LANTRONIX®

NTC-201 User Guide

4G LTE CAT 1 BIS Router

Part Number PMD-00338
Revision A July 2026

Trademark Notice

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

Intellectual Property

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

Warranty

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

Contacts

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

Technical Support

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

Sales Offices

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

Disclaimer

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

Important Notice

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

Safety and Hazards

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

Revision History

Date	Rev.	Comments
July 2026	A	Initial Release

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

Contents

List of Tables

1. Overview

Introduction

The Lantronix NTC-201 router is a 4G LTE Cat 1 bis Industrial IoT router that provides reliable and secure connectivity. This document provides information to install, setup, configure, and use the Lantronix NTC-201 router using the web interface.

Target audience

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

Prerequisites

Before continuing with the installation of your NTC-201 router, please confirm that you have the following:

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

Notation

The following symbols may be used in this document:

Note: *This note contains useful information.*

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

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

2. Product introduction

Product overview

- Ruggedized industrial cellular router that supports 4G LTE Cat 1 bis
- Industrial features including a rugged enclosure, a wide operating temperature range, a wide input voltage range, and multiple wall mounting options.
- Intelligent Tri-Color LED display for clear and easy to read modem status information
- Configurable power save mode with minimum current draw when not operational
- VPN support for establishing a secure connection over public cellular network
- Embedded Linux based OS with a 1GHz processor, 256 MB RAM, and 512MB of flash memory storage that allows the installation of custom, edge processing applications. Software Development (SDK) capability
- Web interface for easy centralized configuration and management from any PC and full feature management via secure SMS
- Support for firmware upgrades locally and Over-the-air
- Remote management capabilities with support for TR-069, SNMP, OMA-LWM2M, HTTP/HTTPS, Telnet/CLI, and SMS.
- Roaming algorithm with prioritization for cost effective, flawless network connection across the globe

Product features

The Lantronix NTC-201 router is a feature-packed Industrial IoT device designed to provide real-time wireless connectivity even in harsh environments at an affordable price. The Software Development Kit (SDK) allows you to develop your own software applications for large scale compatibility and an easy path to large deployments across a broad range of industries. The Lantronix NTC-201 router meets the global demand for a reliable and cost-effective Industrial IoT device that successfully caters to mass deployment across businesses.

Package contents

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

- 1 x Lantronix NTC-201 router
- 1 x Two-way Terminal Block connector
- 1 x Cellular antenna
- 1 x 1 m Ethernet cable
- 1 x DIN Rail bracket
- 1 x DIN Rail Adapter bracket
- 1 x Box insert

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

3. Physical dimensions and indicators

Physical dimensions

Figure 3-1 NTC-201 router top view

Table 3-1 NTC-201 router physical dimensions

NTC-201 router dimensions	
Length	105 mm
Width	88 mm
Height	35 mm

Interfaces

The following interfaces are available on the NTC-201 router:

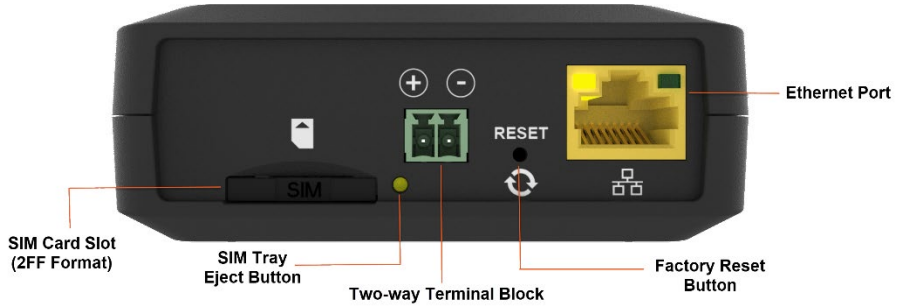


Figure 3-2 NTC-201 router interfaces

Figure 3-3 NTC-201 router interfaces

Table 3-2 Interfaces

Item	Description
Cellular antenna connector	SMA female connector for cellular antenna.
Two-way terminal block	Connect power supply here. Power from a DC power supply may be terminated on terminal block connector and then insert the connector into the terminal block socket on the router. Refer to the diagram and table under the Installation section for correct wiring of the terminal block. Operates in the 8-40V DC range.
Factory Reset button	Press and hold for less than 5 seconds to reboot to normal mode. The green LEDs 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 green LEDs extinguish in sequence and once the last LED extinguishes, the LEDs turn amber. The amber LEDs extinguish in sequence to indicate that the router will reboot to recovery mode if the button is released during this period.

	Press and hold for 15 to 20 seconds to reset the router to factory default settings. The green LEDs extinguish in sequence and once the last LED extinguishes, the LEDs turn amber. The amber LEDs extinguish in sequence and once the last LED extinguishes the LEDS turn red. The red LEDs extinguish in sequence to indicate that the router will reset to factory default settings if the button is released during this period.
SIM card slot	Insert SIM card here.
SIM Tray Eject button	Push to open SIM tray.
RJ45 Ethernet port	Connect a device here using an ethernet cable. You can also connect a network switch through which you can connect several devices.

LED indicators

The NTC-201 router uses LEDs to display the current system and connection status.

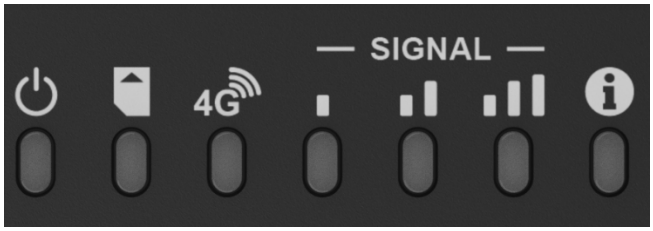


Figure 3-4 NTC-201 router LED indicators

Table 3-3 LED indicators

LED	Name	Color	State	Description
	Power		Off	Power off
			Blinking	Powering up
			On	Power on
	SIM		Off	No SIM detected
			Blinking	SIM error
			On	SIM installed and working
	4G Network		Off	No 4G network connection
			Blinking	Connecting to 4G network
			On	Connected to 4G network
			Off	No signal

LED	Name	Color	State	Description
— SIGNAL —	Signal Strength	■	One lit	Poor signal
		■ ■	Two lit	Fair signal
		■ ■ ■	Three lit	Good signal
	Custom indicator	Customizable		Programmable LED for custom use

Note: *The custom indicator LED is currently not functional.*

Signal strength LEDs

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

LTE signal mapping (Green)

Table 3-4 Signal strength LED descriptions

Number of lit LEDs	Signal Strength
0	No signal
1	−119 dBm to −105 dBm
2	−104 dBm to −90 dBm
3	≥ −89 dBm

LED update interval

The signal strength LEDs update within a few seconds with a rolling average signal strength reading. When selecting a location for the router and connecting 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-201 router has two LED indicators on it.

Figure 3-5 NTC-201 router ethernet port LED indicators

Table 3-5 Ethernet port LED indicators description

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

4. Placement of the router

The external high-performance antenna supplied with the router is designed to provide optimum cellular signal strength in a wide range of environments. If you find the signal strength is weak, try adjusting the orientation of the antennas. If you are unable to get an acceptable signal, try moving the router to a different place or mounting it differently.

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

Mounting options

The NTC-201 router can be mounted in a variety of locations.

DIN rail mounting bracket

The DIN rail mounting bracket provides multiple ways to mount the router.

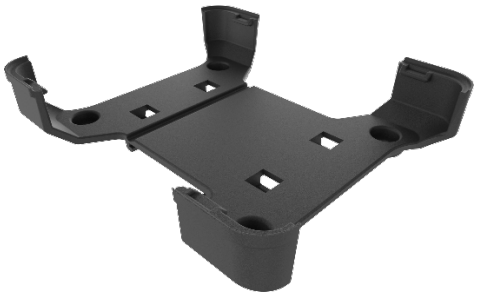


Figure 4-1 DIN rail bracket

Snap the router into the bracket as shown below.

Figure 4-2 Snapping router into bracket

Horizontal DIN rail mounting adapter

The horizontal DIN rail mounting adapter, used in conjunction with the DIN rail mounting bracket allows you to mount the NTC-201 router in a horizontal orientation. With the DIN rail mounting bracket attached to the router, slide the adapter on to the bracket as shown in the image below. You can then mount the device horizontally on a DIN rail. Optionally, you may place a screw (max. 4.5mm diameter) through the centre hole of the adapter so that it doesn't move along the DIN rail.

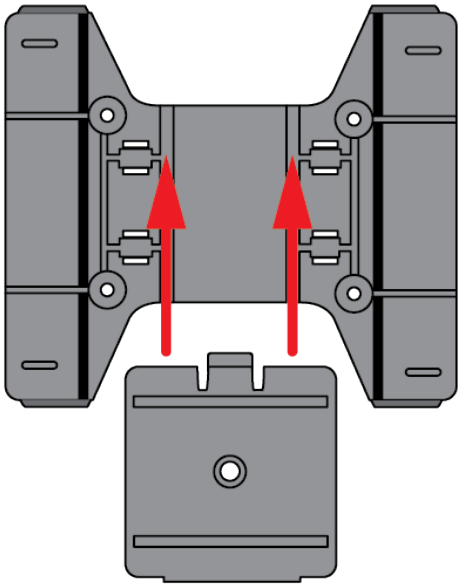


Figure 4-3 DIN rail mounting adapter

DIN rail installation

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

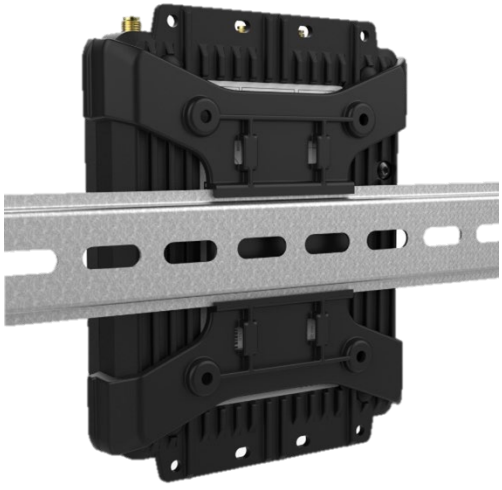


Figure 4-4 DIN rail installation

Wall mount with DIN rail mount adapter

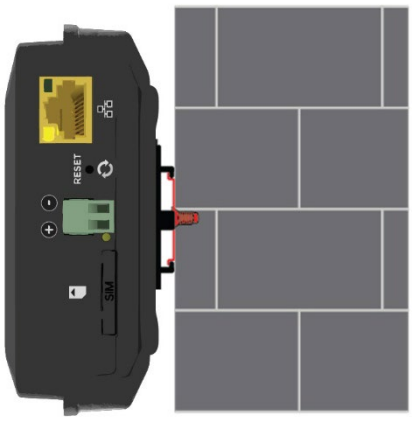


Figure 4-5 Wall mount with DIN rail mount adapter

Wall mount via DIN rail bracket

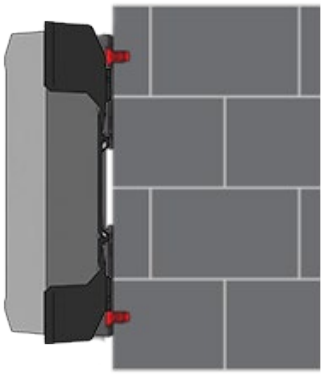


Figure 4-6 Wall mount via DIN rail bracket

DIN rail mount

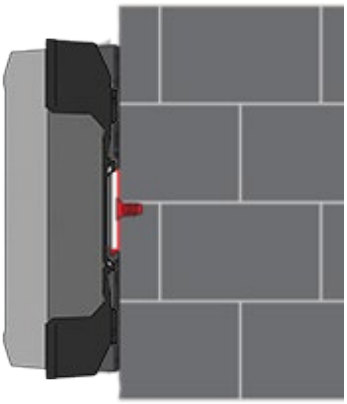


Figure 4-7 DIN rail mount

Ceiling mount via DIN rail bracket

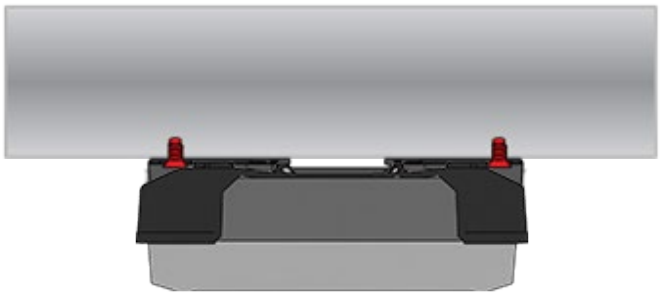


Figure 4-8 Ceiling mount via DIN rail bracket

Pole mount using DIN rail bracket

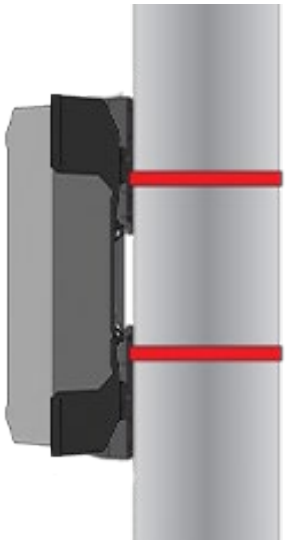


Figure 4-9 Pole mount using DIN rail bracket

Desk mount

Figure 4-10 Desk mount

5. Installation and configuration of the NTC-201 router

Powering the router

The NTC-201 router can be powered in one of two ways:

- DC power input via separately purchased DC power supply (8-40 V DC)
- DC power input via field terminated power source (8-40 V DC)

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

DC power via separately purchased DC power supply

The positive and ground terminals on the 2-pin connector can accept power from a separately sold DC power supply. Both a standard temperature range DC power supply and an extended temperature range DC power supply are available to purchase as accessories.

