User Guide

NTC-500

Doc No. UG01448

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. Casa Systems accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Casa Systems NTC-500 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.

Copyright

Copyright© 2024 Casa Systems. All rights reserved.

The information contained herein is proprietary to Casa Systems. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Casa Systems.

Trademarks and registered trademarks are the property of Casa Systems or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

Note – This document is subject to change without notice.

Document history

This document relates to the following product:

NetComm NTC-500

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

Table i. – Document revision history

Contents

Overview ... 6

Introduction ... 6
Target audience ... 6
Prerequisites ... 6
Notation ... 6

Product introduction ... 7

Product overview ... 7
Product features ... 7
Package contents ... 7

Physical dimensions and indicators ... 9

Physical dimensions ... 9
Interfaces ... 10
LED indicators ... 10
Signal strength LEDs ... 11
LED update interval ... 12
Ethernet port LED indicators ... 12

Placement of the router ... 13

Antenna installation ... 13
Mounting options ... 14
DIN rail mounting bracket ... 14
DIN rail installation ... 15
Wall mounted via DIN bracket ... 15
Ceiling mounted via DIN bracket ... 16
Pole mounted via DIN bracket ... 16
Rail mounting adapter ... 17

Installation and configuration of the NTC-500 router ... 18

Powering the router ... 18
DC power via 2-way connector ... 18
DC power via field terminated power source ... 18
Installing the router ... 18

Advanced configuration ... 20

Initialisation ... 20
Configure as a new device (create new passwords) ... 21
Logging In ... 22

Status........23

Networking........28

Wireless WAN........28

Wireless WAN profiles........28

Band selection........32

SIM management........32

RAT selection........33

Operator setting........33

Roaming control........34

Cell lock........35

SIM security........36

Network slice........37

LAN........38

LAN........38

DHCP........40

VLAN........43

VPN........45

IPSec........45

OpenVPN........49

GRE Tunnelling........57

Server Certificate........60

Firewall........63

NAT........63

MAC whitelist........64

Firewall filtering........65

IPS........66

Routing........67

Static........67

Redundancy........70

DMZ........74

RIP........75

Service assurance........76

Services........78

Network time (NTP)........78

SNMP........80

Configuring SNMP........80

Configuring SNMP traps........81

TR-069........82

DNS server........84

SMS messaging........84

Setup........85

Diagnostics........87

Inbox........100

New message........100

Outbox........101

MQTT........102

Configuring MQTT........103

OMA-LWM2M 106
Supported LWM2M objects 107
Event Configuration 109
Event Notification Configuration 110
Destination configuration 111
Event notification log 113
Email Settings 114
Dynamic DNS 115
System 117
Log 117
System log 117
System log settings 117
Diagnostic log 120
IPSec log 122
Watchdog 123
Periodic ping 123
Periodic reboot 125
System configuration 126
Restore factory defaults 126
Web server setting 127
Administration settings 128
Settings backup/restore 129
Site and location settings 130
Runtime configuration 131
SSH key management 132
LED operation mode 133
Firmware upgrade 134
Updating the router firmware 134
Access control 135
Reboot 136
Field test 137
Encrypted debuginfo 139
Appendix A – Configuring Radio Access Technologies 140
Contact Details 141
Product sales 141
Warranty and support 141
Contact Details 141
Australian Office 141
Head Office US 141

Overview

Introduction

This document provides you all the information you need to set up, configure and use the NetComm NTC-500 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 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 in order to avoid damage or injury.

Product introduction

Product overview

The NTC-500 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 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 NetComm NTC-500 package contains:

- 1 x NTC-500 router
- 1 x Two-way Molex connector
- 1 x 1.5m Ethernet cable
- 1 x DIN rail mounting bracket

- 1 x Welcome Card
- 1 x Compliance leaflet

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

Physical dimensions and indicators

Physical dimensions

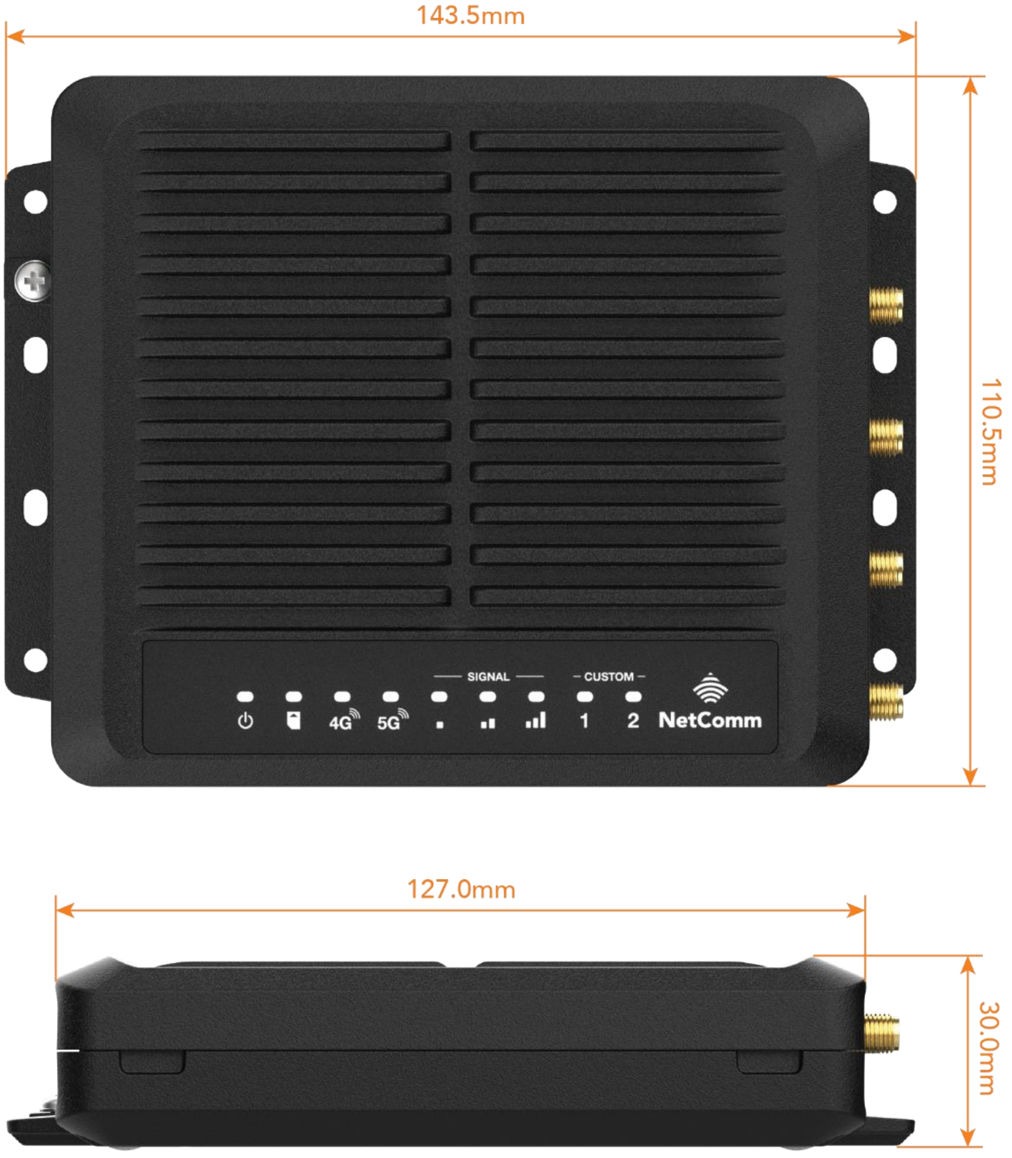


Figure 1 – NTC-500 top and side views

NTC-500 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 router:

ITEM	DESCRIPTION
Antenna sockets	SMA female connector 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 source wires here. Power wires may be terminated on optional terminal block and connected to DC input jack. Refer to the diagram and table under the Installation section for correct wiring of the terminal block. Operates in the 8-40V DC range.
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 15 seconds to reboot to recovery mode. The LEDs are amber and extinguish in sequence to indicate that the router will load the recovery image. Press and hold for 15 to 25 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.

Table 1 - Interfaces

LED indicators

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

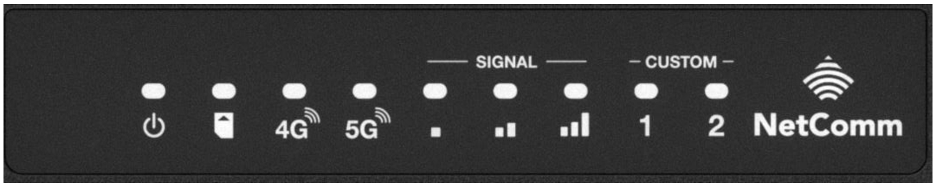


Figure 2

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	Customisable		Programmable LED for custom use
CUSTOM	Custom 2	Customisable		Programmable LED for custom use

Table 2 – LED indicators

Signal strength LEDs

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

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

Table 3 – Signal strength LED indicators

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 router has two LED indicators.

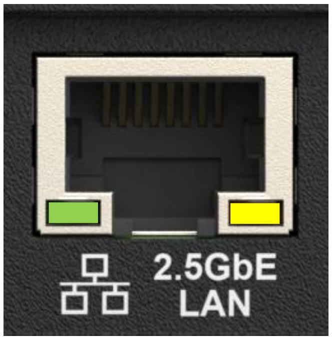


Figure 3 – NTC-500 Ethernet port LED indicators

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

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 100Mbps or 1000Mbps or 2500Mbps.
	Off	Ethernet port is operating at a speed of 10Mbps or no Ethernet cable is connected

Table 4 – Ethernet port LED indicators

Placement of the router

Antenna installation

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

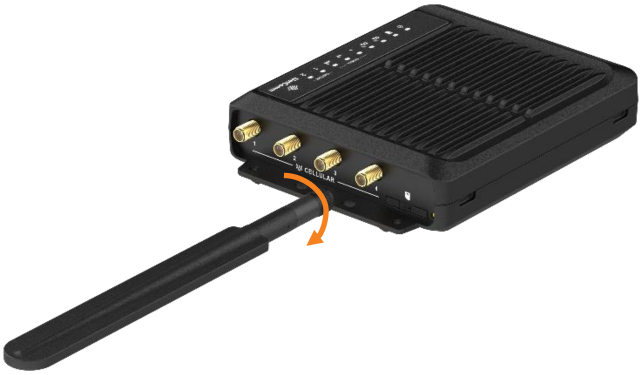


Figure 4 – NTC-500 antenna installation

Connecting antennas to the device should provide optimum cellular and Wi-Fi signal strength in a wide range of environments. If you find the signal strength is weak, try adjusting the orientation of the antennas. If you are unable to get an acceptable signal, try moving the router to a different place or mounting it differently.

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

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

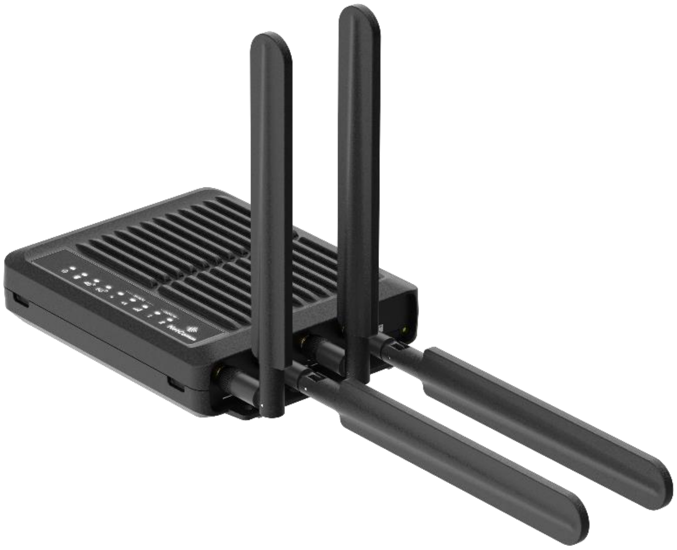


Figure 5 – NTC-500 optimal antenna positioning

Mounting options

The NTC-500 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.

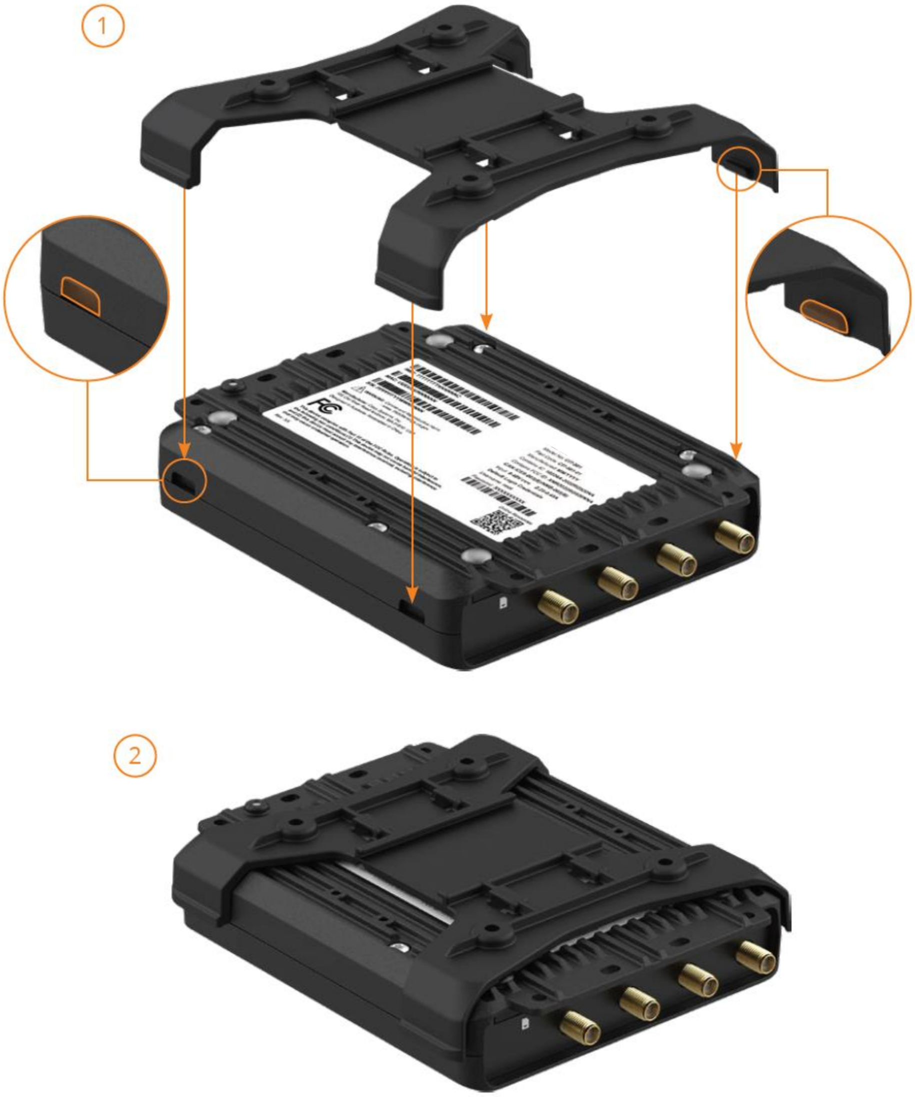


Figure 6 – NTC-500 DIN mounting bracket

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.

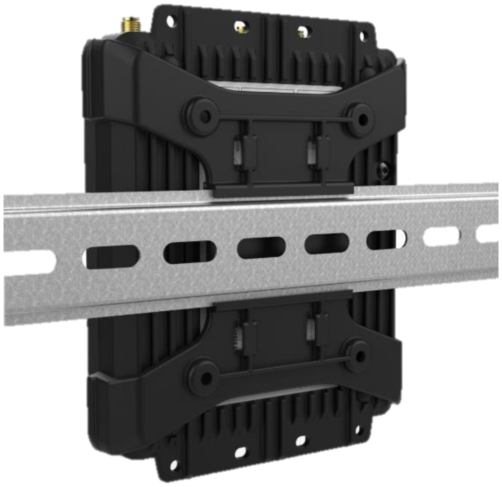


Figure 7 – NTC-500 DIN mounting bracket

Wall mounted via DIN bracket

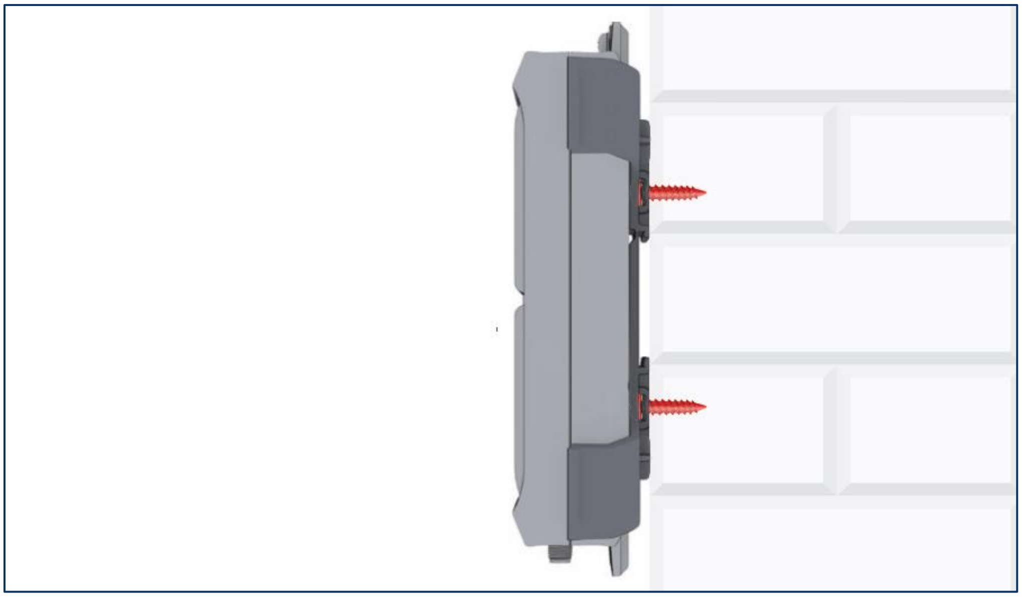


Figure 8 – NTC-500 wall mounted using DIN bracket

Ceiling mounted via DIN bracket

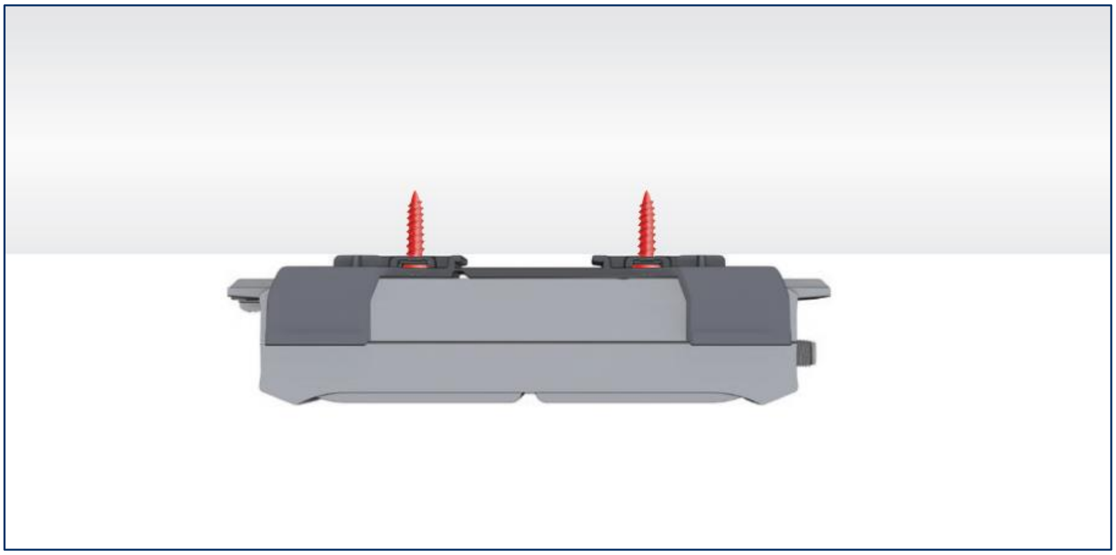


Figure 9 – NTC-500 ceiling mounted using DIN bracket

Pole mounted via DIN bracket

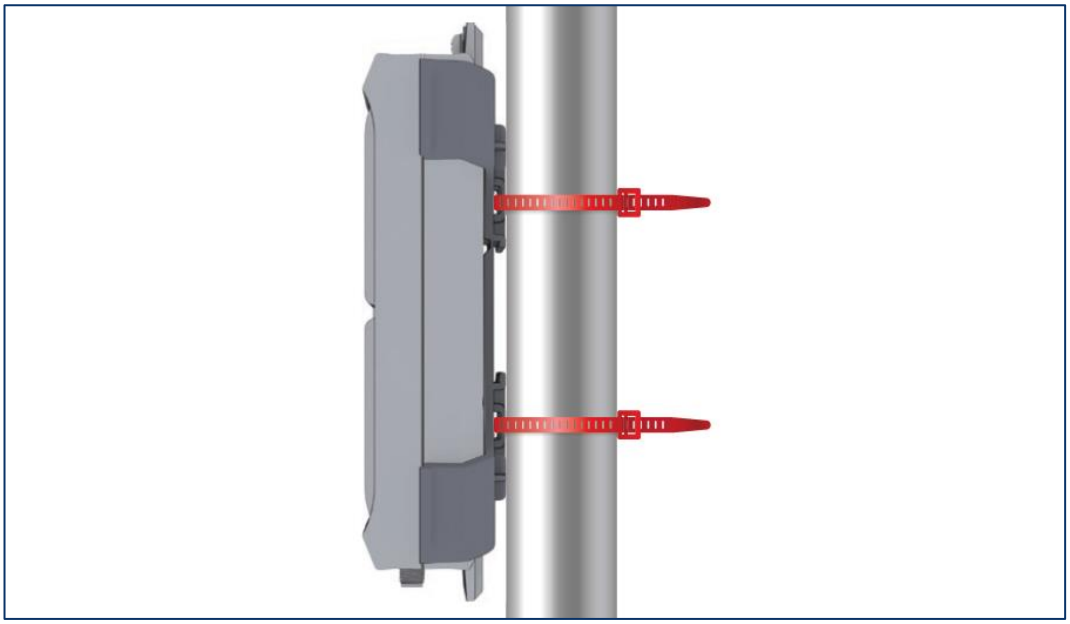


Figure 10 – NTC-500 pole mounted using DIN bracket

Rail mounting adapter

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

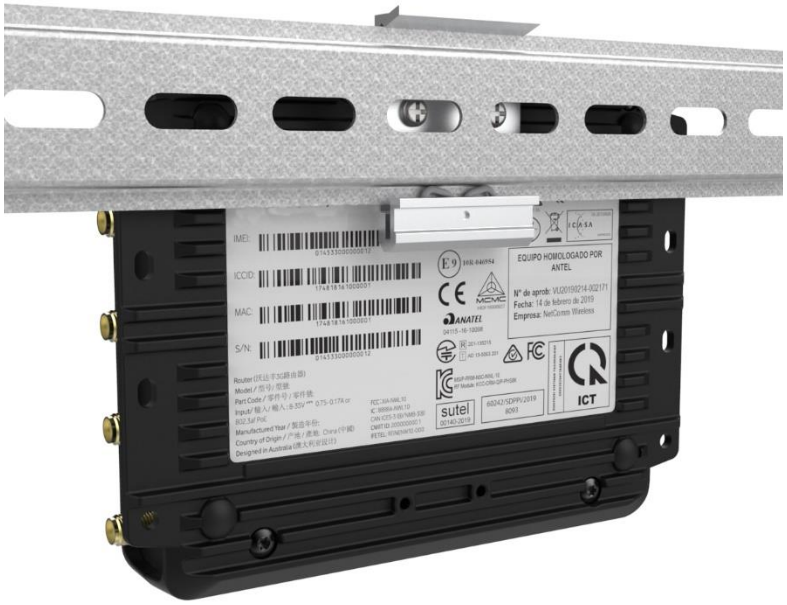


Figure 11 – NTC-500 rail mount adapter

Installation and configuration of the NTC-500 router

Powering the router

The NTC-500 router can be powered in one of two ways:

1 DC power input via 2-pin connector (8-40V DC)

2 DC power input via field terminated power source (8-40V DC)

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

DC power via 2-way connector

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

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

DC power via field terminated power source

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

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 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 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.

Advanced configuration

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

The router's web user interface is displayed.

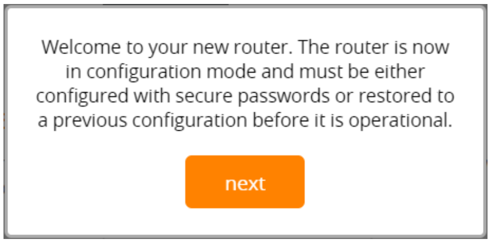
Important – The HTTP protocol is disabled by default, secure HTTP (HTTPS) is the default protocol. HTTP access is available but must be manually enabled.

Initialisation

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

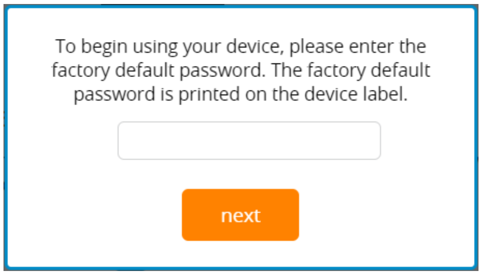
To complete the setup:

1 Select the Next button on the first dialogue box.



Welcome to your new router. The router is now in configuration mode and must be either configured with secure passwords or restored to a previous configuration before it is operational.

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



To begin using your device, please enter the factory default password. The factory default password is printed on the device label.

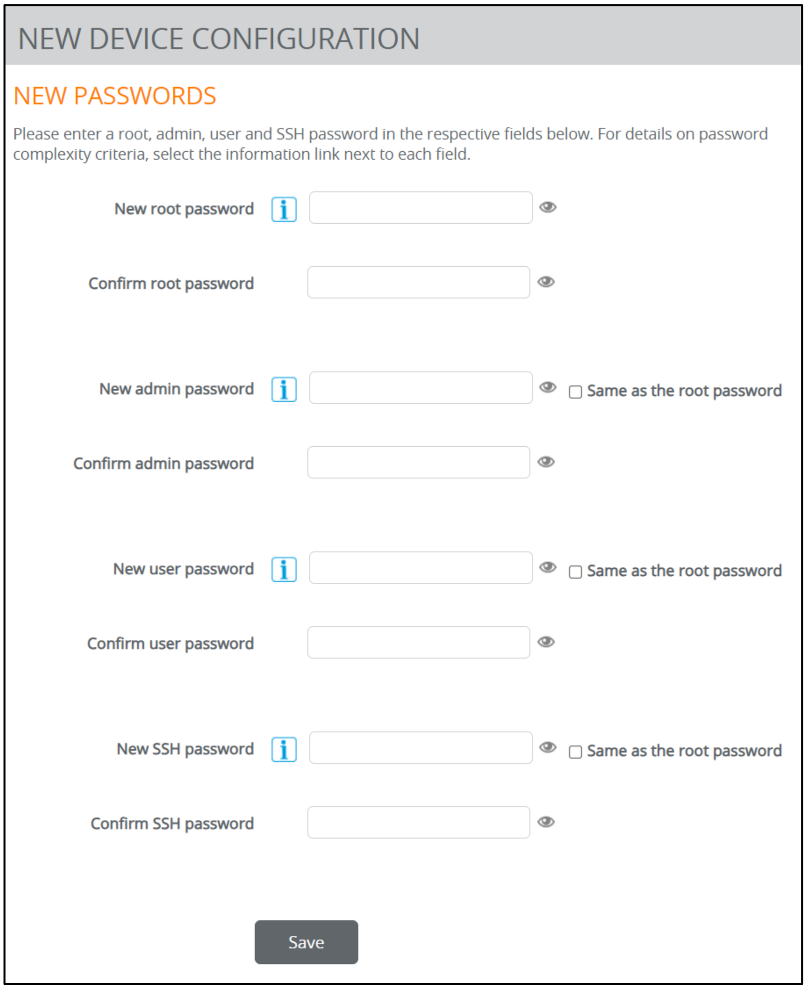
3 Select whether to configure the router as a new device or to restore a previous configuration backup.

Configure as a new device (create new passwords)

Select **I want to configure this as a new device** then select the **OK** button.

In the New Passwords section, enter a strong password in each field. You may configure the same password for all three accounts, but it must meet the security criteria set out below:

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



NEW DEVICE CONFIGURATION

NEW PASSWORDS

Please enter a root, admin, user and SSH password in the respective fields below. For details on password complexity criteria, select the information link next to each field.

New root password

Confirm root password

New admin password □ Same as the root password

Confirm admin password

New user password □ Same as the root password

Confirm user password

New SSH password □ Same as the root password

Confirm SSH password

Save

Figure 12 – New device configuration dialog page

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

Logging In

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

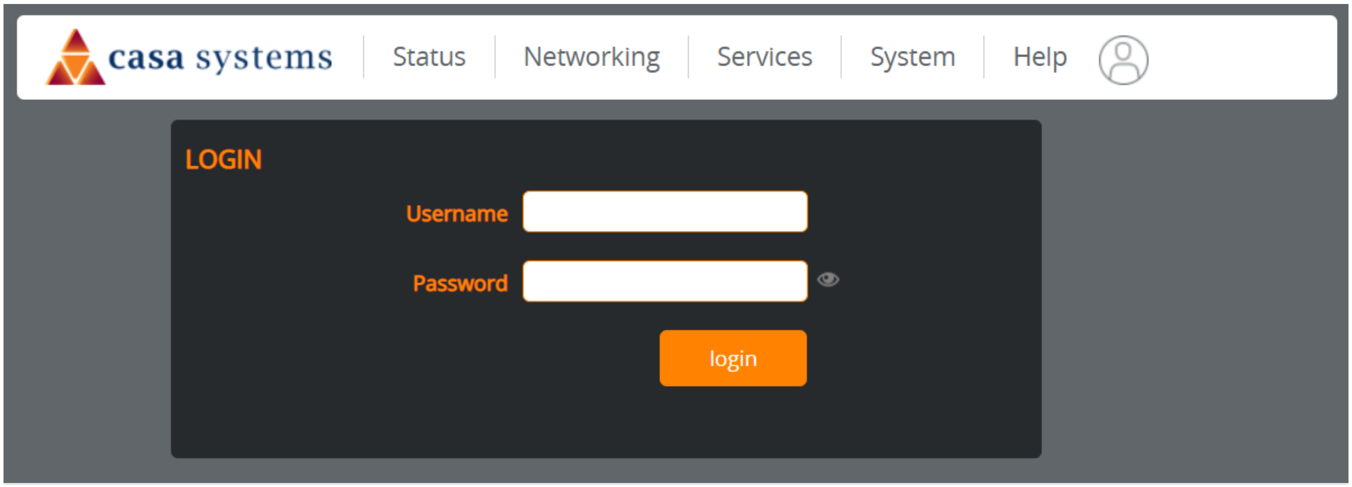
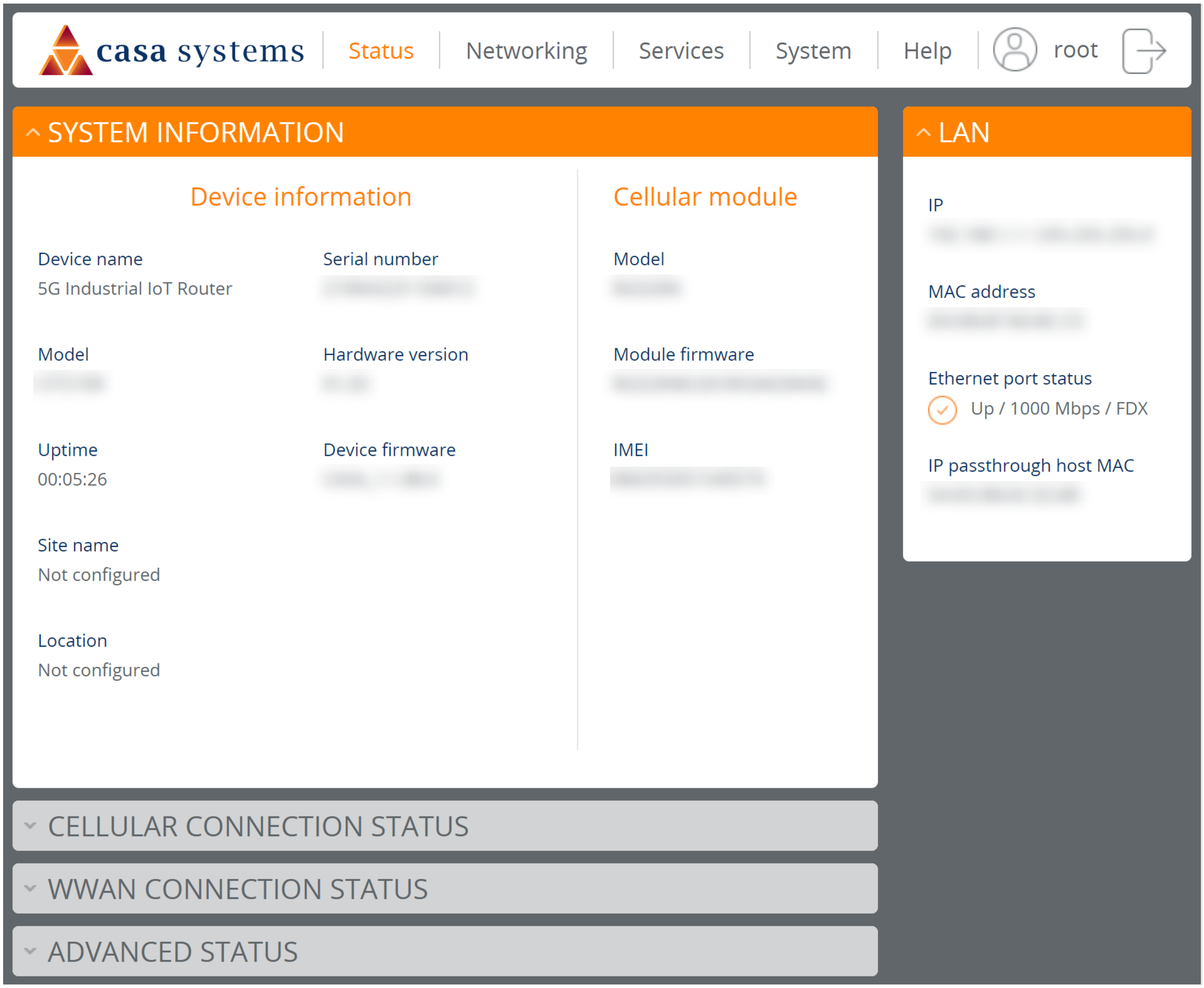


Figure 13 – Log in prompt for web-based user interface

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

Status

The status page of the web interface provides system related information and is displayed when you log in to the NTC-500 router management console. The status page shows System information, LAN details, Cellular connection status, WWAN connection status, Wireless LAN status and Neighbouring cell information. You can toggle the sections from view by selecting the ⌃ or ⌄ buttons to show or hide them. Extra status boxes will appear as additional software features are enabled (e.g. VPN connectivity).



