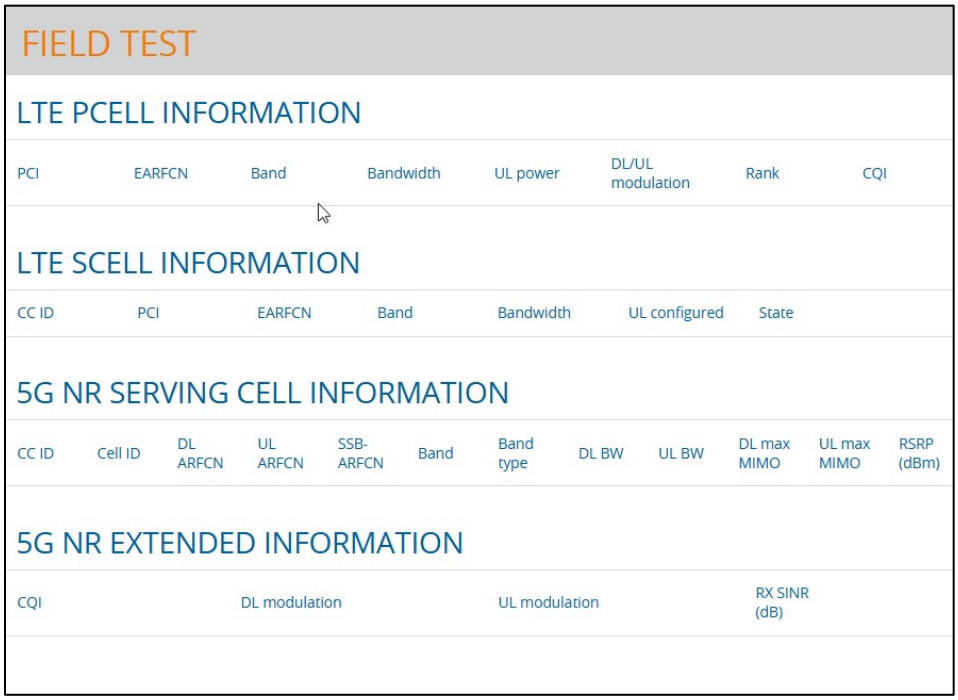


Figure 10-20 Field Test page

Table 10-9 LTE PCELL information

Item	Description
PCI	Physical Cell ID of the LTE Cell.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
Band	The current LTE band.
Bandwidth	The current LTE bandwidth.
UL power	The transmit power used by the device for uplink communication to the serving cell.
DL/UL modulation	The modulation scheme used for downlink (DL) and uplink (UL) transmissions.
Rank	The number of transmission layers used in MIMO communication between the device and the serving cell.

Item	Description
CQI	The quality of the radio channel as reported by the device.

Table 10-10 LTE SCELL information

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

Table 10-11 5G NR serving cell information

Item	Description
CC ID	Component Carrier ID.
Cell ID	The physical cell identifier.
DL ARFCN	Downlink Absolute Radio Frequency Channel Number.
UL ARFCN	Uplink Absolute Radio Frequency Channel Number.
SSB-ARFCN	Absolute Radio Frequency Channel Number corresponding to the Synchronization Signal Block (SSB) of the serving cell.
Band	The NR5G band.
Band Type	The type of the NR5G band, e.g. Sub6 or mmWave.
DL BW	Downlink bandwidth.
UL BW	Uplink bandwidth.
DL max MIMO	Downlink maximum Multiple Input Multiple Output.
UL max MIMO	Uplink maximum Multiple Input Multiple Output.
RSRP (dBm)	The average power level of reference signals received from the serving cell.

Table 10-12 5G NR extended information

Item	Description
CQI	Indicates the quality of the downlink radio channel as reported by the device.
DL modulation	Specifies the modulation scheme used for downlink transmissions from the serving cell to the device.
UL modulation	Specifies the modulation scheme used for uplink transmissions from the device to the serving cell.
RX SINR (dB)	Received Signal to Interference plus Noise Ratio. The ratio of the received signal power to the combined interference and noise.

Encrypted debuginfo

Encrypted debuginfo allows you to generate and download 5G NR cell information which may be useful when troubleshooting signal strength issues.

To access the Encrypted debuginfo page, navigate to **System > Encrypted debuginfo**.