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

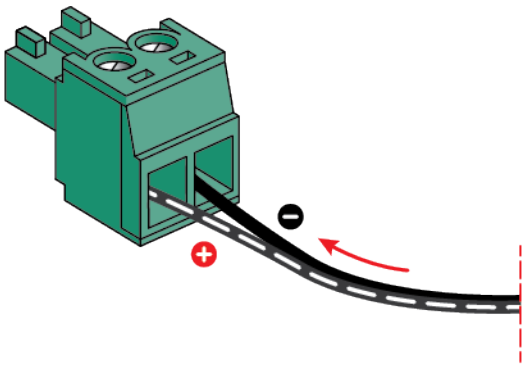


Figure 5-1 Terminal block wiring diagram

Figure 5-2 Terminal Block pinout

DC power via field terminated power source

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

Table 5-1 Locking power block pin outs

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

Power consumption

To assist with power consumption planning, the following table summarises average power consumption during the various states of the NTC-201 router under normal usage conditions. It is important to note that this table serves as an indication only as the power consumed by the device is affected by many variables including signal strength, network type, and network activity.

Table 5-2 Average Power Consumption

Input Voltage (V)	State	Current Consumption (mA)	Power Consumption (mW)	Remarks
12	Power on, all functions disabled (sleep)	55	662	
12	Power on, connected to LTE and idle	151	1807	Signal strength: -68 to -74 dBm
12	Power on and connected to LTE – Packet data transfer with heavy load	187	2238	
12	Power on and connected to LTE – Worst signal and idle	155	1857	Signal strength: -85 to -90 dBm
12	Power on and connected to LTE – Worst signal and data transfer with heavy load	186	2236	

Viewing power source information

You can use the Software Development Kit to access this information for advanced purposes (e.g. configuring SMS alerts to inform you of the power status of the router).

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-201 router. You can connect one device directly, or several devices using a network switch.
2. The NTC-201 router is shipped with a cellular antenna. Screw the antenna onto the antenna connector by turning it in a clockwise direction. Please refer to the Interfaces section for the antenna connector layout.

3. If your router does not come with a pre-installed SIM, insert a SIM card into the SIM card slot. Press the SIM Eject button to eject the SIM card tray, place the SIM card in the tray and then insert the loaded tray into the SIM slot with the gold side facing up, as shown below.

Figure 5-3 Inserting the SIM card

4. Ensure the external power source is switched on and wait 2 minutes for your NTC-201 router to start up and connect to the mobile network. Your router arrives with preconfigured settings that should suit most customers. To check the status of your router, compare the LED indicators on the device with those listed in the LED indicators table.

6. Advanced configuration

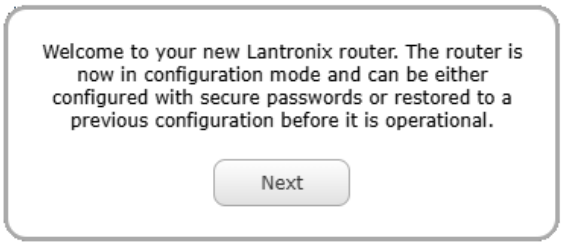
To access the web-based user interface of the NTC-201 router:

1. Establish a direct ethernet connection between your PC and the router using the ethernet cable.
2. Open a web browser (e.g. Mozilla Firefox or Google Chrome), type https://192.168.1.1 into the address bar, and press **Enter**.
3. The web interface of the router displays.

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

Initialization

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

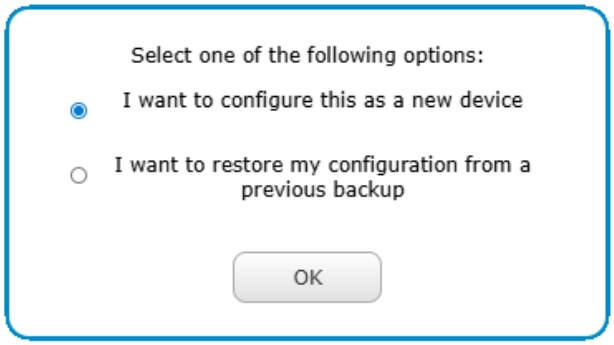


In Configuration mode, the router runs a setup wizard. Once you complete the setup wizard the router will boot into Live mode. This is a security feature which enables you to configure the router as a new device and set strong passwords for web root, web user, and Telnet/SSH access or restore configuration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

To complete the setup:

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

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



3. Select whether to configure the router as a new device or to restore a previous configuration backup and click **OK** (see Configure as a new device and Restore backed up configuration settings for further configuration details).

Configure as a new device

To configure the router as new device:

1. Select ⊙ **I want to configure this as a new device in the** Initialization section and click **OK**. The New passwords page displays.

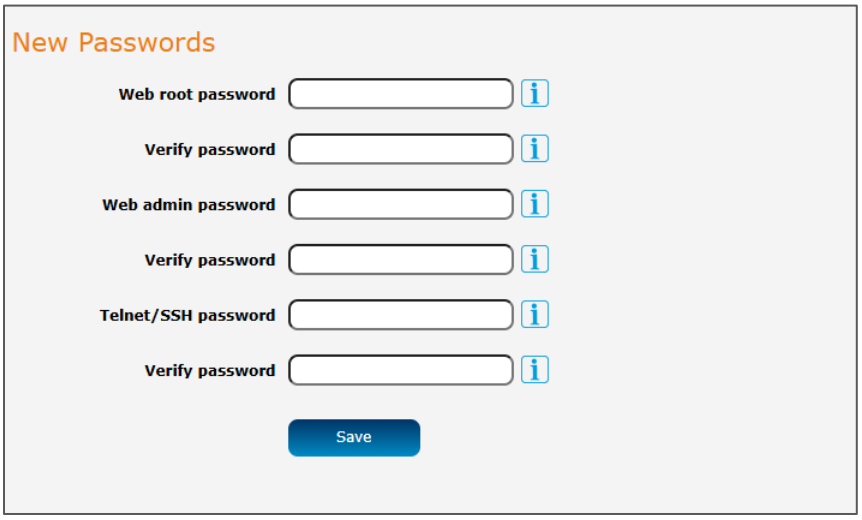
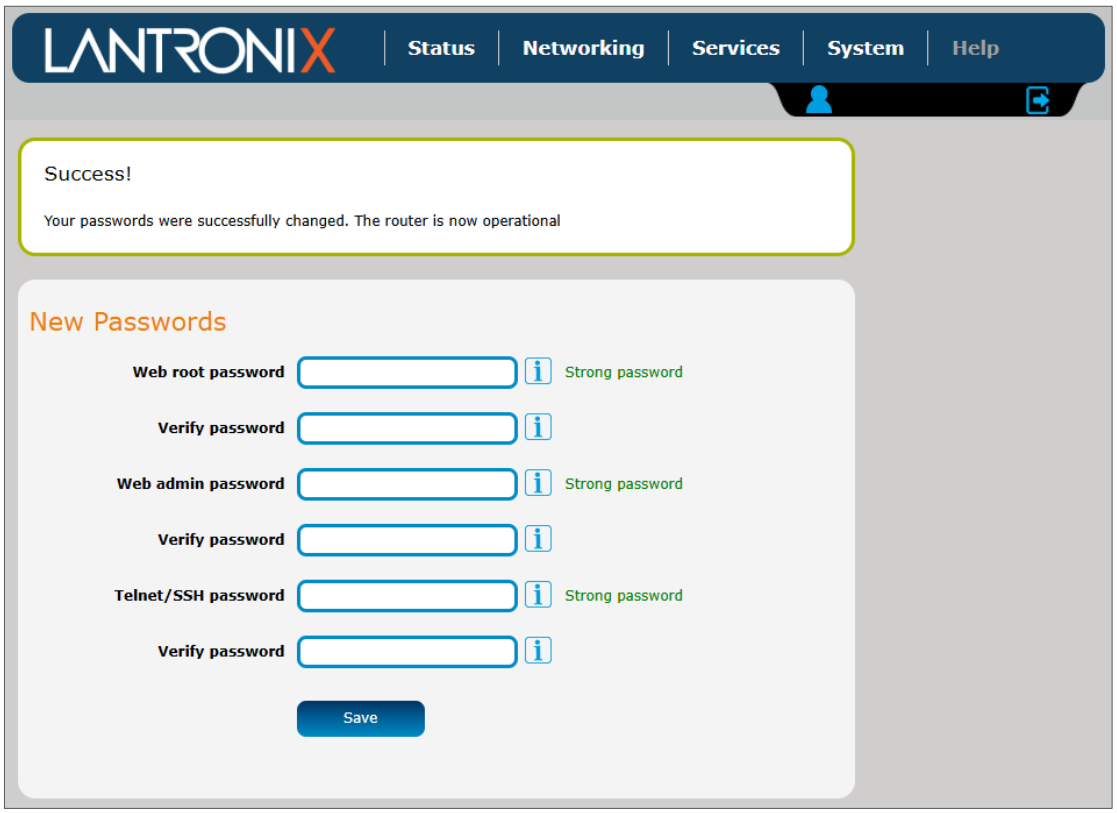


Figure 6-1 New Passwords page

2. Enter a strong password for each user. You can use 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.

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

3. Once you have entered values for all the fields click **Save**. If the passwords meet the security criteria, they are saved and the below success message displays.



4. Click the icon, the login page displays.

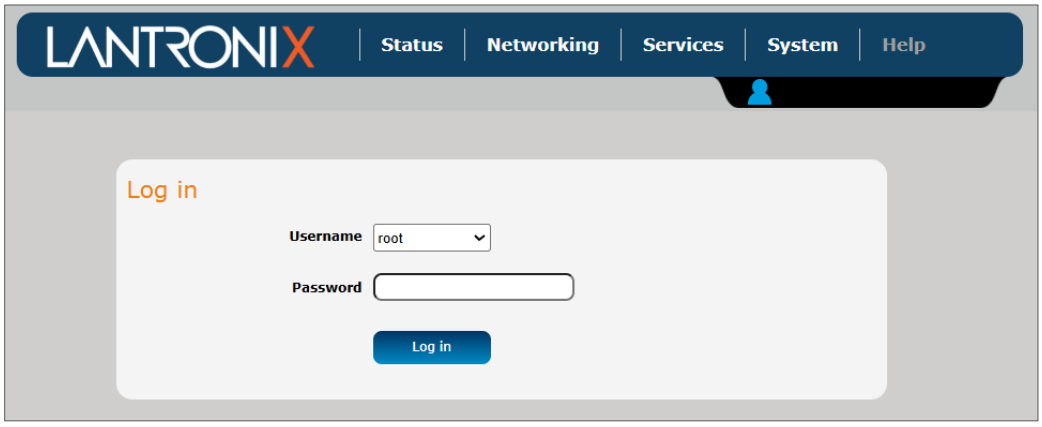


Figure 6-2 Login page for the web-based user interface

Restore backed up configuration settings

To restore configuration from a backup file:

1. Select ⊙ **I want to restore my configuration from a previous backup** in the Initialization section and click **OK**. The Restore saved settings window displays.

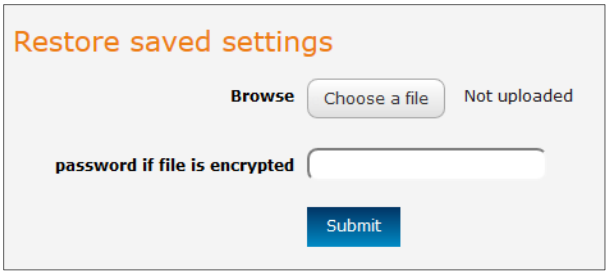


Figure 6-3 Restore backup page

2. Click **Choose a file**, locate and select the backup file on your computer.
3. If the backup file is encrypted, enter the password in the **password if file is encrypted** field and click **Submit**.
4. The router restores the previous configuration and then the login page displays.

Logging in

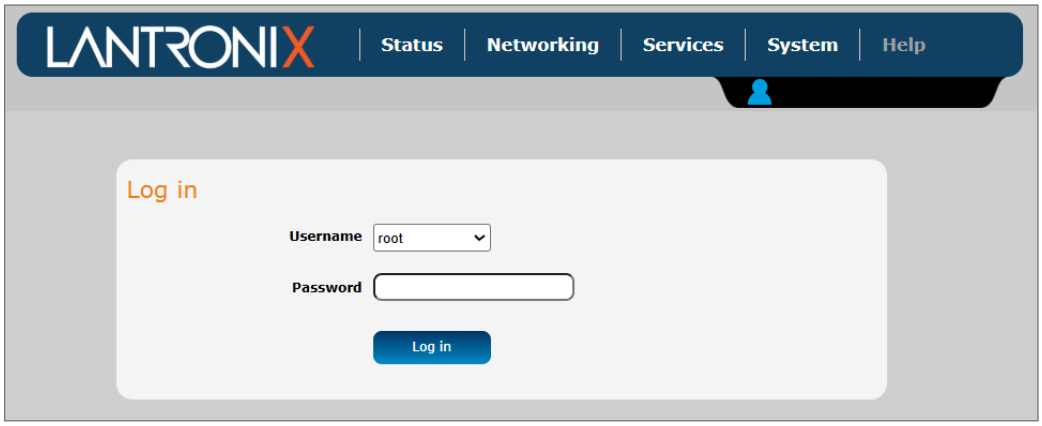


Figure 6-4 Login page for the web-based user interface

To log into the router:

1. In the **Username** field, select the user account you want to use to log in.
2. In the **Password** field, enter the password for the selected user account.
3. Click **Log in**, the Status page displays.