⌃ SYSTEM INFORMATION

Device information

Device name
5G Industrial IoT Router

Serial number
[redacted]

Model
[redacted]

Hardware version
[redacted]

Uptime
00:05:26

Device firmware
[redacted]

Site name
Not configured

Location
Not configured

Cellular module

Model
[redacted]

Module firmware
[redacted]

IMEI
[redacted]

⌃ LAN

IP
[redacted]

MAC address
[redacted]

Ethernet port status
✓ Up / 1000 Mbps / FDX

IP passthrough host MAC
[redacted]

⌄ CELLULAR CONNECTION STATUS

⌄ WWAN CONNECTION STATUS

⌄ ADVANCED STATUS

Figure 14 – NTC-500 status page

The following information is included on the Status page:

Item	Definition
System information	
System up time	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.
Device name	The device name of the NTC-500.
Model	The commercial product name which helps to identify the available features of the router.
Hardware version	The hardware version of the router.
Serial number	The serial number of the router.
Firmware version	The firmware version of the router
Cellular Model	The type of phone module and the firmware version of the module.
Module firmware	The firmware revision of the phone module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
LAN	
IP	The IP address and subnet mask of the router.
MAC address	The MAC address of the router.
LAN Port Status	Displays the current status of the LAN port and its operating speed.
IP passthrough host MAC	The MAC address associated with the passthrough host when IP passthrough is enabled.
Cellular Connection Status	
SIM status	Displays the activation status of the NTC-500 on the carrier network. This includes information about whether there is a SIM inserted or if the SIM card has an error.
Signal strength (dBm)	The current signal strength measured in dBm.
Network registration status	The status of the NTC-500 registration for the current network.
Operator selection	The mode used to select an operator network.
Provider	The current operator network in use.
Roaming status	The roaming status of the NTC-500.
Allowed bands	The bands to which the NTC-500 may connect.
Current band	The current band being used by the NTC-500.

Connection (RAT)	The radio access technology in use.
Coverage	The type of mobile coverage being received by the NTC-500.
WWAN	
Profile name	The name of the active profile.
Status	The IPv4 connection status of the active profile.
IPv6 status	The IPv6 connection status of the active profile.
MTU	The current IPv4 Maximum Transmission Unit (MTU) of the WWAN connection.
IPv6 MTU	The current IPv6 Maximum Transmission Unit of the WWAN connection.
WWAN IP	The IPv4 address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection.
WWAN IPv6	The IPv6 address assigned by the mobile broadband carrier network.
IPv6 DNS server	The primary and secondary IPv6 DNS servers for the WWAN connection.
APN	The Access Point Name currently in use.
Connection uptime	The length of time of the current mobile connection session.
Max DL	The maximum download speed that is possible.
Max UL	The maximum upload speed that is possible.
Current DL	The current download speed.
Current UL	The current upload speed.
Advanced Status	
Mobile country code	The Mobile Country Code (MCC) of the NTC-500.
Mobile network code	The Mobile Network Code (MNC) of the NTC-500.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the NTC-500, a unique number up to 19 digits in length.
IMSI	The International Mobile Subscriber Identity is a unique identifier of the user of a cellular network.
Packet service status	Displays whether the packet service is attached or detached. When APN or username/password is changed, the device detaches and reattaches to the network.
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 communications between UE and a mobile network
gNB Cell ID	A unique code that identifies the base station from within the location area of the current mobile 5G network signal. This is not available when the device is operating in LTE or 5G Non-Standalone mode.
gNB PCI	Physical Cell ID of the 5G NR Cell.
Channel number (NR ARFCN)	The channel number of the current 5G cellular connection.
SSB Channel Number (SSB ARFCN)	The Synchronization Signal Block (SSB) channel number of the current 5G cellular connection.
Subcarrier spacing (SCS)	The size of the current Subcarrier Spacing (SCS) expressed in KHz.
Reference Signal Received Power (SS-RSRP)	Synchronisation Signal Reference Signal Received Power (SS-RSRP). The linear average over the power contributions (in Watts) of the resource elements that carry Secondary Synchronisation Signal (SSS).
Reference Signal Received Quality (SS-RSRQ)	Secondary Synchronisation 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)	Synchronisation Signal – Signal to interference plus noise ratio. The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.
NR CQI	The 5G NR Channel Quality Indicator (CQI).

Synchronisation Signal Block (SSB) Index	This is a key part of beam management. It is a value comprised of Primary Synchronisation Signal (PSS), Secondary Synchronisation Signal (SSS) and the Physical Broadcast Channel (PBCH).
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).
Serving	The radio signal being served e.g., 5G NR, LTE.

Table 5 – Status page item details

Networking

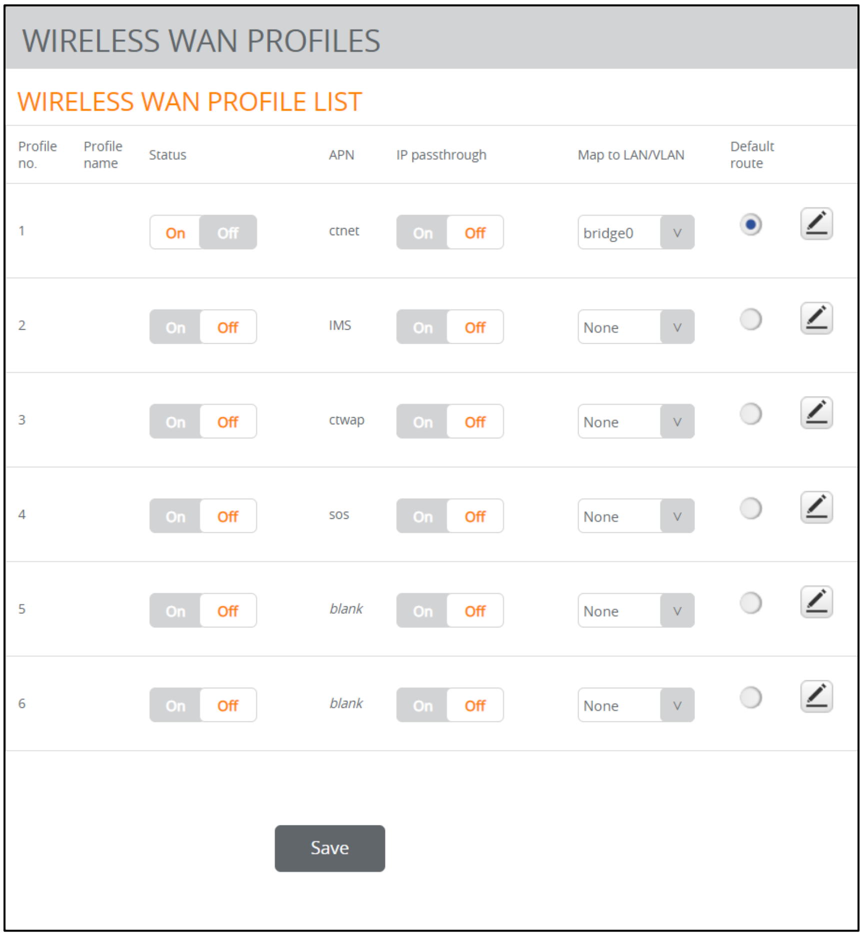
The Networking section provides configuration options for Wireless WAN, LAN, Firewall, Routing and Service Assurance.

Wireless WAN

Wireless WAN profiles

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

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.



WIRELESS WAN PROFILES

WIRELESS WAN PROFILE LIST

Profile no.	Profile name	Status	APN	IP passthrough	Map to LAN/VLAN	Default route	
1		On Off	ctnet	On Off	bridge0	●	✎
2		On Off	IMS	On Off	None	○	✎
3		On Off	ctwap	On Off	None	○	✎
4		On Off	sos	On Off	None	○	✎
5		On Off	*blank*	On Off	None	○	✎
6		On Off	*blank*	On Off	None	○	✎

Figure 15 – Wireless WAN profiles

ITEM	DEFINITION
Profile no.	Number of the profile.
Profile name	Name of the profile.
Status	Toggles the corresponding profile on and off. Only one profile may be turned on at any time.
APN	The APN configured for the corresponding profile.
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) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Map to LAN/VLAN	The LAN or VLAN that the profile is assigned to.
Default Route	Sets the profile as the default route for traffic.

Table 6 – WWAN profile item details

Connecting to the mobile broadband network

The NTC-500 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.

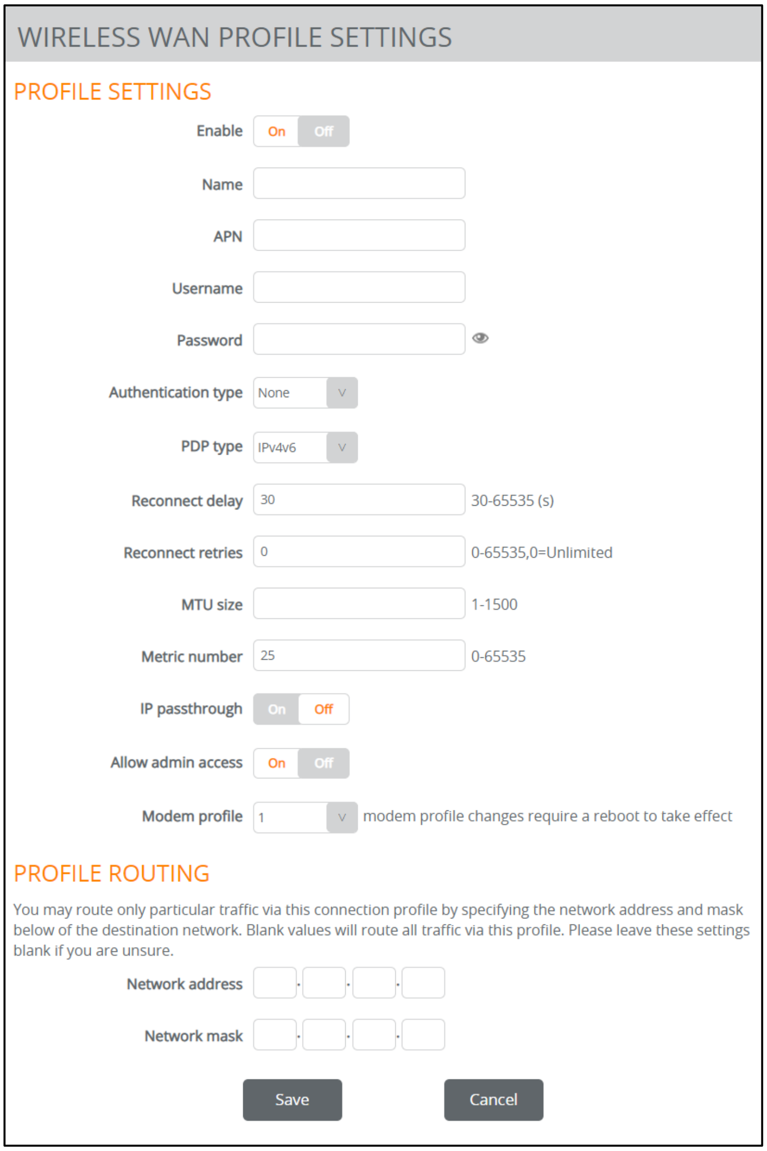
For advanced networking purposes, you may activate a maximum of two profiles simultaneously (dependent on network support). When activating two connection profiles, you should avoid selecting two profiles with the same APN as this can cause only one profile to connect. Similarly, activating two profiles 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.



WIRELESS WAN PROFILE SETTINGS

PROFILE SETTINGS

Enable: On | Off

Name:

APN:

Username:

Password:

Authentication type: None

PDP type: IPv4v6

Reconnect delay: 30 — 30-65535 (s)

Reconnect retries: 0 — 0-65535,0=Unlimited

MTU size: — 1-1500

Metric number: 25 — 0-65535

IP passthrough: On | Off

Allow admin access: On | Off

Modem profile: 1 — modem profile changes require a reboot to take effect

PROFILE ROUTING

You may route only particular traffic via this connection profile by specifying the network address and mask below of the destination network. Blank values will route all traffic via this profile. Please leave these settings blank if you are unsure.

Network address: . . .

Network mask: . . .

Figure 16 – WWAN profiles – WWAN profile settings

Item	Definition
Enable	Toggle the enable button to On or Off, as desired.
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.
APN	Enter the APN (Access Point Name) configured for the corresponding profile.
Username	The username used to log on to the corresponding APN (if required).
Password	The password used to log on to the corresponding APN (if required).
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.

Item	Definition
	a ⦿ **IPv4** – Sets a single stack IPv4 connection through which the NTC-500 receives only IPV4 network and DNS addresses. b ⦿ **IPv6** – Sets a single stack IPv6 connection through which the NTC-500 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. c ⦿ **IPv4v6** – Sets a dual stack connection allowing simultaneous IPV4 and IPV6 network connectivity. The NTC-500 receives both IPv4 and IPV6 network and DNS addresses. This is the default **PDP type**
Reconnect delay	The amount of time that the router should wait before retrying a reconnect.
Reconnect retries	The amount of times the router should try to reconnect.
MTU size	Sets the Maximum Transmission Unit size. This may be from 1 to 1500 bytes.
Metric number	The Metric value is used by router to prioritise routes (if multiple are available) and is set to 25 by default.
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) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Allow Admin Access	Select enable if remote SSH, TR-069 or WebGUI access to the device should be possible via this Wireless WAN Profile. Note – SSH/HTTP/HTTPS can be individually restricted in the **Access Control** menu. Note also that this will automatically be enabled if the profile is selected in the **TR-069 settings** menu.
Modem profile	Assigns the WWAN profile to a specific modem profile, which may be required by your carrier.
Profile routing	See the **Profile routing** section below.
Save button	Select the **Save** button to apply the changes.

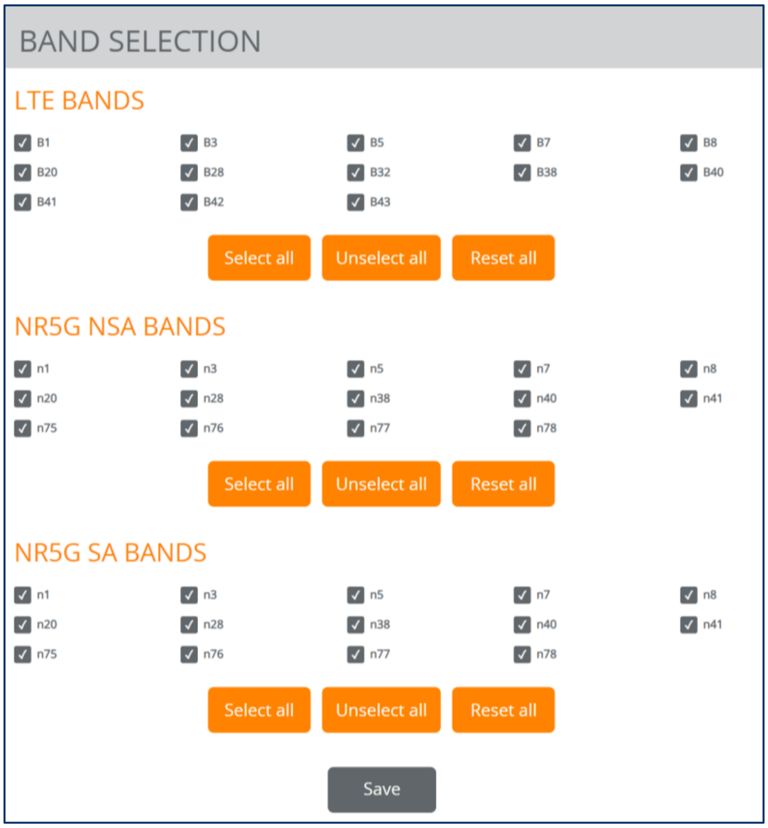
Table 7 - WWAN profiles – WWAN profile settings details

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 settings 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.

Band selection

Select individual bands from the following band groupings: LTE, NR5G NSA, NR5G SA.



BAND SELECTION

LTE BANDS

☑ B1	☑ B3	☑ B5	☑ B7	☑ B8
☑ B20	☑ B28	☑ B32	☑ B38	☑ B40
☑ B41	☑ B42	☑ B43		

NR5G NSA BANDS

☑ n1	☑ n3	☑ n5	☑ n7	☑ n8
☑ n20	☑ n28	☑ n38	☑ n40	☑ n41
☑ n75	☑ n76	☑ n77	☑ n78	

NR5G SA BANDS

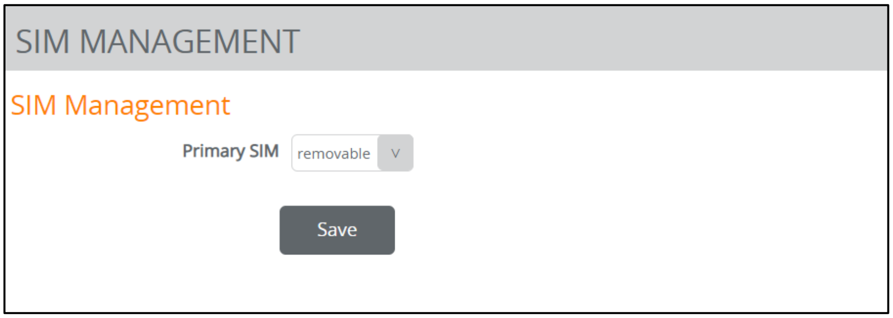
☑ n1	☑ n3	☑ n5	☑ n7	☑ n8
☑ n20	☑ n28	☑ n38	☑ n40	☑ n41
☑ n75	☑ n76	☑ n77	☑ n78	

Figure 17 – NTC-500 band selection

To set a device up for different LTE, 5G Non-Standalone (NR5G NSA) and 5G Standalone (NR5G NSA) modes, refer to: *Appendix A – Configuring Radio Access Technologies*

SIM management

The NTC-500 is equipped with both a removable and internal SIM. To switch between the two types the SIM management page can be used. Use the dropdown to set the primary SIM to either internal SIM or Removable SIM, then select Save.



SIM MANAGEMENT

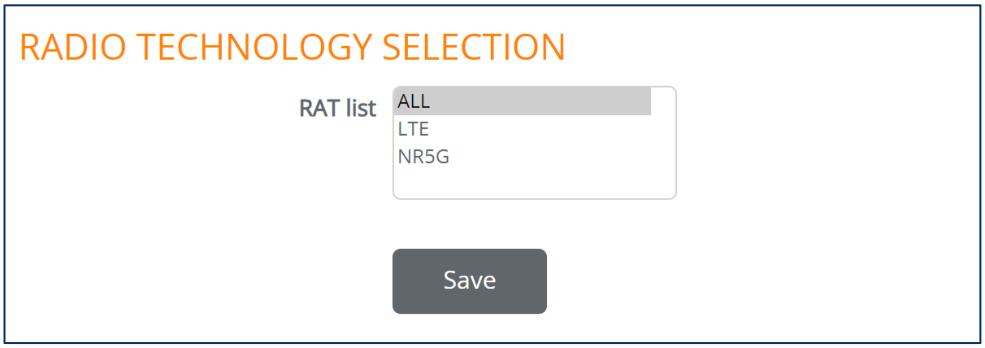
SIM Management

Primary SIM: removable

Figure 18 – SIM management

RAT selection

Select the preferred RAT (Radio Access Technology) from the following: ALL, LTE or NR5G



RADIO TECHNOLOGY SELECTION

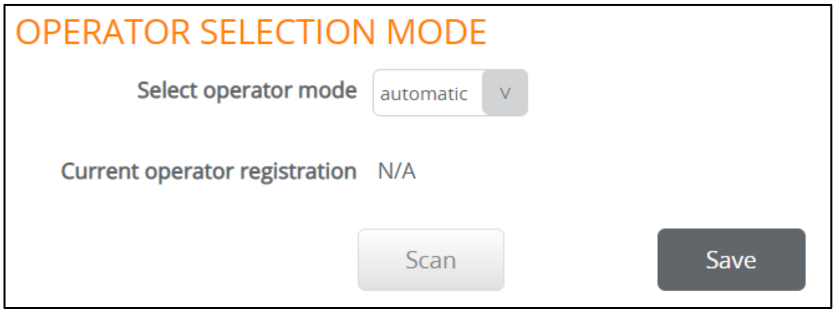
RAT list: ALL (selected), LTE, NR5G

Figure 19 – Radio Access Technology (RAT)

Note – To select two options, hold the Ctrl key whilst selecting the option you wish to use.

Operator setting

The Operator setting screen lets you select whether to have the NTC-500 automatically select the most appropriate operator and access technology, or if you set it to manual, you can override and lock it to a particular carrier or access technology.



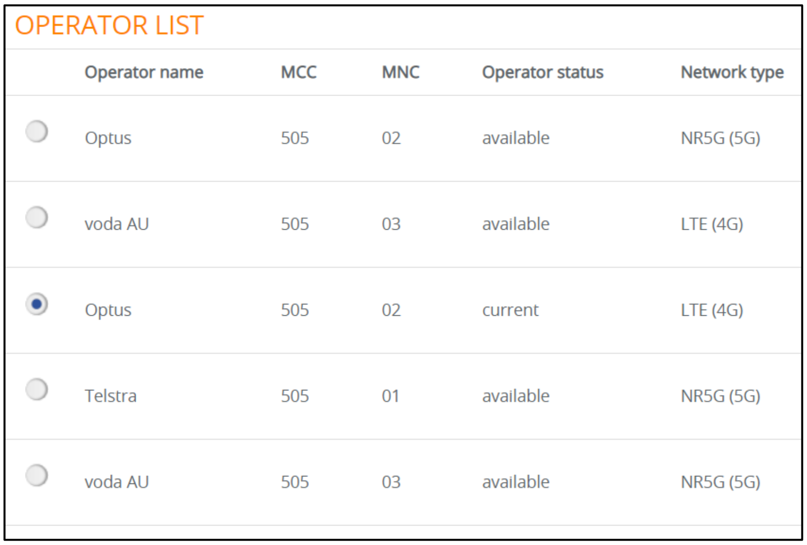
OPERATOR SELECTION MODE

Select operator mode: automatic

Current operator registration: N/A

Figure 20 – Operator selection mode

To scan for available networks, set the Select operator mode from Automatic to Manual then select 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.



OPERATOR LIST

	Operator name	MCC	MNC	Operator status	Network type
○	Optus	505	02	available	NR5G (5G)
○	voda AU	505	03	available	LTE (4G)
●	Optus	505	02	current	LTE (4G)
○	Telstra	505	01	available	NR5G (5G)
○	voda AU	505	03	available	NR5G (5G)

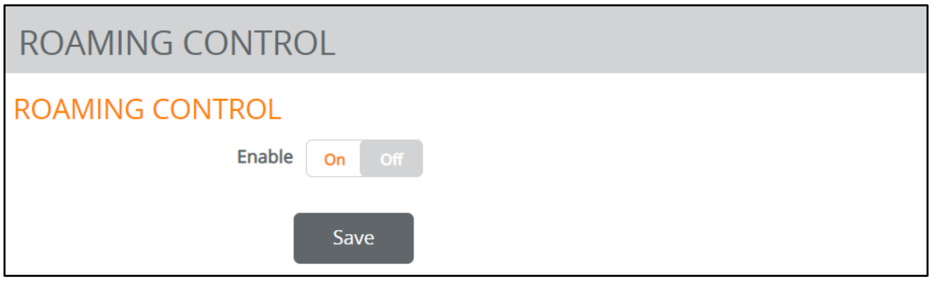
Figure 21 – Operator list

Select the most appropriate service from the list shown and select Apply.

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

Roaming control

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



ROAMING CONTROL

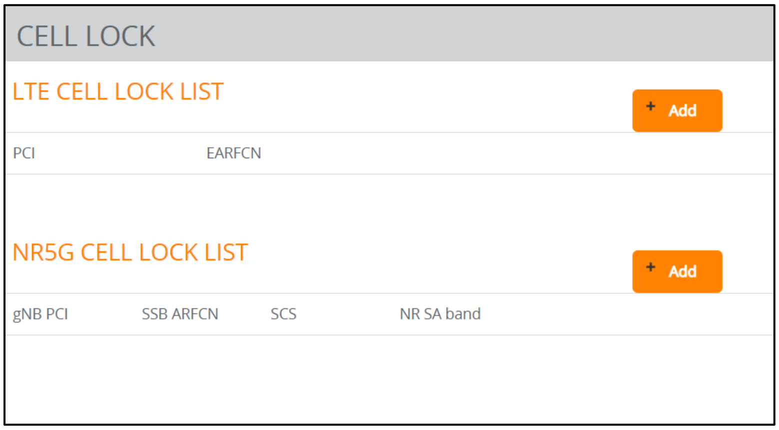
ROAMING CONTROL

Enable [✓ On] Off

Figure 22 – Roaming control toggle

Cell lock

The Cell lock function allows you to specify a list of cells that the NTC-500 will not deviate from. The cells are separated by LTE and NR5G.



CELL LOCK

LTE CELL LOCK LIST

PCI	EARFCN

NR5G CELL LOCK LIST

gNB PCI	SSB ARFCN	SCS	NR SA band

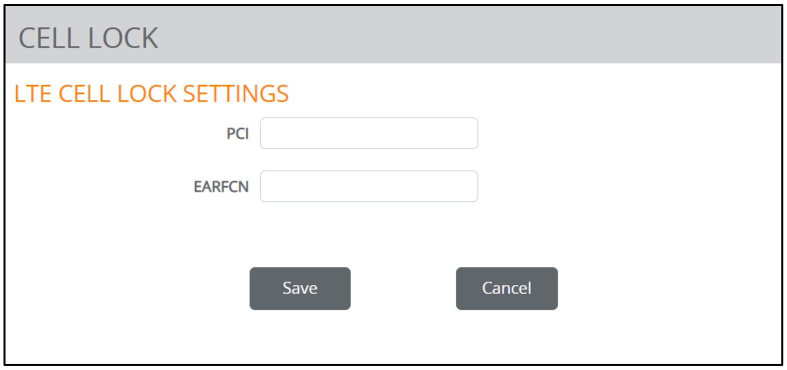
Figure 23 – Cell lock

Adding an LTE cell lock

To add an LTE cell to the list:

1 Next to **LTE Cell Lock List**, select the **Add** button.

2 Enter the **PCI** and **EARFCN** values of the cell that you want to lock to.



CELL LOCK

LTE CELL LOCK SETTINGS

PCI

EARFCN

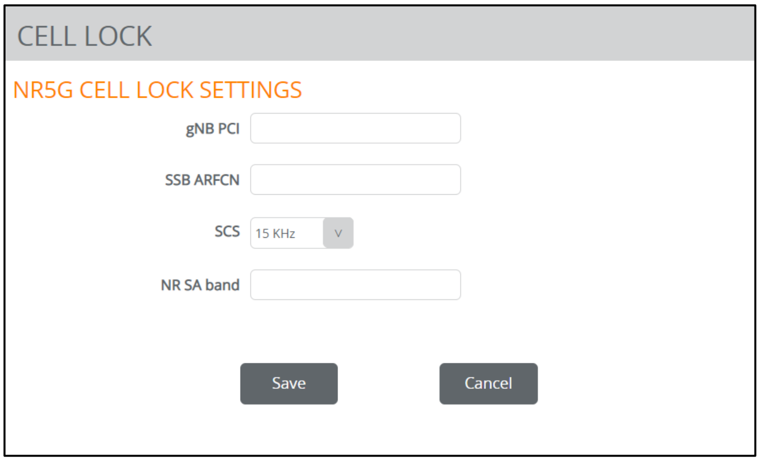
Figure 24 – Cell lock – Add LTE cell lock

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

Adding an NR cell lock

1 Next to the **NR5G Cell Lock List**, select on the **Add** button.

2 Enter the gNB, NR ARFCN, Subcarrier Spacing and NR SA band values for the NR5G cell that you want to lock to.



CELL LOCK

NR5G CELL LOCK SETTINGS

gNB PCI

SSB ARFCN

SCS: 15 KHz

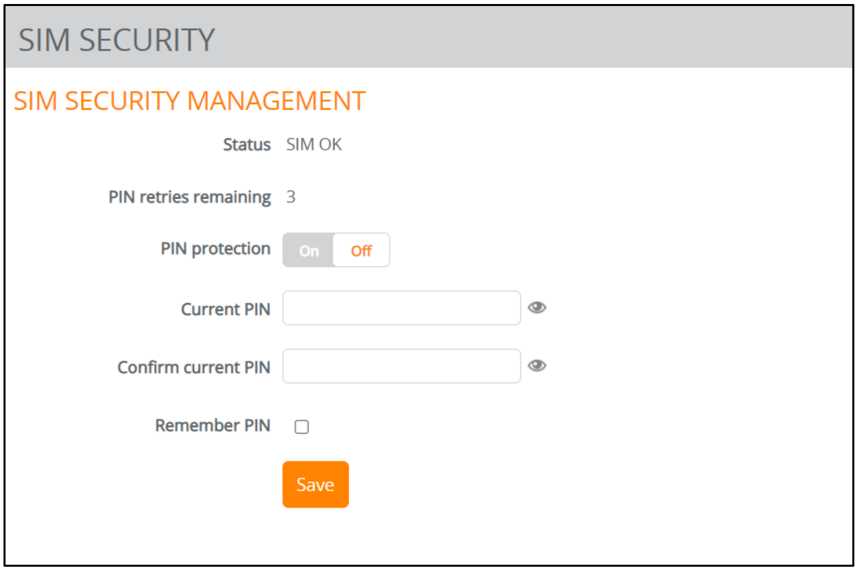
NR SA band

Figure 25 – Cell lock – Add NR5G cell lock

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

SIM security

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



SIM SECURITY

SIM SECURITY MANAGEMENT

Status: SIM OK

PIN retries remaining: 3

PIN protection: On [✓ Off]

Current PIN

Confirm current PIN

Remember PIN □

Figure 26 – SIM security settings

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

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

1 Select the **Networking** menu from the top menu bar, and then select **SIM security settings**.

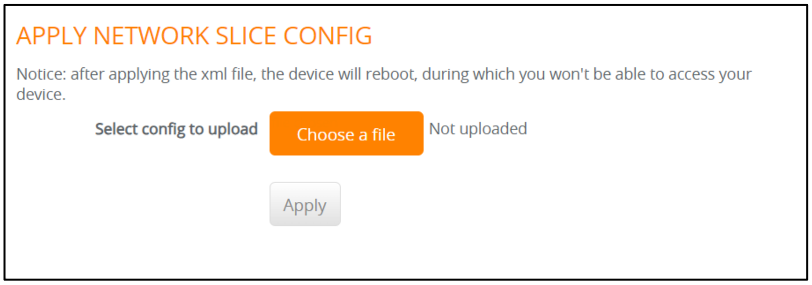
2 Enter the PIN in the **Current PIN** field (enter numbers only).

3 Select on the **Save** button to save the PIN and unlock access.

4 Once unlocked, you may toggle the **PIN protection** switch to the **Off** position if you no longer wish to have access locked by a PIN.

Network slice

The Network slice page is used to apply a network slice configuration.



APPLY NETWORK SLICE CONFIG

Notice: after applying the xml file, the device will reboot, during which you won't be able to access your device.

Select config to upload

Figure 27 – Network slice configuration

To apply a network slice configuration:

1 Select the **Networking** menu from the top menu bar, and then select **Network slice**.

2 Select the **Choose a file** button. Locate a valid network slice .xml file on your computer and select **Open**.

3 Select the **Apply** button to apply the network slice configuration.

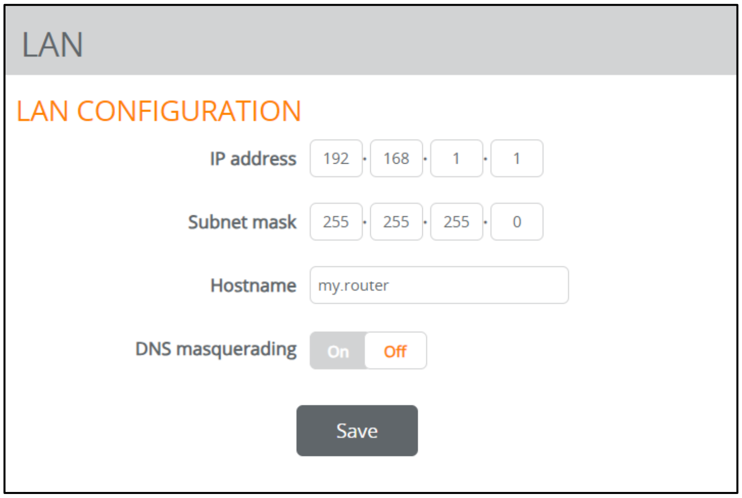
LAN

LAN

The **LAN configuration** page is used to configure the LAN settings of the NTC-500. To access the LAN configuration page, select on the Networking menu at the top of the screen, then select on the LAN menu on the left.

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.



LAN

LAN CONFIGURATION

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Hostname: my.router

DNS masquerading: On [✓ Off]

Figure 28 – LAN configuration

DNS masquerading

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

The DNS masquerading toggle key is OFF by default.