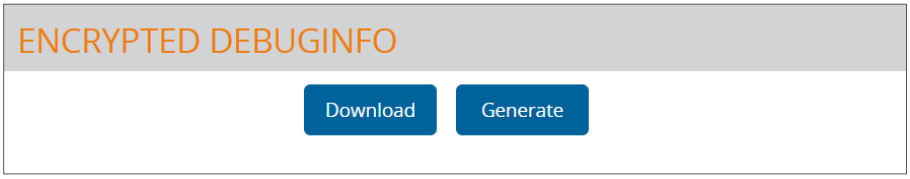


Figure 10-21 Encrypted debuginfo page

11. Help

The Help page provides links to access the NTC-500 Series User Guide and Lantronix Support Portal. To access the Help page, click the **Help** tab on the top menu bar.

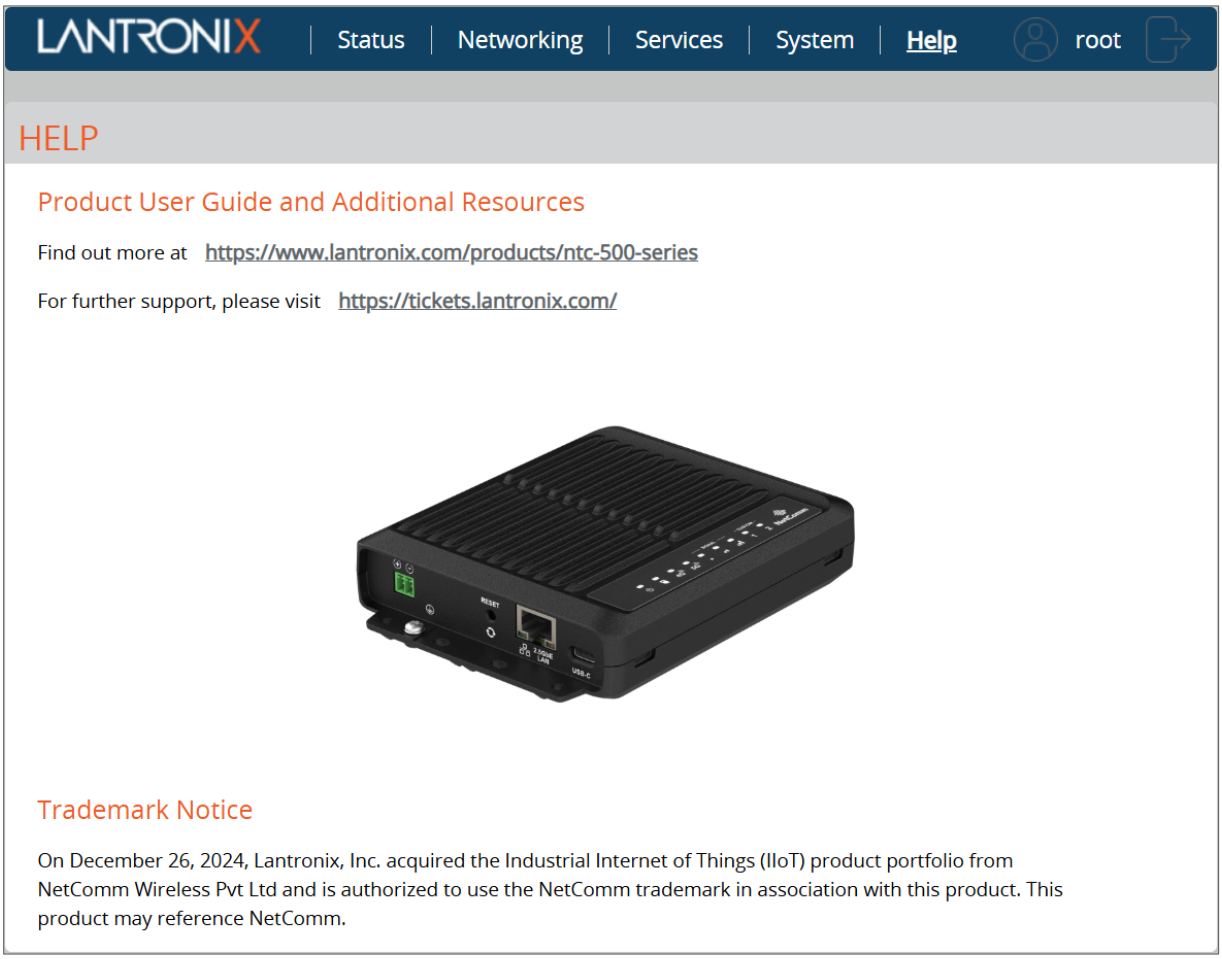


Table 11-1 Help page

Appendix A. Configuring Radio Access Technologies

This device supports the following modes of operations in various combinations.