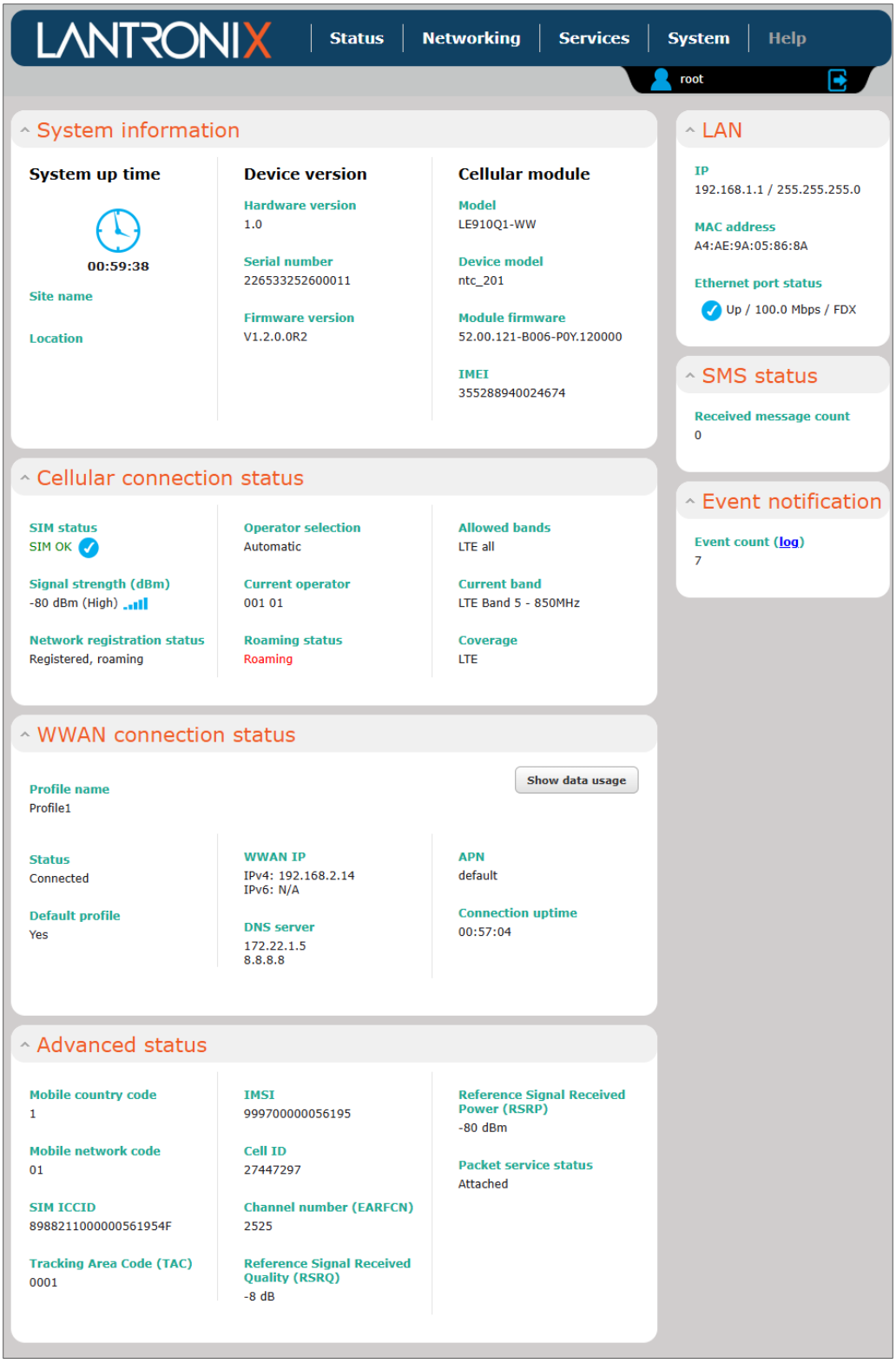


Figure 6-5 Status page

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

7. Status

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

- System Information
- Cellular connection status
- WWAN connections status
- Advanced status
- LAN
- SMS status
- Event notification

The Status page is displayed when you log into the NTC-201 router web interface after initialization or reboot. When using the web interface, you can click **Status** tab on the top menu bar to access the Status page. On the Status page click each section tab to show or hide the details in that section. New sections are added to the Status page for additional software features when enabled (e.g. VPN connectivity).

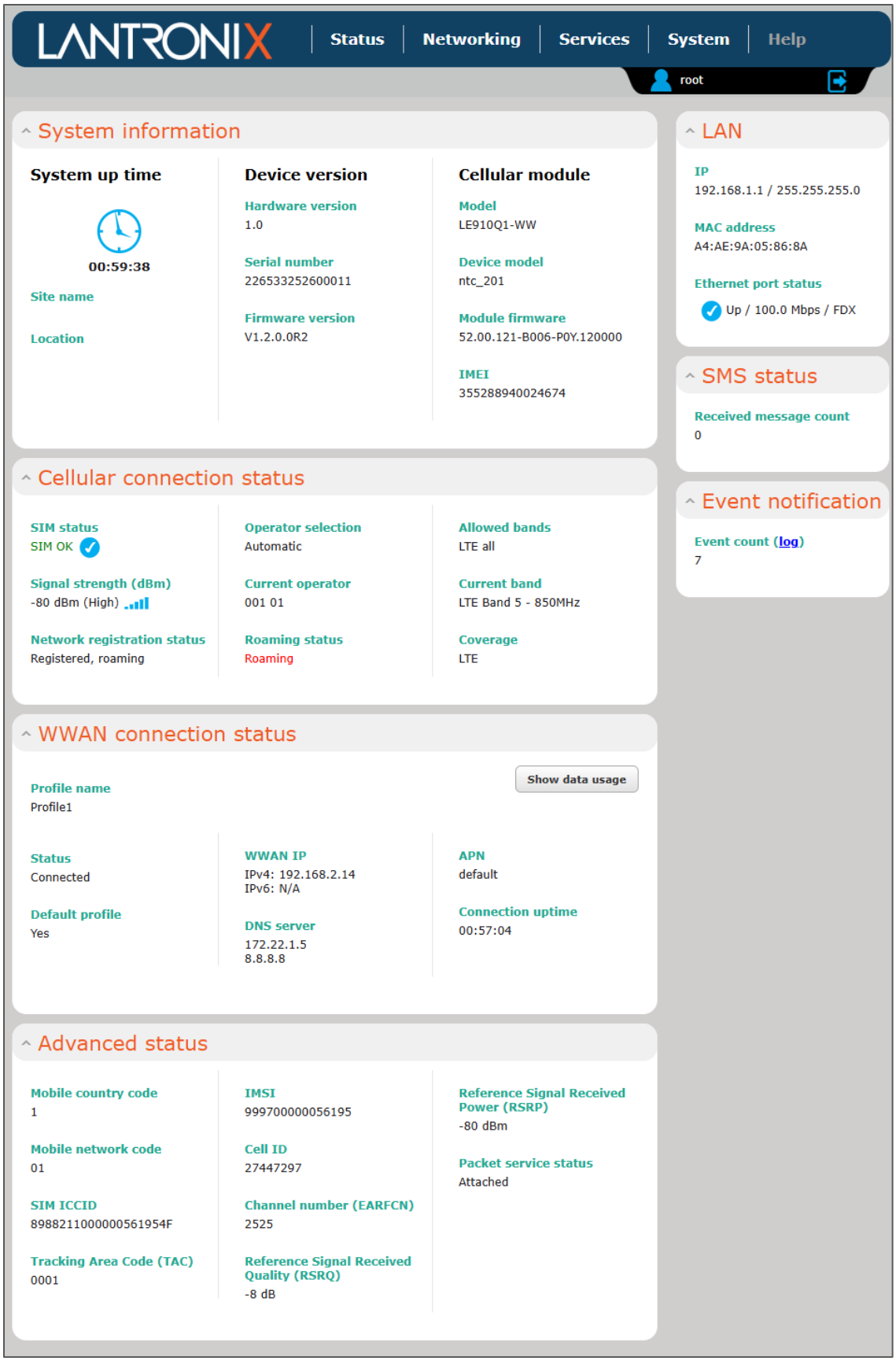


Figure 7-1 Status page

Table 7-1 Status page details

Parameter	Description
System information	
System up time	The current up time of the router (the time since the router was last turned on).
Site name	The configured site name.
Location	The configured location.
Hardware version	The hardware version of the router.
Serial number	The serial number of the router.
Firmware version	The current firmware version of the router.
Model	The model of the cellular module.
Device model	The model of the router.
Module firmware	The current firmware version of the cellular module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
Cellular connection status	
SIM status	Displays the SIM status of the router. It shows if a SIM is inserted and whether it is active.
Signal strength (dBm)	The current signal strength measured in dBm.
Network registration status	It shows if the SIM is registered on the network.
Operator selection	The mode used to select an operator network.
Current operator	The operator of the network on which the device is currently registered.
Roaming status	The roaming status of the connected network.
Allowed bands	The bands to which the router can connect.
Current band	The current band in use.
Coverage	The mobile network currently is use (e.g., 2G, 3G, LTE etc.).
WWAN connection status	
Profile name	The name of the active profile.
Status	The connection status of the active profile.
Default profile	Indicates whether the current profile in use is the default profile.

Parameter	Description
WWAN IP	The IP address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary DNS servers for the WWAN connection.
APN	The Access Point Name currently in use.
Connection uptime	The duration of the current mobile connection session.
Show data usage button	Click to display the session details and data usage details. For each session you can select **Show duration** or **Show end time**. To close the display click **Hide data usage** button.
Advanced Status	
Mobile country code	The Mobile Country Code (MCC) of the router.
Mobile network code	The Mobile Network Code (MNC) of the router.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the router. A unique number up to 19 digits in length.
Power input mode	The power supply mode that is currently in use.
Tracking Area Code (TAC)	The ID of the cell tower grouping from which the current signal is broadcast.
IMSI	International Mobile Subscriber Identity. It is a unique identifier for the user of a cellular network.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile network signal.
Channel number (EARFCN)	The channel number of the current cellular connection.
Reference Signal Received Quality (RSRQ)	RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by N x RSRP / RSSI where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.
Reference Signal Received Power (RSRP)	Average power received from a single reference signal within a specific bandwidth.
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.
LAN	
IP	The IP address and subnet mask of the router.
MAC address	The MAC address of the router.
Ethernet Port Status	Displays the status of the LAN port and its operating speed.

Parameter	Description
SMS status	
Received message count	Number of SMS messages received.
Event notification	
Event count (**log**)	Displays the number of notifications sent using the Event notification feature. Click **log** to display the Event notification log.

8. Networking

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

- Wireless WAN
- LAN
- Ethernet LAN/WAN
- PPPoE
- Routing
- VPN

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

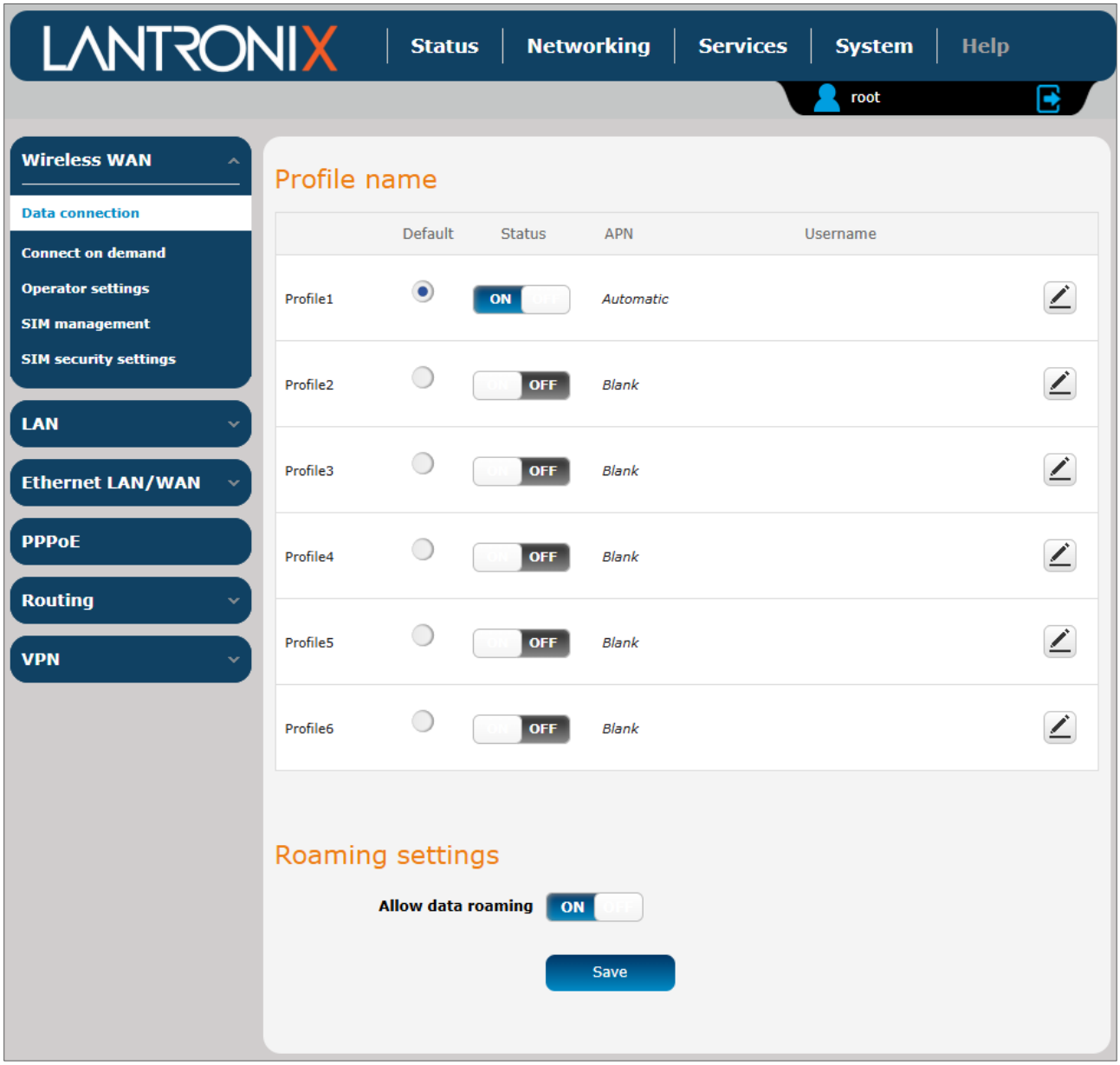


Figure 8-1 Networking page

Wireless WAN

Data connection

The Data connection page allows you to configure, enable, and disable connection profiles. To access this page, navigate to **Networking > Wireless WAN > Data connection**.