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

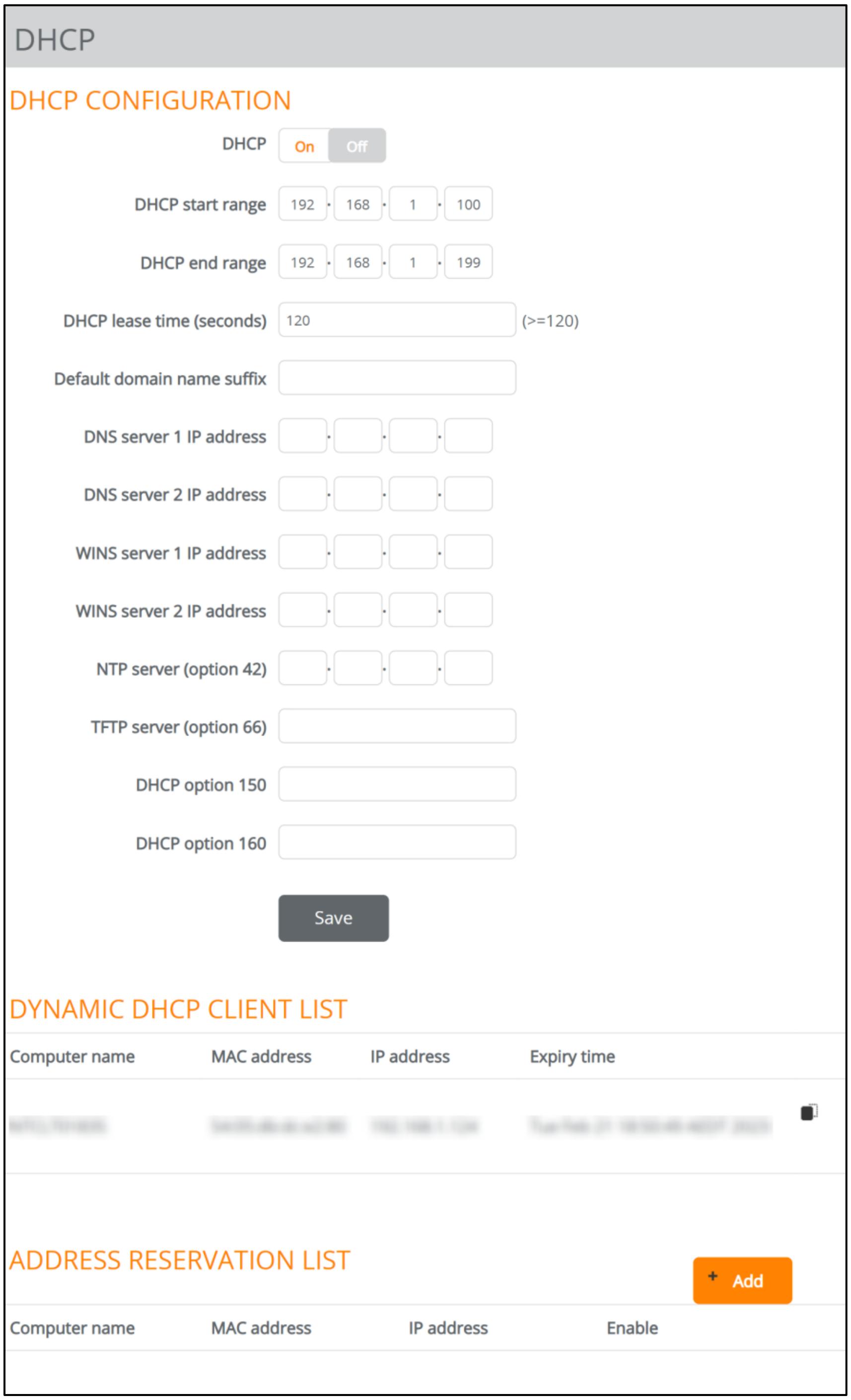
With DNS masquerading ON, the DHCP server embedded in the NTC-500 hands out its own IP address (e.g., 192.168.1.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NTC-500, which proxies them to the upstream DNS servers.

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

The DNS masquerading toggle key is OFF by default.

DHCP

The **DHCP configuration** page is used to configure the DHCP settings of the NTC-500. You can manually set the start and end address range to be used to automatically assign addresses, the lease time of the assigned address, the default domain name suffix, primary and secondary DNS server, the primary and secondary WINS server, as well as the advanced DHCP settings such as NTP, TFTP and Option 150/Option 160 (VoIP options).



DHCP

DHCP CONFIGURATION

DHCP	On Off
DHCP start range	192 . 168 . 1 . 100
DHCP end range	192 . 168 . 1 . 199
DHCP lease time (seconds)	120 (>=120)
Default domain name suffix	
DNS server 1 IP address	. . .
DNS server 2 IP address	. . .
WINS server 1 IP address	. . .
WINS server 2 IP address	. . .
NTP server (option 42)	. . .
TFTP server (option 66)	
DHCP option 150	
DHCP option 160	

Save

DYNAMIC DHCP CLIENT LIST

Computer name	MAC address	IP address	Expiry time
[redacted]	[redacted]	[redacted]	[redacted]

ADDRESS RESERVATION LIST

Computer name	MAC address	IP address	Enable

Figure 29 – DHCP configuration

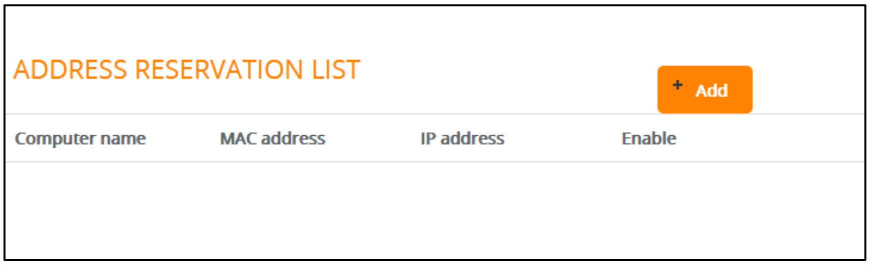
Option	Description
DHCP start range	Sets the first IP address of the DHCP range
DHCP end range	Sets the last IP address of the DHCP range
DHCP lease time (seconds)	The length of time in seconds that DHCP allocated IP addresses are valid
Default domain name suffix	Specifies the default domain name suffix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

Table 8 – DHCP configuration items

Enter the desired DHCP options and select the Save button.

Address Reservation List

DHCP clients are dynamically assigned an IP address as they connect, but you can reserve an address for a particular device using the ADDRESS RESERVATION LIST.



ADDRESS RESERVATION LIST

Computer name	MAC address	IP address	Enable

Figure 30 – Address reservation list

To add a device to the address reservation list:

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

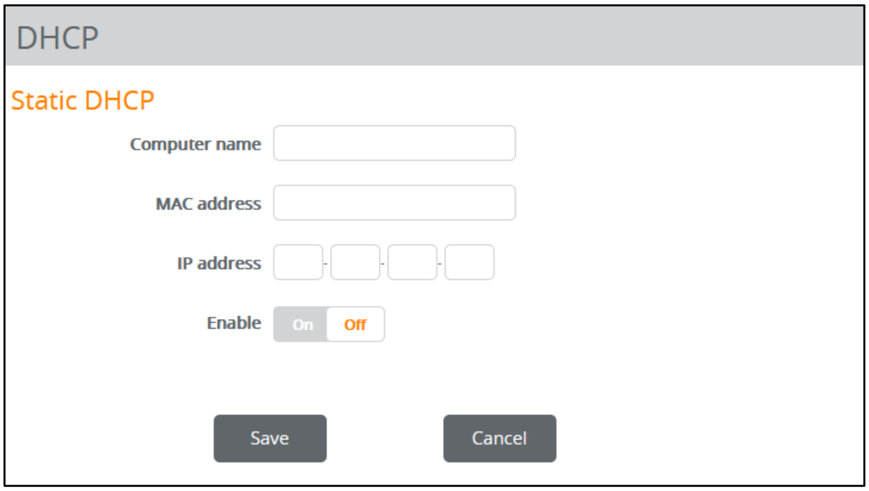


Figure 31 – Address reservation list – Add Static DHCP settings

2 In the **Computer Name** field enter a name for the device.

3 In the **MAC Address** field, enter the device's MAC address.

4 In the **IP Address** fields, enter the IP address that you wish to reserve for the device.

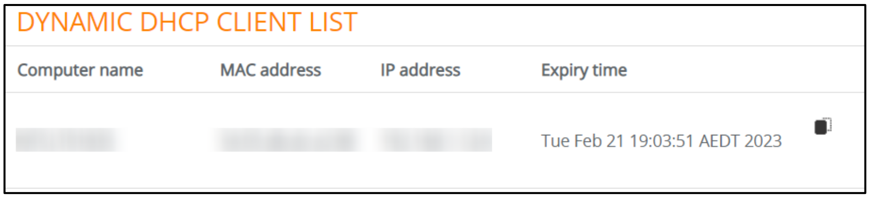
5 Set the **Enable** toggle to **On** to enable the setting.

6 Select the **Save** button to save the settings.

To delete a port forwarding rule, select the × button on the **ADDRESS RESERVATION LIST** for the corresponding rule that you would like to delete.

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** ⧉ button and the details will be copied to the address reservation list fields.



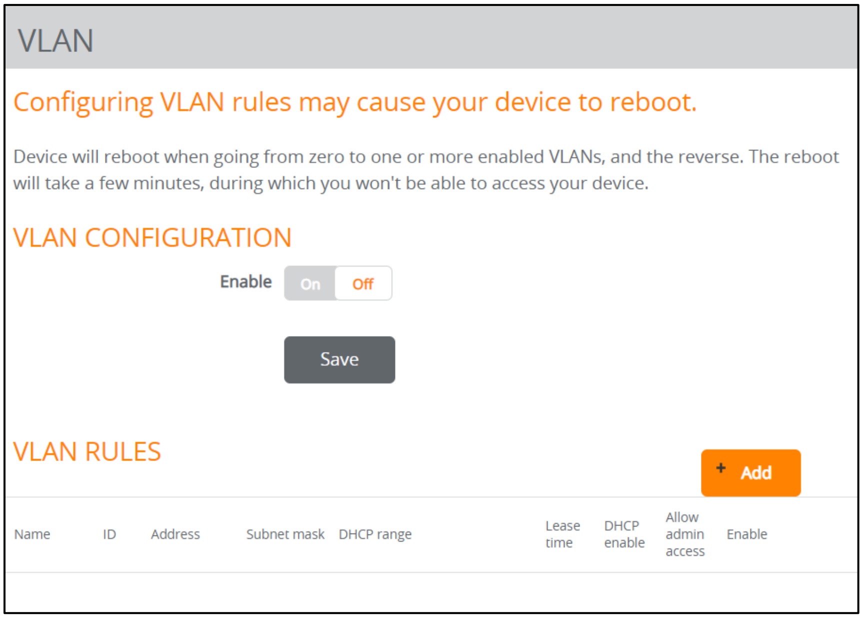
DYNAMIC DHCP CLIENT LIST

Computer name	MAC address	IP address	Expiry time	
[redacted]	[redacted]	[redacted]	Tue Feb 21 19:03:51 AEDT 2023	⧉

Figure 32 – Dynamic DHCP client 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.



VLAN

Configuring VLAN rules may cause your device to reboot.

Device will reboot when going from zero to one or more enabled VLANs, and the reverse. The reboot will take a few minutes, during which you won't be able to access your device.

VLAN CONFIGURATION

Enable: On [✓ Off]

VLAN RULES

Name	ID	Address	Subnet mask	DHCP range	Lease time	DHCP enable	Allow admin access	Enable

Figure 33 - VLAN

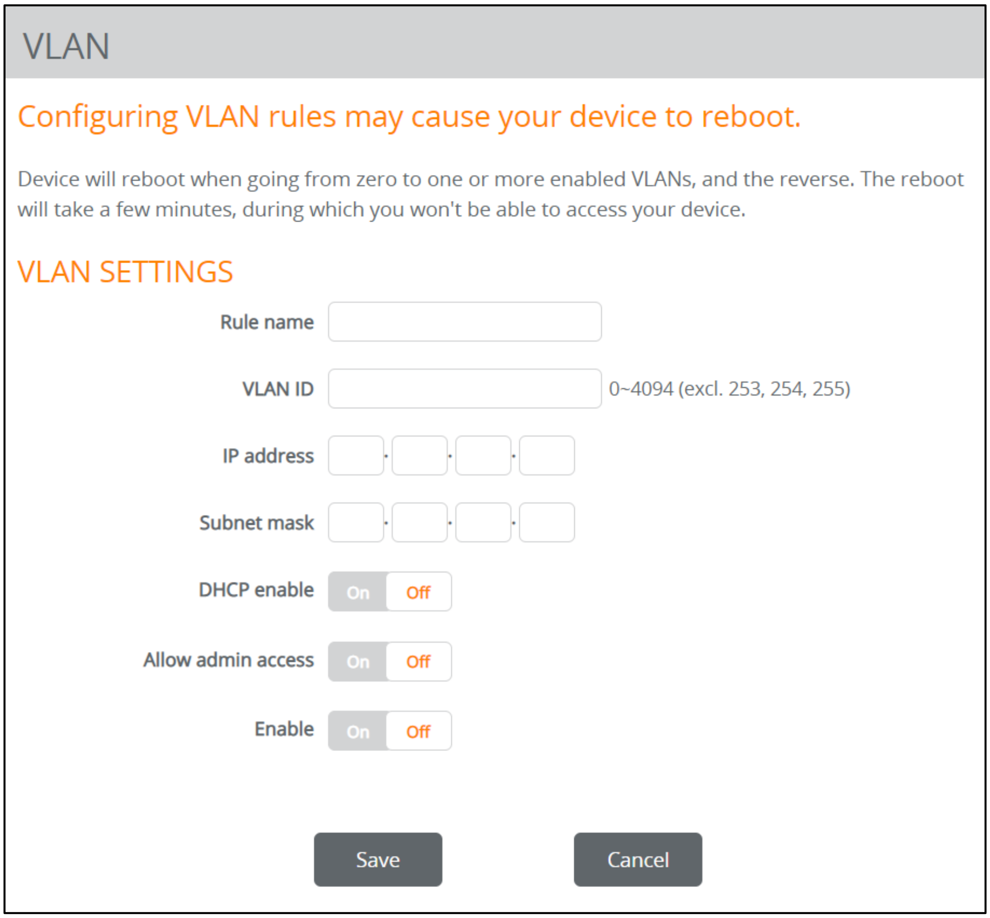
VLAN Settings

To create a VLAN:

1. Select on the **+Add** button on the VLAN Configuration page.
2. In the **Rule name** field, enter a name for the VLAN rule. This is a name that allows you to easily identify the VLAN.
3. In the **VLAN ID** field, enter a number between 0 and 4094 which will be used by the network to identify the VLAN uniquely.
4. In the **IP address** field, enter the IP address for this device on the VLAN.
5. In the **Subnet mask** field, enter the Subnet mask for the device on the VLAN.
6. To use DHCP, set the **DHCP 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.
7. 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.
8. To allow access to the administration web interface, set the **Allow admin access** toggle to the on position.

9 Set the **Enable** toggle to the **ON** position.

10 Select on the **Save** button to apply the settings.



VLAN

Configuring VLAN rules may cause your device to reboot.

Device will reboot when going from zero to one or more enabled VLANs, and the reverse. The reboot will take a few minutes, during which you won't be able to access your device.

VLAN SETTINGS

Rule name

VLAN ID 0~4094 (excl. 253, 254, 255)

IP address . . .

Subnet mask . . .

DHCP enable On Off

Allow admin access On Off

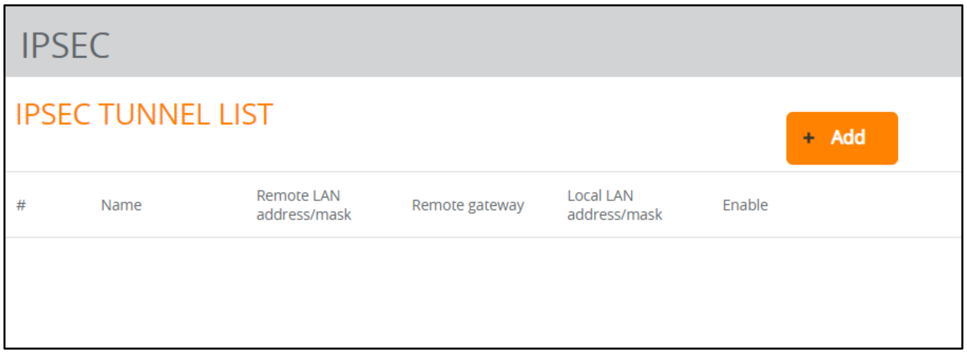
Enable On Off

Figure 34 – VLAN – VLAN rule configuration

VPN

IPSec

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



IPSEC

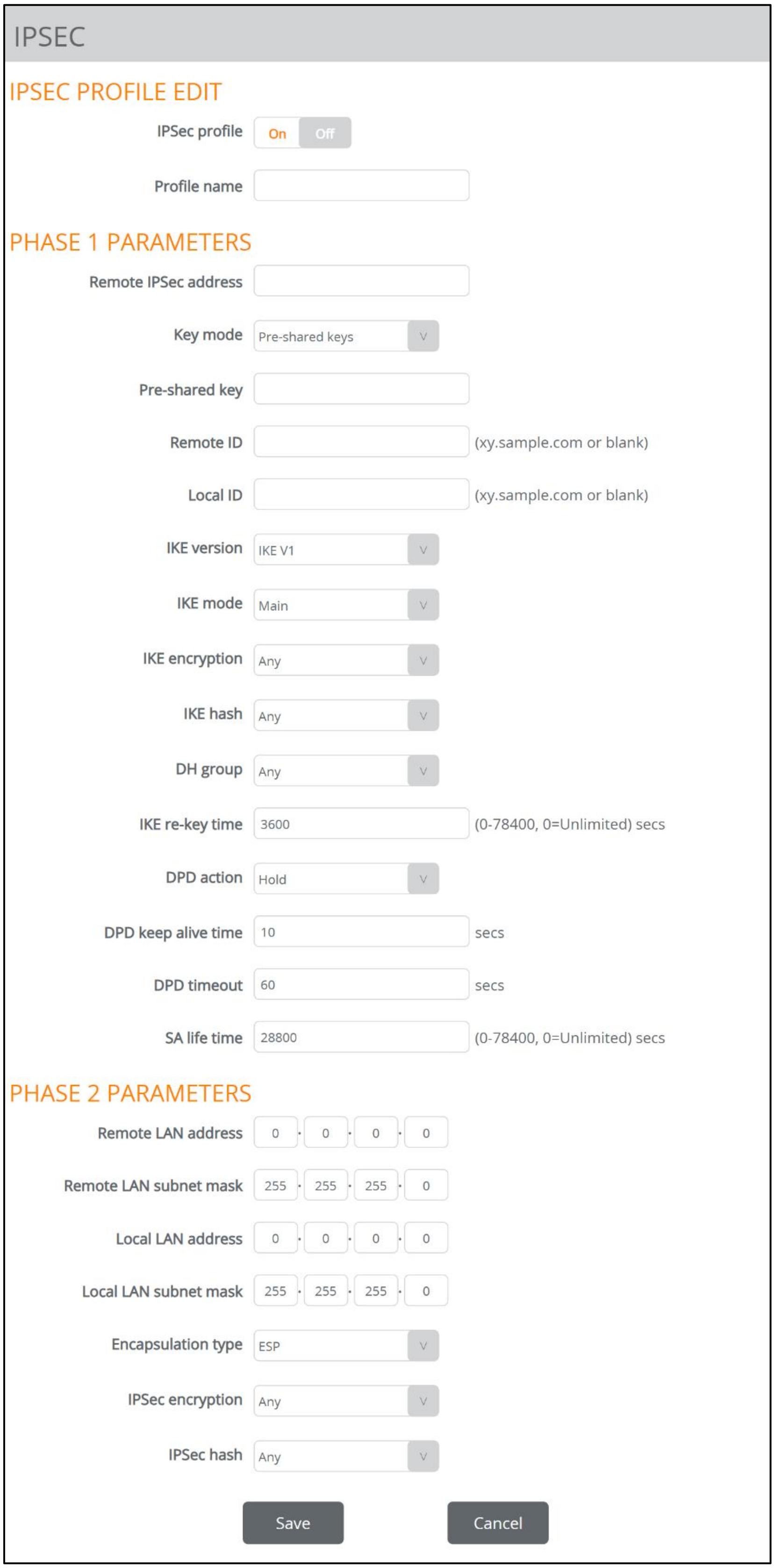
IPSEC TUNNEL LIST

#	Name	Remote LAN address/mask	Remote gateway	Local LAN address/mask	Enable

Figure 35 – VPN – IPSec

Configuring an IPSec VPN

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



IPSEC

IPSEC PROFILE EDIT

IPSec profile	On Off
Profile name	

PHASE 1 PARAMETERS

Remote IPSec address	
Key mode	Pre-shared keys
Pre-shared key	
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
IKE version	IKE V1
IKE mode	Main
IKE encryption	Any
IKE hash	Any
DH group	Any
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

PHASE 2 PARAMETERS

Remote LAN address	0 . 0 . 0 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	0 . 0 . 0 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	Any
IPSec hash	Any

Figure 36 – VPN – IPSec Profile Edit

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

Parameter	Description
IPSec profile	Enables or disables the VPN profile.
Profile name	A name used to identify the VPN connection profile.
Phase 1 parameters	
Remote IPSec address	The IP address or domain name of the IPSec server.
Key mode	Select the type of key mode in use for the VPN connection. You can select from: Pre Shared Key RSA keys Certificates SCEP client
Pre-shared key	The pre-shared key is the key that peers used to authenticate each other for Internet Key Exchange. The pre-shared key must meet the requirements for a strong password. See the Configuring a strong password section. This field appears if using **Pre-shared key** as the key mode.
Remote ID	Remote ID of the connection. Refer to the documentation of the remote IPSec server for further details. This field may be left blank.
Local ID	Local ID of the connection. Refer to the documentation of the remote IPSec server for further details. This field may be left blank.
Local RSA key upload	Upload the **Local RSA key** if using **RSA Keys** as the Key mode.
Remote RSA key upload	Upload the **Remote RSA key** if using **RSA Keys** as the Key mode
Private key passphrase	The Private key passphrase is required if using **Certificates** as the Key mode.
Key / Certificate	Select the **Key / Certificate** type for the IPSec connection if using **Certificates** as the Key mode.
IPSec certificate upload	Upload the **IPSec certificate** if using **Certificates** as the Key mode.
SCEP remote id	Enter the SCEP remote ID if using **SCEP client** as the Key mode.
IKE version	Set the IKE version for the connection. There are two options available **IKE V1** and **IKE V2.**
IKE mode	Set the IKE mode for the connection. There are three options **Any, Main** and **Aggressive.**
IKE encryption	Select the cipher type to use for the Internet Key Exchange.
IKE hash	Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.
DH group	Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.
IKE re-key time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.

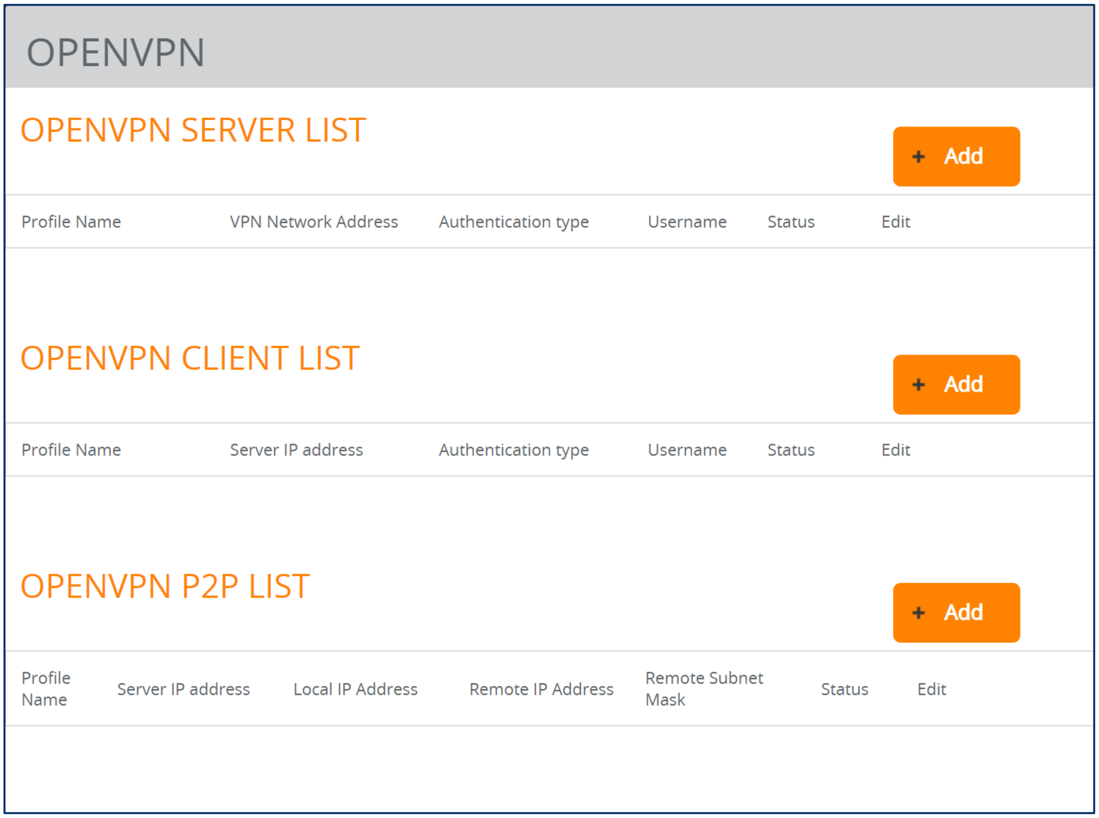
DPD action	Select the desired Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.
DPD keep alive time	Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.
DPD timeout	Enter the time in seconds of no response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

Table 9 – IPSec configuration items

OpenVPN

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

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



OPENVPN

OPENVPN SERVER LIST

Profile Name	VPN Network Address	Authentication type	Username	Status	Edit

OPENVPN CLIENT LIST

Profile Name	Server IP address	Authentication type	Username	Status	Edit

OPENVPN P2P LIST

Profile Name	Server IP address	Local IP Address	Remote IP Address	Remote Subnet Mask	Status	Edit

Figure 37 – VPN - OpenVPN

Configuring an OpenVPN Server

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

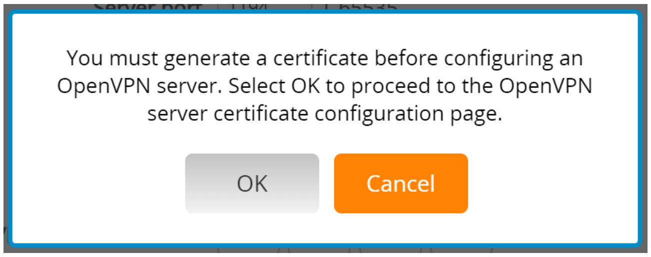

You must generate a certificate before configuring an OpenVPN server. Select OK to proceed to the OpenVPN server certificate configuration page.

Figure 38 – VPN – OpenVPN – Generate server certificate prompt

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.

To configure an OpenVPN server:

1 Select the **OpenVPN profile** toggle key to switch it to the **ON** position.

2 Type a name for the OpenVPN server profile you are creating.

3 In the **Type** drop-down list, select the **OpenVPN connection type** (**TUN**/**TAP**). Default is **TUN**.

4 Use the **Port type** field and **Server port** field to select a port number and use the drop-down list to select a packet type to use for your OpenVPN Server. The default OpenVPN port is 1194 and default packet type is UDP.

5 Use the **Encryption cipher** field to select the encryption type for the connection. The default is **AES-256** as this is the strongest encryption level.

6 Enter a maximum transmission unit value into the **MTU** field. The default is 1500.

7 In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.

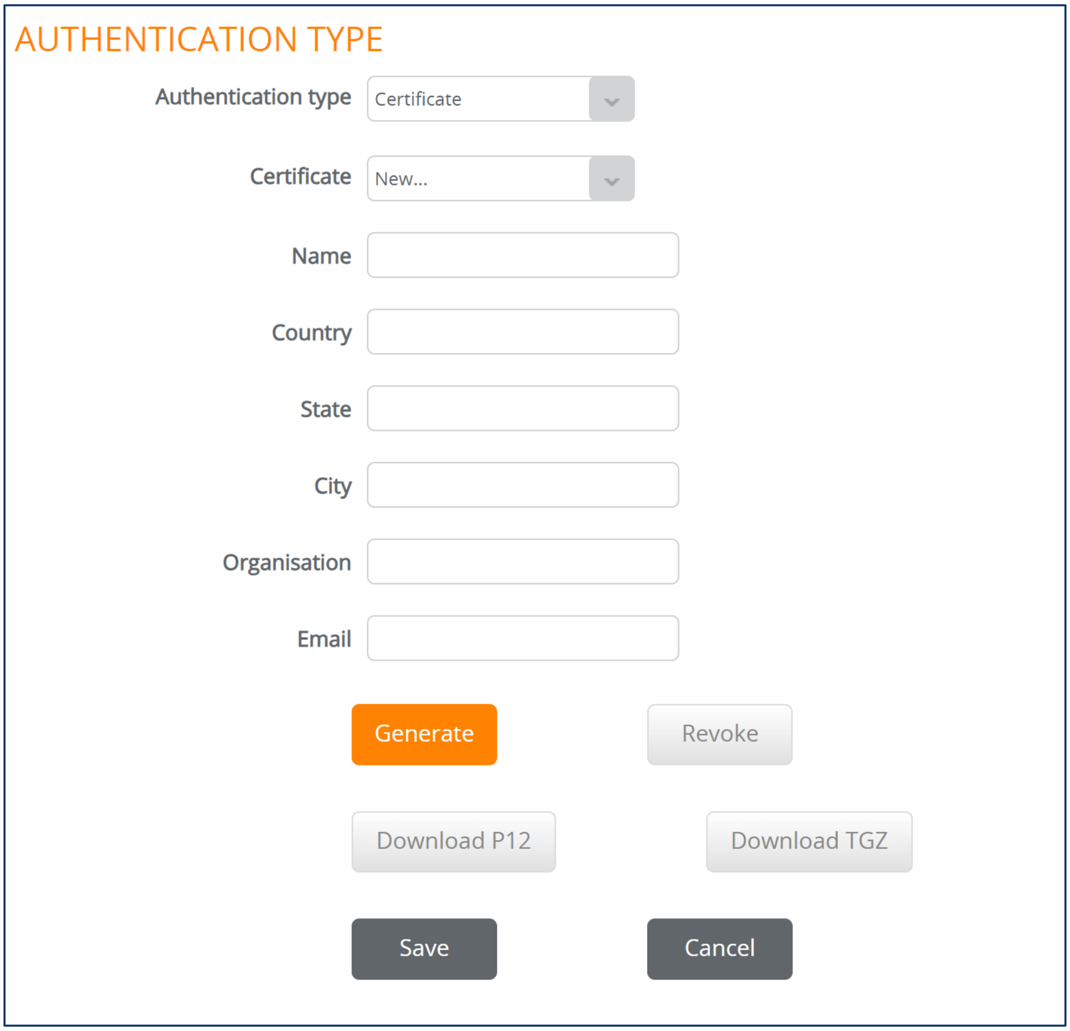
8 The Server certificates section displays the details of the certificate. If you wish to change the certificate, select the **Change** button.

9 HMAC or Hash-based Message Authentication Code is a means of 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, click the **Use HMAC Signature** toggle key so that it is in the **ON** position, then select 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. Select the **Download** button to download the key file so that it can be uploaded on the client.

10 Select an **Authentication type**. Authentication may be done using a Certificate or Username / Password. See the below sections for information on each of the certificate types.

Certificate authentication

In the Certificate Management section, enter the required details to create a client certificate. All fields are required. After filling out the required fields, select the Generate button.



AUTHENTICATION TYPE

Authentication type: Certificate

Certificate: New...

Name:

Country:

State:

City:

Organisation:

Email:

Figure 39 – VPN – OpenVPN – Certificate Authentication type

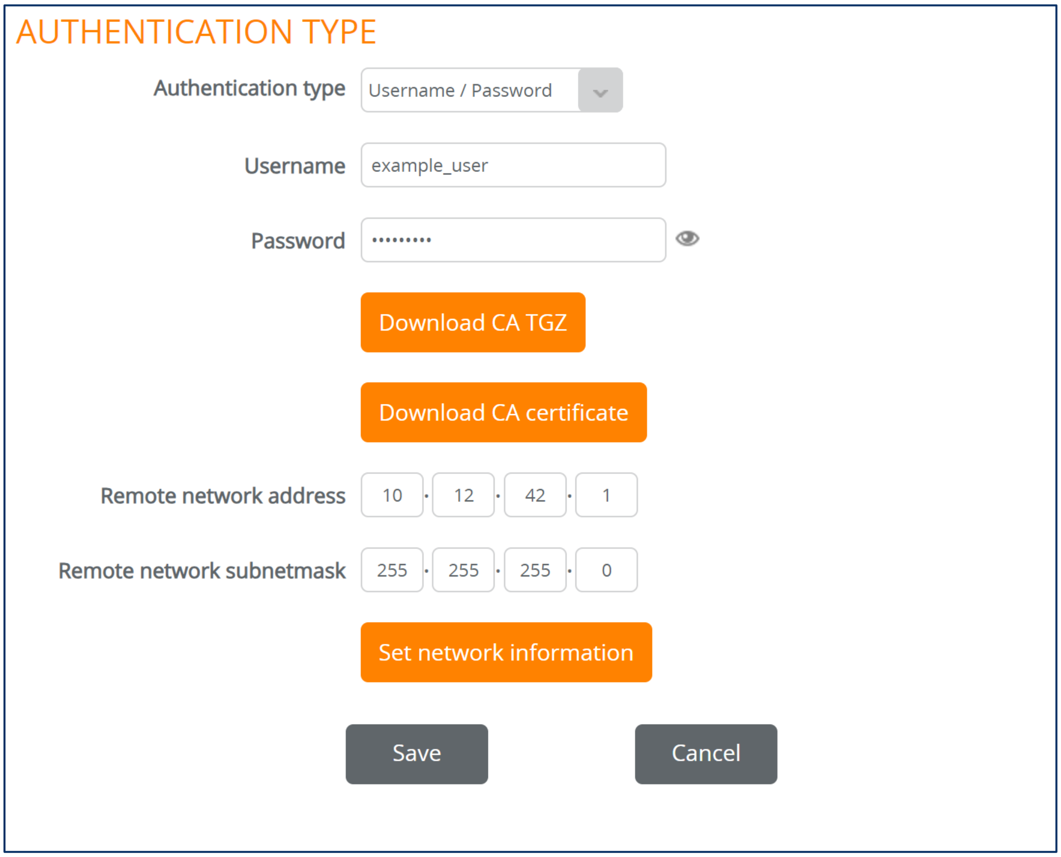
Once the certificate is generated, select the Download P12 button or the Download TGZ button to save the certificate file, depending on which format you would like. If for some reason the integrity of your network has been compromised, return to this screen, use the Certificate drop-down list to select the certificate and then select the Revoke button to make the certificate invalid.