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

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

Table A-1 RAT/Band Selection table

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

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

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

Appendix B. NetComm Document History

Table B-1 NetComm Document History

Ver.	Document description	Date
v1.00	Initial document release based on firmware version 1.1.74.0	12 October 2023
v1.01	Updated for firmware version 1.1.88.0. New features include OpenVPN, GRE Tunnelling, RIP, VRRP Redundancy, minor WebUI updates. Updated naming of device. Updated document theme.	20 December 2023
v1.02	Updated for firmware version 1.2.2.1. MQTT added as a new feature.	15 February 2024
V2.00	Updated for firmware version 1.2.15.0. New WebUI with NetComm branding. Document images updated throughout to match WebUI changes. Updated sections on Network Slicing, A/B configuration, Administration Settings.	March 2024

Appendix C. Compliance Information

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

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

Product Family:

NTC-500 Series
Conforms to the following standards or other normative documents:

Country	Models	Specification
USA – FCC	NTC-501	Contains FCC ID: XMR2022RG520NNA
Canada – IC	NTC-501	Contains IC: 10224A-2022RG520NA
Australia – RCM	NTC-502	Supplier's Declaration of Conformity
EU	NTC-502	See EU Declaration of Conformity (*Figure C-1*)
United Kingdom	NTC-502	See UK Declaration of Conformity (*Figure C-2*)
Safety	NTC-502	EN IEC 62368-1 AS/NZS 62368-1

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 20 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.

EU Declaration of Conformity

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250 Irvine, CA 92618 USA
Model Name: NTC-502
Rated: 12Vdc, 1.5A
Intended use: Commercial installations, indoor use
SW version: v2.0.0.0

Manufacturer's Quality System:

TÜVRheinland

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

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)

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

EMC Directive (2014/30/EU)

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

RF Radio Directive (2014 / 53 / EU)

- EN 301 908-1 V15.2.1(2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.2.1 (2022-02)
- Draft EN 301-908-25 V15.1.1_15.0.9 (2021-06)

Health Directive (2014 / 53 / EU)

- EN IEC 62311:2020

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

- EN 6300-2018

Radio Equipment Directive 2014/53/EU (RED) article 3.3 (d, e, f) essential requirements for cybersecurity

- **EN 18031-1:2024 (Article 3.3(d))**

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

Signature: _____ Date: 27 Nov 2025
Name: _____Steve Burrington_____ ___ Title: Vice President R&D

CERT-00510 rev B

Figure C-1 EU Declaration of Conformity

Table C-1 EU Statements

Code	Language	Statement
bg	Bulgarian	Lantronix, Inc., декларира, че този NTC-502 device отговаря на основните изисквания и други приложими разпоредби на Директива 2014/53/EU. Пълният текст на декларацията на ЕС за съответствие е достъпен на следния интернет адрес: http://www.lantronix.com/products/ntc-500-series/ Известие на ЕС за ограничения при употреба: Това устройство е ограничено само за вътрешна употреба. Може да не се работи наоткрито.
cs	Česky [Czech]	Lantronix, Inc. tímto prohlašuje, že tento NTC-502 device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. Úplné znění ES prohlášení o shodě je k dispozici na této internetové adrese: http://www.lantronix.com/products/ntc-500-series/ Oznámení EU o omezení používání: Toto zařízení je omezeno pouze na použití uvnitř. Nesmí být provozován venku.
da	Dansk [Danish]	Undertegnede Lantronix, Inc. erklærer herved, at følgende udstyr NTC-502 device overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. Den fulde tekst til EU-overensstemmelseserklæringen er tilgængelig på følgende internetadresse: http://www.lantronix.com/products/ntc-500-series/ EU-meddelelse om begrænsninger i brug: Denne enhed er kun begrænset til indendørs brug. Det betjenes måske ikke udendørs.
de	Deutsch [German]	Hiermit erklärt Lantronix, Inc., dass sich das Gerät NTC-502 device in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EUbefindet. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse abrufbar: http://www.lantronix.com/products/ntc-500-series/ EU-Hinweis zu Nutzungsbeschränkungen: Dieses Gerät darf nur in Innenräumen verwendet werden. Es darf nicht im Freien betriebenwerden.
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix, Inc. seadme NTC-502 device vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. EL-i vastavusdeklaratsiooni täielik tekst on saadaval järgmisel Interneti-aadressil: http://www.lantronix.com/products/ntc-500-series/ EL-i teade kasutuspiirangute kohta: seda seadet saab kasutada ainult siseruumides. Seda ei tohi õues kasutada.
en	English	Hereby, Lantronix, Inc., declares that this NTC-502 device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