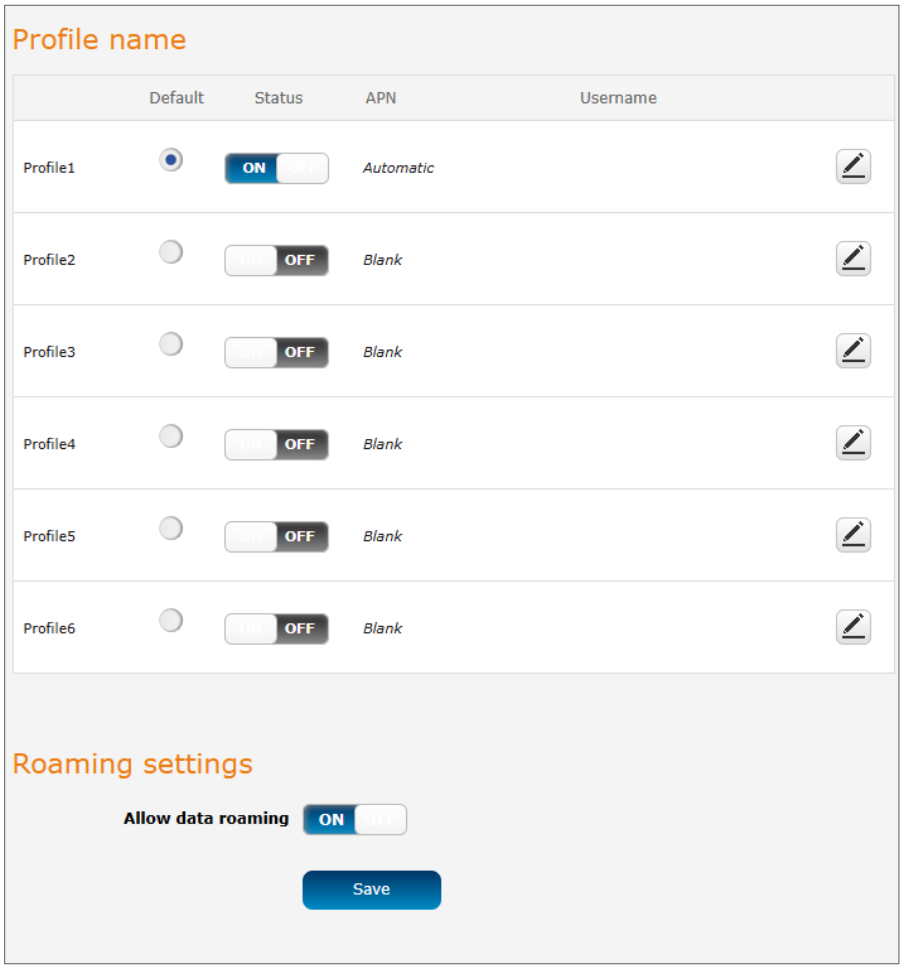


Figure 8-2 Data connection settings

Each profile refers to a set of configuration items which are used by the router to activate a Packet Data Protocol (PDP) context. You can enable a single profile to establish connection.

Table 8-1 Data connection details

Parameter	Description
Profile name (Displays the list of available profiles)	
Default	Select to set the profile as default gateway for all outbound traffic except for which there are configured static route rules or profile routing settings.
Status	Set to **ON** to enable.
APN	The APN configured for the profile.

Parameter	Description
Username	The username for the configured APN.
	Click to manually configure a connection profile.
Roaming Settings	
Allow data roaming	Set to **ON** to enable.

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

The router supports the configuration of up to six APN profiles. These profiles allow you to configure the settings that the router will use to connect to the cellular network and switch easily between different connection settings.

To manually configure a connection profile:

1. Click  button corresponding to the profile that you want to configure. The configuration settings display.

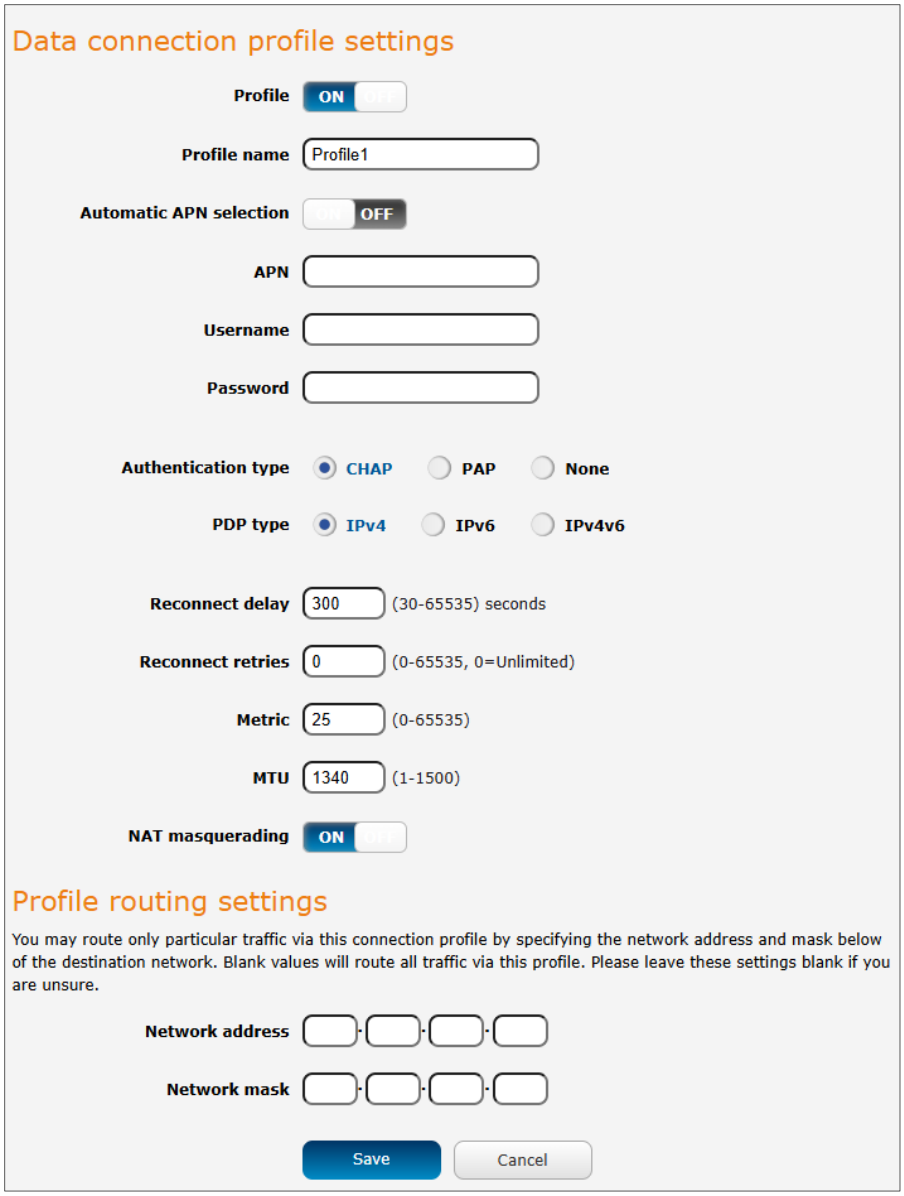


Figure 8-3 Data Profile configuration page

Table 8-2 Data Profile Configuration details

Parameter	Description
Data connection profile settings	
Profile	Set to **ON** to enable.
Profile name	Enter profile name.
Automatic APN selection	Set to **ON** to enable. When enabled the most appropriate APN will be chosen based on the MCC and MNC contained in your SIM card. When disabled, the below fields display: • **APN** - Enter the APN name (Access Point Name)

Parameter	Description
	• **Username** – Enter the username for the APN. • **Password** – Enter the password for the APN. • **Authentication type** - Select **CHAP**, **PAP** or **None**, depending on the type of authentication used by your network provider. • **PDP type** – Select PDP type: ○ **IPv4** – Sets a single stack IPV4 connection through which the router receives only IPV4 network and DNS addresses. ○ **IPv6** – Sets a single stack IPV6 connection through which the router receives only IPV6 network and DNS addresses.  ***Note**: Check with your carrier to confirm that single stack IPV6 connectivity is supported.* ○ **IPv4v6** – Sets a dual stack connection allowing simultaneous IPV4 and IPV6 network connectivity. The router receives both IPv4 and IPV6 network and DNS addresses.
Reconnect delay	Enter the time is seconds the router waits before attempting to reconnect after a connection failure.
Reconnect retries	Enter the number of times the router attempts to reconnect to the network after a disconnection or a failed connection attempt.
Metric	Enter Metric value. The Metric value is used by router to prioritize routes (if multiple are available) and is set to 25 by default. This value is sufficient in most cases, but you may modify it if you are aware of the effect your changes will have on the service.
MTU	Enter the Maximum Transmission Unit (MTU) value. The MTU size value is specific to your carrier and the value will be automatically displayed in this field once the carrier network registration is complete.
NAT masquerading	Set to **ON** to enable. NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode the router modifies network traffic sent and received, to inform remote computers on the internet that packets originating from a machine behind the router originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required, and local devices require WAN IP addresses.
Profile routing settings*	
Network address	Enter network address of the remote network.
Network mask	Enter network mask of the remote network.

For advanced networking, you can configure a particular profile to route only certain traffic via that profile with a custom address and mask for traffic to send via that profile. To do this, in the **Profile Routing section, enter the **Network address** and **Network mask** of the remote network. If you do not*

want to use this feature, or are unsure, please leave these fields blank. This will not designate any traffic to be routed via this profile.

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

To confirm as successful mobile broadband connection, go to Status page. In the WWAN connection status section, the Status shows connected.

Connect on demand

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

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

To access Connect on demand page navigate to **Network > Wireless WAN > Connect on demand**. The Connect on demand page displays.

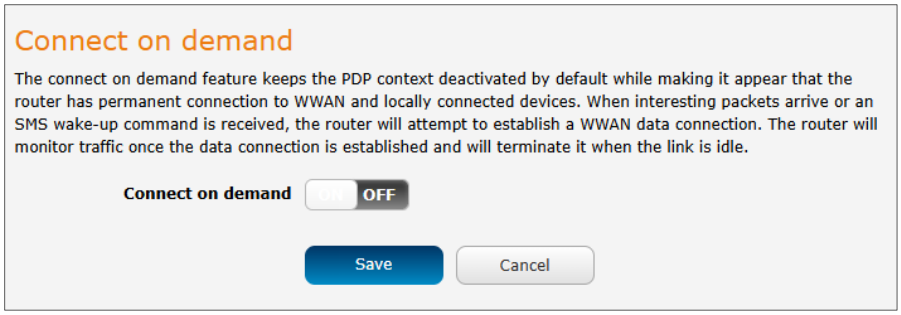


Figure 8-4 Connect on demand

Set **Connect on demand** to **ON** to enable it. The different connection settings display.

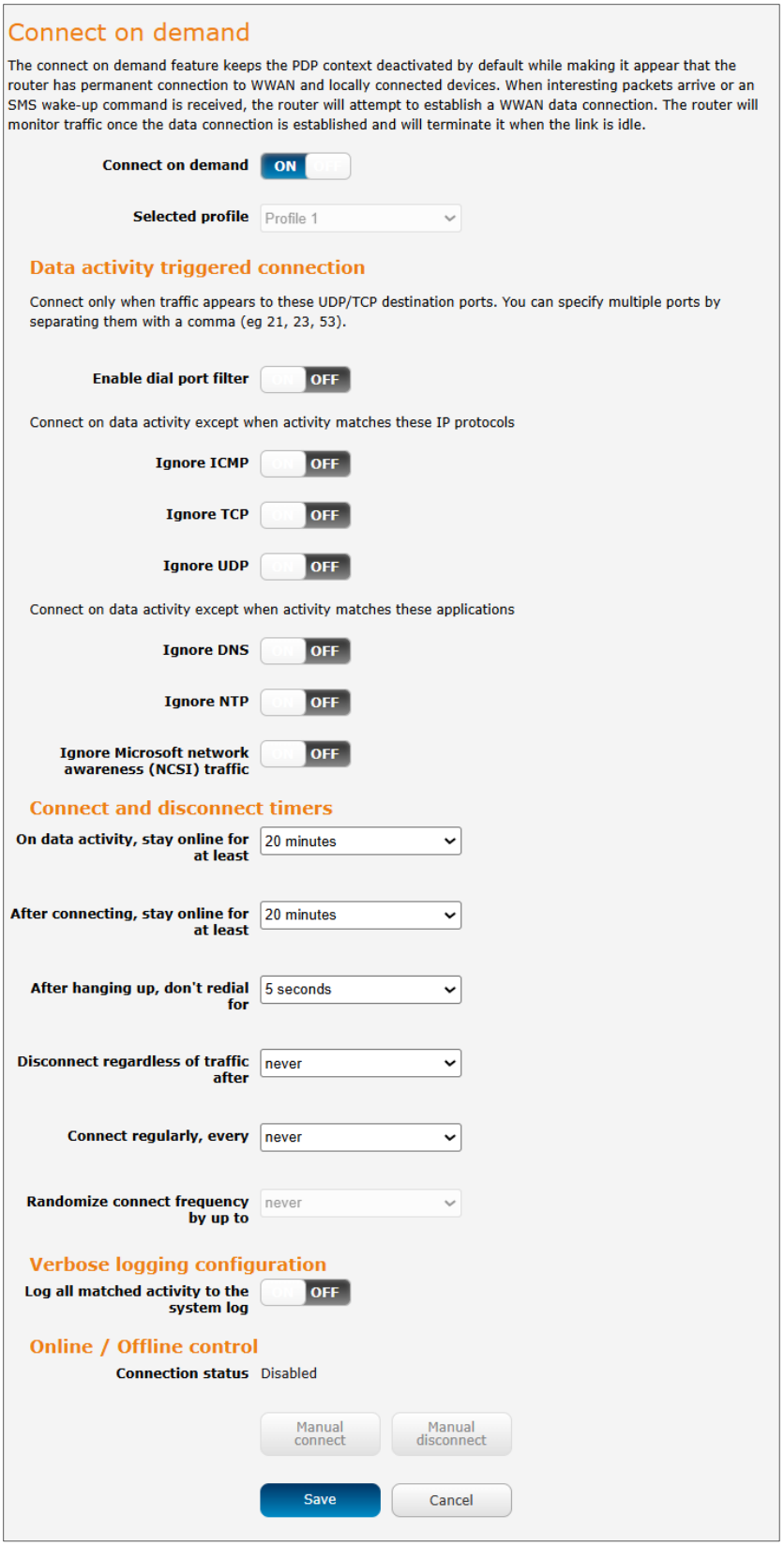


Figure 8-5 Connect on demand settings

The **Selected profile** drop-down list is greyed out and is used to display the currently selected default profile for which the Connect on demand configuration will apply.