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

Username / Password Authentication

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

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



AUTHENTICATION TYPE

Authentication type: Username / Password

Username: example_user

Password: •••••••••

Remote network address: 10 . 12 . 42 . 1

Remote network subnetmask: 255 . 255 . 255 . 0

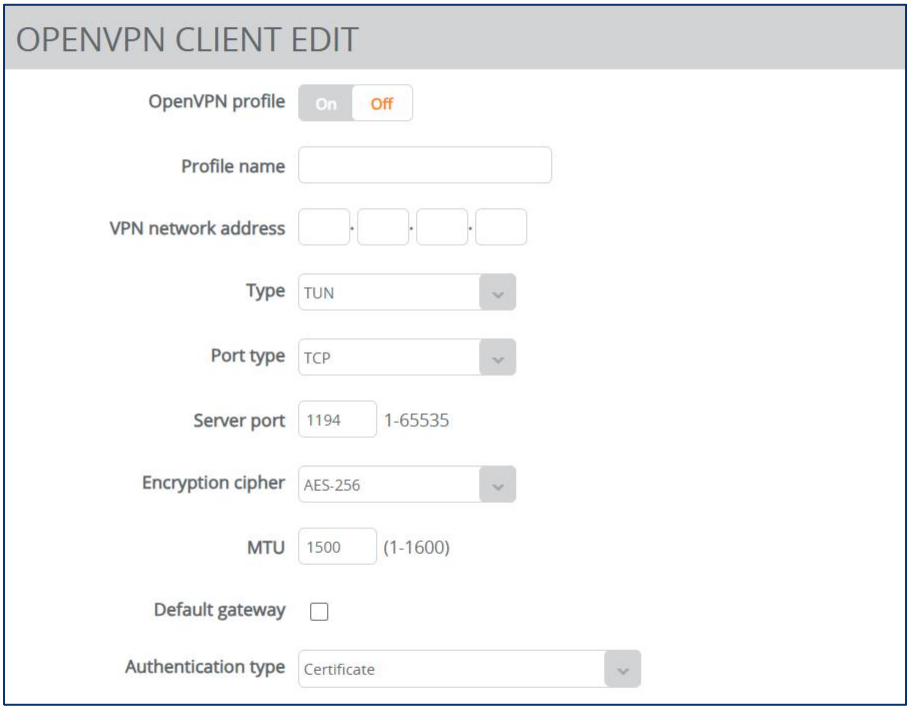
Figure 40 – VPN – OpenVPN – Username / Password Authentication type

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

When you have finished entering all the required information, select Save to finish configuring the OpenVPN server.

Configuring an OpenVPN client

1 From the OpenVPN page select the **Add** button to the right of **OpenVPN Client List.** The OpenVPN Client Edit page is shown.



OPENVPN CLIENT EDIT

OpenVPN profile	On Off
Profile name	
VPN network address	. . .
Type	TUN
Port type	TCP
Server port	1194 1-65535
Encryption cipher	AES-256
MTU	1500 (1-1600)
Default gateway	☐
Authentication type	Certificate

Figure 41 – VPN – OpenVPN – Configure OpenVPN client

2 Set the **OpenVPN profile** toggle key to the **On** position.

3 In the Profile name field, enter a name for the OpenVPN client profile you are creating.

4 In the Server IP address field, enter the WAN IP address / host domain name of the OpenVPN server.

5 Select OpenVPN connection type (TUN/TAP). Default is TUN.

6 Use the Server port field to select a port number and then use the drop-down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.

7 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.

8 Use the Authentication type options to select the Authentication type that you would like to use for the OpenVPN client. The available options are **Certificate, Username and Password,** or **Combination Certificate and Username / Password.** See the below sections to understand the different authentication types.

Certificate Authentication

To use Certificate Authentication, a certificate must be uploaded.

1 Set the **Authentication Type** field to **Certificate**.

2 Scroll down to the Select certificate to upload field and select the Choose a file button.

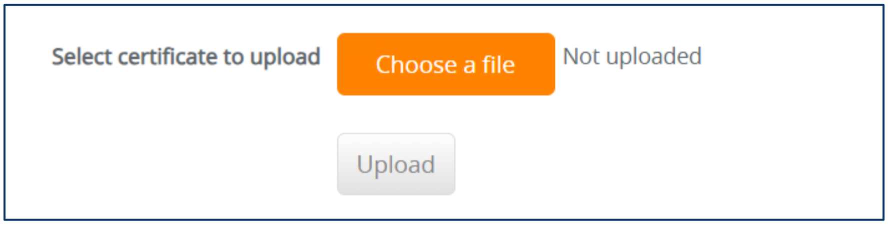


Figure 42 – OpenVPN – Certificate upload

3 Locate the certificate on your computer, select **Open,** then select **Upload**.

4 Once the certificate is uploaded, select the **Save** button to confirm the connection.

Username / Password Authentication

To use Username / Password Authentication, the credentials for the OpenVPN VPN server are required.

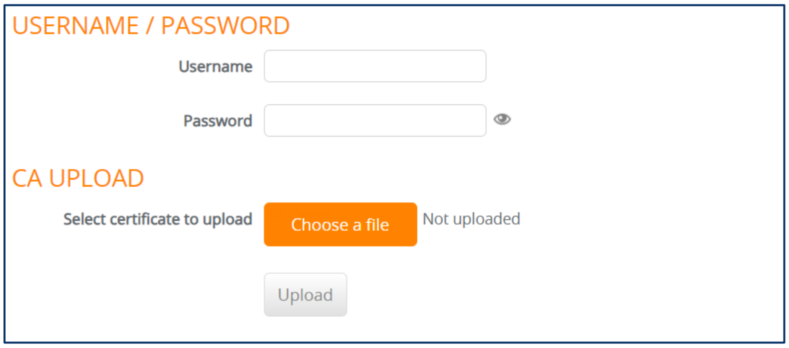


Figure 43 – OpenVPN – Username / Password Authentication

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

2 In the **Username** field, enter the username of the OpenVPN server.

3 In the **Password** field, enter the password of the OpenVPN server.

4 Use the **Choose a file button** to locate the CA certificate file you saved from the OpenVPN Server and then select the **Upload** button.

5 If you have an additional SSL/TLS key created on the server, click on the **Use HMAC Signature** toggle key so that it is in the **ON** position. Select the **Choose a file** button then locate the key file on your computer. Select the **Upload** button to upload it to the router.

6 Select the **Save** button to confirm the connection.

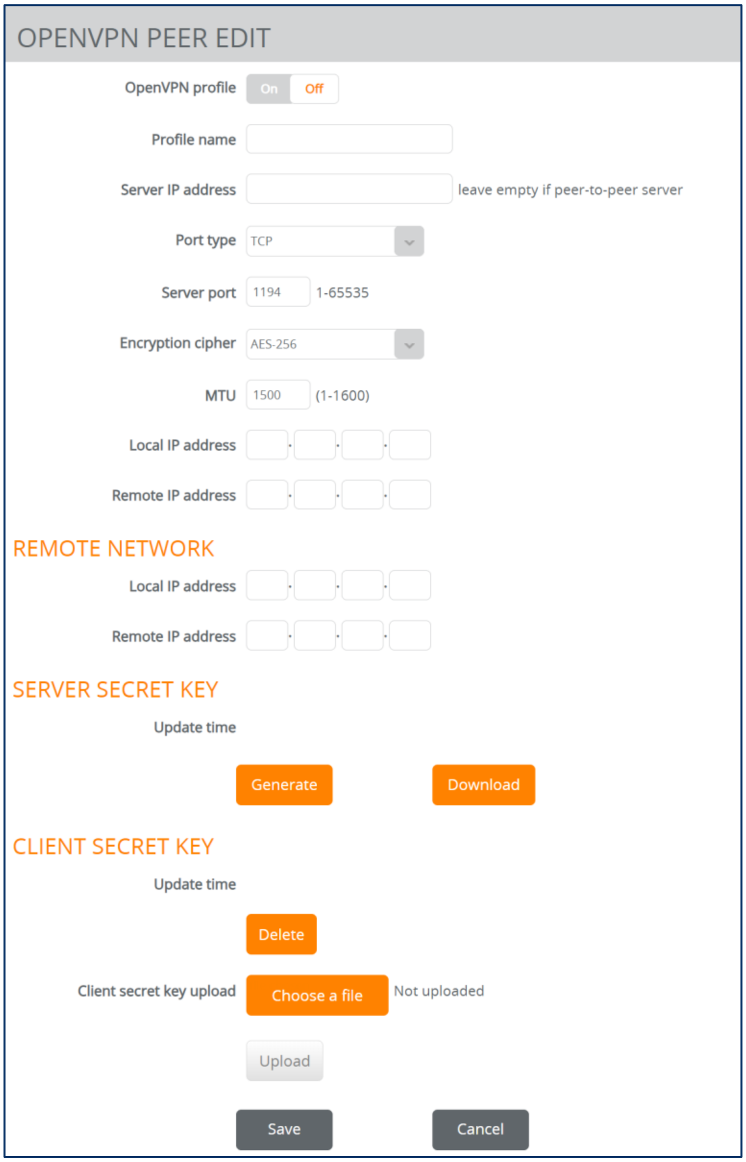
Certificate and Username / Password authentication

The Certificate and Username / Password Authentication options 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 both of the above sections to complete the configuration.

Configuring an OpenVPN P2P Connection

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

1 From the OpenVPN page select the Add button to the right of OpenVPN P2P List. The OpenVPN Peer Edit page is shown.



OPENVPN PEER EDIT

OpenVPN profile: On | Off

Profile name:

Server IP address: leave empty if peer-to-peer server

Port type: TCP

Server port: 1194 1-65535

Encryption cipher: AES-256

MTU: 1500 (1-1600)

Local IP address: . . .

Remote IP address: . . .

REMOTE NETWORK

Local IP address: . . .

Remote IP address: . . .

SERVER SECRET KEY

Update time

CLIENT SECRET KEY

Update time

Client secret key upload: Not uploaded

Figure 44 – OpenVPN – P2P Peer Edit Page

2 Set the **OpenVPN profile** toggle key to switch it to the **ON** position.

3 In the **Profile** name field, type a name for the OpenVPN P2P profile you are creating.

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

5 Use the **Port type** and **Server port** fields to select a port number and then use the drop-down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.

6 In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The secondary router should have the reverse settings of the primary router.

7 Under the **Remote network** section, In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The secondary router should have the reverse settings of the primary router.

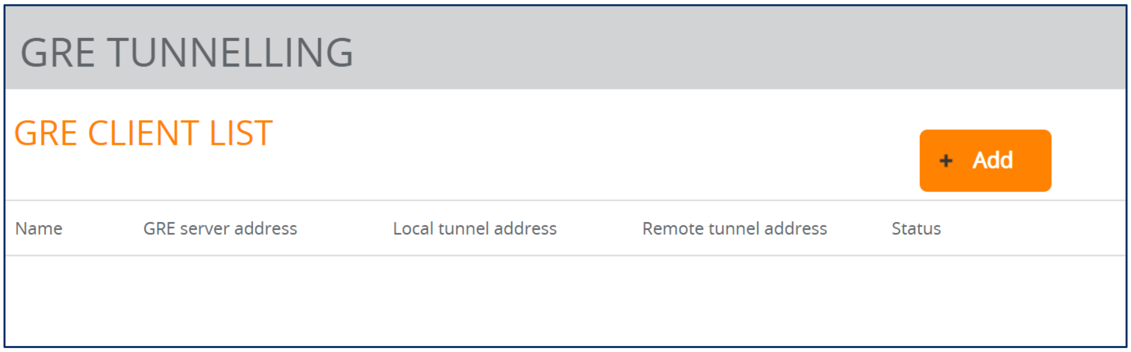
8 Press the **Generate** button to create a secret key to be shared with the other router. When the timestamp appears, you can click the **Download** button to save the file to exchange with the other router.

9 When you have saved the secret key file on each router, use the **Choose a file button** to locate the secret key file for the master and then select the Upload button to send it to the secondary router. Perform the same for the other router, uploading the secondary secret key file to the primary router.

10 Select the **Save** button to confirm the peer-to-peer VPN connection.

GRE Tunnelling

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



GRE TUNNELLING

GRE CLIENT LIST

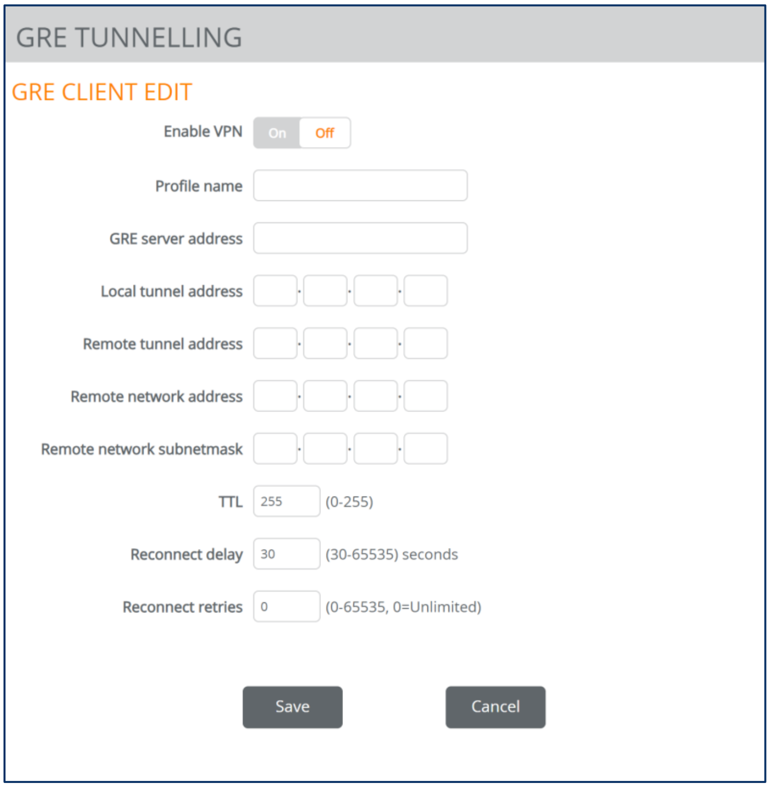
Name	GRE server address	Local tunnel address	Remote tunnel address	Status

Figure 45 – VPN – GRE Tunnelling

Configuring GRE tunnelling

To configure GRE tunnelling:

1 To the right of the GRE client list, select the **Add** button. The **GRE client edit** screen is displayed.



GRE TUNNELLING

GRE CLIENT EDIT

Enable VPN	On Off
Profile name	
GRE server address	
Local tunnel address	. . .
Remote tunnel address	. . .
Remote network address	. . .
Remote network subnetmask	. . .
TTL	255 (0-255)
Reconnect delay	30 (30-65535) seconds
Reconnect retries	0 (0-65535, 0=Unlimited)

Figure 46 – VPN – GRE Tunnelling – GRE Client Edit

2 Set the Enable VPN toggle to On.

3 In the Profile name field, enter a profile name for the tunnel. This name is used to identify the tunnel on the router.

4 In the GRE server address field, enter the IP address or domain name of the GRE server.

5 In the Local tunnel address field, enter the IP address you want to assign the tunnel locally.

6 In the Remote tunnel address field, enter the IP address you want to assign to the remote tunnel.

7 In the Remote network address field, enter the IP address scheme of the remote network.

8 In the Remote network subnetmask field, enter the subnet mask of the remote network.

9 The TTL (Time To Live) field is an 8-bit field used to remove an undeliverable data packet from a network to avoid unnecessary network traffic across the internet. The default value of 255 is the upper limit on the time that an IP datagram can exist. The value is reduced by at least one for each hop the data packet takes to the next router on the route to the datagram's destination. If the TTL field reaches zero before the datagram arrives at its destination the data packet is discarded and an error message is sent back to the sender.

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.

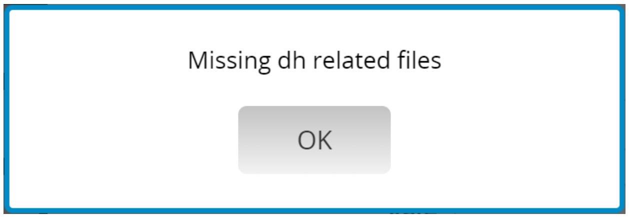
12 Select the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Select the Status button at the top left of the interface to return to the status window and monitor the VPN's connection state.

Server Certificate

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

Generating Diffie-Helman files

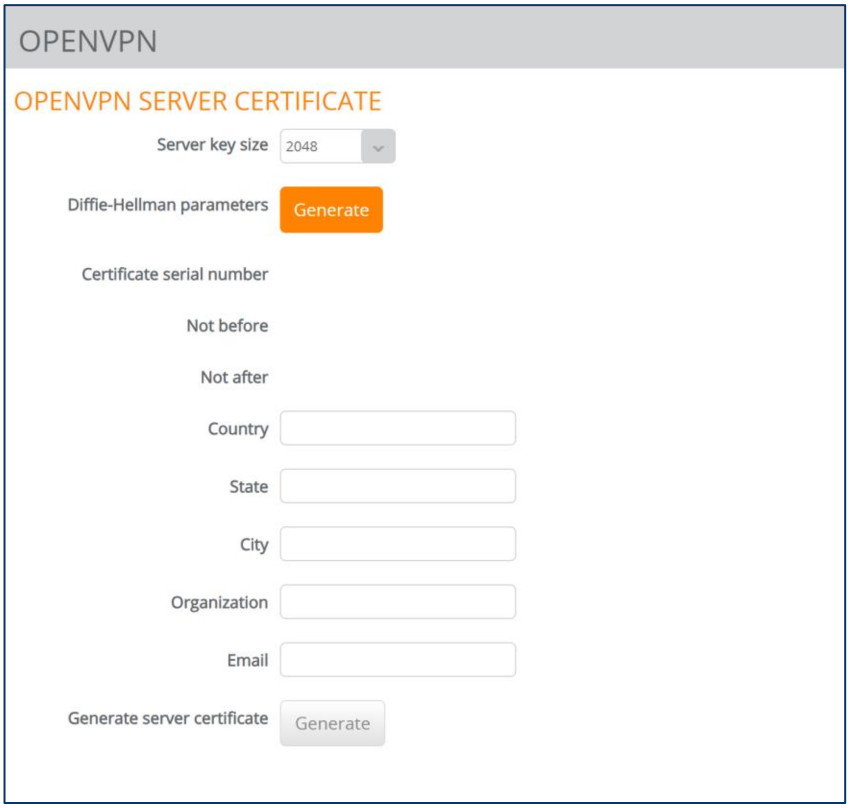
On first use of the certificate page, you will see the following prompt, where dh refers to Diffie-Hellman.



Missing dh related files

Figure 47 – VPN – Server Certificate – Missing dh related files

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



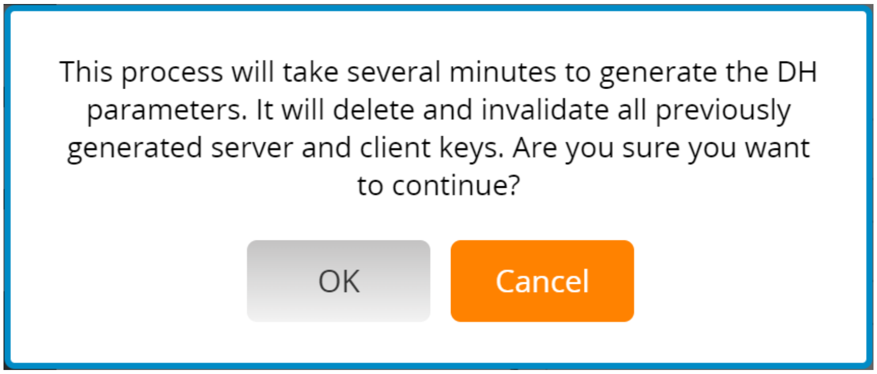
OPENVPN

OPENVPN SERVER CERTIFICATE

Server key size	2048
Diffie-Hellman parameters	Generate
Certificate serial number	
Not before	
Not after	
Country	
State	
City	
Organization	
Email	
Generate server certificate	Generate

Figure 48 – VPN – Server Certificate – Missing dh related files

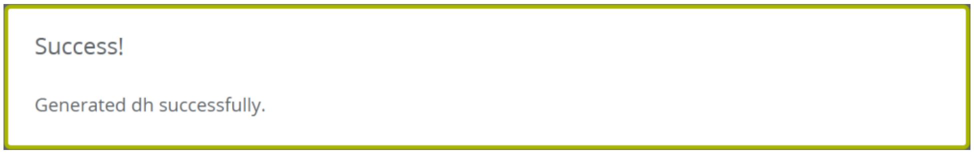
To the left of Diffie-Hellman Parameters, select Generate. The following prompt is shown.



This process will take several minutes to generate the DH parameters. It will delete and invalidate all previously generated server and client keys. Are you sure you want to continue?

Figure 49 – VPN – Server Certificate – Generate Diffie-Hellman prompt

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



Success!

Generated dh successfully.

Figure 50 – VPN – Server Certificate – Missing dh related files

The Server Certificate can now be generated.

Generating the OpenVPN Server Certificate

To generate an OpenVPN Server Certificate:

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

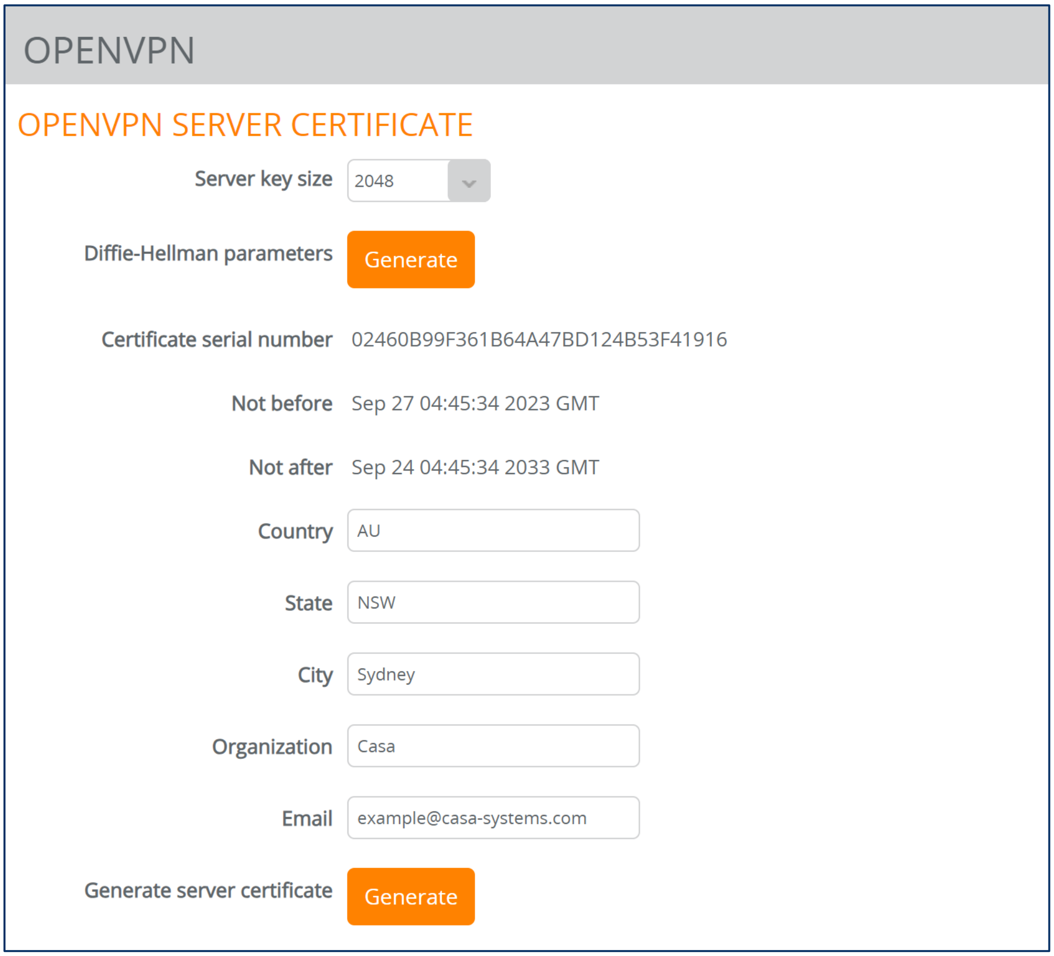
2 In the **State** field, enter the state the certificate is issued for.

3 In the **City** field, enter the city the certificate is issued for.

4 In the **Organization** field, enter the name of the organization for the certificate.

5 In the **Email** field, enter a contact email for the certificate.

6 To the right of **Generate Server Certificate** select **Generate** to generate the certificate. A success prompt is shown, and the certificate serial number and validity dates are shown in **Certificate serial number**, **Not before** and **Not after fields**.



OPENVPN

OPENVPN SERVER CERTIFICATE

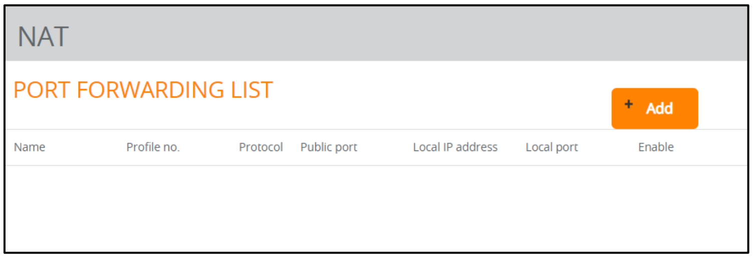
Server key size	2048
Diffie-Hellman parameters	Generate
Certificate serial number	02460B99F361B64A47BD124B53F41916
Not before	Sep 27 04:45:34 2023 GMT
Not after	Sep 24 04:45:34 2033 GMT
Country	AU
State	NSW
City	Sydney
Organization	Casa
Email	example@casa-systems.com
Generate server certificate	Generate

Figure 51 – VPN – Server Certificate – Generate certificate

Firewall

NAT

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the NTC-500. To access the Port forwarding page, select on the **Networking** menu at the top of the screen, select on the **Firewall** menu on the left.



Name	Profile no.	Protocol	Public port	Local IP address	Local port	Enable

Figure 52 - NAT

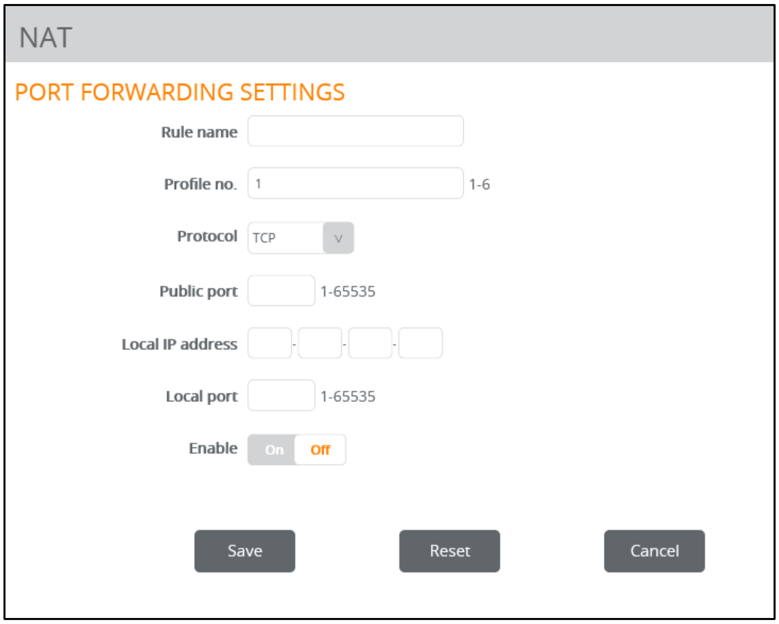
The purpose of the port forwarding feature is to allow mapping of inbound requests to a specific port on the WAN IP address to any connected device.

Note – Some carriers block inbound connections or require a public IP address in order to get inbound requests.

Adding a port forwarding rule

To create a new port forwarding rule:

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



Rule name
Profile no. 1 1-6
Protocol TCP
Public port 1-65535
Local IP address . . .
Local port 1-65535
Enable On Off

Figure 53 - IPv4 Port Forwarding Settings

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

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.

MAC whitelist

The MAC whitelist feature allows you to restrict devices that are allowed to connect to the NTC-500 by their MAC address.

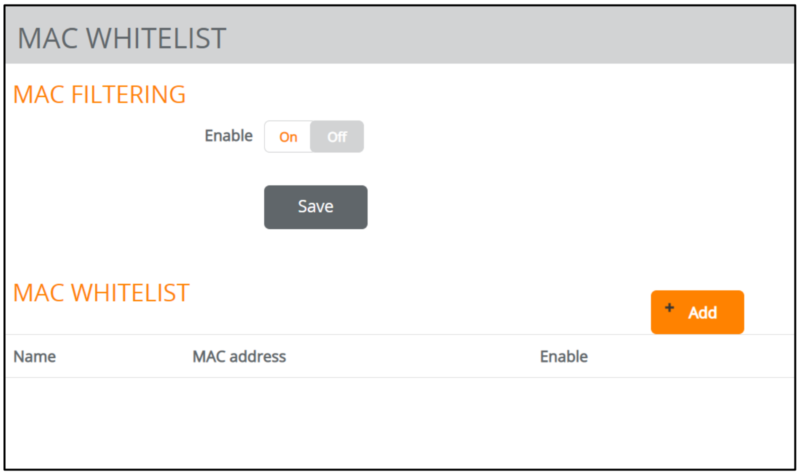


Figure 54 – MAC filtering

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

Adding and removing devices from the whitelist

1. To add a device to the whitelist first press the **+Add** button. The **MAC whitelist settings** page appears.

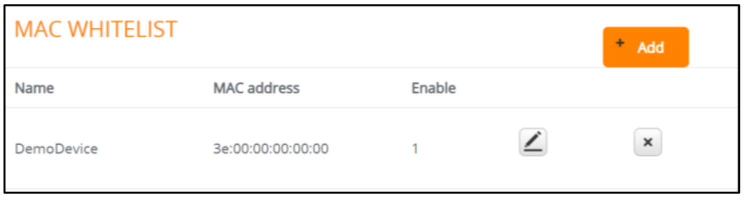
2 In the **Name** field, enter a name to identify the device.

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.



MAC WHITELIST

Name	MAC address	Enable		
DemoDevice	3e:00:00:00:00:00	1	✎	✖

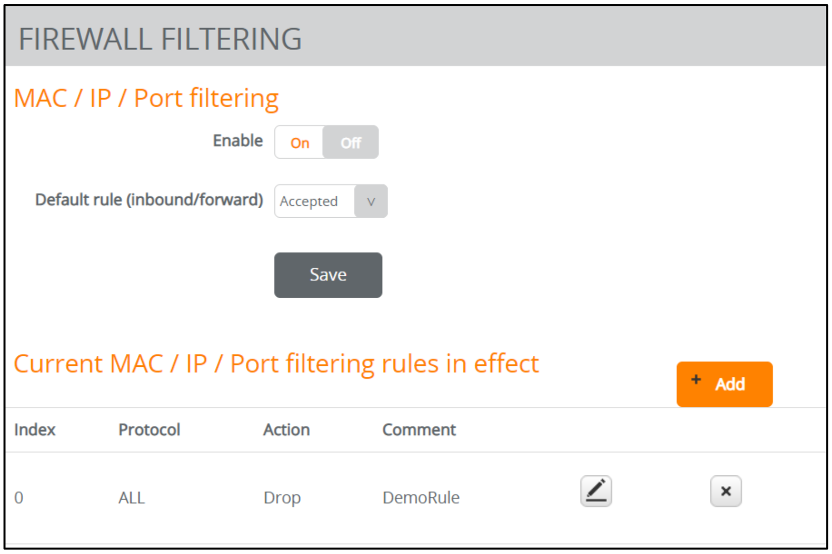
Figure 55 – MAC - MAC filtering whitelist settings

To remove the device, select the ✖ button to the right of the entry. To edit the device, including to temporarily disable it, select the ✎ button.

Firewall filtering

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

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



FIREWALL FILTERING

MAC / IP / Port filtering

Enable: [✓ On] Off

Default rule (inbound/forward): Accepted

Current MAC / IP / Port filtering rules in effect

Index	Protocol	Action	Comment		
0	ALL	Drop	DemoRule	✎	✖

Figure 56 – Firewall Filtering

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

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

1 Select the **MAC / IP / Port** filtering toggle key to switch it to the ON position.

2 Using the **Default rule (inbound/forward)** drop-down list, select the default action for the router to take when traffic reaches it. By default, this is configured to Accepted. If you change this to Dropped, you should first configure a filter rule that allows at least one device access to the router, otherwise you will effectively be locked out of the router.

3 Select the **Save** button to confirm the default rule.

4 In the Current MAC / IP / Port filtering rules in the effect section, select the **+Add** button.

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

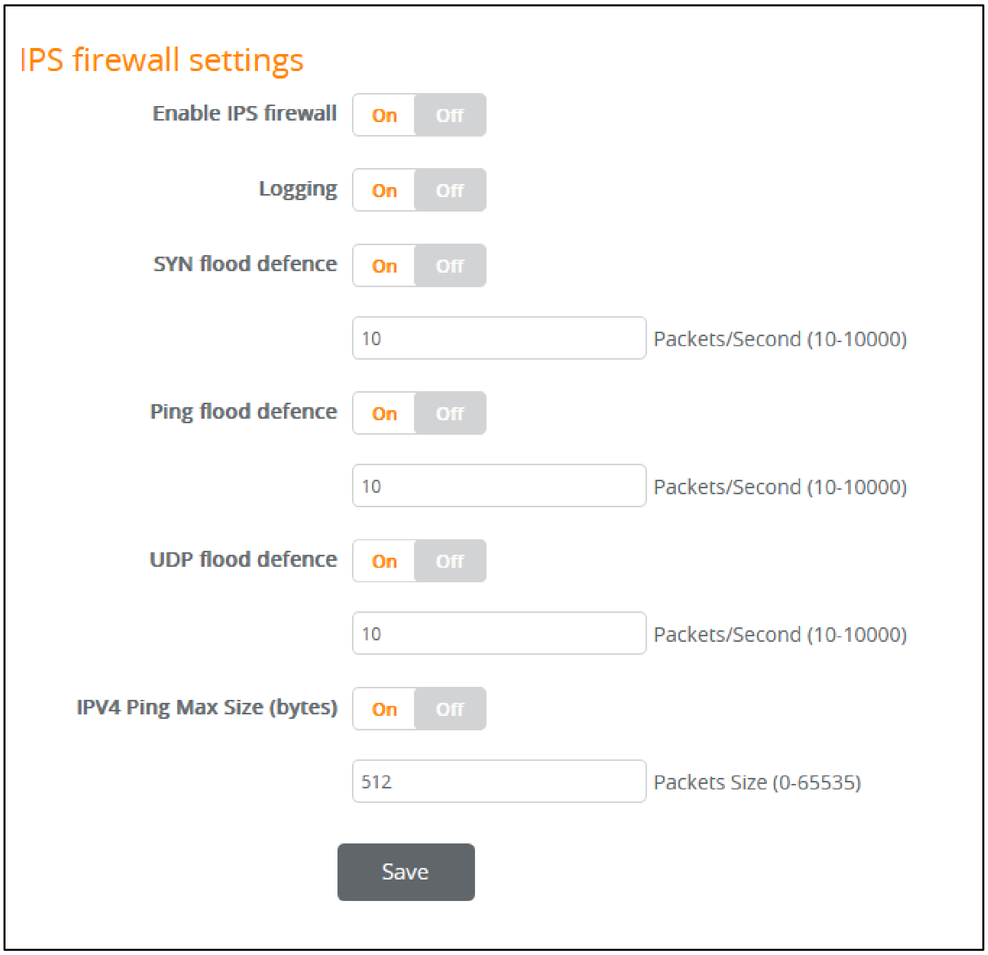
6 The new rule is displayed in the filtering rules list. You can edit the rule by selecting the ✎ Edit button or delete the rule by selecting the × button.