Code	Language	Statement
		The full text of the EU declaration of conformity is available at the following internet address: http://www.lantronix.com/products/ntc-500-series/ EU Notice of Restrictions on Use: This device is limited to indoor use only. It may not be operated outdoors.
es	Español [Spanish]	Por medio de la presente Lantronix, Inc. declara que el NTC-502 device module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: http://www.lantronix.com/products/ntc-500-series/ Aviso de restricciones de uso de la UE: este dispositivo está limitado solo para uso en interiores. No puede ser operado al aire libre.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix, Inc. ΔΗΛΩΝΕΙ ΟΤΙ NTC-502 device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ διατίθεται στην ακόλουθη διεύθυνση διαδικτύου: http://www.lantronix.com/products/ntc-500-series/ Ειδοποίηση της ΕΕ για περιορισμούς χρήσης: Η συσκευή αυτή περιορίζεται μόνο σε εσωτερικούς χώρους χρήσης. Μπορεί να μην λειτουργεί σε εξωτερικούς χώρους.
fr	Français [French]	Par la présente Lantronix, Inc. déclare que l'appareil NTC-502 device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante: http://www.lantronix.com/products/ntc-500-series/ Avis de restrictions d'utilisation de l'UE: Cet appareil est limité à une utilisation en intérieur uniquement. Il ne doit pas être utilisé àl'extérieur
is	Icelandic	Hér með lýsir Lantronix, Inc. því yfir að NTC-502 device sé í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53 / ESB. Í heildartexta ESB-samræmisyfirlýsingarinnar er að finna á eftirfarandi internetfangi: http://www.lantronix.com/products/ntc-500-series/ Tilkynning ESB um takmarkanir á notkun: Þetta tæki er eingöngutakmarkað við notkun innanhúss. Það má ekki nota það úti.
it	Italiano [Italian]	Con la presente Lantronix, Inc. dichiara che questo NTC-502 device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: http://www.lantronix.com/products/ntc-500-series/

Code	Language	Statement
		Avviso di restrizioni d'uso dell'UE: questo dispositivo è limitato esclusivamente all'uso in interni. Potrebbe non essere utilizzatoall'aperto.
lv	Latviski [Latvian]	Ar šo Lantronix, Inc. deklarē, ka NTC-502 device atbilst Direktīvas 2014/ 53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā tīmekļa vietnē: http://www.lantronix.com/products/ntc-500-series/ ES paziņojums par lietošanas ierobežojumiem: šo ierīci var izmantot tikai iekštelpās. To nedrīkst darbināt ārpus telpām.
lt	Lietuvių [Lithuanian]	Šiuo Lantronix, Inc. deklaruoja, kad šis NTC-502 device atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. Visą ES atitikties deklaracijos tekstą galite rasti šiuo interneto adresu: http://www.lantronix.com/products/ntc-500-series/ ES pranešimas apie naudojimo apribojimus: Šis prietaisas skirtas naudoti tik patalpose. Jo negalima naudoti lauke.
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix, Inc. dat het toestel NTC-502 device overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: http://www.lantronix.com/products/ntc-500-series/ EU kennisgeving van gebruiksbeperkingen: dit apparaat is beperkt tot gebruik binnenshuis. Het mag niet buitenshuis worden gebruikt.
mt	Malti [Maltese]	Hawnhekk, Lantronix, Inc., jiddikjara li dan NTC-502 device jikkonforma malħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU. It-test sħiħ tad-dikjarazzjoni ta 'konformità tal-UE huwa disponibbli flindirizz tal-internet li ġej: http://www.lantronix.com/products/ntc-500-series/ Avviż tal-UE dwar Restrizzjonijiet fuq l-Użu: Dan l-apparat huwa limitat għal użu ġewwa biss. Ma jistax jitħaddem barra.
hu	Magyar [Hungarian]	Alulírott, Lantronix, Inc. nyilatkozom, hogy a NTC-502 device megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. Az EU-megfelelőségi nyilatkozat teljes szövege a következő internetes címen érhető el: http://www.lantronix.com/products/ntc-500-series/ EU értesítés a korlátozásokról: Ez az eszköz csak beltéri használatra korlátozódik. Lehet, hogy szabadban nem üzemeltethető.
no	Norwegian	Lantronix, Inc. erklærer herved at denne NTC-502 device er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53 / EU. Den fullstendige teksten til EU-samsvarserklæringen er tilgjengelig på følgende internettadresse: http://www.lantronix.com/products/ntc-500-series/