Data activity triggered connection

You can use this feature to establish connection only when the traffic appears on certain destination ports. To use this feature, set **Enable dial port filter** to **ON** and enter the port number or list of port numbers separated by commas. When you select this option, all outbound TCP/UDP packets to any remote host on the specified port(s) will trigger the connection to dial. Note that when this feature is enabled, the options to ignore specific packet types are not available.

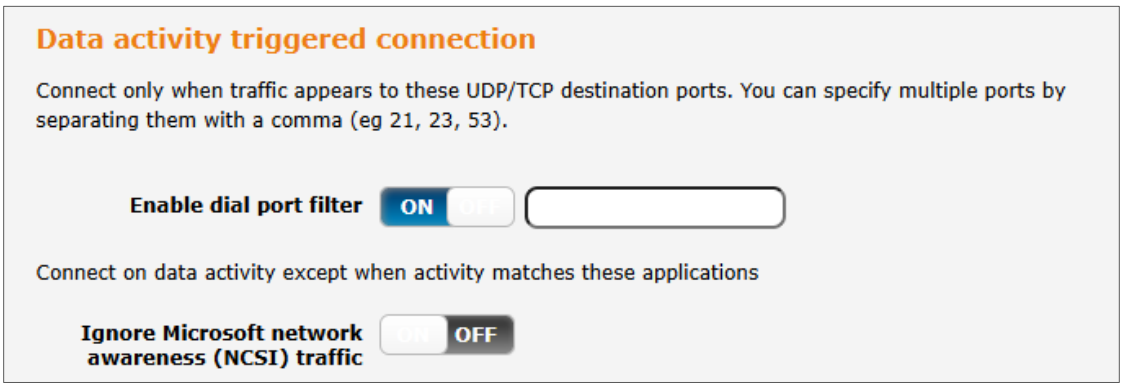


Figure 8-6 Data activity triggered connection

You can set **Ignore Microsoft network awareness (NCSI) traffic** to **ON** to prevent this traffic from triggering a connection or set it to **OFF** to allow this traffic.

When **Enable dial port filter** is set of **OFF**, the below conditions for connection display.

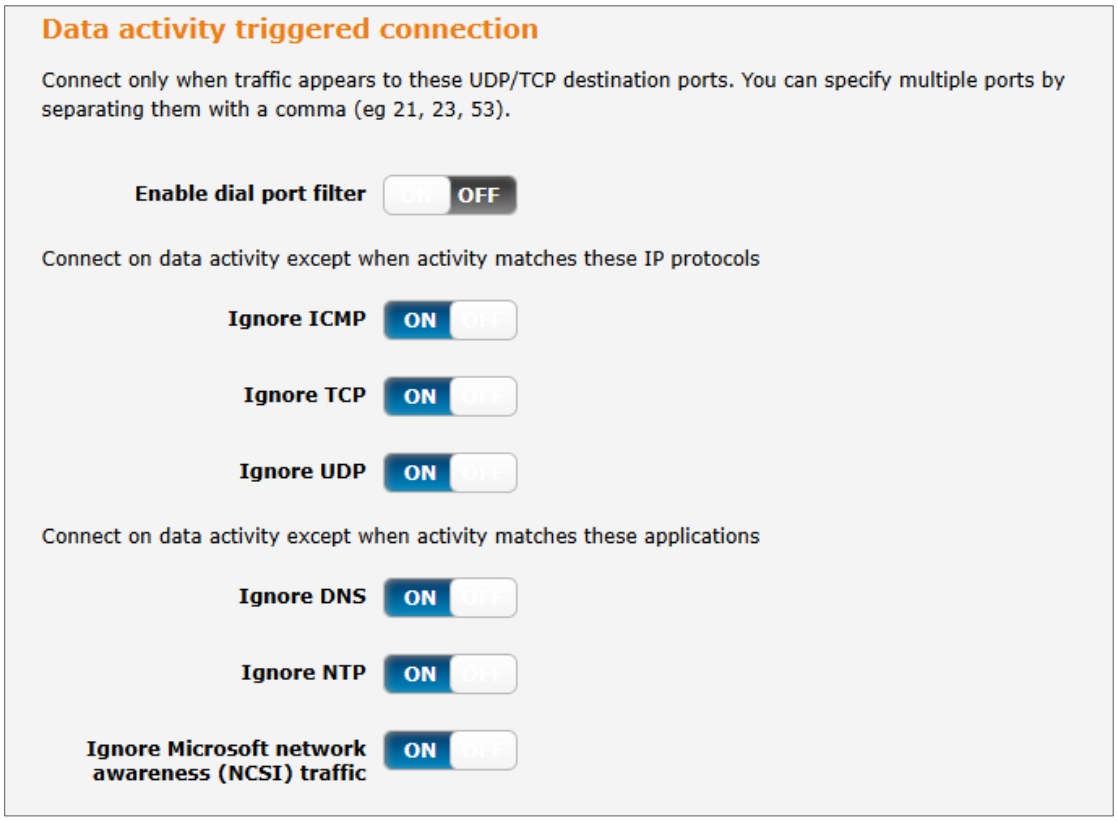


Figure 8-7 IP protocol and application conditions

Set the following connect conditions for IP protocols:

- **Ignore ICMP** – Set to **ON** to enable.
- **Ignore TCP** – Set to **ON** to enable.
- **Ignore UDP** – Set to **ON** to enable.

Set the following connect conditions for applications:

- **Ignore DNS** – Set to **ON** to enable.
- **Ignore NTP** – Set to **ON** to enable.
- **Ignore Microsoft network awareness (NCSI) traffic** - Set to **ON** to enable.

Connect and disconnect timers

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

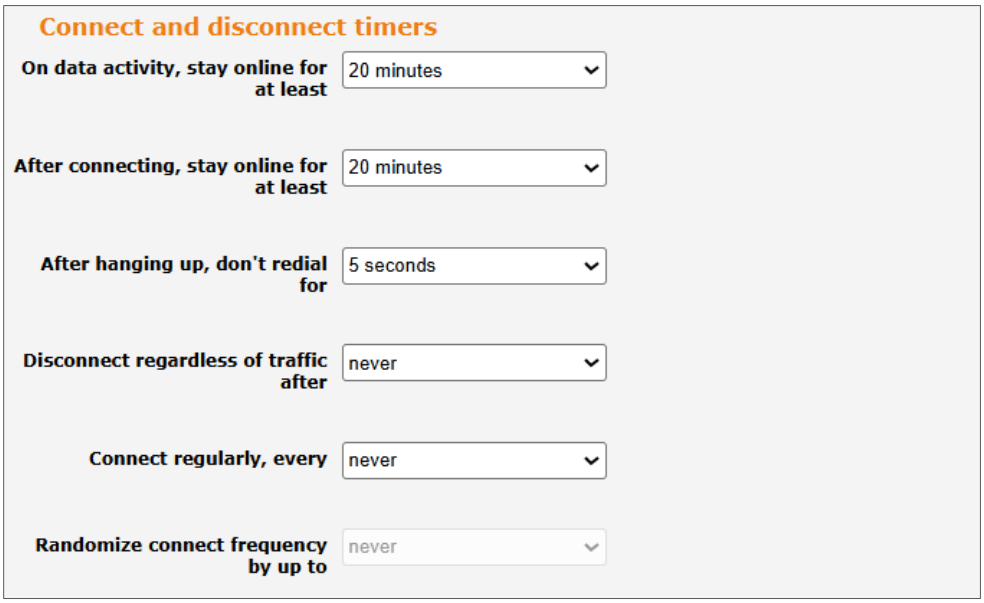


Figure 8-8 Connect and disconnect timers

Table 8-3 Description of connect and disconnect timers

Parameter	Description
On data activity, stay online for at least	Select the required value. When traffic as per the configured settings above appears, the router will either continue to stay online or dial a connection and will not disconnect it for the specified time (min. 1 minute, max. 1 hour). This timer is continuously reset throughout the duration of a dial-up session, whenever data activity is detected matching the rules above.
After connecting, stay online for at least	Select the required value. This timer configures the router to not hang-up the connection for the specified time after initially dialing the connection. This setting cannot be less than the stay online period above. This timer affects the connection only once per dial up session, at the beginning of the session.
After hanging up, don’t redial for	Select the required value. After a connection has been disconnected, you can tell the router to rest for certain period before re-dialing.

Parameter	Description
Disconnect regardless of traffic after	Select the required value. Forces the router to disconnect the connection regardless of the traffic passing through it. The default setting is never.
Connect regularly, every / Randomize connect frequency by up to	Select the required value. If you want to have the router dial a connection at regular intervals, use **Connect regularly, every** to specify the interval between dials. Setting this to **never** effectively disables this option. The router also features the ability to randomize the time at which the first dial action is performed. This is useful in situations where you have numerous routers in an area where a power outage has occurred. Setting a random dial time helps reduce network congestion when all the routers are powered on, and they do not all try to connect simultaneously. When **Connect regularly, every** is set to at least 2 minutes, you are able to configure the router to randomize the time it begins to dial. The randomized dial timer only affects the initial dial after the unit powers on or after the settings are saved. For example, if you configure the router to dial every 2 minutes with a randomized dial starting time of 1 minute, the router waits for the Connect regularly, every time (2 minutes) and then randomly selects a time less than or equal to the Randomize connect frequency by up to time (1 minute). After the randomly selected time has elapsed, the router dials the connection. After the first dial, the router dials the connection every 2 minutes, ignoring the Randomize connect frequency by up to time.

Verbose logging configuration

The router provides the option to log all the data activity which matches the settings for the Connect on demand feature, for advanced troubleshooting purposes. To enable the recording of detailed logs, set **Log all matched activity to the system log** to **ON** to enable Verbose logging. See the System log section for more information.

Figure 8-9 Verbose logging configuration

Online / Offline control

In situations where you need to forcefully make a connection or forcefully disconnect a connection, you can use the **Manual connect** and **Manual disconnect** buttons. The online status of the connection is displayed above the buttons.

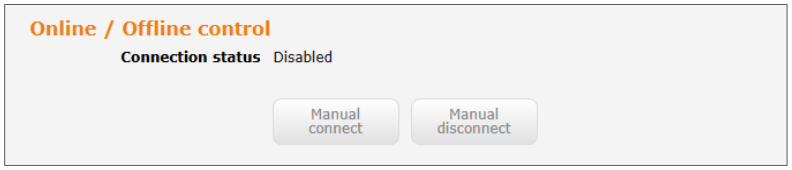


Figure 8-10 Online/Offline control

Once you complete the configuration of all the settings for Connect on demand, click **Save** to save and apply the settings.

Operator settings

The Operator settings page allows you to select the frequency band to use for your connection and set the mode of connection, whether automatic or manual. To access the Operator settings page, navigate to **Networking > Wireless WAN > Operator settings**.

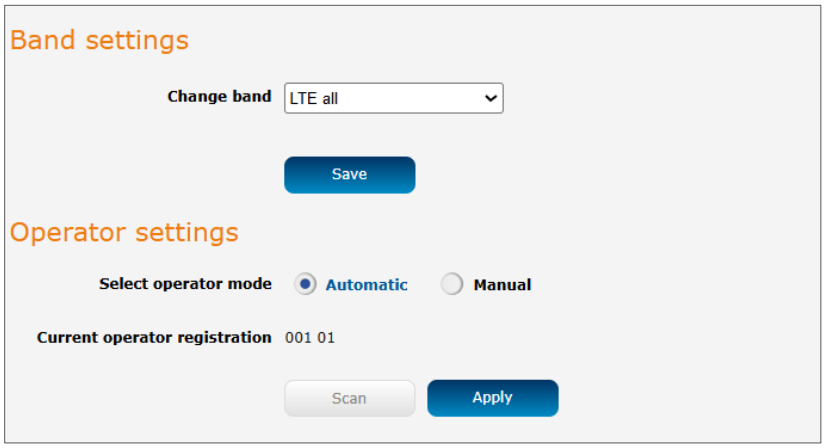


Figure 8-11 Operator settings page

Band settings

Band settings allows you to select the required frequency band for the network.

Select the required frequency in **Change band** field, from the options available in the drop down list. Click **Save**.

If you select the **LTE all** option, the router automatically scans for the available LTE bands and selects the suitable band.

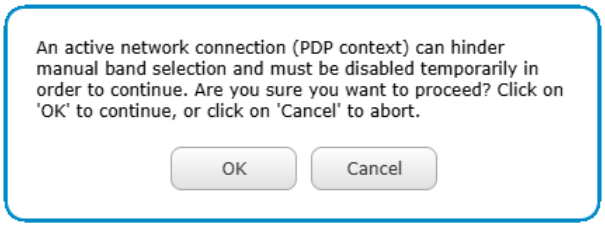
Operator settings

The operator settings feature allows you to set how the router connects to a network. Select one of the following options:

- **Automatic** – Allows the router to automatically connect to preferred network
- **Manual** – Allows you to scan for available networks and select the preferred network

When you select the **Manual** option:

1. Click **Scan** button, the below warning message displays.



2. Click **OK** to continue, a list of the detected service carriers in your area is displayed.

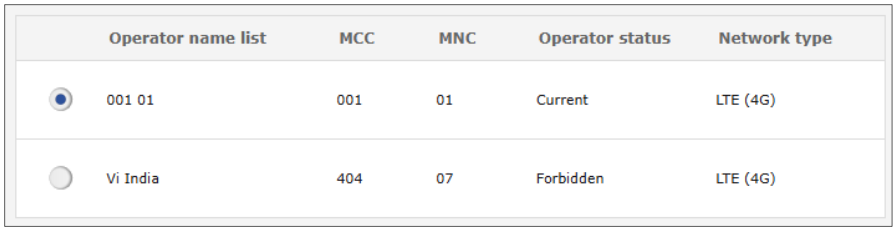


Figure 8-12 Detected network operator list

3. Select the preferred operator from the list and click **Apply**.

SIM management

Note: *The SIM Management feature is available only for devices that have an embedded SIM installed.*

The SIM management page allows you to manage SIM settings. To access the SIM management page, navigate to **Networking > Wireless WAN > Sim management**.