IPS

Intrusion Prevention Systems (IPS) work 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 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.



IPS firewall settings

Enable IPS firewall [✓ On] Off

Logging [✓ On] Off

SYN flood defence [✓ On] Off

10 Packets/Second (10-10000)

Ping flood defence [✓ On] Off

10 Packets/Second (10-10000)

UDP flood defence [✓ On] Off

10 Packets/Second (10-10000)

IPV4 Ping Max Size (bytes) [✓ On] Off

512 Packets Size (0-65535)

Figure 57 – IPS router firewall

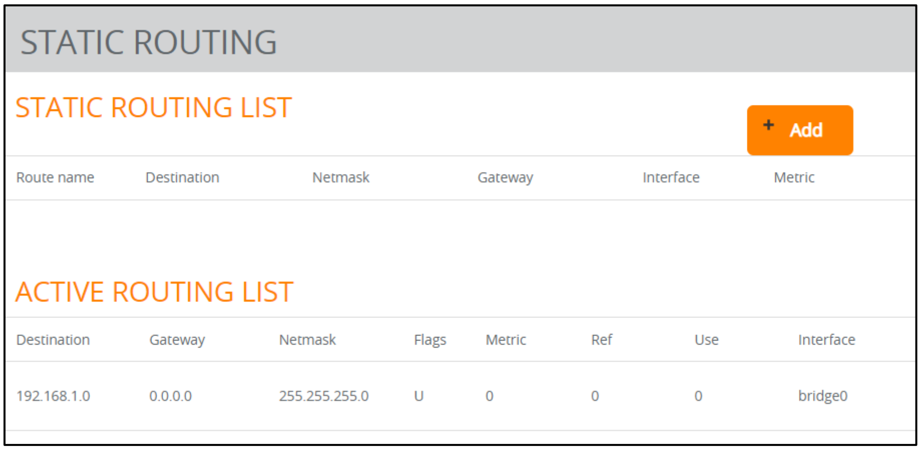
To enable the IPS, set the Enable router firewall toggle to On and then select the Save button.

Routing

Static

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

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



STATIC ROUTING

STATIC ROUTING LIST

Route name	Destination	Netmask	Gateway	Interface	Metric

ACTIVE ROUTING LIST

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	bridge0

Figure 58 – Static routing

Adding Static Routes

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

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

2 From the **Network interface** drop-down list, select the interface for which you would like to create a static route.

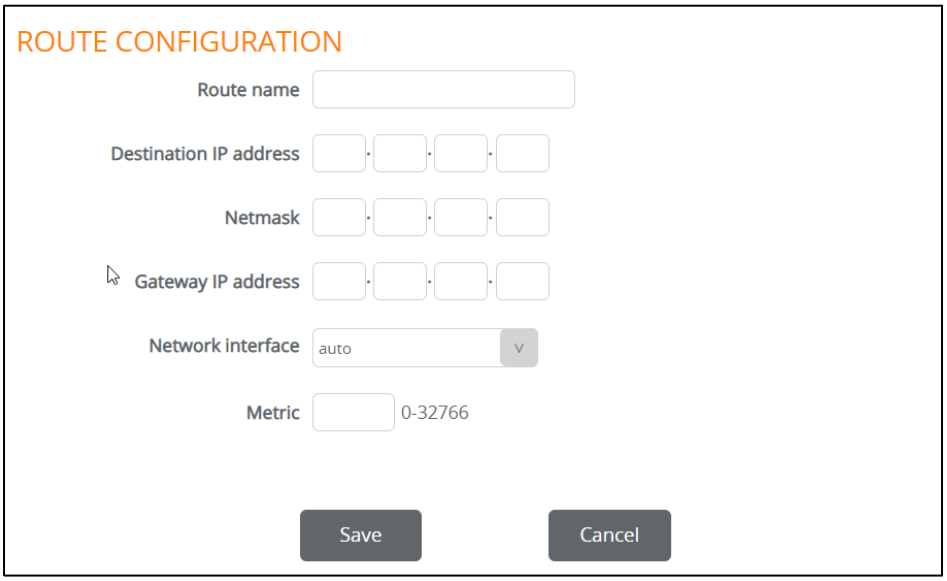
3 In the **Destination IP address** field, enter the IP address of the destination of the route.

4 In the **Destination 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 In the **Metric field** enter the metric for the route. The metric value is used by the router to prioritise routes. The lower the value, the higher the priority. To give the route the highest priority, set it to 0.

7 Select the **Save** button to save your settings.



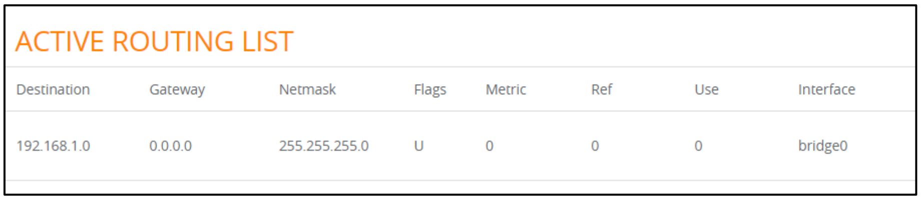
ROUTE CONFIGURATION

Route name	
Destination IP address	. . .
Netmask	. . .
Gateway IP address	. . .
Network interface	auto
Metric	0-32766

Figure 59 – Static routing – Route configuration

Active Routing List

Static routes are displayed in the Active routing list.



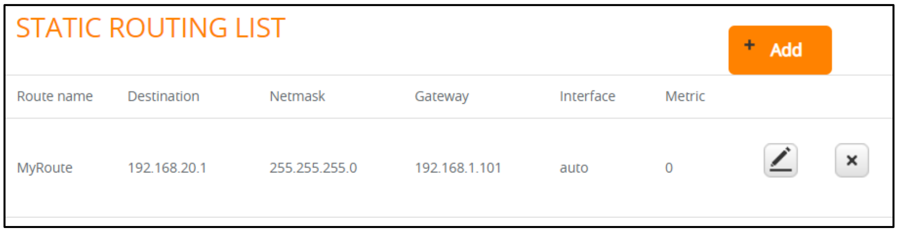
ACTIVE ROUTING LIST

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	bridge0

Figure 60 – Static routing – Active routing list

Static Routing List

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



STATIC ROUTING LIST

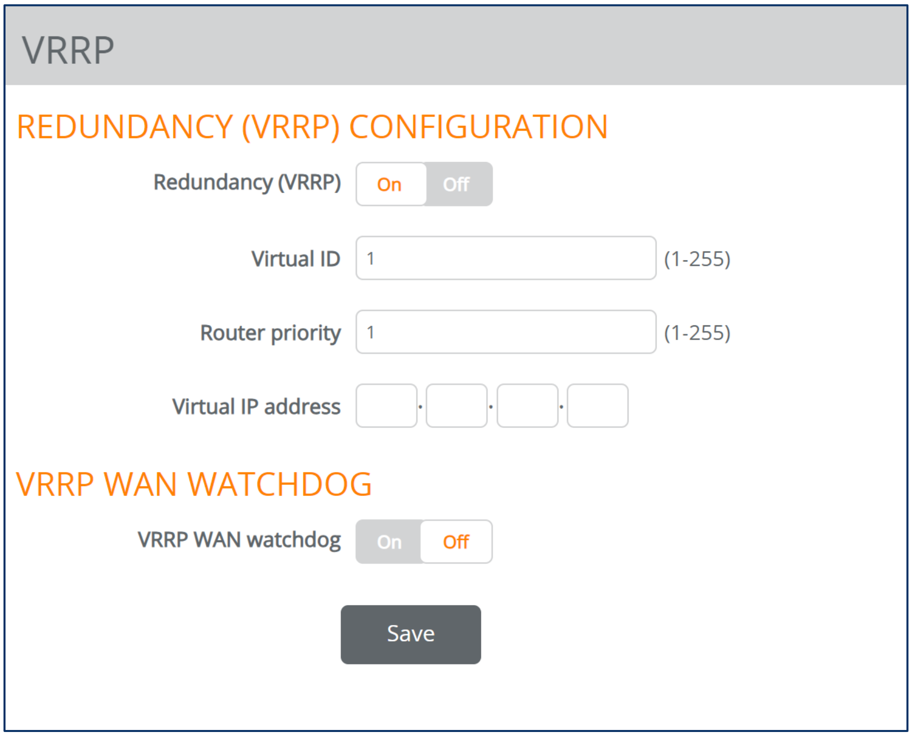
Route name	Destination	Netmask	Gateway	Interface	Metric		
MyRoute	192.168.20.1	255.255.255.0	192.168.1.101	auto	0	✎	×

Figure 61 – Static routing – Static routing list

Redundancy

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.



VRRP

REDUNDANCY (VRRP) CONFIGURATION

Redundancy (VRRP): On

Virtual ID: 1 (1-255)

Router priority: 1 (1-255)

Virtual IP address: . . .

VRRP WAN WATCHDOG

VRRP WAN watchdog: Off

Figure 62 – Redundancy

Configuring VRRP

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

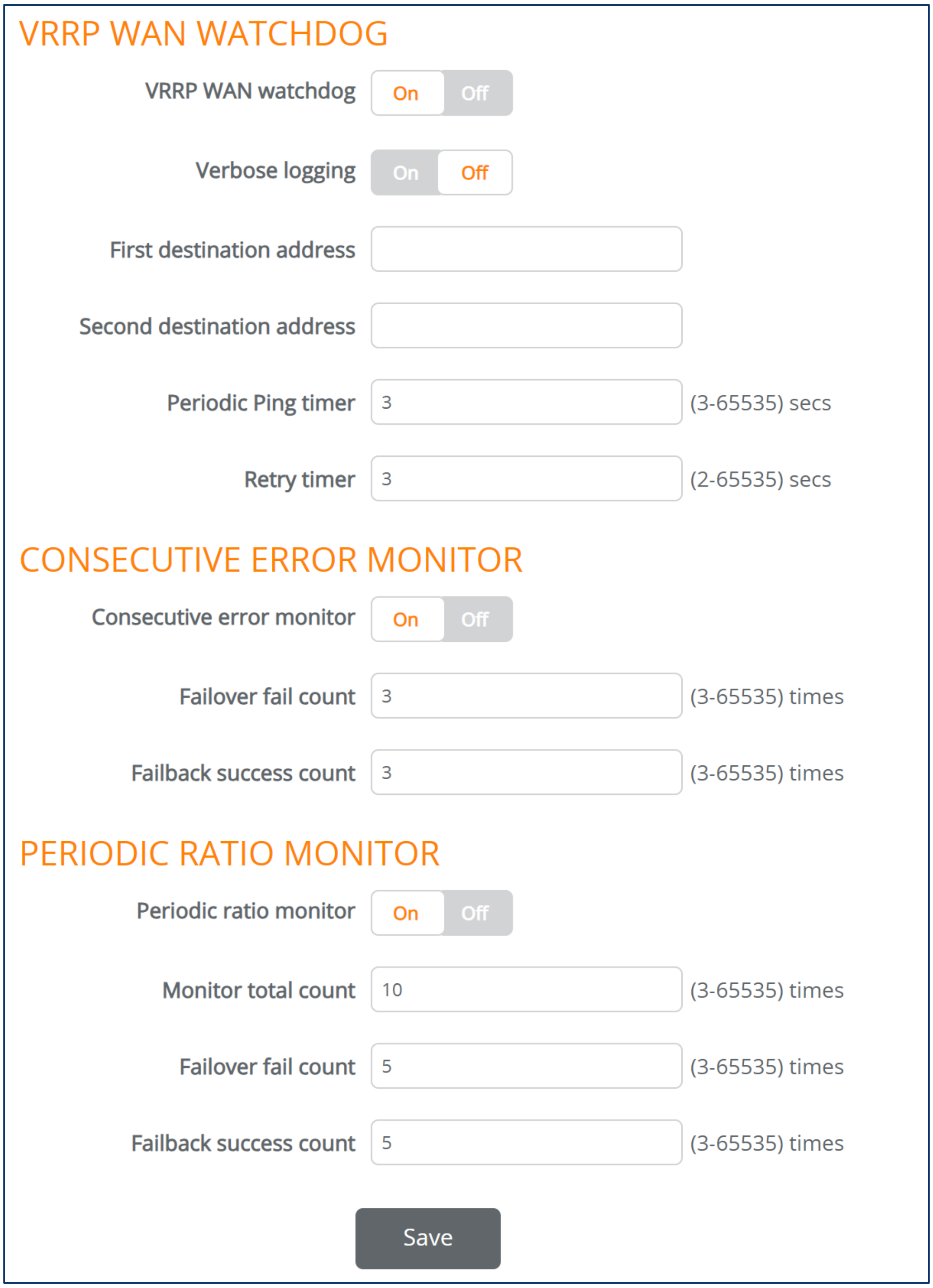
1. Set the **Redundancy (VRRP)** toggle to **On** to enable VRRP.
2. In the **Virtual ID** field, enter an ID between 1 and 255. This is the VRRP ID which is different for each virtual router on the network.
3. In the **Router priority** field, enter a value for the priority – a higher value is a higher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



VRRP WAN WATCHDOG

VRRP WAN watchdog	[✓ On] Off	
Verbose logging	On [✓ Off]	
First destination address		
Second destination address		
Periodic Ping timer	3	(3-65535) secs
Retry timer	3	(2-65535) secs

CONSECUTIVE ERROR MONITOR

Consecutive error monitor	[✓ On] Off	
Failover fail count	3	(3-65535) times
Failback success count	3	(3-65535) times

PERIODIC RATIO MONITOR

Periodic ratio monitor	[✓ On] Off	
Monitor total count	10	(3-65535) times
Failover fail count	5	(3-65535) times
Failback success count	5	(3-65535) times

Figure 63 – Redundancy – VRRP WAN Watchdog

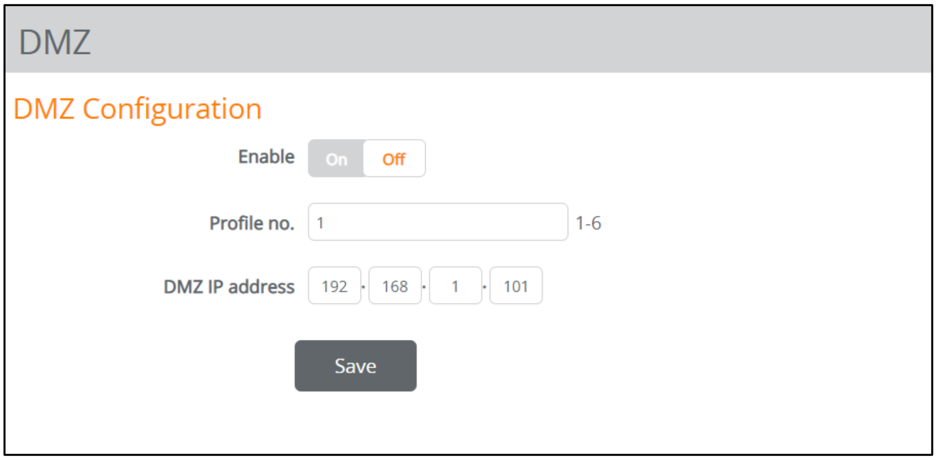
The following table details each field on the VRRP WAN Watchdog page.

Parameter	Description
VRRP WAN Watchdog	Set the VRRP WAN Watchdog to On to enable the watchdog.
Verbose logging	When enabled verbose comments are logged in the system log related to the failover monitoring.
First destination address	The first address the router that the router should ping in order to confirm the connection is up. This may be an IP address or a domain name.
Second destination address	The second address the router that the router should ping in order to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	The time in seconds between ping attempts.
Retry timer	The time in seconds between attempts when a ping failure occurs.
Consecutive error monitor	
Consecutive Error Monitor	Set the Consecutive Error Monitor toggle 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 the Periodic ratio monitor toggle 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.
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.

DMZ

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

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



DMZ

DMZ Configuration

Enable: On [✓ Off]

Profile no.: 1 (1-6)

DMZ IP address: 192 . 168 . 1 . 101

Figure 64 – DMZ configuration

Enabling the DMZ

1 Select the **DMZ** toggle key to turn the DMZ function **ON**.

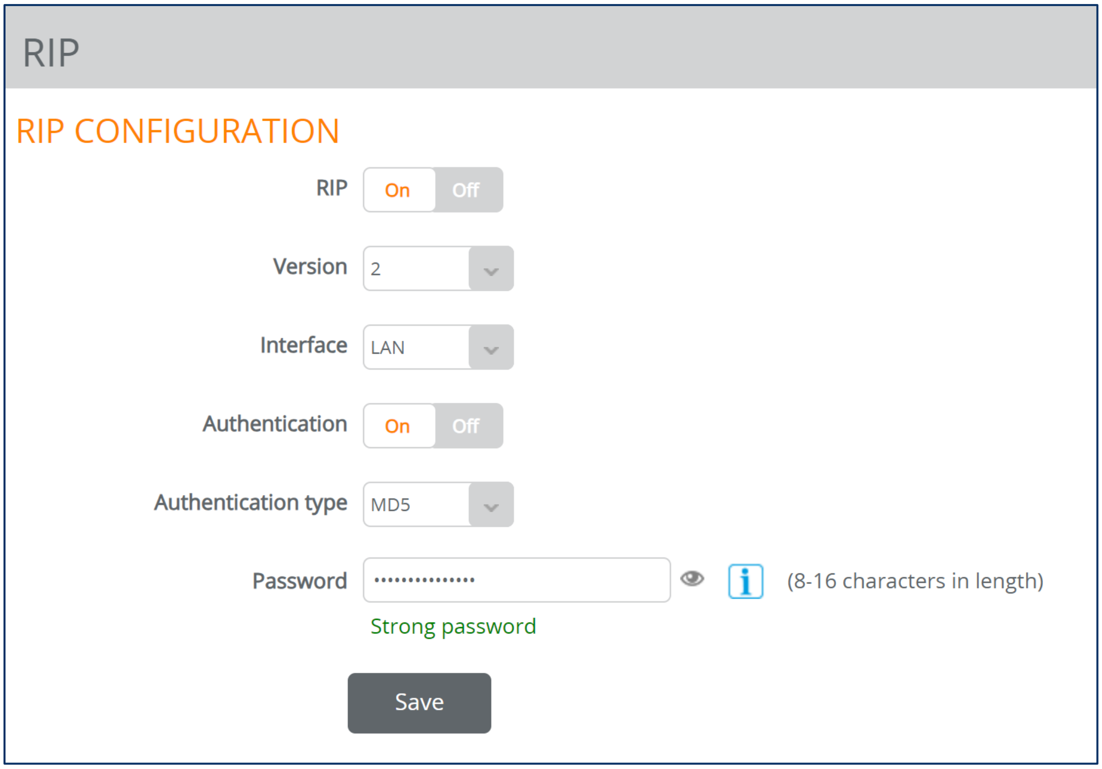
2 Enter the IP Address of the device to be the DMZ host into the **DMZ IP Address** field.

3 Enter the WWAN profile number that you wish to associate the DMZ configuration with.

4 Select the **Save** button to save your settings.

RIP

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



RIP

RIP CONFIGURATION

RIP: On Off

Version: 2

Interface: LAN

Authentication: On Off

Authentication type: MD5

Password: ••••••••••••••• (8-16 characters in length)

Strong password

Figure 65 – RIP configuration

Note – Other routers may ignore RIP.

To enable Routing Information Protocol (RIP)

1 Set the **RIP** toggle to **On** to enable RIP.

2 Using the **Version** drop-down list, select the version of RIP that you would like to use.

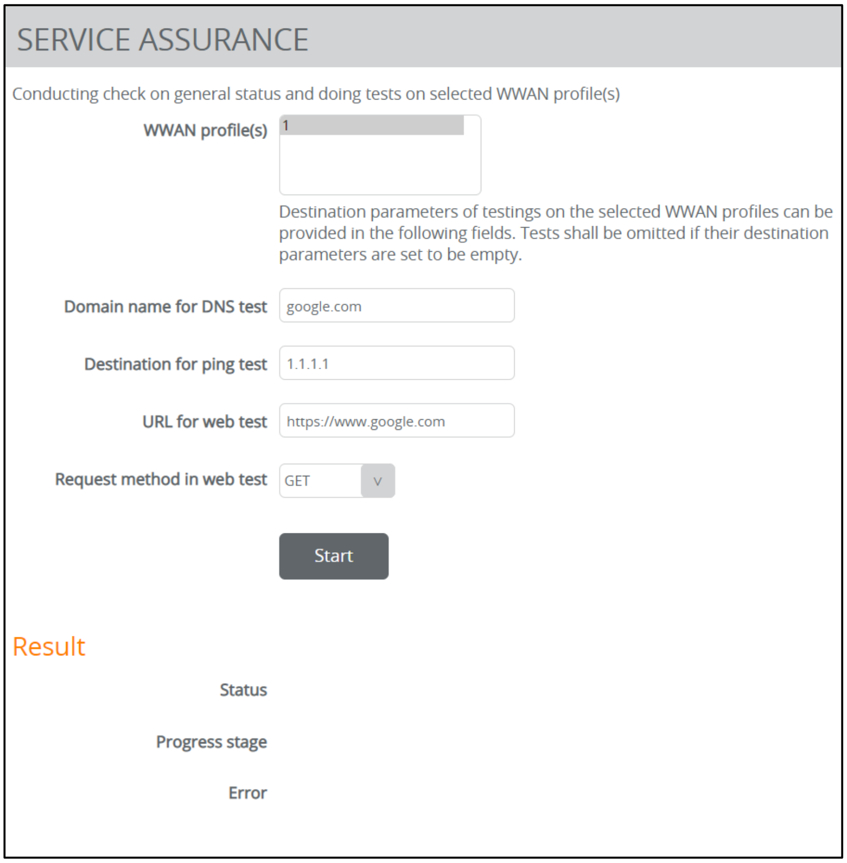
3 Select the **Interface** that RIP should apply on. Options are **LAN**, **WWAN** or **Both**.

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.

Service assurance

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


SERVICE ASSURANCE

Conducting check on general status and doing tests on selected WWAN profile(s)

WWAN profile(s): 1

Destination parameters of testings on the selected WWAN profiles can be provided in the following fields. Tests shall be omitted if their destination parameters are set to be empty.

Domain name for DNS test: google.com

Destination for ping test: 1.1.1.1

URL for web test: https://www.google.com

Request method in web test: GET

Result

Status

Progress stage

Error

Figure 66 – Service assurance

To run a service assurance test:

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

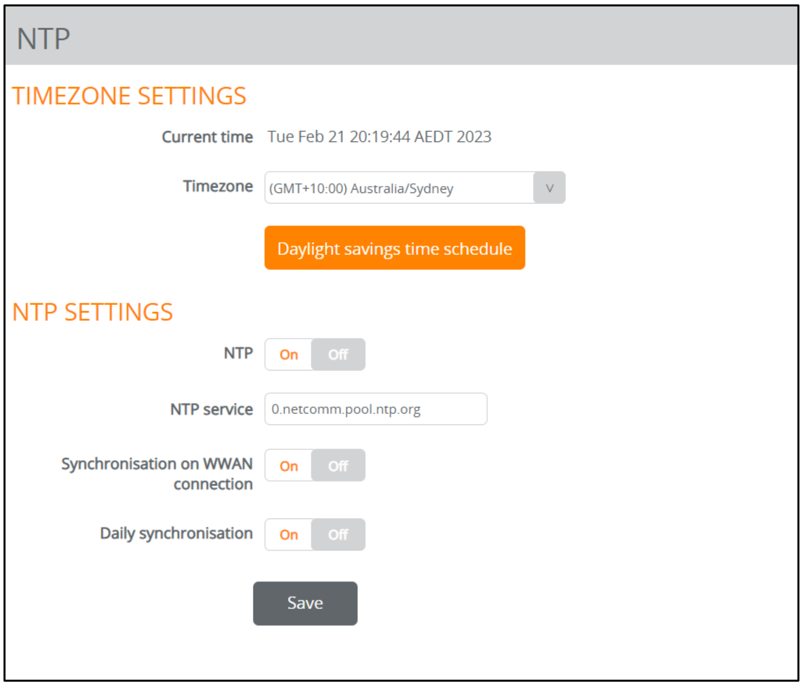
In the **Results** section, a successful test will show a **Passed** whilst a failed test will show **Failed** and which of the tests did not pass.

Services

Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the NTC-500 router to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded. Any NTP server available publicly on the internet may be used. The default NTP server is 0.netcomm.pool.ntp.org.

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



Current time Tue Feb 21 20:19:44 AEDT 2023

Timezone (GMT+10:00) Australia/Sydney

NTP On Off

NTP service 0.netcomm.pool.ntp.org

Synchronisation on WWAN connection On Off

Daily synchronisation On Off

Figure 67 - NTP

Configuring Timezone settings

To configure time zone settings:

1 The Current time field shows the time and date configured on the router. If this is not accurate, use the Timezone drop-down list to select the correct time zone for the router. If the selected zone observes daylight savings time, a Daylight savings time schedule link appears below the drop-down list. Select the link to see the start and end times for daylight savings.

2 When you have selected the correct time zone, select the **Save** button to save the settings.

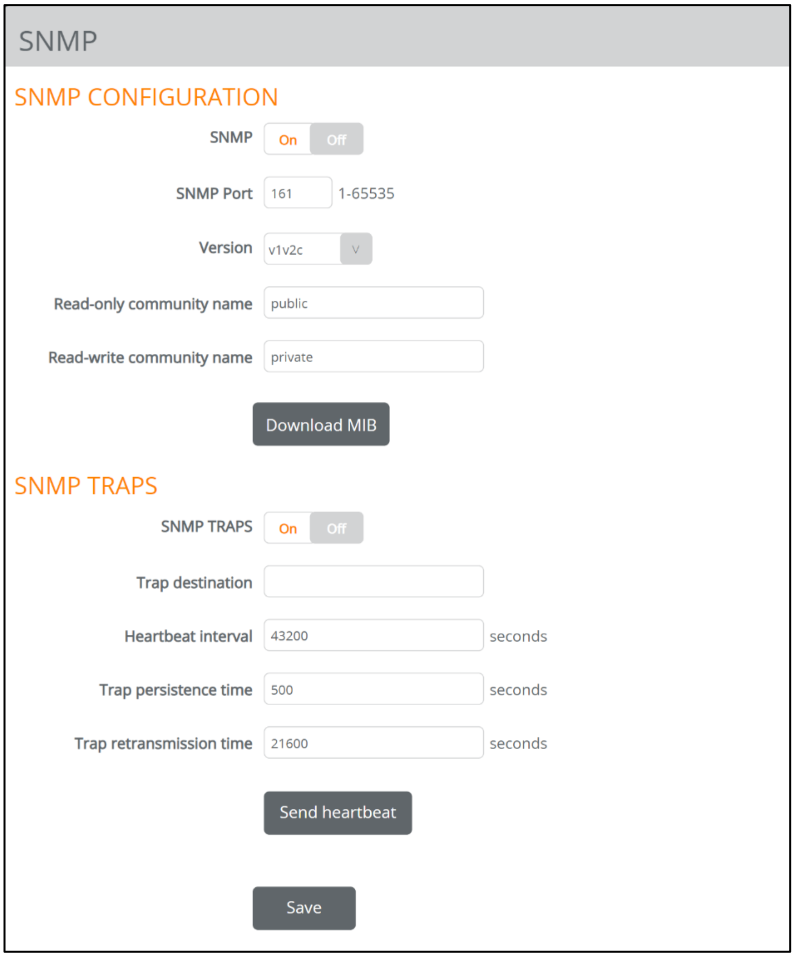
Configuring NTP settings

To configure NTP settings:

1. Select the **Network time (NTP) toggle** key to switch it to the **ON** position.
2. In the **NTP service field**, enter the address of the NTP server you wish to use.
3. The **Synchronization on WWAN** connection toggle key enables or disables the router from performing a synchronization of the time each time a mobile broadband connection is established.
4. The **Daily synchronisation** toggle key enables or disables the router from performing a synchronization of the time each day.
5. When you have finished configuring NTP settings, select the **Save** button to save the settings.

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 typically 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 (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.



SNMP

SNMP CONFIGURATION

SNMP: On | Off

SNMP Port: 161 1-65535

Version: v1v2c

Read-only community name: public

Read-write community name: private

SNMP TRAPS

SNMP TRAPS: On | Off

Trap destination:

Heartbeat interval: 43200 seconds

Trap persistence time: 500 seconds

Trap retransmission time: 21600 seconds

Figure 68 – SNMP Configuration

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 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 should send a heartbeat.

4 In the **Trap persistence time** field, enter the interval in seconds that the NTC-500 should attempt to send a specific trap after the initial occurrence that triggered the trap.

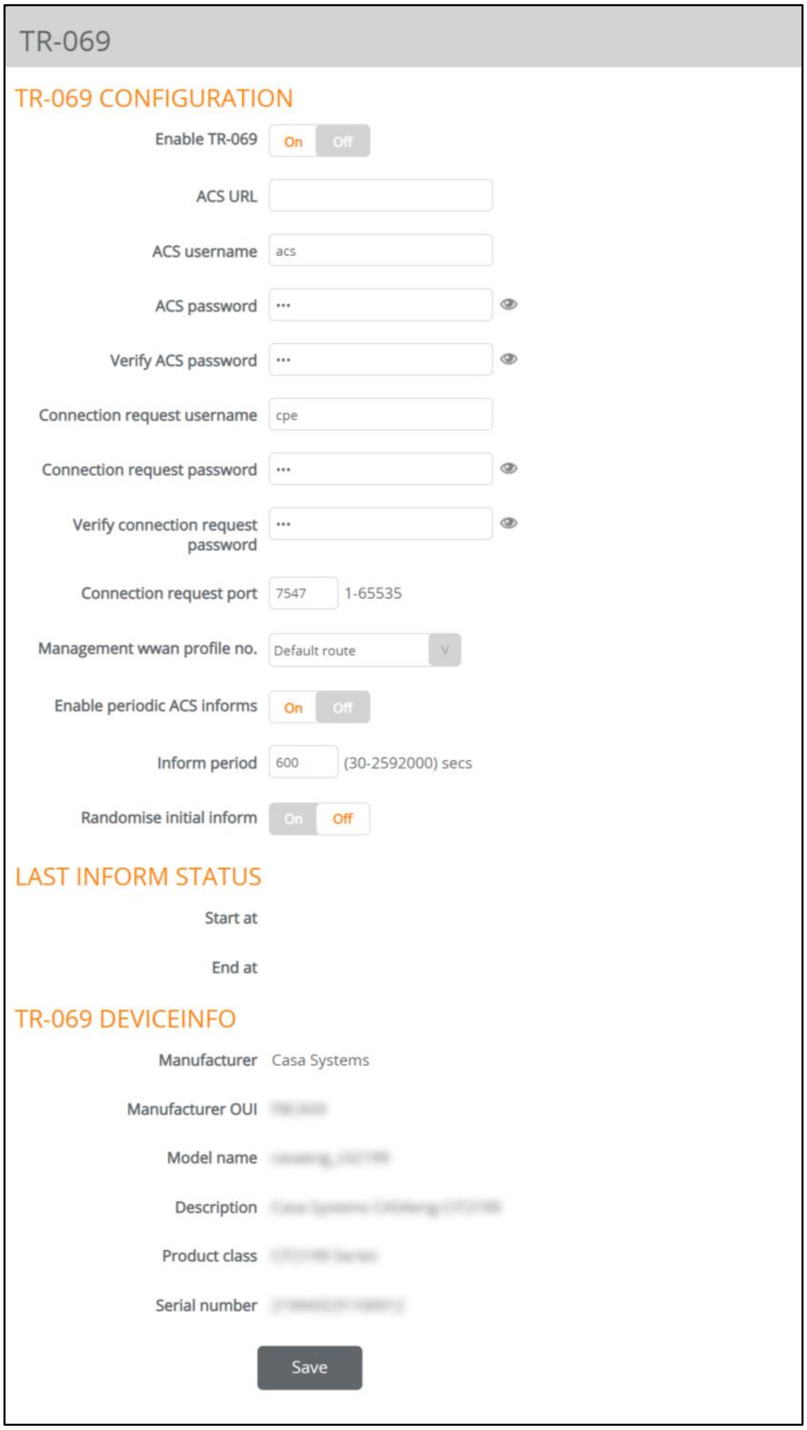
5 In the **Trap retransmission time** field, enter the interval in seconds that the NTC-500 should wait before retransmitting the trap.

6 Use the **Send heartbeat** button to send a test heartbeat.

7 Select the **Save** button to apply the changes.

TR-069

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



TR-069

TR-069 CONFIGURATION

Enable TR-069	On ● / Off
ACS URL	
ACS username	acs
ACS password	•••
Verify ACS password	•••
Connection request username	cpe
Connection request password	•••
Verify connection request password	•••
Connection request port	7547 1-65535
Management wwan profile no.	Default route
Enable periodic ACS informs	On ● / Off
Inform period	600 (30-2592000) secs
Randomise initial inform	On / Off ●

LAST INFORM STATUS

Start at	
End at	

TR-069 DEVICEINFO

Manufacturer	Casa Systems
Manufacturer OUI	[redacted]
Model name	[redacted]
Description	[redacted]
Product class	[redacted]
Serial number	[redacted]

Figure 69 – TR069 configuration

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

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

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

Note – You must have your own compatible ACS infrastructure to use TR-069. To access and configure the TR-069 settings, you must be logged into the router with the root account.
When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

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

TR-069 configuration

To configure TR-069:

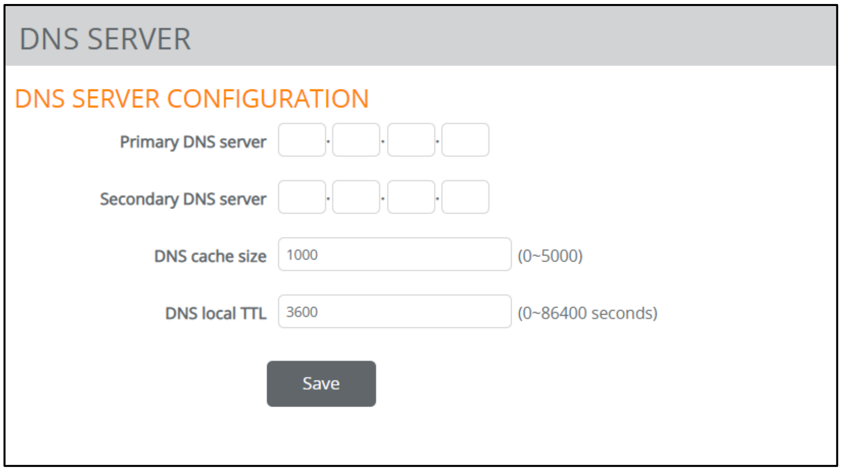
1. Select the **Enable TR-069** toggle key to switch it to the **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server’s full domain name or IP address.
3. Use the **ACS** username field to specify the username used by the server to authenticate the CPE when it sends an “inform” message.
4. In the **ACS password** and **Verify ACS password** fields, enter the password used by the server to authenticate the CPE when it sends an “inform” message.
5. In the **Connection request** username field, enter the username that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
6. In the **Connection request password** and **Verify password** fields, enter the password that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
7. In the **Connection request port** field, enter the port that the request should connect to.
8. In the **Management wwan profile no.** field, enter the WAN profile that should handle the request.
9. The inform message acts as a beacon to inform the ACS of the existence of the router. Select **Enable periodic ACS informs** toggle key to ON in order to turn on the periodic ACS inform messages.