Code	Language	Statement
		EUs merknad om bruksbegrensninger: Denne enheten er bare begrenset til innendørs bruk. Det kan hende at den ikke brukesutendørs.
pl	Polski [Polish]	Niniejszym Lantronix, Inc. oświadcza, że NTC-502 device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. Pełny tekst deklaracji zgodności EU jest dostępny pod następującym adresem internetowym: http://www.lantronix.com/products/ntc-500-series/ Zawiadomienie UE o ograniczeniach użytkowania: To urządzenie jest przeznaczone wyłącznie do użytku w pomieszczeniach. Nie można go obsługiwać na zewnątrz.
pt	Português [Portuguese]	Lantronix, Inc. declara que este NTC-502 device está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. O texto completo da declaração UE de conformidade está disponível no seguinte endereço na Internet: http://www.lantronix.com/products/ntc-500-series/ Aviso da UE de restrições de uso: Este dispositivo está limitado apenas ao uso interno. Não pode ser operado ao ar livre.
ro	Romanian	Prin prezenta, Lantronix, Inc., declară că acest NTC-502 device respect cerințele esențiale și alte dispoziții relevante din Directiva 2014/53 / UE. Textul complet al declarației de conformitate a UE este disponibil la următoarea adresă de internet: http://www.lantronix.com/products/ntc-500-series/ Notificarea UE privind restricțiile de utilizare: Acest dispozitiv este limitat numai la uz interior. Este posibil să nu funcționeze în aer liber.
sr	Serbian	Овиме, Лантроник, Инц., изјављује да је овај NTC-502 device у складу са суштинским захтевима и осталим релевантним одредбама Директиве 2014/53 / ЕУ. Комплетан текст ЕУ изјаве о усаглашености доступан је на следећој Интернет адреси: http://www.lantronix.com/products/ntc-500-series/ Обавештење ЕУ о ограничењима употребе: Овај уређај је ограничен само на унутрашњу употребу. Можда се не користи на отвореном.
sl	Slovensko [Slovenian]	Lantronix, Inc. izjavlja, da je ta NTC-502 device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu: http://www.lantronix.com/products/ntc-500-series/ Obvestilo EU o omejitvah uporabe: Ta naprava je omejena samo na notranjo uporabo. Morda ga ne uporabljate na prostem.
sk	Slovensky [Slovak]	Lantronix, Inc. týmto vyhlasuje, že NTC-502 device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU. Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: http://www.lantronix.com/products/ntc-500-series/ Oznámenie EÚ o obmedzeniach pri používaní: Toto zariadenie je obmedzené iba na použitie v interiéri. Nesmie sa používať vonku.

Code	Language	Statement
fi	Suomi [Finnish]	Lantronix, Inc. vakuuttaa täten että NTC-502 device tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavana seuraavassa Internet-osoitteessa: http://www.lantronix.com/products/ntc-500-series/ EU: n ilmoitus käyttörajoituksista: Tämä laite on rajoitettu vain sisäkäyttöön. Sitä ei saa käyttää ulkona.
sv	Svenska [Swedish]	Härmed intygar Lantronix, Inc. att denna NTC-502 device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: http://www.lantronix.com/products/ntc-500-series/ EU-meddelande om begränsningar för användning: Den här enheten är endast begränsad till inomhusbruk. Det får inte användas utomhus.

UK Declaration of Conformity

LANTRONIX®

UK CA

UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250 Irvine, CA 92618 USA
Model Name: NTC-502
Rated: 12Vdc, 1.5A
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

TÜVRheinland

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

Applicable EU Directives:

Electrical Equipment Regulations 2016

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

Electromagnetic Compatibility Regulations 2016

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

Radio Equipment Regulations 2017

- EN 301 908-1 V15.2.1(2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.2.1 (2022-02)
- Draft EN 301-908-25 V15.1.1_15.0.9 (2021-06)

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

- BS EN 62321-2:2021

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

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

CERT-00511 rev A

Figure C-2 UK Declaration of Conformity