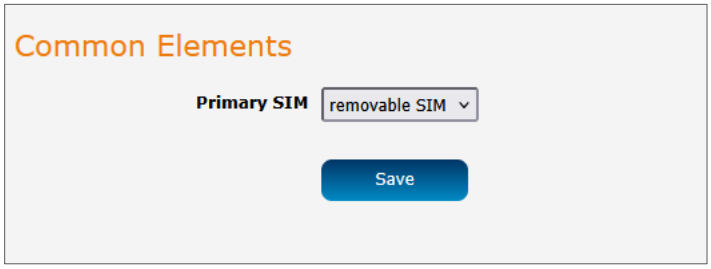


Figure 8-13 SIM Management page

The **Primary SIM** field allows you to select the SIM to use, whether **internal SIM** or **removable SIM**. Click **Save** to save the settings.

SIM security settings

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

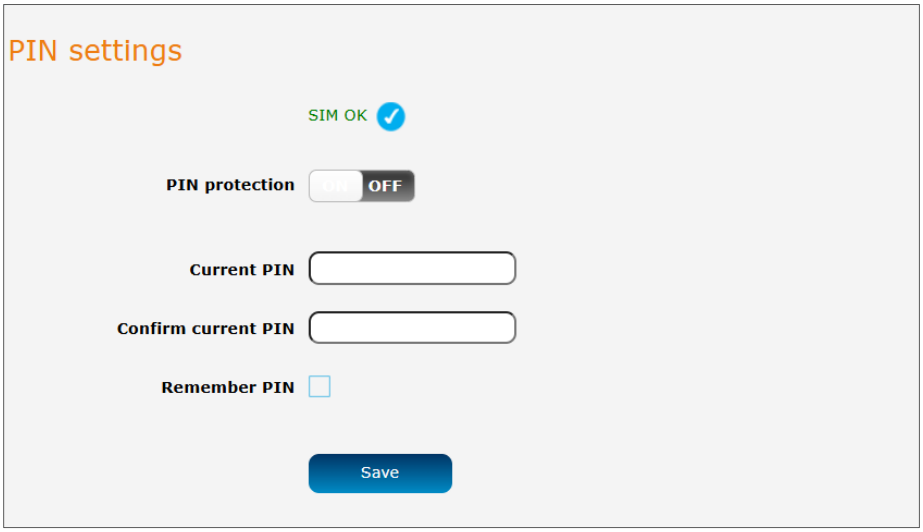


Figure 8-14 PIN settings page

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

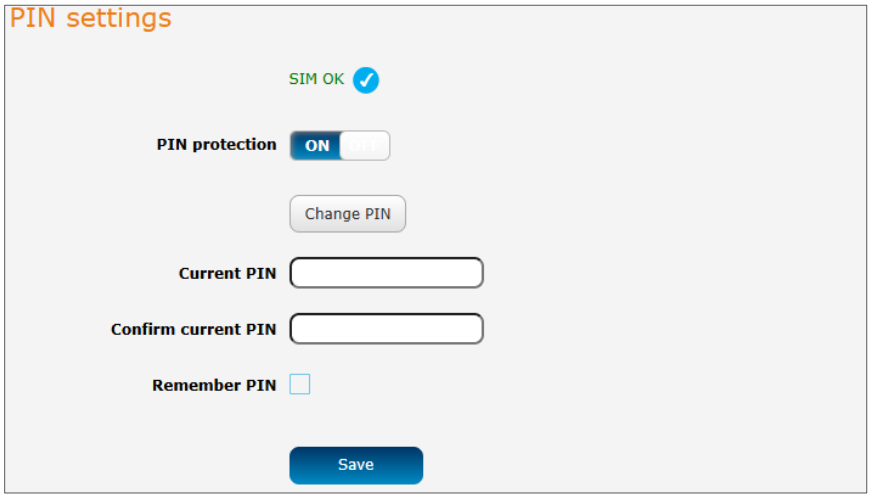
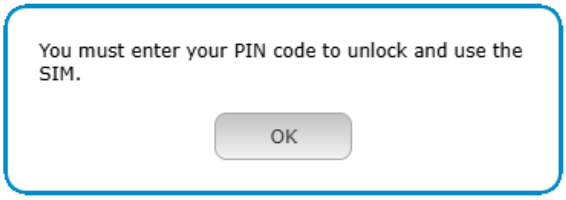


Figure 8-15 PIN settings page after enabling PIN protection

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



Click **OK**, you are directed to SIM security settings page.

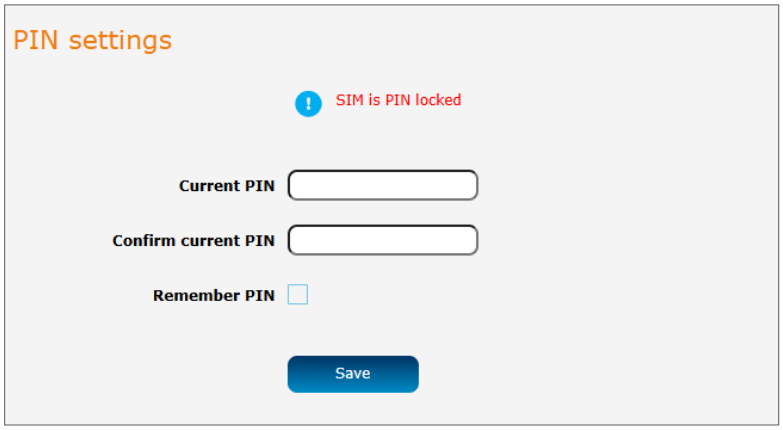


Figure 8-16 PIN settings page when SIM is PIN locked

Enter the PIN in **Current PIN** and **Confirm Current PIN** fields and click **Save**, to unlock the SIM.

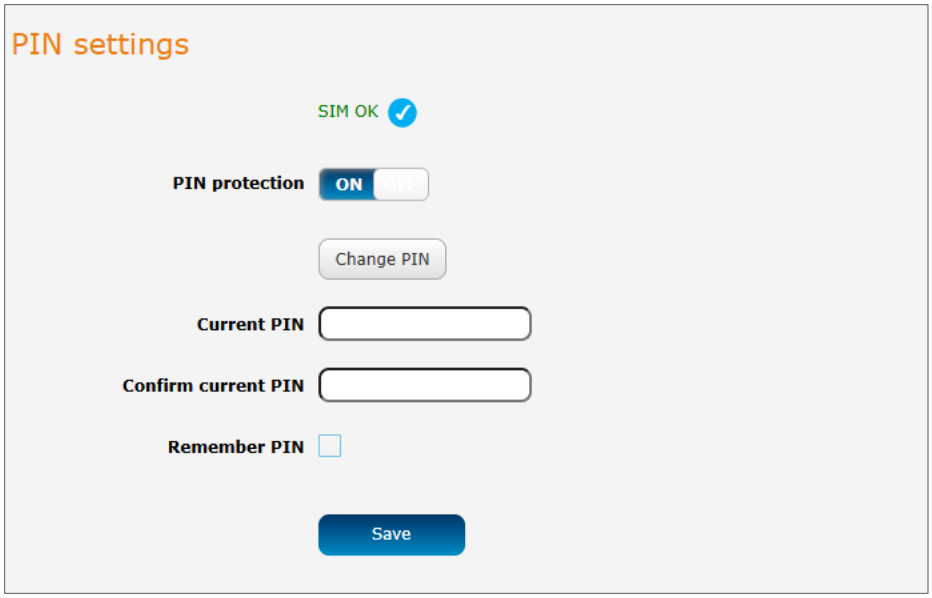


Figure 8-17 PIN settings page after SIM is unlocked

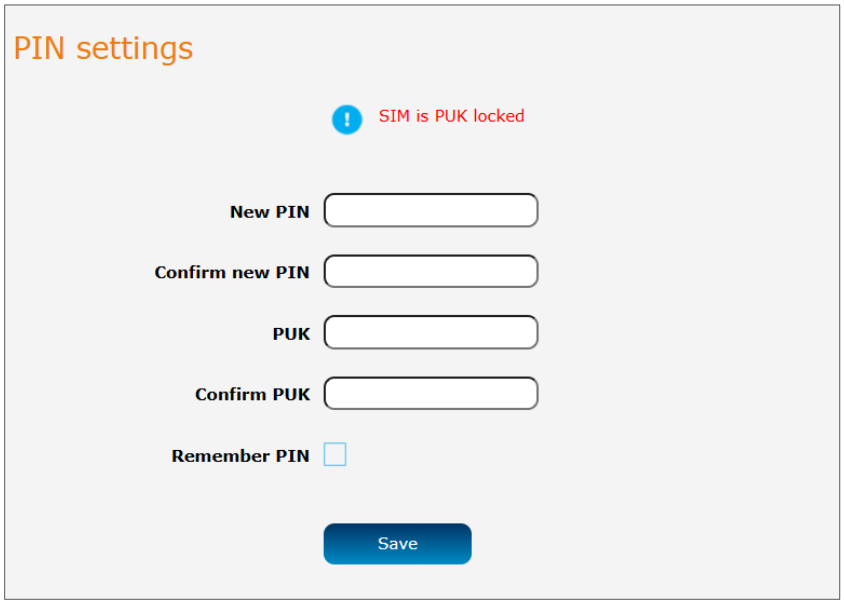
Once unlocked, you can disable PIN protection, if you do not wish to have access locked by a PIN. To disable PIN protection set **PIN protection** to **OFF**, enter the PIN number in the **Current PIN** and **Confirm current PIN** fields and click **Save**.

If you are placing the router in a remote, unattended location, you can check **Remember PIN** option to enable it. This feature allows the router to automatically send the PIN to the SIM each time the SIM asks for it (usually at power up). This enables the SIM to be PIN locked (to prevent unauthorized re-use of the SIM elsewhere), while still allowing the router to connect to the cellular service. When this feature is enabled, the PIN you enter is encrypted and stored locally on the router. The next time the SIM asks the router for the PIN the router decrypts the PIN and automatically sends it to the SIM without user intervention.

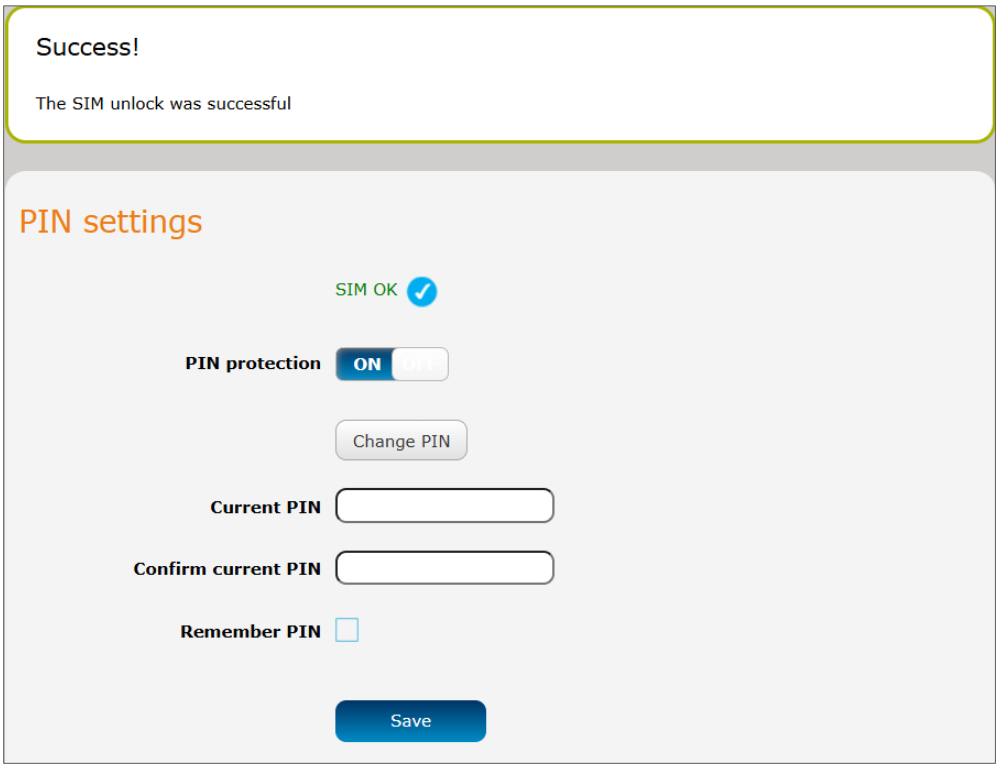
Note: *Select Remember PIN if you do not want to enter the PIN code each time the SIM is inserted.*

SIM PUK Lock

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



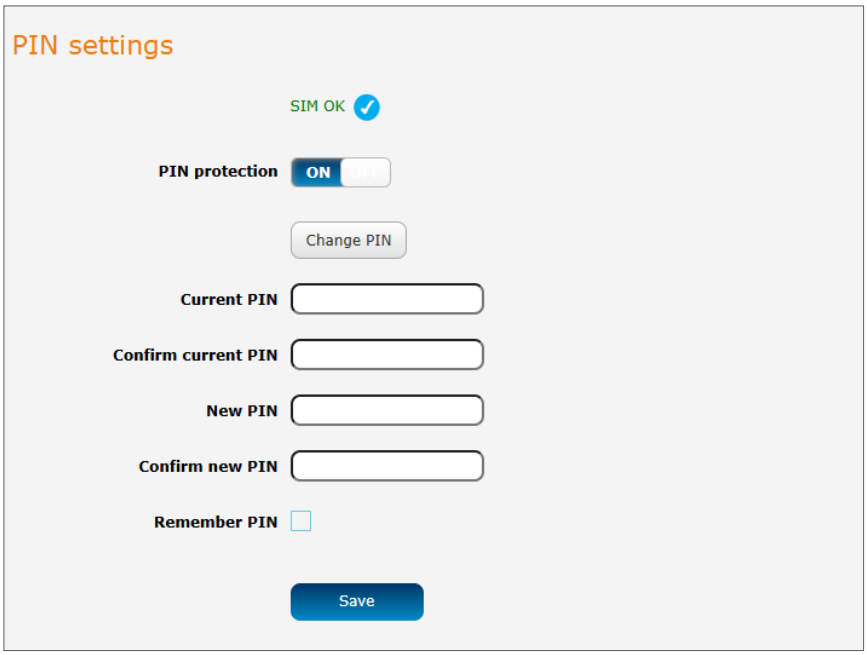
To unlock the SIM, you have to request your service provider for a PUK code. Once you have the PUK code, enter it in the **Current PUK** and **Confirm current PUK** fields, enter a new PIN in the **New PIN** and **Confirm new PIN** fields, and then click **Save**. The below prompt is displayed if the SIM is unlocked.