10 In the **Inform Period** field, enter the number of seconds between the inform messages.

11 Select the **Save** button to save the settings.

DNS server

The NTC-500 router can be configured to use custom DNS servers if required.



Primary DNS server . . .

Secondary DNS server . . .

DNS cache size 1000 (0~5000)

DNS local TTL 3600 (0~86400 seconds)

Figure 70 – DNS configuration

To set the DNS servers:

1 In the **Primary DNS server** field, enter the primary DNS server.

2 In the **Secondary DNS server** field, enter the secondary DNS server.

3 In the **DNS Cache Size** field, enter the size of the cache that should be kept on the router.

4 In the **DNS local TTL** field, enter the time to live (TTL) value, which indicates how long a cached request should remain in the router.

5 Select the **Save** button to save the configuration.

SMS messaging

The NTC-500 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:

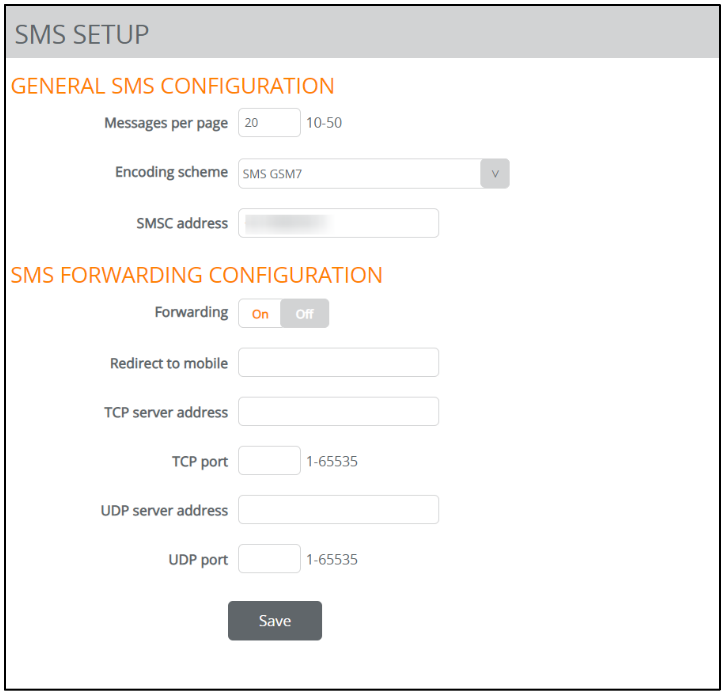
- Ability to send a text message via a cellular network and store it in permanent storage.
- Ability to receive a text message via a cellular network and store it in permanent storage.

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

To access the SMS messaging functions of the NTC-500 router, select on the Services menu item from the top menu bar, and then select one of the options under the SMS messaging section on the left-hand menu.

Setup

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



SMS SETUP

GENERAL SMS CONFIGURATION

Messages per page: 20 (10-50)

Encoding scheme: SMS GSM7

SMSC address: [redacted]

SMS FORWARDING CONFIGURATION

Forwarding: On | Off

Redirect to mobile:

TCP server address:

TCP port: (1-65535)

UDP server address:

UDP port: (1-65535)

Figure 71 – SMS - SMS setup configuration

Option	Definition
General SMS configuration	
SMS messaging	Toggles the SMS functionality of the router on and off.

Messages per page (10-50)	The number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding scheme	The encoding method used for outbound SMS messages. GSM 7-bit mode permits up to 160 characters per message but drops to 50 characters if the message includes special characters. UCS-2 mode allows the sending of Unicode characters and permits a message to be up to 50 characters in length.
SMS forwarding configuration	
Forwarding	Toggles the SMS forwarding function of the router on and off.
Redirect to mobile	Enter a mobile number as the destination for forwarded SMS messages.
TCP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP.
TCP port	The TCP port on which to connect to the remote destination.
UDP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP.
UDP port	The UDP port on which to connect to the remote destination.

Table 10 – SMS - SMS setup configuration items

SMS forwarding configuration

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

Redirect to mobile

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

For Example:

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

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

Redirect to TCP / UDP server address

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

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

For Example:

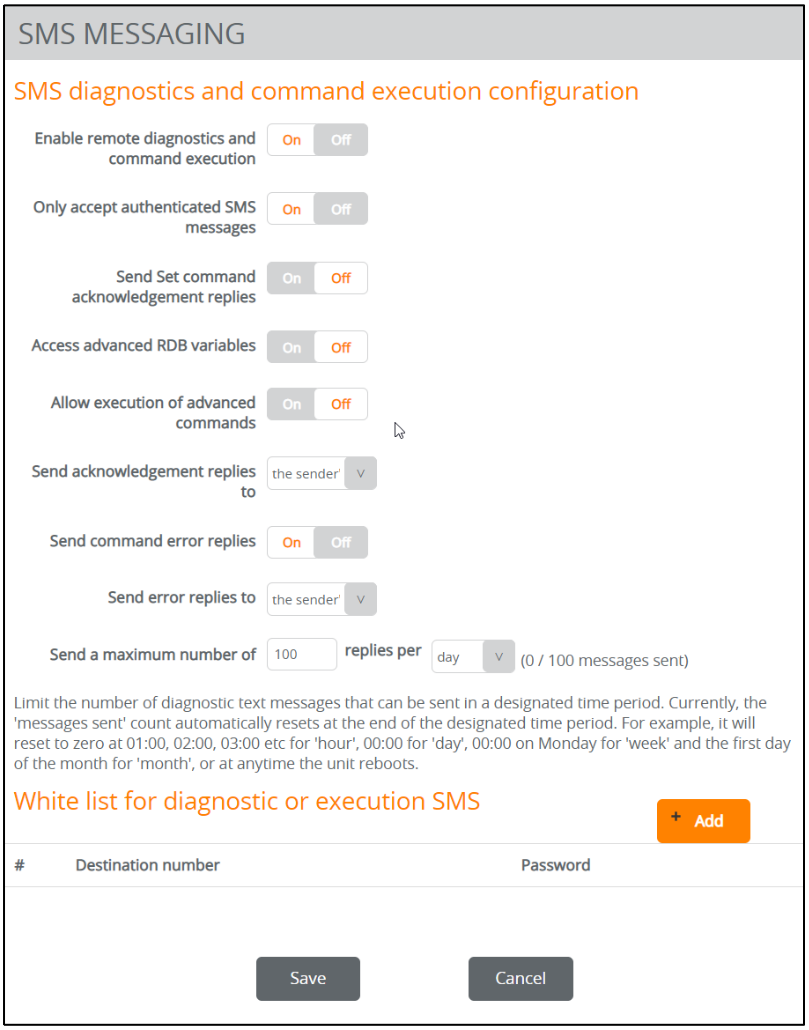
If someone sends a text message and TCP server address is set to “192.168.20.3” and TCP port is set to “2002”, this text message is stored in the router and forwarded to “192.168.20.3” on port “2002” at the same time.

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

Diagnostics

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

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



SMS MESSAGING

SMS diagnostics and command execution configuration

Enable remote diagnostics and command execution: On

Only accept authenticated SMS messages: On

Send Set command acknowledgement replies: Off

Access advanced RDB variables: Off

Allow execution of advanced commands: Off

Send acknowledgement replies to: the sender

Send command error replies: On

Send error replies to: the sender

Send a maximum number of 100 replies per day (0 / 100 messages sent)

Limit the number of diagnostic text messages that can be sent in a designated time period. Currently, the 'messages sent' count automatically resets at the end of the designated time period. For example, it will reset to zero at 01:00, 02:00, 03:00 etc for 'hour', 00:00 for 'day', 00:00 on Monday for 'week' and the first day of the month for 'month', or at anytime the unit reboots.

White list for diagnostic or execution SMS

#	Destination number	Password

Figure 72 – SMS – SMS diagnostics configuration

SMS diagnostics and command execution

Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands.

If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox.

Note – It is possible to adjust settings and prevent your router from functioning correctly using remote diagnostics. If this occurs, you will need to perform a factory reset in order to restore normal operation.

Important – We highly recommended that you use the white list and a password when utilising this feature to prevent unauthorised access. See the White list description for more information.

Only accept authenticated SMS messages

Enables or disables checking the sender's phone number against the allowed sender white list for incoming diagnostics and command execution SMS messages.

If authentication is enabled, the router will check if the sender's number exists in the white list. If it exists, the router then checks the password (if configured) in the incoming message against the password in the white list for the corresponding sending number. If they match, the diagnostic or command is executed.

If the number does not exist in the white list or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message.

This is enabled by default and it is strongly advised that you leave this feature enabled to maintain security.

Sent set command acknowledgement replies

The NTC-500 router will automatically reply to certain types of commands received, such as get commands, or execute commands. However, acknowledgement replies from the NTC-500 router are optional with set commands and the Wakeup command. This option Enables or disables sending an acknowledgment message after execution of a set command or SMS Wakeup command. If disabled, the router does not send any acknowledgement after execution of a set command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.

Access advanced RDB variables

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 acknowledgment replies to

This option allows you to specify where to send acknowledgment messages after the execution of a set, get, or exec command.

If a fixed number is selected, the acknowledgement message will be sent to the number defined in the Fixed number to send replies to field. If the sender’s number is selected, the acknowledgement message will be sent to the number that the SMS diagnostic or command message originated from. The default setting is to use the sender’s number.

Fixed number to send replies to

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

Send a maximum number of

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

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

White list for diagnostic execution SMS

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

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

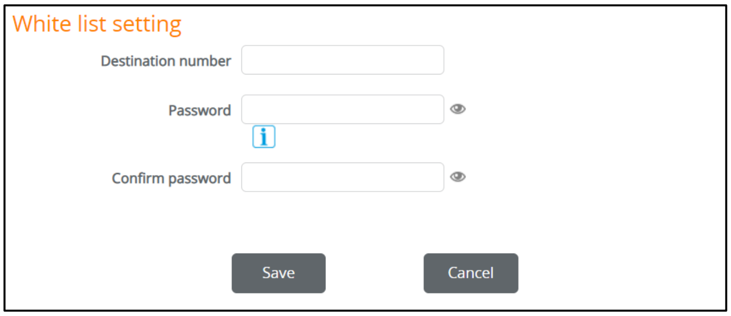


Figure 73 – SMS - SMS diagnostics configuration – White list settings

To add a number to the white list, enter it in the Destination number field and define a password in the Password field. The SMS white list password must meet the following criteria for a strong password:

- Be a minimum of eight characters and no more than 128 characters in length.
- Contain at least one upper case, one lower case character and one number.
- Contain at least one of the following special characters: !*()?/

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

Sending an SMS diagnostic command

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

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

Note – An alternative method of adding a number to the white list is to send an SMS message to the router, navigate to **Services** > **SMS messaging** > **Inbox** and then select the button next to the message which corresponds to the sender's number. You will then need to set a Password in the White list for diagnostic execution SMS list.

5. Select the **Save** button.

Types of SMS diagnostic commands

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

- execute COMMAND
- get VARIABLE
- set VARIABLE=VALUE

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

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

The following are some examples of SMS diagnostic commands:

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

SMS acknowledgement replies

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

SMS command format

Generic Format for reading variables:

```
get VARIABLE
PASSWORD get VARIABLE
```

Generic Format for writing to variables:

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

Generic Format for executing a command:

```
Execute COMMAND
PASSWORD execute COMMAND
```

Replies

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

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

Table 11 – SMS – SMS diagnostics command syntax

Where “VARIABLE” is the name of the value to be read

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

Where “VALUE” is the content to be written to the “VARIABLE”

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

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

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

For Example:

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

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

For Example:

```
“set VARIABLE=’VALUE’”
“set VARIABLE=”VALUE””
“set VARIABLE=`VALUE`”
“get VARIABLE”
```

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

```
“PASSWORD get Variable1”; “get VARIABLE2”
“PASSWORD set VARIABLE1=VALUE1”; “set VARIABLE2=VALUE2”
```

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

For Example:

```
“PASSWORD execute reboot; getVariable1”; “get VARABLE2”
“PASSWORD execute reboot; PASSWORD get Variable1”; “get VARABLE2”
```

⚠ Important – Commands, variables and values are case sensitive.

List of basic commands

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

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

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

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

Table 12 – List of basic SMS diagnostic commands

List of get/set commands

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

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.
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.

Table 13 – SMS - List of get/set commands

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').

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

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

Table 14 – SMS - List of basic SMS diagnostics RDB variables

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
```

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.

Table 15 - Operator status codes returned by get plmnscan SMS command

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.

Mobile Network Code	Mobile Network Provider
1	Telstra

2	Optus
3	Vodafone

Table 16 – SMS - Mobile Network Provider codes (Australia)

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 located in the user interface at Services > SMS messages> Diagnostics.

Description	Input Command (without PASSWORD prefix)
Send SMS to change the data connection username	set username=’NetComm’
Send SMS to change the data connection password	set password= `NetComm`
Send SMS to change the data connection authentication	set authtype= ‘pap’
Send SMS to reboot	execute reboot
Send SMS to check the WAN IP address	get wanip
Send SMS to check the mobile signal strength	get rssi
Send SMS to check the IMEI number	get imei

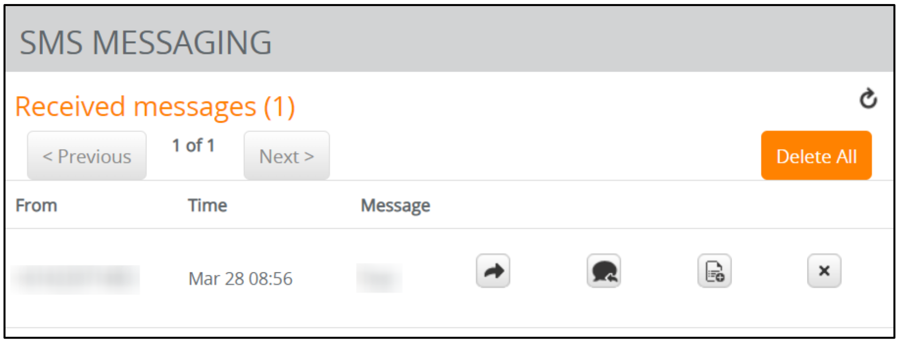
Send SMS to check the current band	get band
Send SMS to Disconnect (if connected) and reconnect the data connection	execute pdpcycle
Send SMS to disconnect the data connection	execute pdpdown
Send SMS to connect the data connection	execute pdpup
Send multiple get command	get wanip; get rssi
Send multiple set command	set ssh.genkeys=1; set username=test; set auth=pap
Send SMS to reset to factory default settings	execute factorydefaults
Send SMS to retrieve status of router	get status
Send SMS to retrieve the history of the session, including start time, end time and total data usage	get sessionhistory
Send SMS to configure the router to send syslog to a remote syslog server	set syslogserver=123.209.56.78
Send SMS to 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
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

Table 17 – SMS – SMS diagnostics example commands

Inbox

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



SMS MESSAGING

Received messages (1)

From	Time	Message
[redacted]	Mar 28 08:56	[redacted]

Figure 74 – SMS - Inbox

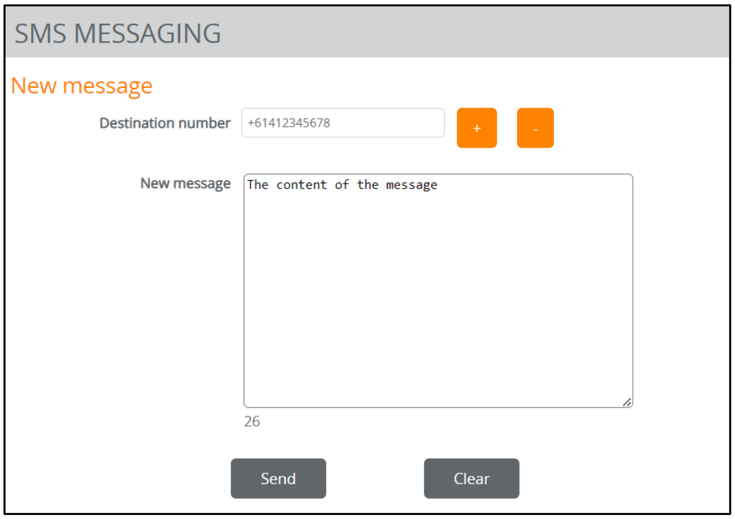
Icon	Name	Description
➦	Forward	Opens a new message window where you can forward the corresponding message to another recipient.
💬	Reply	Opens a new message window where you can reply to the sender.
📄	Add to White list	Add the sender's mobile number to the white list on the router.
×	Delete	Delete the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

Table 18 – SMS - Inbox

New message

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

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



SMS MESSAGING

New message

Destination number: +61412345678

New message: The content of the message

26

Figure 75 – SMS – New message

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

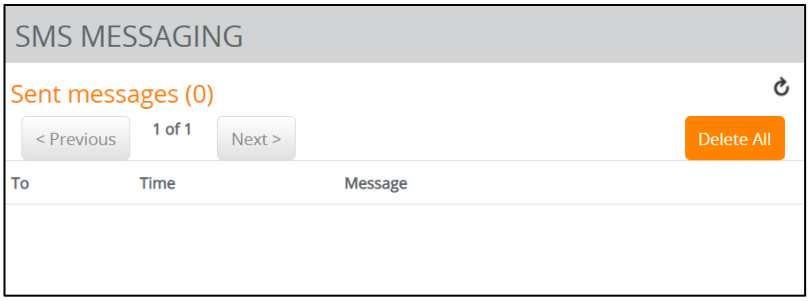
For example:

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

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

Outbox

The outbox displays all sent messages.



SMS MESSAGING

Sent messages (0)

1 of 1

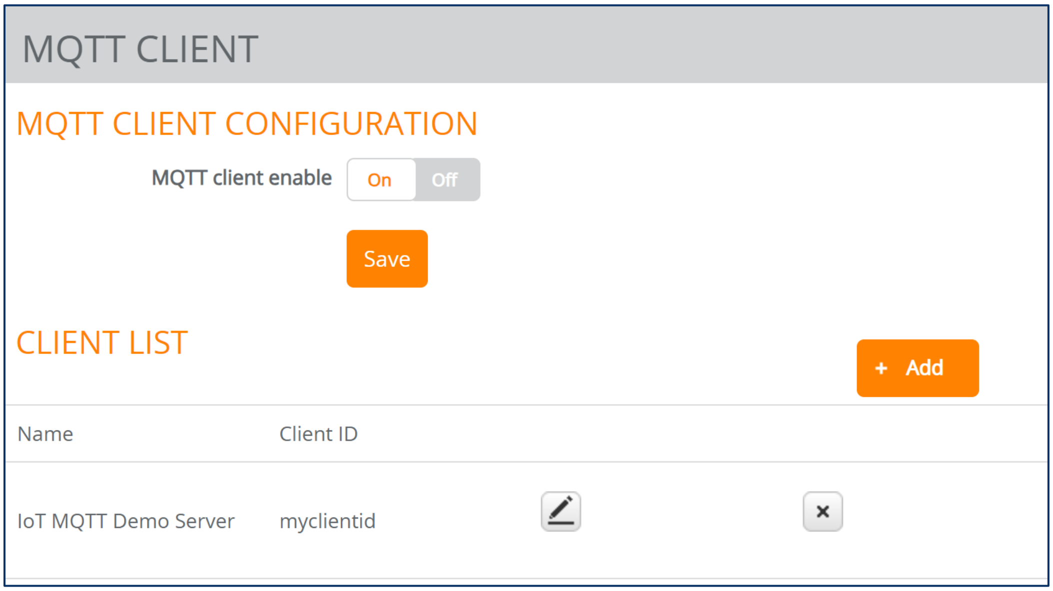
To	Time	Message

Figure 76 – SMS - Outbox

Use the **Delete All** button to empty the outbox.

MQTT

The MQTT page is used to configure the NTC-500 to use the MQTT protocol. MQTT is a standards-based messaging protocol used for machine-to-machine communication. Information is sent to clients in the form of a 'topic'. The NTC-500 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.



MQTT CLIENT

MQTT CLIENT CONFIGURATION

MQTT client enable [✓ On] Off

CLIENT LIST

Name	Client ID		
IoT MQTT Demo Server	myclientid	✎	×

Figure 77 – MQTT Client

Configuring MQTT

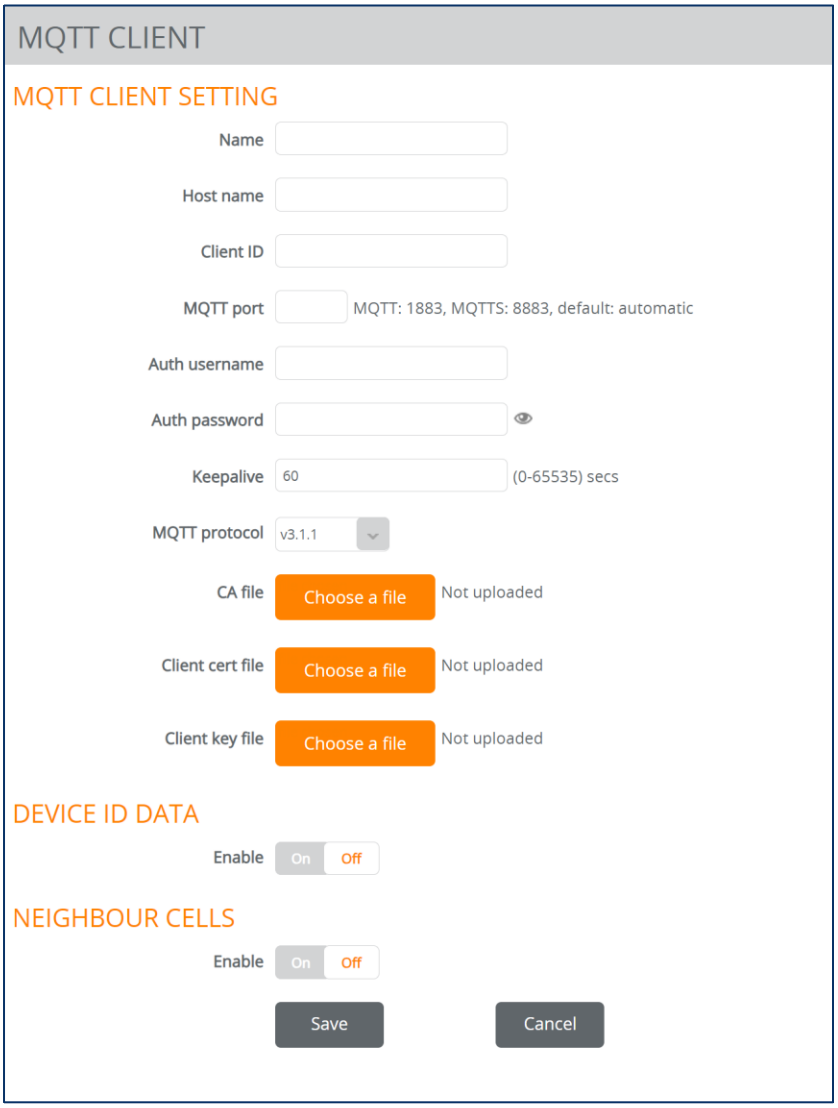
Prerequisites

Before configuring MQTT on the NTC-500, you may 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.

Configuration

1 Set the MQTT client enable toggle to **On**, then select the **Save** button.

2 Select the **Add+** button to add a new client. The **MQTT client** page is displayed.



MQTT CLIENT

MQTT CLIENT SETTING

Name

Host name

Client ID

MQTT port — MQTT: 1883, MQTTS: 8883, default: automatic

Auth username

Auth password

Keepalive: 60 (0-65535) secs

MQTT protocol: v3.1.1

CA file — Choose a file — Not uploaded

Client cert file — Choose a file — Not uploaded

Client key file — Choose a file — Not uploaded

DEVICE ID DATA

Enable: On [✓ Off]

NEIGHBOUR CELLS

Enable: On [✓ Off]

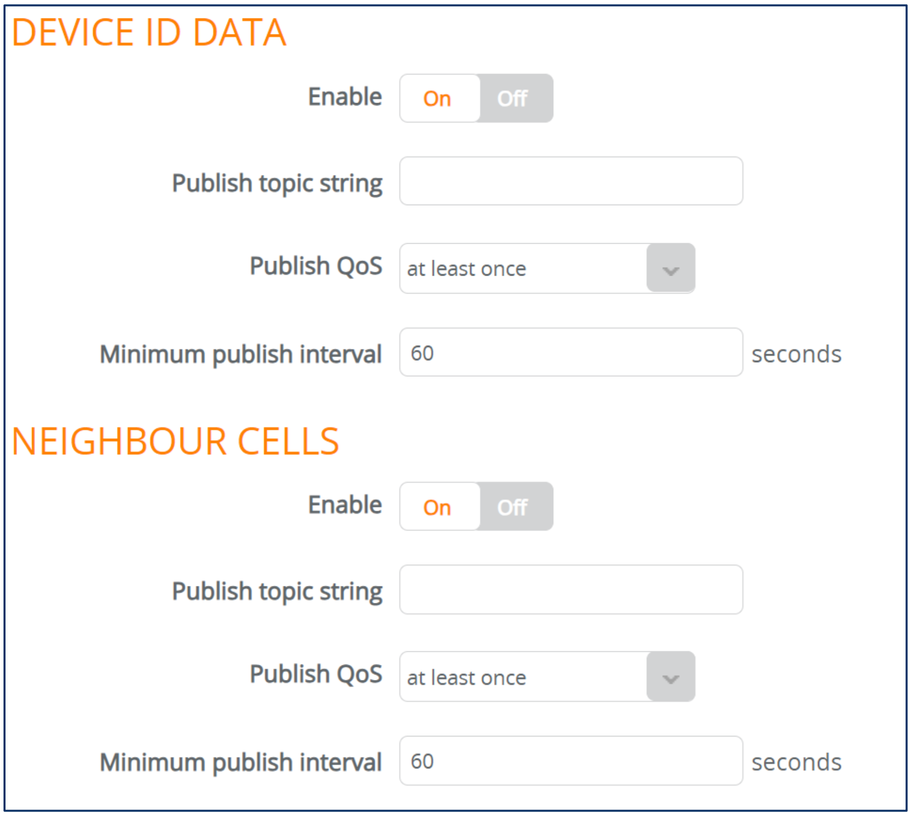
Figure 78 – MQTT – MQTT Client configuration

3 Under MQTT configuration, enter the parameters as required. The following table details each field:

Parameter	Description
Name	Name of the client which will identify the client on the NTC-500
Host name	Hostname of your client
Client ID	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	The port MQTT should be initiated over.
Auth username	The username of the connection.
Auth password	The password of the connection.
Keepalive	Number of seconds that the connection should be kept alive.
MQTT protocol	Version of MQTT that should be used.
CA file	The Certificate Authority used to generate your Client Certificate file.
Client cert file	The client certificate file generated as part of your client's configuration.
Client key file	The client key file generated as part of your client's configuration.

Table 19 – MQTT Client configuration parameters

4 Set the Enable toggle to On to enable the 'topic' that should be sent from the NTC-500.



DEVICE ID DATA

Enable: On | Off

Publish topic string:

Publish QoS: at least once

Minimum publish interval: 60 seconds

NEIGHBOUR CELLS

Enable: On | Off

Publish topic string:

Publish QoS: at least once

Minimum publish interval: 60 seconds

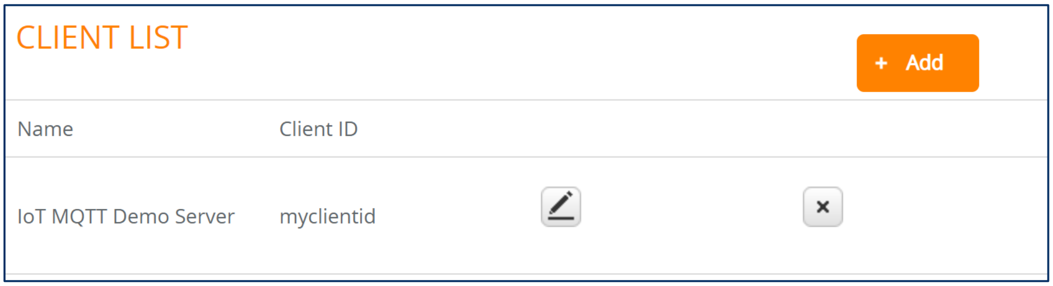
Figure 79 – MQTT – MQTT Client Configuration – MQTT topics

5 Configure the following parameters as required:

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

Table 20 – MQTT Client topic parameters

6 Select the Save button to create the client. The client appears in the MQTT client list.



CLIENT LIST

Name	Client ID
IoT MQTT Demo Server	myclientid

Figure 80 – MQTT – MQTT Client Configuration – MQTT client list

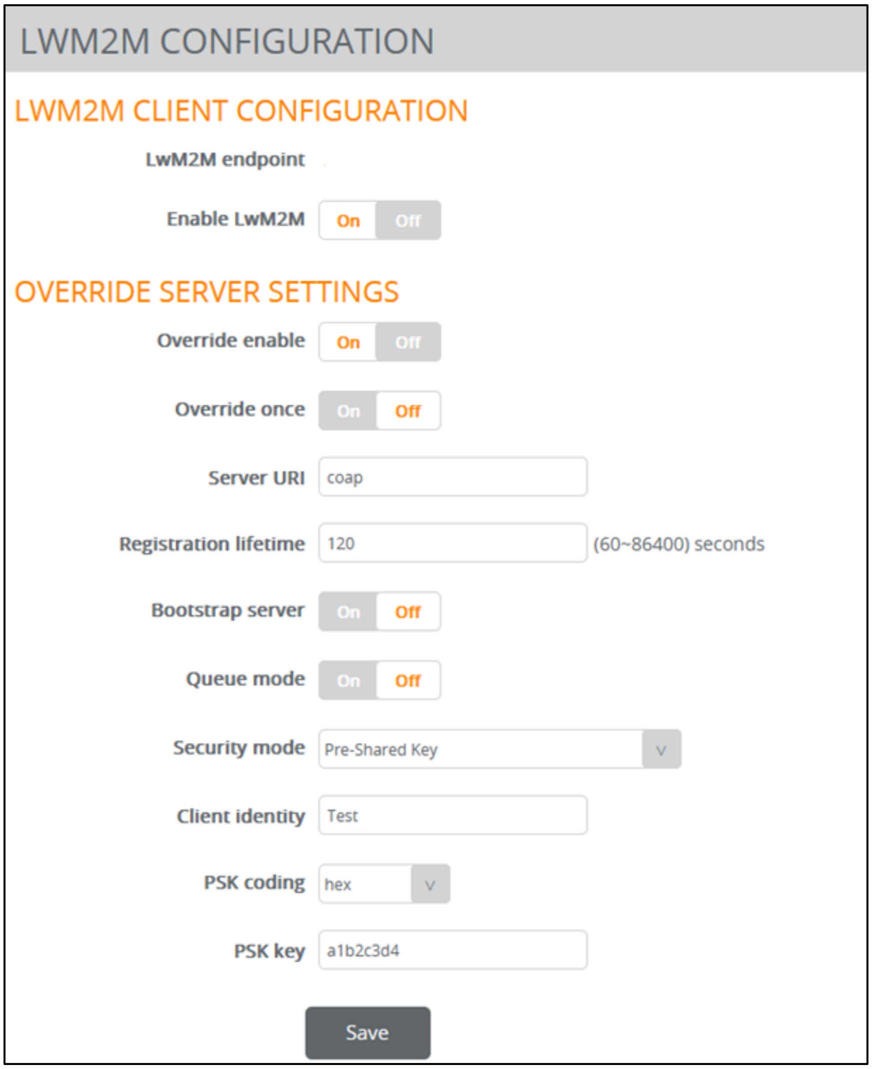
OMA-LWM2M

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

It provides:

- Firmware upgrades
- Device monitoring and configuration
- Server provisioning

To configure the Lightweight M2M client, select the Enable LwM2M toggle key so that it is in the ON position.



LWM2M CONFIGURATION

LWM2M CLIENT CONFIGURATION

LwM2M endpoint

Enable LwM2M: On

OVERRIDE SERVER SETTINGS

Override enable: On

Override once: Off

Server URI: coap

Registration lifetime: 120 (60~86400) seconds

Bootstrap server: Off

Queue mode: Off

Security mode: Pre-Shared Key

Client identity: Test

PSK coding: hex

PSK key: a1b2c3d4

Figure 81 - OMA-LWM2M configuration

Item	Description
LwM2M Endpoint Name	This is the unique ID the device will use to identify itself with LwM2M servers.
Enable LwM2M	Toggle key which enables or disables the LwM2M function.
Override Server Settings	The LwM2M client maintains the list of servers that it will connect to as part of its internal state. Enabling this setting will allow a user to specify new server details that will override whatever current settings the client has.
Override Once	When 'Override Settings' is enabled, this option allows you to specify whether the new server details they provide will be applied once when the client is restarted (normal flow for configuring/reconfiguring the client) or, when disabled, applied every time the client restarts (used for debugging/troubleshooting.)
Server URI	When 'Override Settings' is enabled, this allows you to specify the URI of the LwM2M server to connect to. Must be a fully specified CoAP or CoAPS URI, including port number, e.g. coap://server.com:5683 or coaps://server.com:5864.
Registration Lifetime	When 'Override Settings' is enabled, this allows you to specify the interval (in seconds) at which the LwM2M client will send registration updates (i.e. heartbeat messages) to the server.
Bootstrap Server	When 'Override Settings' is enabled, this allows you to specify whether the new server is a LwM2M bootstrap server.
Queue Mode	When 'Override Settings' is enabled, this allows you to specify whether to report the UDP binding mode to the server as queued ("UQ" binding mode) or not ("U" binding mode.)
Security Mode	When 'Override Settings' is enabled, this allows you to choose the security mode that will be used to connect to the LwM2M server. Currently supported options are 'No Security' and 'Pre-Shared Key' (PSK).
Client Identity	When PSK security mode is selected this field is where you must specify the identity string associated with your pre-shared key.
PSK coding	When PSK security mode is select this field is where you must specify the coding for the key. The coding can be either ‘hex’ or ‘plain text’.
PSK Key	When PSK security mode is selected this field is where you must provide the pre-shared key. The key must be entered as a hexadecimal string or a plain text string, depending on the selected setting in the PSK coding field.

Table 21 - OMA-LWM2M configuration items

Supported LWM2M objects

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

Object	Object ID	Note
LWM2M Server	1	

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

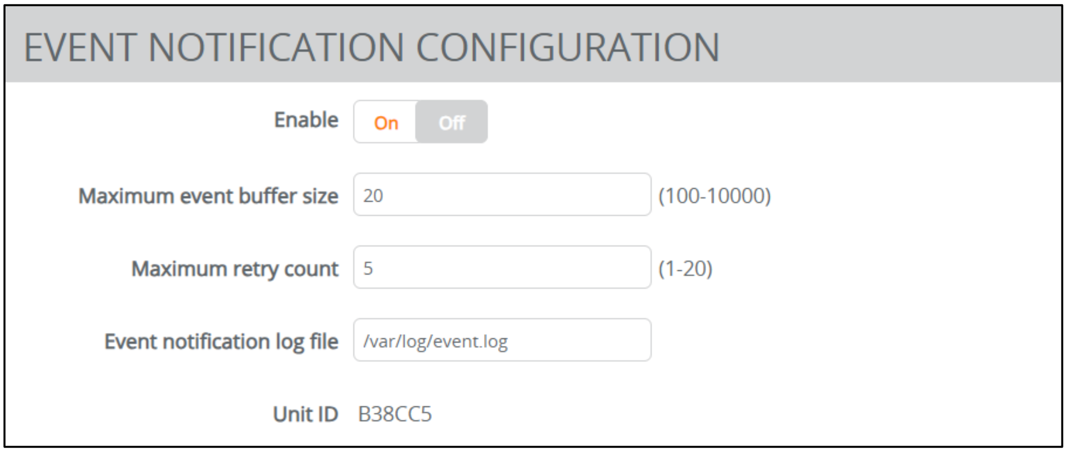
Table 22 – LWM2M supported objects

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.

Event Configuration

The NTC-500 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.



EVENT NOTIFICATION CONFIGURATION

Enable: On | Off

Maximum event buffer size: 20 (100-10000)

Maximum retry count: 5 (1-20)

Event notification log file: /var/log/event.log

Unit ID: B38CC5

Figure 82 – Event Notification – Configuration

Event Notification Configuration

To use Event Notifications:

1 Enable event notifications by setting the **Enable** toggle to **On.**

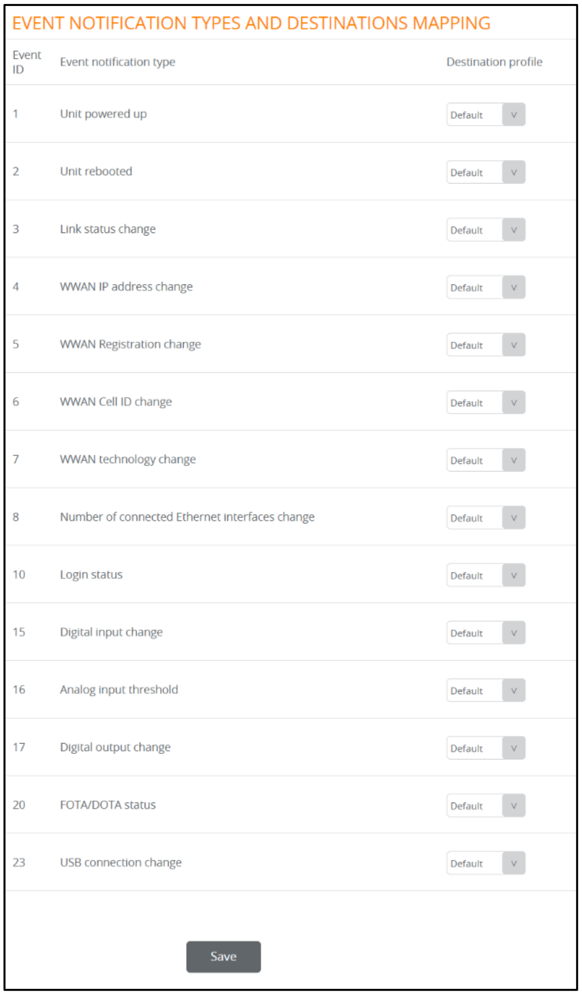
2 In the **Maximum buffer event size** field, specify the buffer size for event notifications which failed to be delivered or are yet to be sent.

3 In the **Maximum retry count** field, enter the number of times the NTC-500 should attempt to deliver the notification in the event of a delivery failure.

4 If required, adjust the output location of the **Event notification log file.**

5 For each of the **Event Notification Types** select the **Destination Profile** which should send the notification when the notification is triggered. For details on how to configure the Destination Profiles, view the Destination Configuration section.

6 Select the **Save** button to apply the configuration.



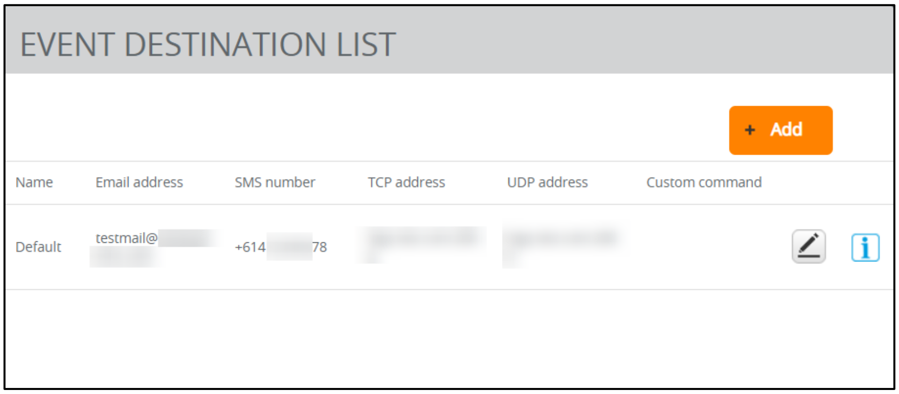
EVENT NOTIFICATION TYPES AND DESTINATIONS MAPPING

Event ID	Event notification type	Destination profile
1	Unit powered up	Default
2	Unit rebooted	Default
3	Link status change	Default
4	WWAN IP address change	Default
5	WWAN Registration change	Default
6	WWAN Cell ID change	Default
7	WWAN technology change	Default
8	Number of connected Ethernet interfaces change	Default
10	Login status	Default
15	Digital input change	Default
16	Analog input threshold	Default
17	Digital output change	Default
20	FOTA/DOTA status	Default
23	USB connection change	Default

Figure 83 – Event Configuration – Available notification types

Destination configuration

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



EVENT DESTINATION LIST

+ Add

Name	Email address	SMS number	TCP address	UDP address	Custom command		
Default	testmail@[redacted]	+614[redacted]78	[redacted]	[redacted]		✎	ℹ

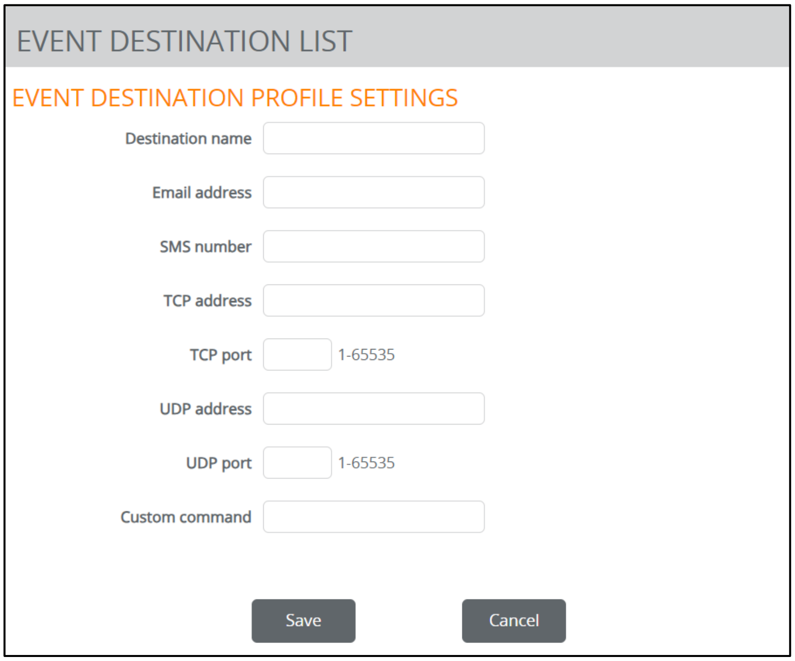
Figure 84 – Log – Event destination list

Configuring a destination

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

To configure or edit an event destination:

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



EVENT DESTINATION LIST

EVENT DESTINATION PROFILE SETTINGS

Destination name	
Email address	
SMS number	
TCP address	
TCP port	1-65535
UDP address	
UDP port	1-65535
Custom command	

Save Cancel

Figure 85 – Services – Event configuration – Destination Configuration – Event Destination Profile settings

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

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

3 In the **Email address** field, enter an email address to receive the notification.

4 In the **SMS number** field, enter a phone number to receive the notification as an SMS.

5 In the **TCP address** and **TCP port** fields, enter a TCP address and TCP port to receive the notification over TCP.

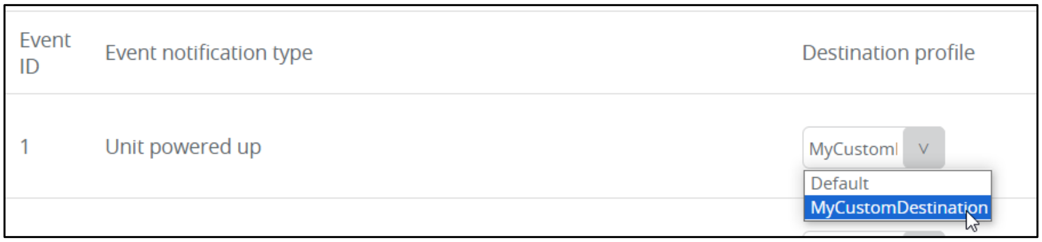
6 In the **UDP address** and **UDP port** fields, enter a UDP address and UDP port to receive the notification over UDP.

7 In the **Custom command** field, enter a custom command to execute when the notification is triggered. The command should be a bash compatible command.

8 Select the **Save** button to save the destination profile.

9 Apply the destination profile by returning to the **Event Configuration > Event Notification Configuration** page.

10 Set the **Destination profile** dropdown on the appropriate Event Notification and Destination Mapping item to the new destination.



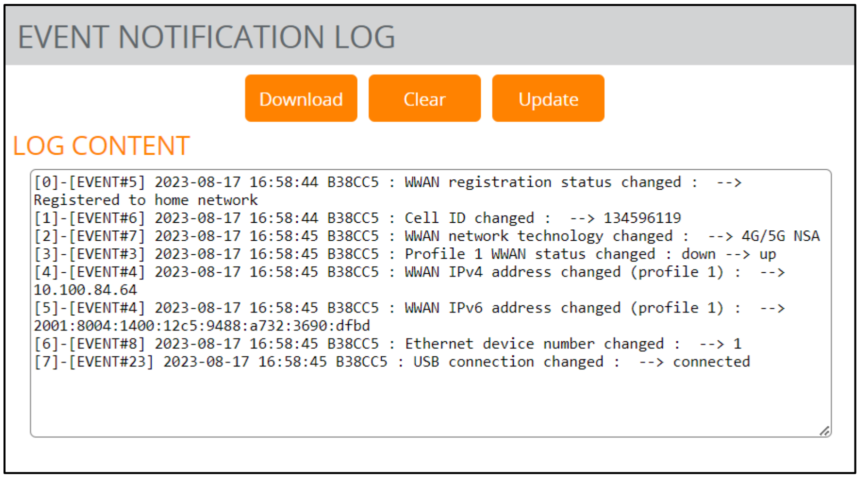
Event ID	Event notification type	Destination profile
1	Unit powered up	MyCustomI

Figure 86 – Services – Event Configuration – Destination profile mapping

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

Event notification log

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

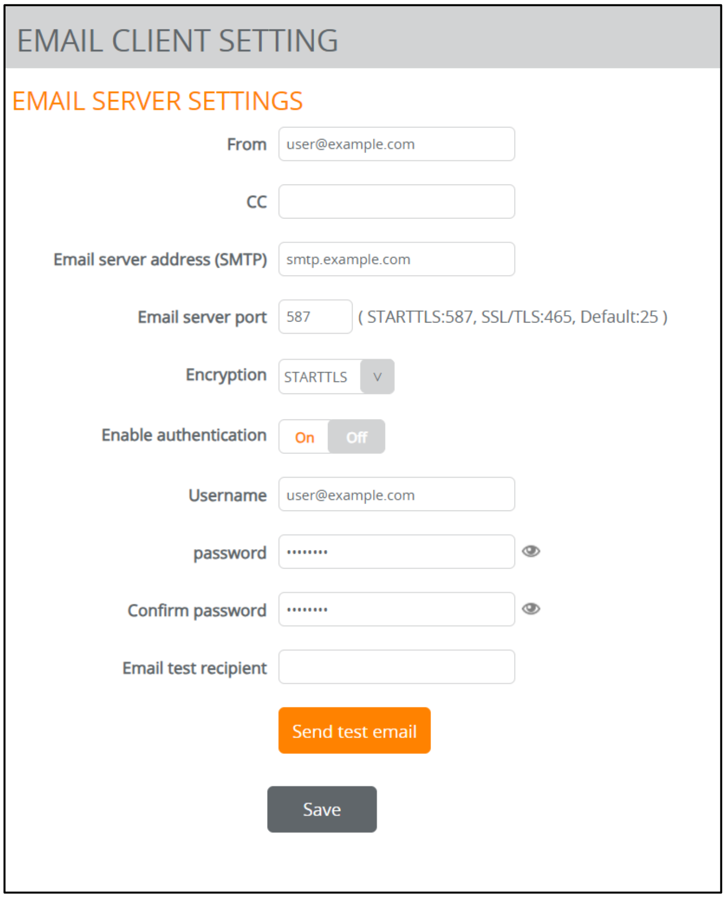