Changing SIM PIN

To change the PIN of the SIM:

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



0

Figure 8-18 PIN settings page when changing PIN

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

LAN

LAN

The LAN configuration page is used to configure the LAN settings of the router and to enable or disable DNS Masquerading. To access the LAN configuration page, navigate to **Networking > LAN > LAN**.

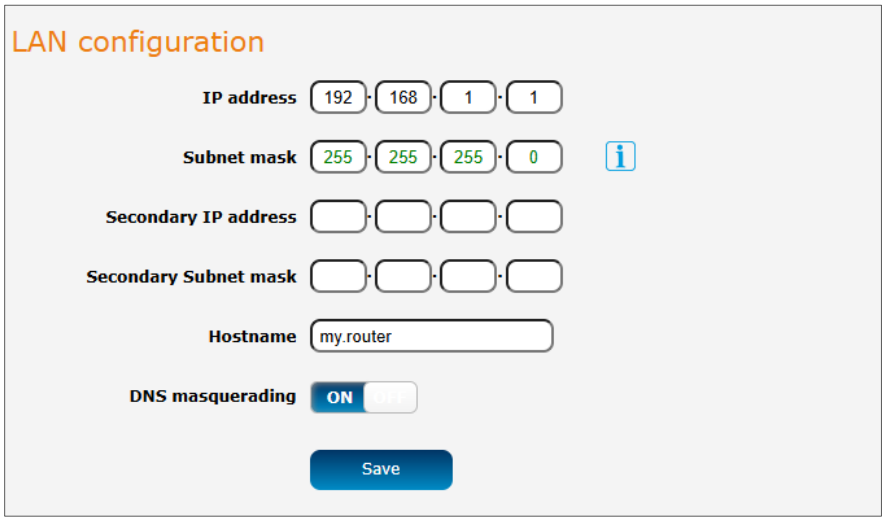


Figure 8-19 LAN configuration settings

Table 8-4 LAN configuration details

Parameter	Description
IP address	Default IP address of the LAN port. You can change the IP address
Subnet mask	Default Subnet mask of the LAN port. You can change the Subnet mask
Secondary IP address	Enter secondary IP address
Secondary Subnet mask	Enter secondary Subnet mask
Hostname	Default Hostname
DNS masquerading	Set to **ON** to enable and **OFF** to disable. DNS masquerading allows the router to proxy DNS requests from LAN clients to dynamically assigned DNS servers. When enabled, clients on the router's LAN can then use the router as a DNS server without needing to know the dynamically assigned cellular network DNS servers. When **DNS masquerading** is set to **ON**, the DHCP server embedded in the NTC-201 router hands out its own IP address (e.g. 192.168.1.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NTC-201 router which proxies them to the upstream DNS servers. When **DNS masquerading** is set to **OFF**, the DHCP server hands out the upstream DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the NTC-201 router.

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

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

DHCP

The DHCP page is used to configure the settings used by the router's built in DHCP Server which assigns IP addresses to locally connected devices. To access DHCP page navigate to **Networking > LAN > DHCP**.

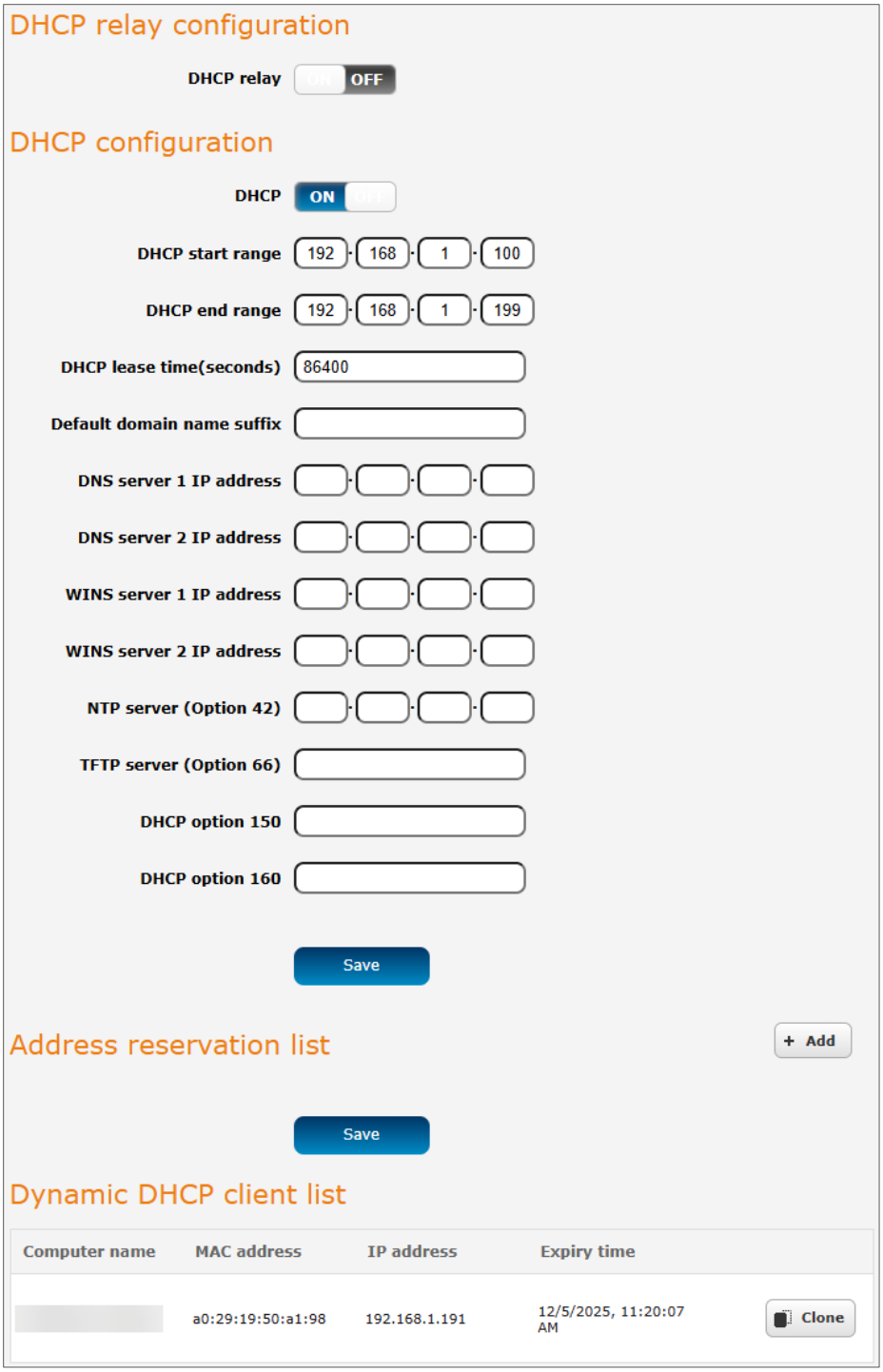


Figure 8-20 DHCP page

DHCP relay configuration

In advanced network configurations where the NTC-201 router should not be responsible for DHCP assignment, an existing DHCP server is located on the Wireless WAN or LAN connections. The clients behind the NTC-201

router will be able to communicate with the DHCP server when DHCP relay is enabled. This enables the NTC-201 router to accept client broadcast messages and to forward them onto another subnet.

To configure the router to act as a DHCP relay agent set **DHCP relay** to **ON** and enter the DHCP server address into the **DHCP server address** field. DHCP relay is disabled by default. Click **Save** to save the setting.

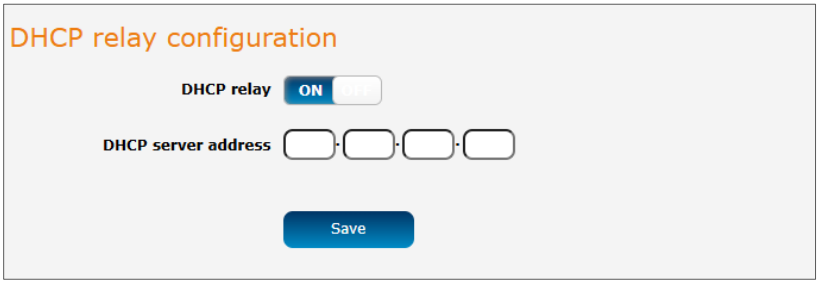


Figure 8-21 DHCP relay configuration

DHCP configuration

Set **DHCP** to **ON** to enable it. The configuration settings display.

Table 8-5 DHCP configuration details

Parameter	Description
DHCP start range	Enter the first IP address of the DHCP range.
DHCP end range	Enter the last IP address of the DHCP range.
DHCP lease time (seconds)	Enter the duration for which the DHCP allocated IP addresses are valid.
Default domain name suffix	Enter 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	Enter the primary DNS (Domain Name System) server's IP address.
DNS server 2 IP address	Enter the secondary DNS (Domain Name System) server's IP address.
WINS server 1 IP address	Enter the primary WINS (Windows Internet Name Service) server IP address.
WINS server 2 IP address	Enter the secondary WINS (Windows Internet Name Service) server IP address.
NTP server (Option 42)	Enter the IP address of the NTP (Network Time Protocol) server.
TFTP Server (Option 66)	Enter the IP address of the TFTP (Trivial File Transfer Protocol) server.

Parameter	Description
DHCP option 150	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	Used to configure Polycom IP phones. When a Polycom IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 160 request.

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

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.

To add a device to the Address reservation list:

1. Click the **+Add** button for the Address reservation list, the different fields display as shown below.

Figure 8-22 Address reservation list

2. In the **Computer Name** field enter a name for the device.
3. In the **MAC Address** field, enter the device's MAC address.
4. In the **IP Address** field, enter the IP address that you wish to reserve for the device.
5. Set **Enable** to **ON**.
6. Click **Save** to save and apply the settings.

Dynamic DHCP client list

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

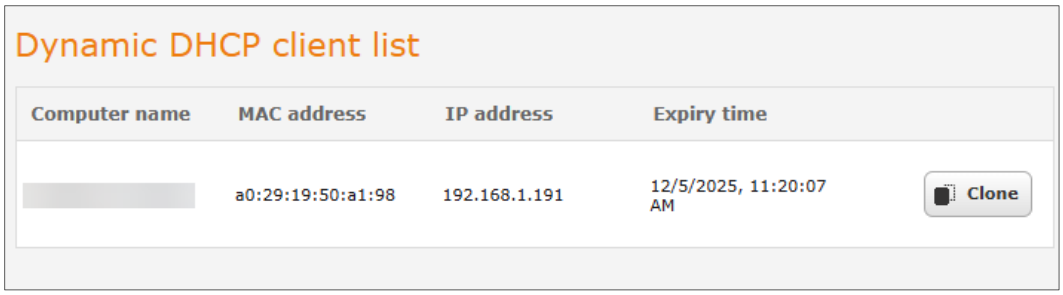


Figure 8-23 Dynamic DHCP client list

PPPoE

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

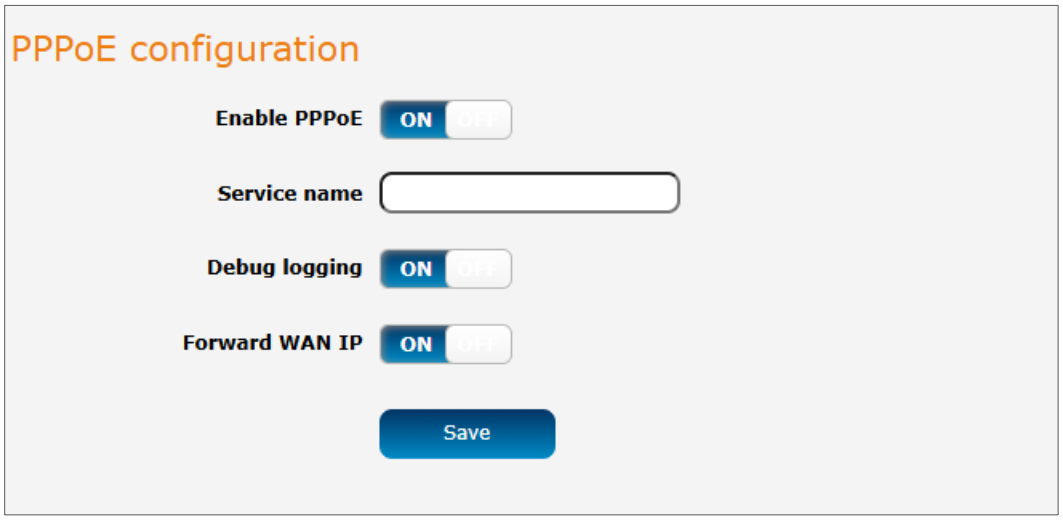


Figure 8-24 PPPoE configuration

Table 8-6 PPPoE configuration details

Parameter	Description
Enable PPPoE	Set to **ON** to enable PPPoE.
Service Name	Enter a name to use for the connection. This name is displayed on the Status page to identify the PPPoE connection. Any name you enter here must also be entered in the PPPoE connection profile for it to work.

Parameter	Description
Debug logging	Set to **ON** to enable Debug logging. This enables additional logging and displays PPPoE negotiation details in the System log.
Forward WAN IP	Set to **ON** to enable. When enabled, the router passes the WAN IP address to the PPPoE client. The first PPPoE client to connect will receive the WAN IP address and no further clients will be able to make a connection. In this mode, the router transparently bridges the connection and many of the router's features are disabled. When disabled, the router retains the WAN IP address and performs Network Address Translation (NAT) for connected clients. In this mode, you can connect multiple PPPoE clients and all of the router's features are available.

Click **Save** to save and apply the settings. If Forward WAN IP is enabled, the Status page displays a Transparent bridge mode section which shows the WAN IP.