```
[0]-[EVENT#5] 2023-08-17 16:58:44 B38CC5 : WWAN registration status changed :  -->
Registered to home network
[1]-[EVENT#6] 2023-08-17 16:58:44 B38CC5 : Cell ID changed :  --> 134596119
[2]-[EVENT#7] 2023-08-17 16:58:45 B38CC5 : WWAN network technology changed :  --> 4G/5G NSA
[3]-[EVENT#3] 2023-08-17 16:58:45 B38CC5 : Profile 1 WWAN status changed : down --> up
[4]-[EVENT#4] 2023-08-17 16:58:45 B38CC5 : WWAN IPv4 address changed (profile 1) :  -->
10.100.84.64
[5]-[EVENT#4] 2023-08-17 16:58:45 B38CC5 : WWAN IPv6 address changed (profile 1) :  -->
2001:8004:1400:12c5:9488:a732:3690:dfbd
[6]-[EVENT#8] 2023-08-17 16:58:45 B38CC5 : Ethernet device number changed :  --> 1
[7]-[EVENT#23] 2023-08-17 16:58:45 B38CC5 : USB connection changed :  --> connected
```

Figure 87 – Services – Event Configuration – Event notification log

Email Settings

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



EMAIL CLIENT SETTING

EMAIL SERVER SETTINGS

From: user@example.com

CC:

Email server address (SMTP): smtp.example.com

Email server port: 587 (STARTTLS:587, SSL/TLS:465, Default:25)

Encryption: STARTTLS

Enable authentication: On | Off

Username: user@example.com

password: ••••••••

Confirm password: ••••••••

Email test recipient:

Figure 88 – Email Client Setting

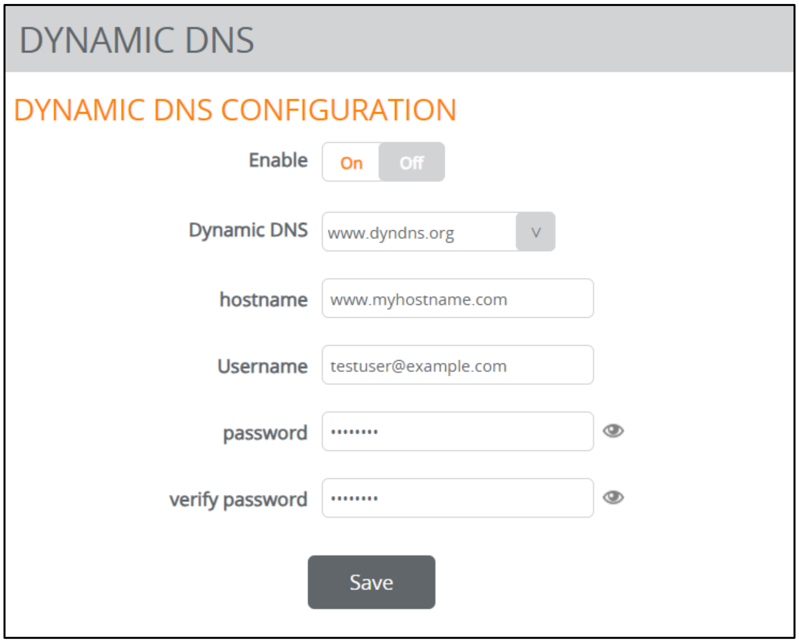
To configure the Email Server Settings, the following information is required:

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.
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	Applies the email setting configuration.

Dynamic DNS

Dynamic DNS (DDNS) allows your NTC-500 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 and its internal network more easily for maintenance.



DYNAMIC DNS

DYNAMIC DNS CONFIGURATION

Enable: On Off

Dynamic DNS: www.dyndns.org

hostname: www.myhostname.com

Username: testuser@example.com

password: ••••••••

verify password: ••••••••

Figure 89 – Services – Dynamic DNS

To use DDNS, you will need to sign up for a DDNS provider which is supported by the NTC-500. The supported providers are DHS.org, No-IP, DynDNS, easyDNS, and ZoneEdit. To configure DDNS on the NTC-500 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 To enable DDNS, 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.

System

Log

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

System log

The System Log enables you to troubleshoot any issues you may be experiencing with your NTC-500 router. To access the System Log page, select on the System menu. The System Log page is displayed.

The display level dropdown allows for filtering of the logs that you wish to see.

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.

Table 23 – Log – System log levels

Use the Display level dropdown to select the level of log that you wish to view, then select Download.

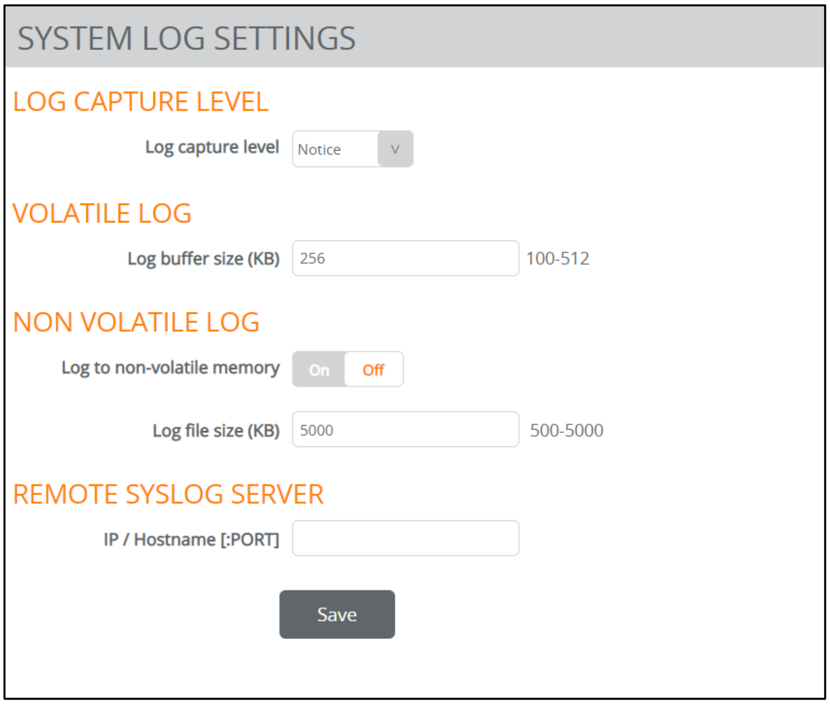
The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore in order to be displayed correctly with new lines shown, it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

System log settings

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

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

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


SYSTEM LOG SETTINGS

LOG CAPTURE LEVEL

Log capture level: Notice

VOLATILE LOG

Log buffer size (KB): 256 100-512

NON VOLATILE LOG

Log to non-volatile memory: On [✓ Off]

Log file size (KB): 5000 500-5000

REMOTE SYSLOG SERVER

IP / Hostname [:PORT]:

Figure 90 – Log – System log settings

Log capture level

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

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.

Table 24 – Log - System log detail levels

Volatile Log

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

Non-volatile Log

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

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

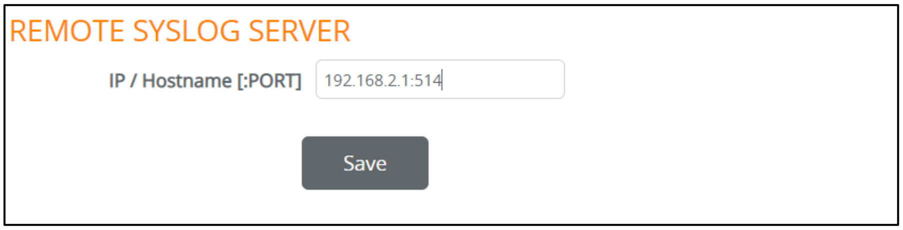
Remote syslog server

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

To configure the NTC-500 router to output log data to a remote syslog server:

1 Select on the System menu from the top menu bar. The System log item is displayed.

2 Under the Remote syslog server section, enter the IP address or hostname of the syslog server in the IP / Hostname [PORT] field.


REMOTE SYSLOG SERVER

IP / Hostname [:PORT]: 192.168.2.1:514

Figure 91 – Log – System log settings – Remote syslog server

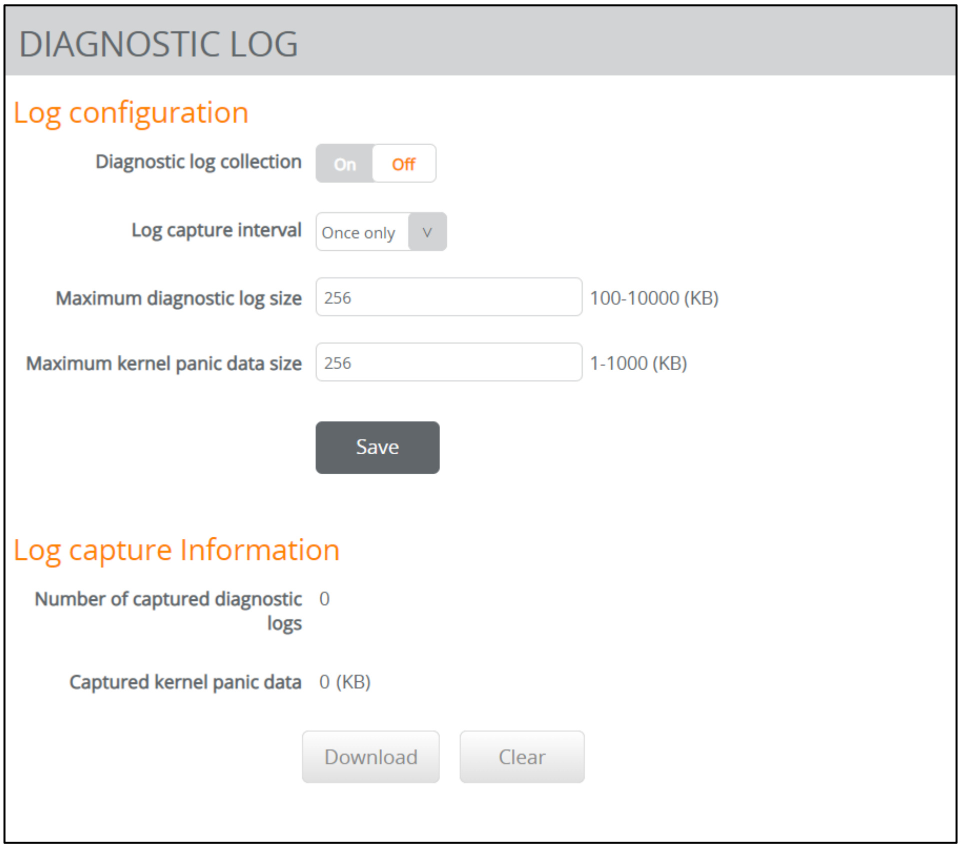
You can also specify the port number after the IP or hostname by entering a semi-colon and then the port number e.g. 192.168.1.102:514.

If you do not specify a port number, the router will use the default UDP port 514.

3 Select the Save button to save the configuration.

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 NetComm 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 NetComm technical support staff.



DIAGNOSTIC LOG

Log configuration

Diagnostic log collection: On | Off

Log capture interval: Once only

Maximum diagnostic log size: 256 — 100-10000 (KB)

Maximum kernel panic data size: 256 — 1-1000 (KB)

Log capture Information

Number of captured diagnostic logs: 0

Captured kernel panic data: 0 (KB)

Figure 92 – Log – Diagnostic log configuration and download

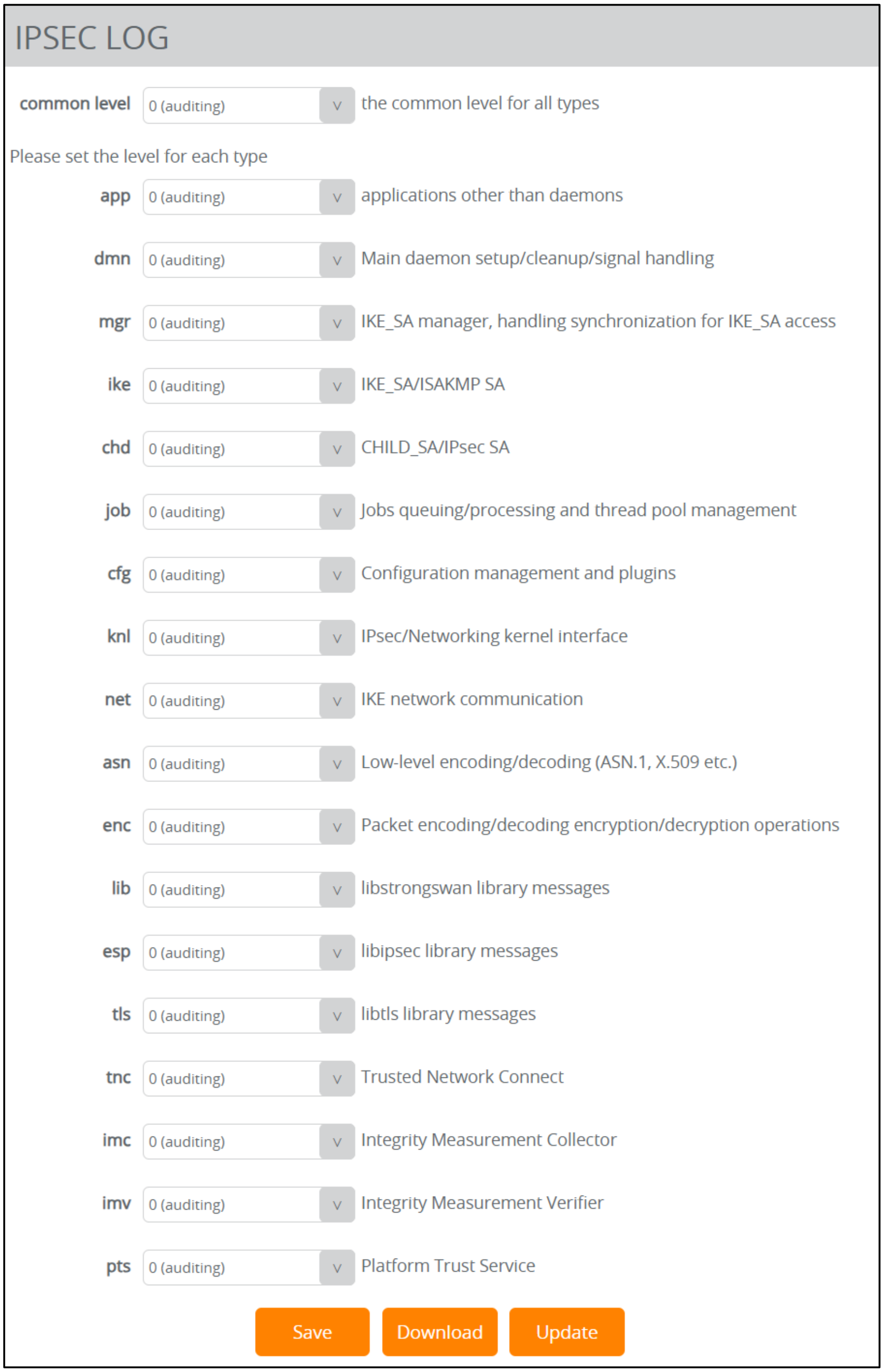
Item	Description
Diagnostic log configuration	
Periodic log collection	Turn on this toggle key to enable diagnostic log collection.
Log capture interval	Specifies the interval at which the router should collect diagnostic log data.
Maximum periodic log size (KB)	Specifies the maximum size of the log file in kilobytes.
Maximum kernel panic data size (KB)	Specifies the maximum size of the kernel panic data file in kilobytes.
Save button	Saves the Log Configuration.

Log capture information	
Number of captured periodic logs	Displays the number of captured periodic logs.
Captured kernel panic data (KB)	Displays the total size of captured kernel panic data in kilobytes.
Clear all captured periodic logs	Press the “Clear” button to clear all captured periodic logs.
Download all captured logs	Press the “Download” button to download all captured logs.

Table 25 – Diagnostic log descriptions

IPSec log

The IPsec Log enables you to identify and troubleshoot issues with the IPsec VPN connection. To access the IPsec Log page, select IPSec Log on the System menu. The IPSec Log page is displayed.



IPSEC LOG

common level	0 (auditing)	the common level for all types

Please set the level for each type

app	0 (auditing)	applications other than daemons
dmn	0 (auditing)	Main daemon setup/cleanup/signal handling
mgr	0 (auditing)	IKE_SA manager, handling synchronization for IKE_SA access
ike	0 (auditing)	IKE_SA/ISAKMP SA
chd	0 (auditing)	CHILD_SA/IPsec SA
job	0 (auditing)	Jobs queuing/processing and thread pool management
cfg	0 (auditing)	Configuration management and plugins
knl	0 (auditing)	IPsec/Networking kernel interface
net	0 (auditing)	IKE network communication
asn	0 (auditing)	Low-level encoding/decoding (ASN.1, X.509 etc.)
enc	0 (auditing)	Packet encoding/decoding encryption/decryption operations
lib	0 (auditing)	libstrongswan library messages
esp	0 (auditing)	libipsec library messages
tls	0 (auditing)	libtls library messages
tnc	0 (auditing)	Trusted Network Connect
imc	0 (auditing)	Integrity Measurement Collector
imv	0 (auditing)	Integrity Measurement Verifier
pts	0 (auditing)	Platform Trust Service

Figure 93 – Log - IPSec Log

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

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

Table 26 – IPSec log descriptions

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

Viewing and downloading the IPsec log

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

To view the logs in an external tool, select the **Download** button.

Watchdog

Periodic ping

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

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

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

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:

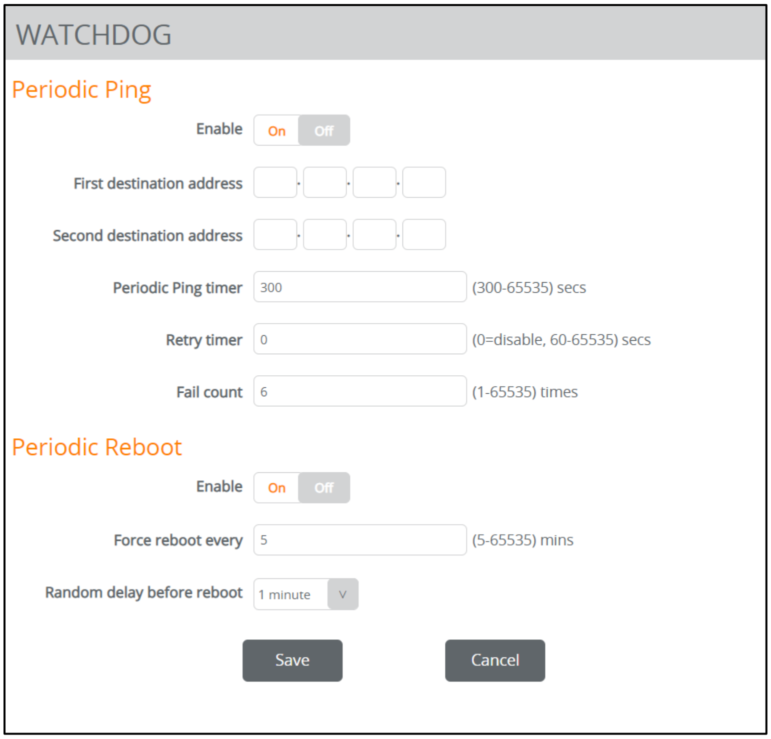
a After every "Periodic Ping timer" configured interval, the router sends 3 consecutive pings to the "First destination address".

b If all 3 pings fail the router sends 3 consecutive pings to the "Second address".

c The router then sends 3 consecutive pings to the "Destination address" and 3 consecutive pings to the "Second address" every "Retry timer" configured interval.

d If all retry pings in step C above fail the number of times configured in "Fail count", the router reboots.

e If any ping succeeds, the router returns to step A and does not reboot.



WATCHDOG

Periodic Ping

Enable	On / Off	
First destination address	. . .	
Second destination address	. . .	
Periodic Ping timer	300	(300-65535) secs
Retry timer	0	(0=disable, 60-65535) secs
Fail count	6	(1-65535) times

Periodic Reboot

Enable	On / Off	
Force reboot every	5	(5-65535) mins
Random delay before reboot	1 minute	

Figure 94 – Watchdog – Periodic ping and reboot configuration

Configuring Periodic Ping settings

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

To configure the ping watchdog:

1 Enable the ping watchdog by setting the Periodic Ping Enable toggle to **On.**

2 In the **First destination address** field, enter a website address or IP address to which the router will send the first round of ping requests.

3 In the **Second destination address** field, enter a website address or IP address to which the router will send the second round of ping requests.

4 In the **Periodic Ping timer** field, enter a number between 300 and 65535 for the number of seconds the router should wait between ping attempts. Setting this to 0 disables the ping watchdog function.

5 In the **Retry timer** field, enter a number between 60 and 65535 for the number of seconds the router should wait between retry ping attempts, i.e. pings to the second destination address.

6 In the **Fail count** field, enter an integer between 1 and 65535 for the number of times an accelerated ping should fail before the router reboots. Setting this to 0 disables the ping watchdog function.

7 Select the **Save** button to save the configuration.

Disabling the ping watchdog

To disable the ping watchdog by setting the **Periodic Ping Enable** toggle to Off, then select the **Save** button.

Periodic reboot

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

1 In the **Force reboot every** field, enter the time in minutes between forced reboots. The default value is 0 which disables the Periodic reboot function. The minimum period between reboots is 5 minutes while the maximum value is 65535 minutes.

2 If you have configured a forced reboot time, you can use the **Randomise reboot time** drop-down list to select a random reboot timer. Randomising the reboot time is useful for preventing a large number of devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured Force reboot every time and then randomly selects a time that is less than or equal to the Randomise reboot time setting. After that randomly selected time has elapsed, the router reboots.

⚠ Important – The randomise reboot time is not persistent across reboots; each time the router is due to reboot, it randomly selects a time less than or equal to the Randomise reboot time.

3 Select the **Save** button to save the settings.

System configuration

Restore factory defaults

Restoring factory defaults will reset the NTC-500 router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-500 router. There are three levels of factory reset:

- Installer reset
- Carrier reset
- Full factory reset

Installer reset

The installer reset only resets settings that have changed after the NTC-500 was installed. The settings that are included are those that were likely changed through the web interface. This reset level is generally the first one that should be attempted, as it will reset less important configurations.

Carrier reset

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

Full factory reset

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

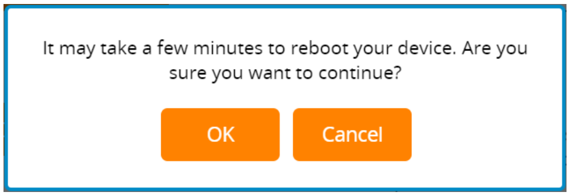
⚠ Important – The full factory reset will require the NTC-500 to be completely reconfigured.

To complete a reset at any level

1 On the **Restore Factory Defaults** page, select the **Clear HTTPS certificate** checkbox if you want to clear the HTTPS certificate.

2 Select the appropriate reset level.

3 You will be prompted to confirm. Select the **Ok** button to proceed with the reset.

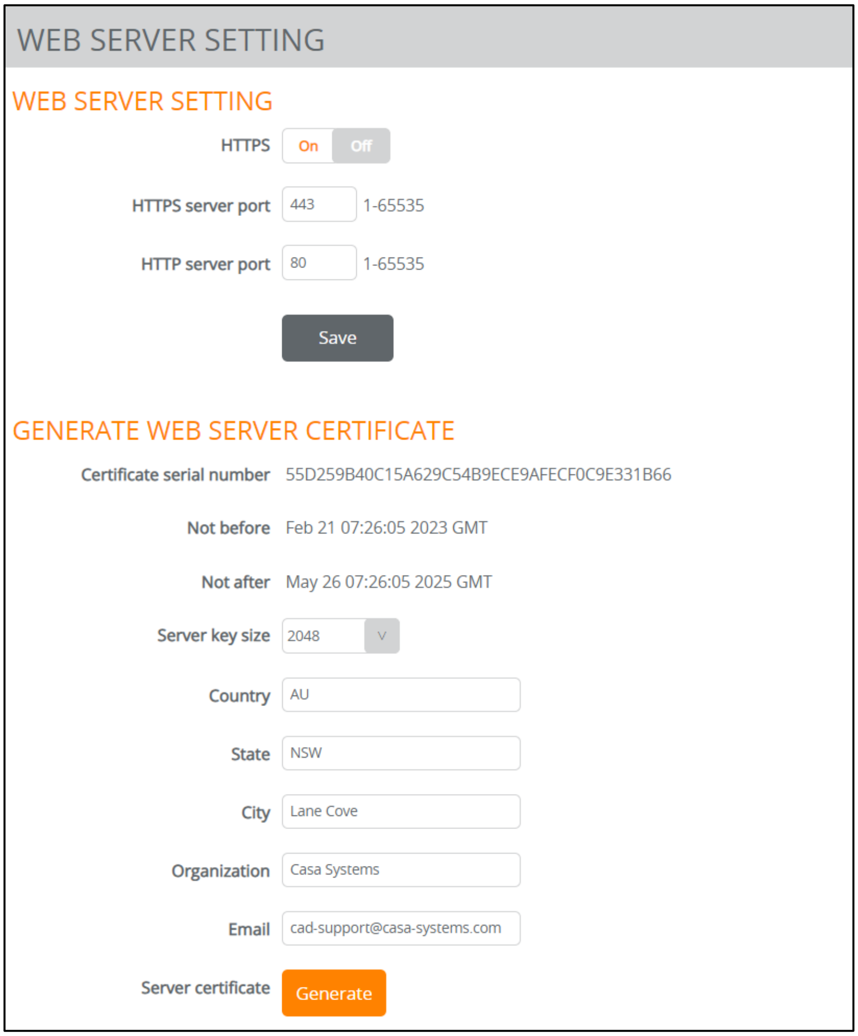


It may take a few minutes to reboot your device. Are you sure you want to continue?

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

You can configure whether the NTC-500's web server uses HTTP or HTTPS and the server port. Additionally, you can generate a web server certificate by entering data in all the fields under the Generate web server certificate section.



WEB SERVER SETTING

WEB SERVER SETTING

HTTPS: On

HTTPS server port: 443 1-65535

HTTP server port: 80 1-65535

GENERATE WEB SERVER CERTIFICATE

Certificate serial number: 55D259B40C15A629C54B9ECE9AFECF0C9E331B66

Not before: Feb 21 07:26:05 2023 GMT

Not after: May 26 07:26:05 2025 GMT

Server key size: 2048

Country: AU

State: NSW

City: Lane Cove

Organization: Casa Systems

Email: cad-support@casa-systems.com

Server certificate

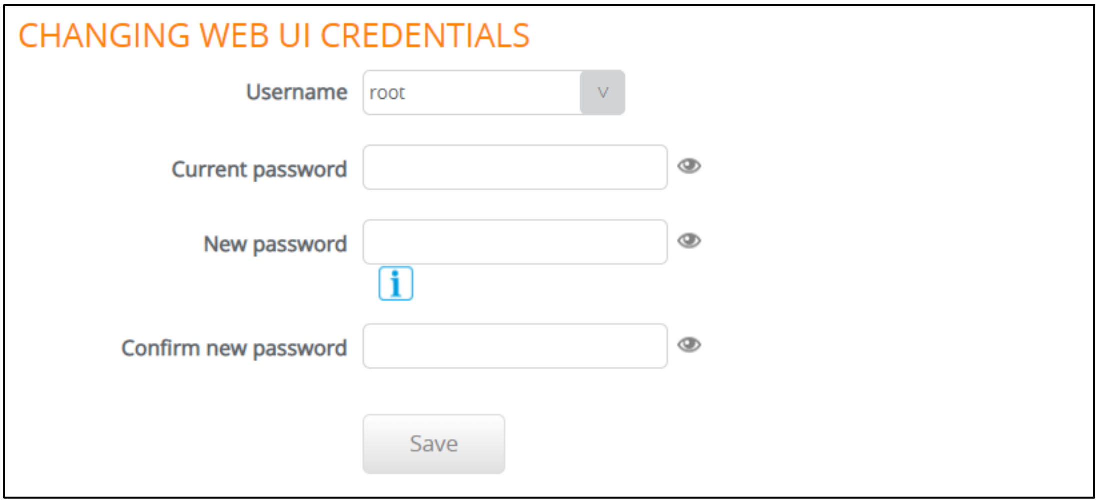
Figure 95 – Web server setting configuration

Administration settings

The Administration settings page allows for updating administration credentials and Web UI login limits.

Web UI credentials

Use this section to configure the username and password used to access the NTC-500 via the web interface.



CHANGING WEB UI CREDENTIALS

Username: root

Current password:

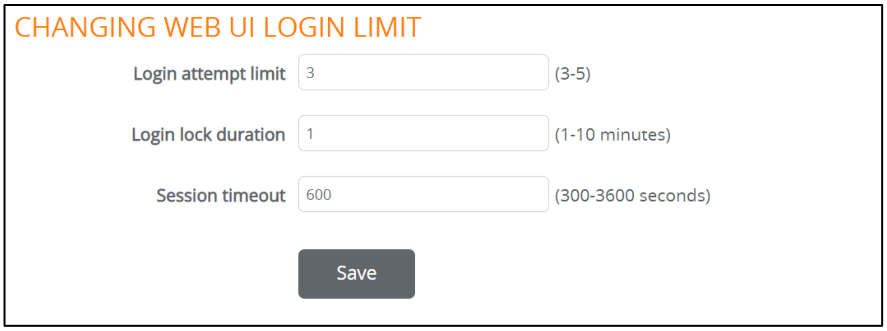
New password:

Confirm new password:

Figure 96 – Administration settings – Web UI credentials configuration

Web UI logon limits

The Web UI login limit section allows configuration of the timeout and lock of the web interface. It is designed to improve security by reducing the risk of brute force attacks on the web interface.



CHANGING WEB UI LOGIN LIMIT

Login attempt limit: 3 (3-5)

Login lock duration: 1 (1-10 minutes)

Session timeout: 600 (300-3600 seconds)

Figure 97 – Administration settings – Web UI login limit configuration

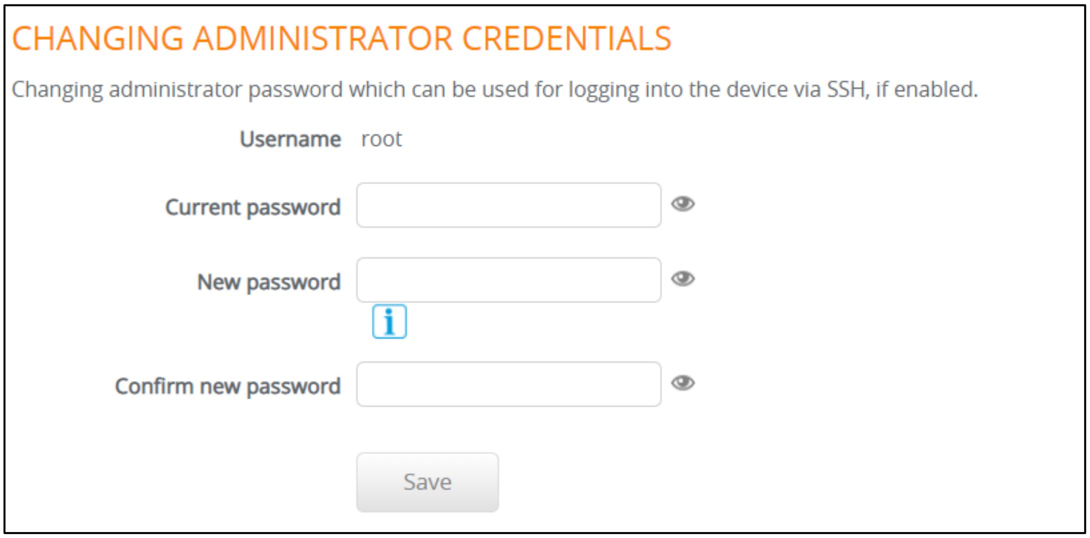
Item	Description
Login attempt limit	The number of times an incorrect password can be entered into the web interface before it locks out any further attempts
Login lock duration	The amount of time the login lock lasts for

Session timeout	The amount of time in seconds that a logged in session lasts on the web interface. The web interface will log the current user out after the configured time.

Table 27

Administration credentials

Use this section to configure the username and password used to access the NTC-500 via SSH.



CHANGING ADMINISTRATOR CREDENTIALS

Changing administrator password which can be used for logging into the device via SSH, if enabled.

Username root

Current password

New password

Confirm new password

Figure 98 – Administration – Administrator credentials configuration

Settings backup/restore

The settings backup and restore page is used to backup or restore the router's configuration or to reset it to factory defaults. In order to view the settings page, you must be logged into the web user interface as root using the password admin. The backup / restore functions can be used to easily configure a large number of NTC-500 routers by configuring one router with your desired settings, backing them up to a file and then restoring that file to multiple NTC-500 routers.

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

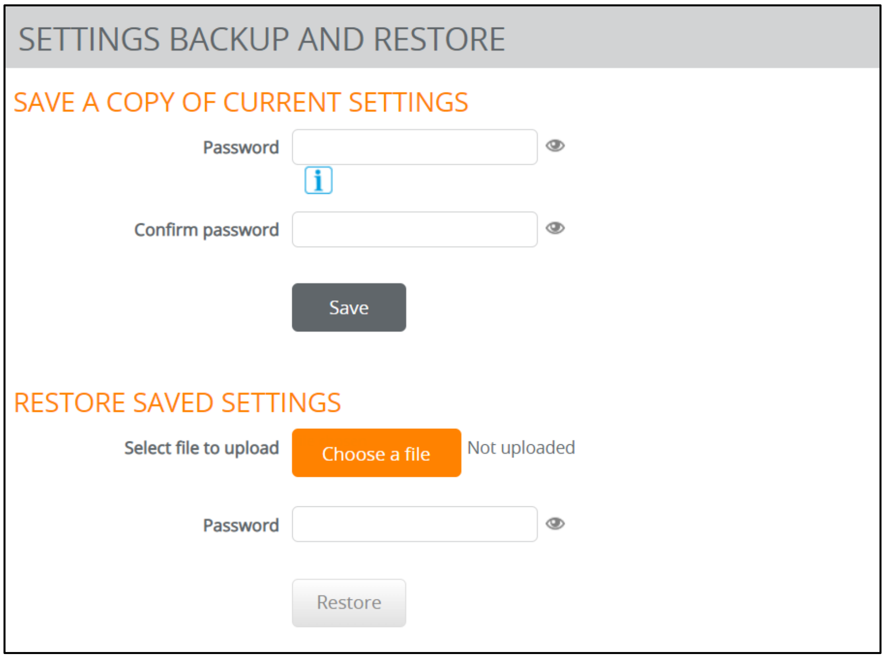


Figure 99 – System configuration - Backup and restore

Creating a settings backup

To create a settings backup, under the Save a copy of current settings section select the Save button. The configuration will download. If you wish to protect the configuration with a password, enter a password into the Password and Confirm password fields, then press Save.

Restoring a settings backup

To restore a settings backup, under the Restore saved settings section, select Choose a file, then locate the saved configuration. If the file was saved with a password, enter the password, then select Restore. You will be prompted to confirm, select Ok to proceed. The device will reboot with the saved settings.

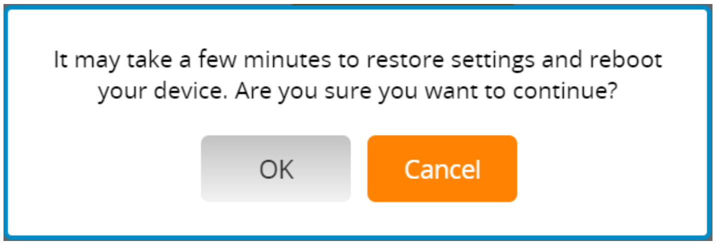

It may take a few minutes to restore settings and reboot your device. Are you sure you want to continue?

Figure 100 – Systems configuration – Restoring a settings backup confirmation

Site and location settings

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

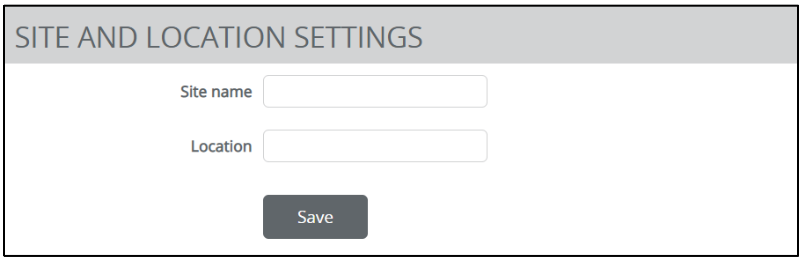


Figure 101 – System configuration – Site and location settings

Update the site name and location by entering the information in the fields, then pressing Save.

Runtime configuration

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

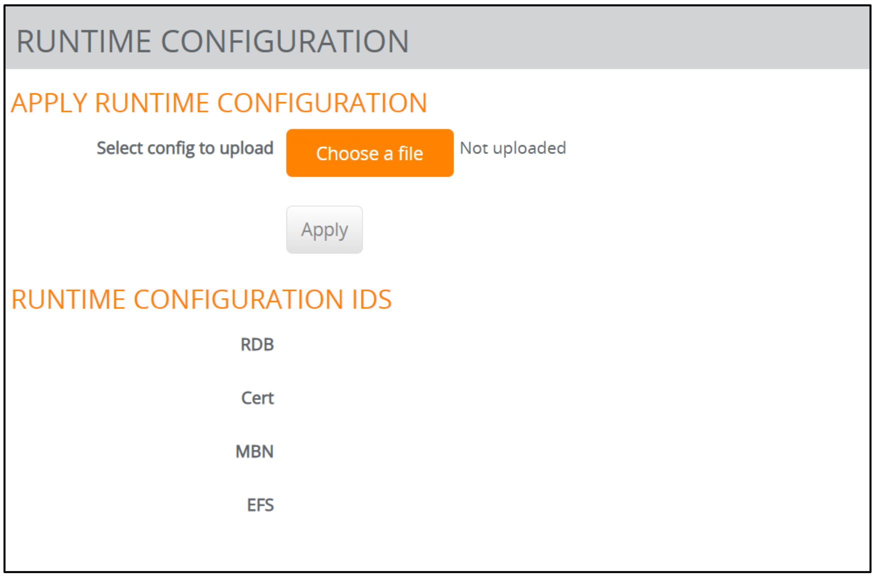


Figure 102 – System configuration – Runtime configuration upload

To apply runtime configuration:

1. Select the Choose a file button and locate the configuration file.
2. Select the file. The word Uploaded appears next to the button.
3. Select the Apply button to install the configuration file.
4. The device automatically reboots after successful upload of the configuration file.

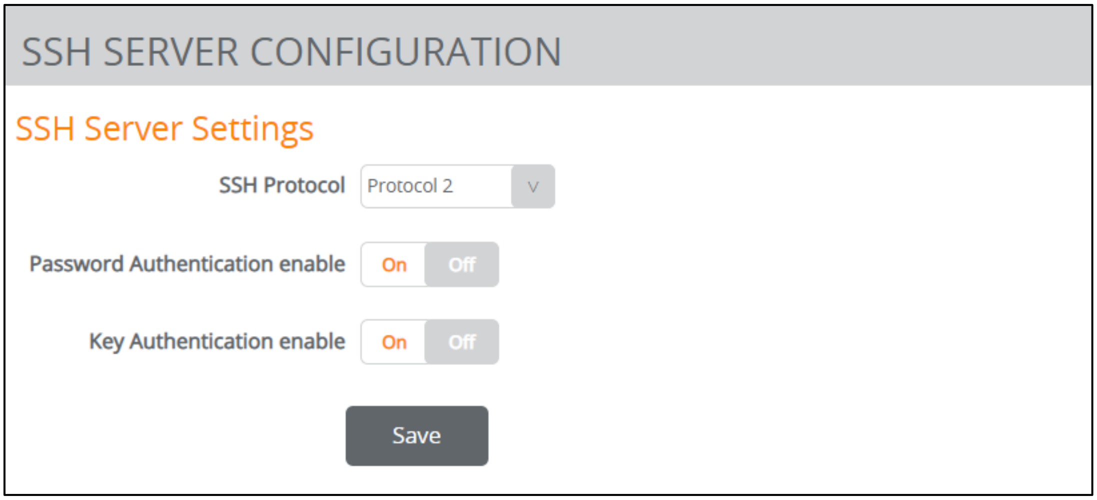
SSH key management

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

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

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

To access the SSH key management page, select the **System** menu then the **Administration** menu on the left and then select on **SSH key management**.



SSH SERVER CONFIGURATION

SSH Server Settings

SSH Protocol: Protocol 2

Password Authentication enable: On

Key Authentication enable: On

Figure 103 – System configuration – SSH server configuration

SSH Server Configuration

To configure the SSH server settings:

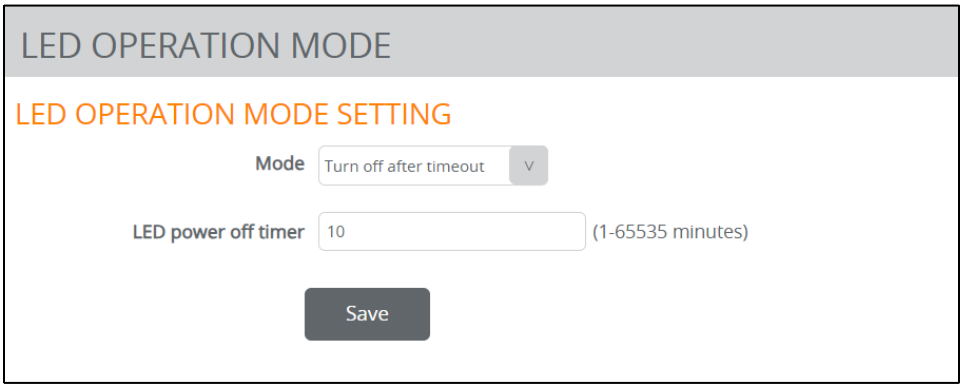
1 Use the **SSH Protocol** drop-down list to select the protocol that you want to use. Protocol 2 is more recent and is considered more secure.

2 Select the type of authentication you want to use by turning the **Enable password** authentication and **Enable key authentication** toggle keys on or off. Note that you may have both authentication methods on, but you may not turn them both off.

3 Select the **Save** button to confirm your settings.

LED operation mode

Use the **LED operation mode** page to control the operation of the LED indicator lights on the NTC-500. 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.



LED OPERATION MODE

LED OPERATION MODE SETTING

Mode: Turn off after timeout

LED power off timer: 10 (1-65535 minutes)

Figure 104 – LED operation mode

Setting the LED operation mode

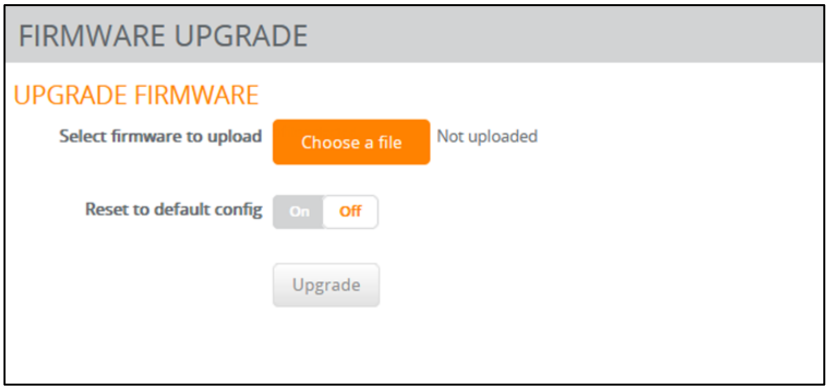
To set the LED operation mode:

1. Use the **Mode** dropdown to set the mode to be configured.
2. If using the **Turn off after timeout** mode, set the LED power off timer to the number of **minutes** that the indicator LEDs should be lit after the device has started.
3. Select the **Save** button to apply the configuration.

Firmware upgrade

To access the **Firmware upgrade** page, select the **System** menu, then **Firmware upgrade.**

The **Firmware upgrade** page allows you to upload firmware files to update the **NTC-500** router. When firmware files have been uploaded, they can also be installed from this page.



FIRMWARE UPGRADE

UPGRADE FIRMWARE

Select firmware to upload Not uploaded

Reset to default config Off

Figure 105 – File uploads

Updating the router firmware

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

To update the NTC-500 router's firmware:

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

2 Log in to the router with the root user account (See the Advanced configuration section for details)

3 Select the **System** item from the top menu bar, then select the **Firmware upgrade** menu item.

4 Under the **Select firmware to upload** section, select the **Choose a file** button. Locate the firmware image file on your computer and select **Open**.

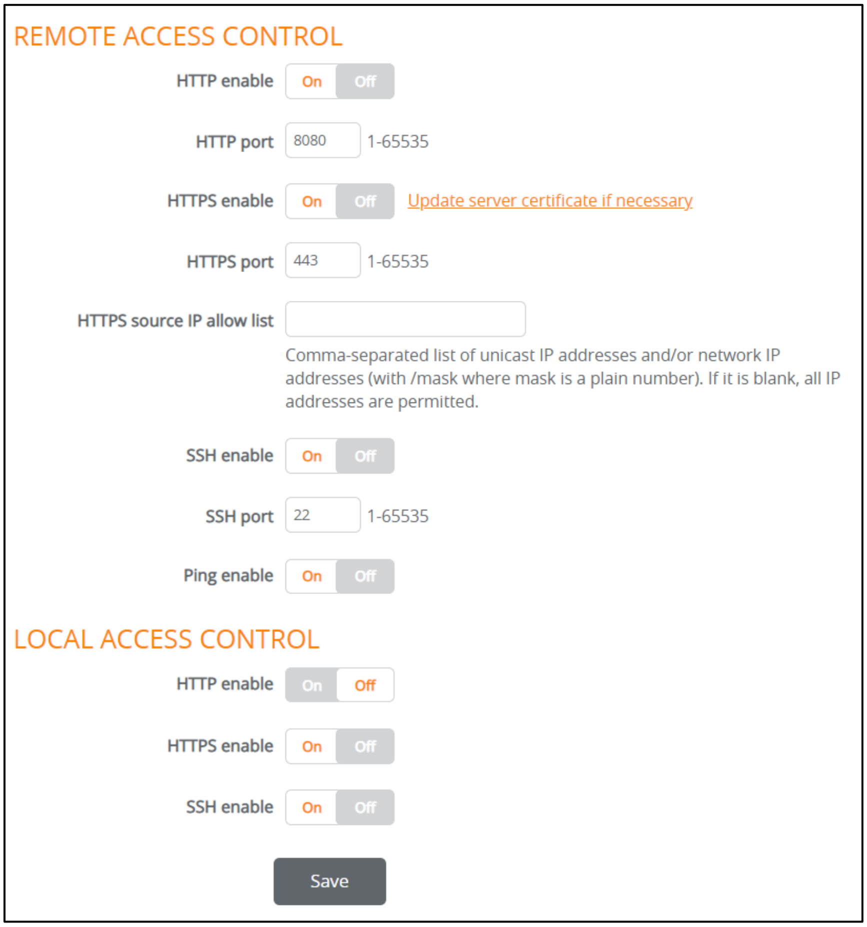
5 If required set the **Reset to default config** toggle to **On** to reset the NTC-500 to the default configuration.

6 Select the **Upgrade** button to upgrade the firmware.

Access control

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

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



REMOTE ACCESS CONTROL

HTTP enable On Off

HTTP port 8080 1-65535

HTTPS enable On Off Update server certificate if necessary

HTTPS port 443 1-65535

HTTPS source IP allow list

Comma-separated list of unicast IP addresses and/or network IP addresses (with /mask where mask is a plain number). If it is blank, all IP addresses are permitted.

SSH enable On Off

SSH port 22 1-65535

Ping enable On Off

LOCAL ACCESS CONTROL

HTTP enable On Off

HTTPS enable On Off

SSH enable On Off

Figure 106 – Access control configuration

OPTION	DEFINITION
Remote Access Control	
HTTP enable	Enable or disable remote HTTP access to the router.
HTTP port	When HTTP is enabled (see previous) you can set the HTTP management port. Enter a port number between 1 and 65534 to use when accessing the router remotely.
HTTPS enable	Enable or disable remote HTTPS access to the router using a secure connection.

HTTPS port	When HTTPS is enabled you can set the HTTPS remote access port. Enter a port number between 1 and 65534 to use when accessing the router remotely over a secure HTTPS connection.
HTTPS source IP allow list	When HTTPS is enabled (see Enable HTTPS above) you can enter a 'whitelist' of IP addresses that will be permitted to access the router. Enter a list of comma-separated unicast IP addresses. You may also enter IP addresses in CIDR notation, however, no spaces are permitted. Note that if this field is left blank, all IP addresses will be permitted to access the router.
SSH enable	Enable or disable Secure Shell on the router.
SSH port	When SSH is enabled you can set the remote SSH access port. Enter the port number for remote SSH access. The port number must be between 1 and 65534.
Ping enable	Enable or disable remote ping responses on the WWAN connection.
Local Access Control	
HTTP enable	Enable or disable local HTTP access to the router. The default setting is disabled.
HTTPS enable	Enable or disable local secure HTTP access (https). The default setting is enabled.
SSH enable	Enable or disable local Secure Shell on the router. The default setting is enabled.
Save button	Select the Save button to save the configuration.

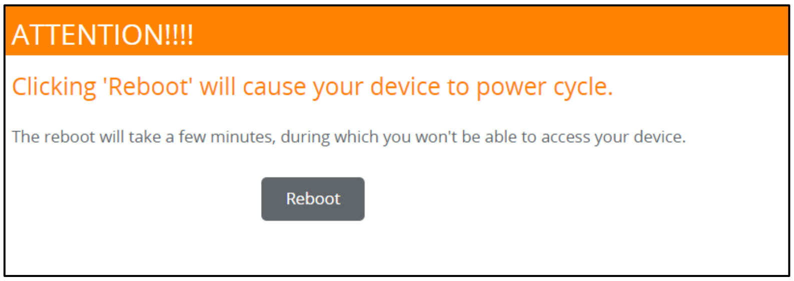
Table 28 – Access control configuration items

Reboot

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

To reboot the NTC-500:

1 Select the System menu item from the top menu bar.



ATTENTION!!!!

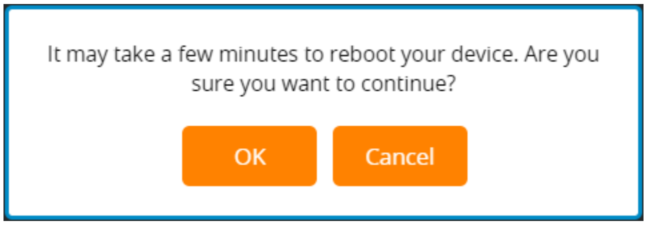
Clicking 'Reboot' will cause your device to power cycle.

The reboot will take a few minutes, during which you won't be able to access your device.

Figure 107 – Reboot

2 Select the Reboot button from the menu on the left side of the screen.

3 The NTC-500 displays a warning that you are about to perform a reboot.



It may take a few minutes to reboot your device. Are you sure you want to continue?

Figure 108 – Reboot – Reboot confirmation

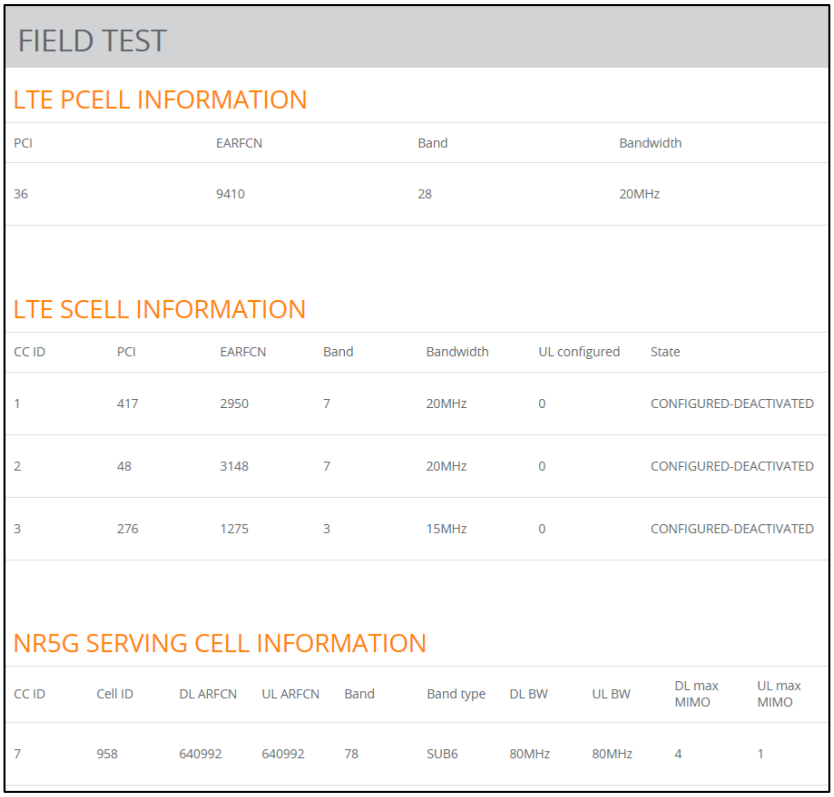
4 If you wish to proceed, select the Reboot button.

5 A warning popup will advise that "It may take a few minutes to reboot your device. Are you sure you want to continue?"

6 Select OK to continue with the reboot process.

Field test

The Field test page contains LTE, LTE SCELL and NR5G cell information which may be useful when troubleshooting signal strength issues. This screen can be found by navigating to System > Field test.



FIELD TEST

LTE PCELL INFORMATION

PCI	EARFCN	Band	Bandwidth
36	9410	28	20MHz

LTE SCELL INFORMATION

CC ID	PCI	EARFCN	Band	Bandwidth	UL configured	State
1	417	2950	7	20MHz	0	CONFIGURED-DEACTIVATED
2	48	3148	7	20MHz	0	CONFIGURED-DEACTIVATED
3	276	1275	3	15MHz	0	CONFIGURED-DEACTIVATED

NR5G SERVING CELL INFORMATION

CC ID	Cell ID	DL ARFCN	UL ARFCN	Band	Band type	DL BW	UL BW	DL max MIMO	UL max MIMO
7	958	640992	640992	78	SUB6	80MHz	80MHz	4	1

Figure 109 – Field Test

LTE PCELL INFORMATION

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

Table 29 – LTE PCELL Information

LTE SCELL INFORMATION

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

Table 30 – LTE SCELL Information

NR5G Serving Cell Information

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

Table 31 - NR5G Serving cell information

Encrypted debuginfo

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

Select the **Generate** button to force the NTC-500 to create a debug file. A success message will appear when the debug file generation is complete. Select the **Download** button to download the generated file.

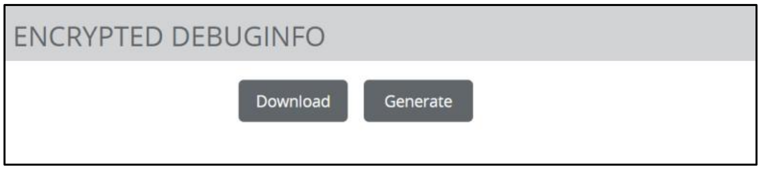


Figure 110 – Encrypted debuginfo download

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.

	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

Appendix table 1 – RAT/Band Selection table

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.

Contact Details

Product sales

Email: cad-sales@casa-systems.com
Website: https://www.casa-systems.com

Warranty and support

For warranty and support please visit https://support.netcommwireless.com/

Contact Details

Australian Office

NetComm Wireless Pty Ltd
18 – 20 Orion Road, Lane Cove
Sydney, NSW, 2066
Australia

+61 2 9424 2070

Head Office US

Casa Systems
100 Old River Road,
Andover, MA 01810
USA

+1 978 688 6706