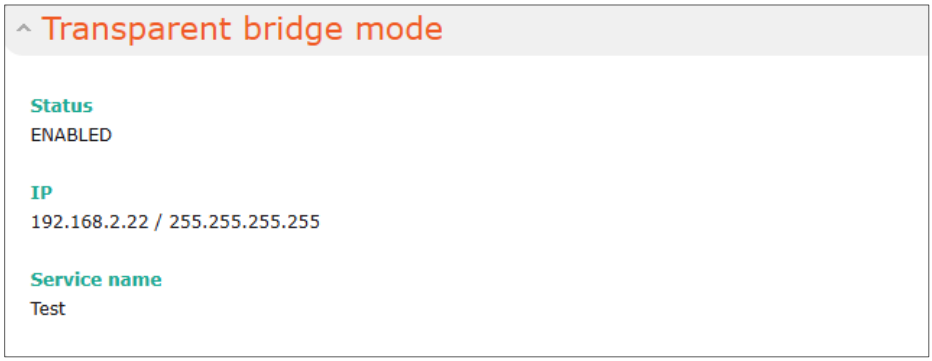


Figure 8-25 Transparent bridge mode section

Use your downstream device to initiate a connection using a PPPoE client.

Routing

Static

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, navigate to **Networking > Routing > Static**.

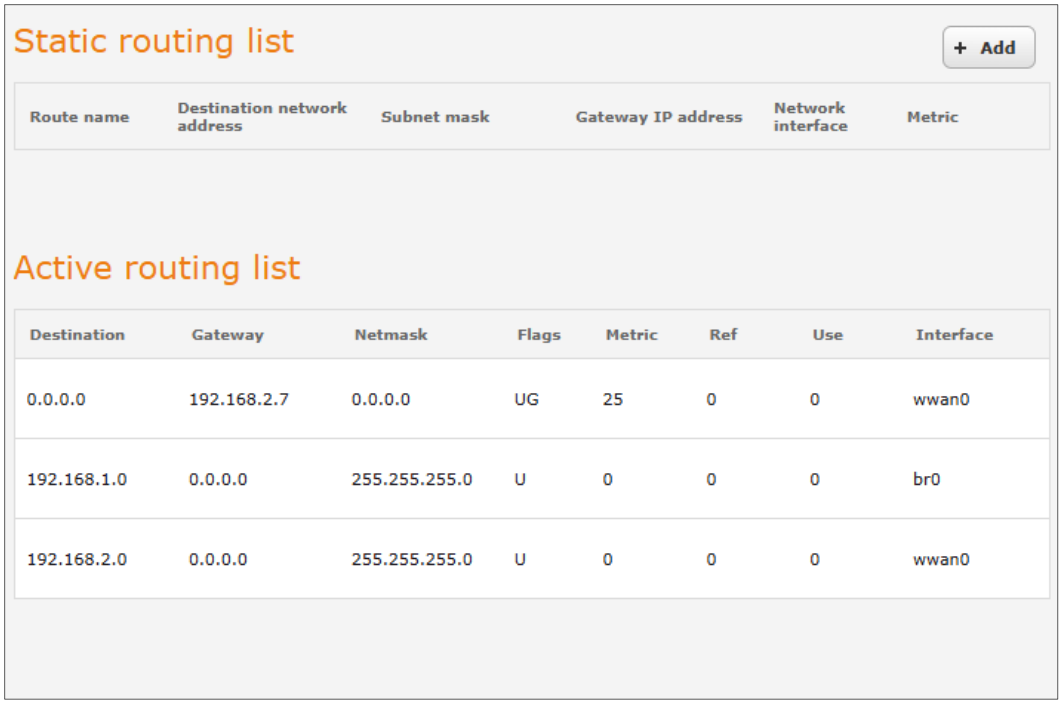


Figure 8-26 Static routing page

The Static routing page displays the Static routing list and Active routing list.

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

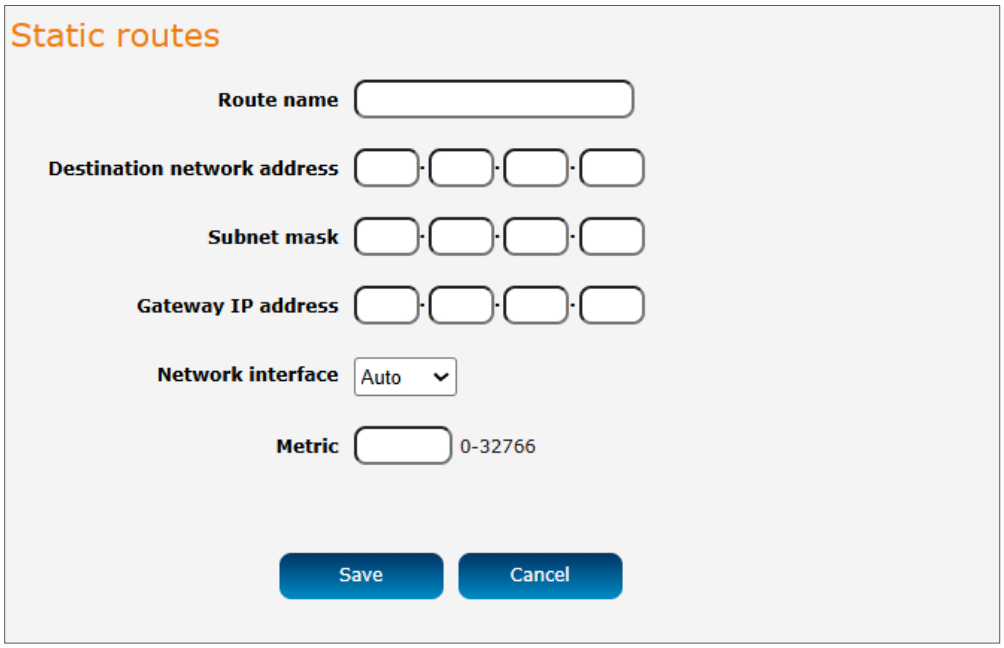


Figure 8-27 New static route configuration Page

Table 8-7 New static route configuration details

Parameter	Description
Route name	Enter route name to identify the route in the Static routing list.
Destination network address	Enter the IP address of the destination of the route.
Subnet mask	Enter the subnet mask of the destination IP address.
Gateway IP address	Enter the IP address of the gateway that will facilitate the route.
Network interface	Select Network interface. Options are: • **Auto** • **WWAN** • **br0**
Metric	Enter the Metric value for the route. This value is used by the router to prioritize routes. The lower the value, the higher the priority.

Click **Save** to save and apply the settings. The new route is added to the Static routing list.

Click the icon for a route to edit it, and the icon to delete it.

Active routing list

The Active routing list displays the routes added by the router by default, such as the Ethernet subnet route for routing to a device on the Ethernet subnet.

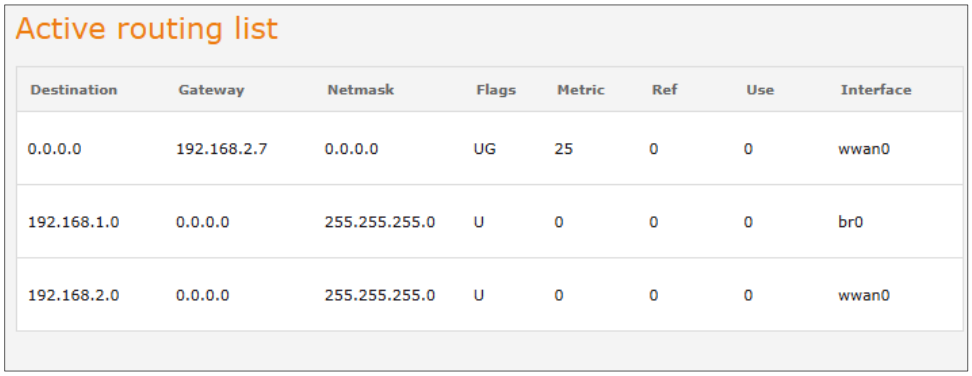


Figure 8-28 Active routing list

RIP

Routing Information Protocol (RIP) allows you to advertise routes to other routers. Thus, all the routes in the router's routing list 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.

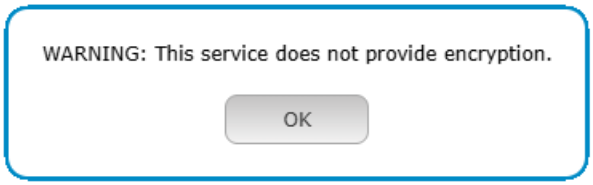
Note: *Some routers will ignore RIP.*

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

Figure 8-29 RIP configuration page

To configure RIP:

1. Set RIP to **ON**, the below prompt displays.



2. Click **OK**, the RIP configuration details display.

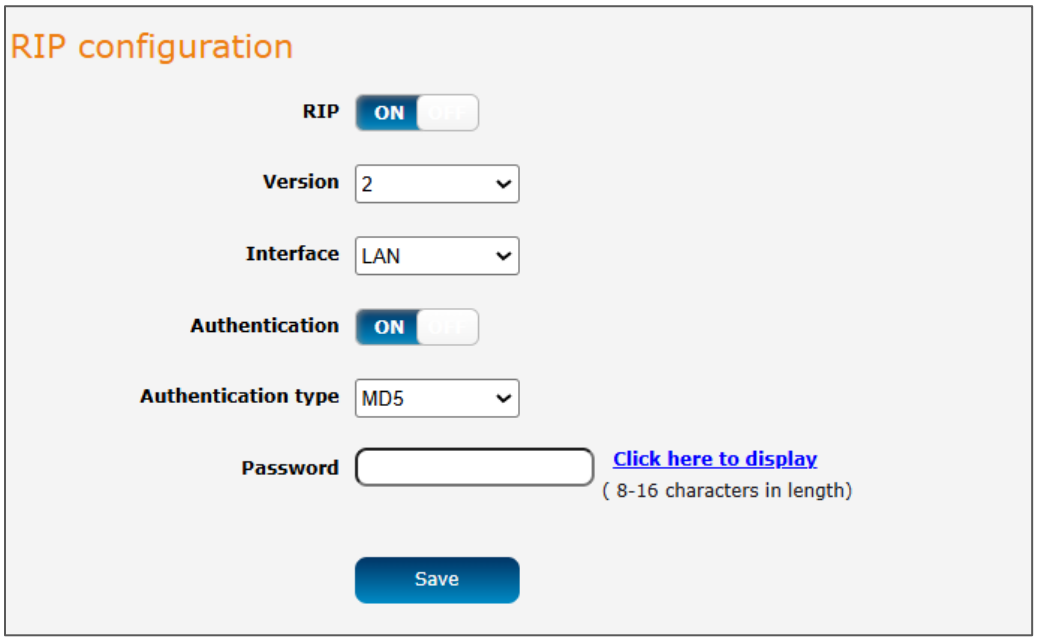


Figure 8-30 RIP configuration details

3. Select **Version**. Options are **1** and **2**.
4. Select **Interface**. Options are:
   - **LAN**
   - **WWAN**
   - **Both**
5. Set **Authentication** to **ON** enable it, then select **Authentication type**. Options are **MD5** and **Password**.
6. In the **Password** field, enter password.
7. Click **Save** to save and apply the settings.

OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol that enables a router to automatically exchange routing information with other OSPF enabled routers. It allows the router to automatically discover network routes and determine the best path for forwarding IP packets within an IP network.

To access the OSPF configuration page, navigate to **Networking > Routing > OSPF**.

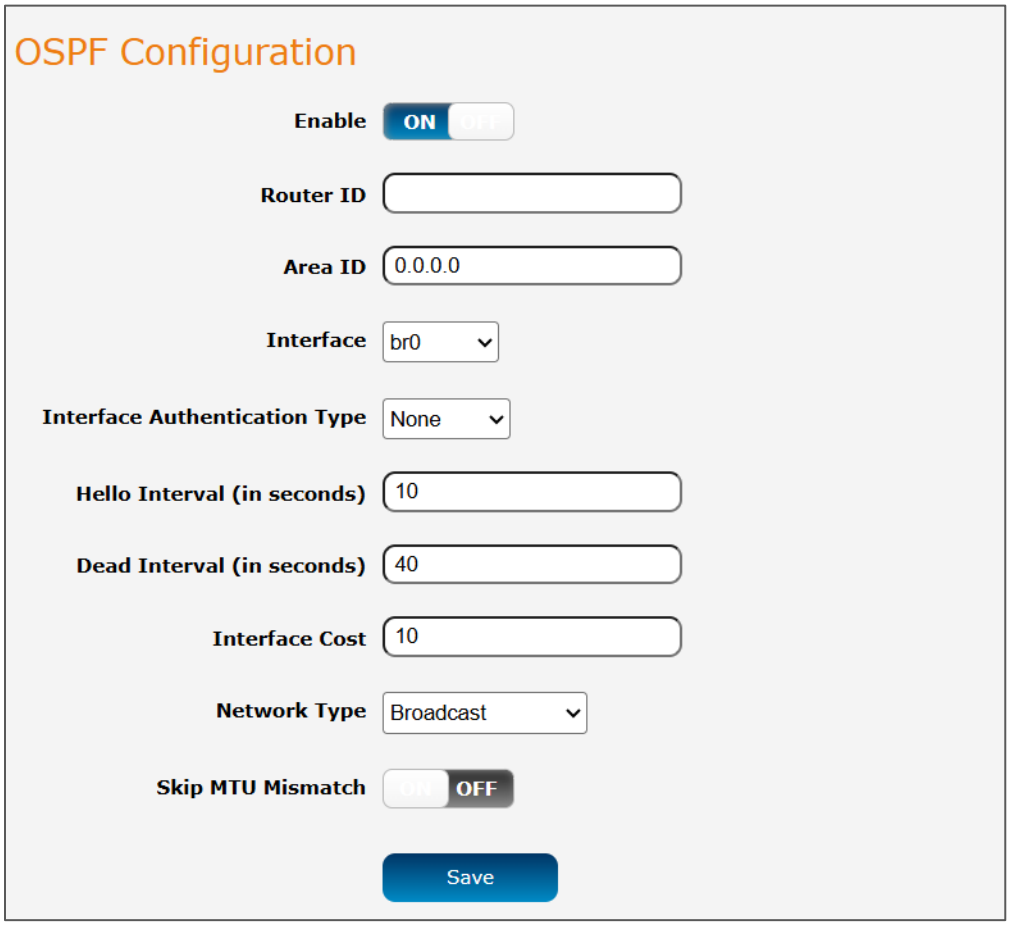


Figure 8-31 OSPF configuration page

Table 8-8 OSPF configuration details

Parameter	Description
Enable	Set to **ON** to enable
Router ID	Enter a unique 32-bit identifier assigned to the router to identify it within the OSPF network, typically configured as an IPv4 address (e.g., 1.1.1.1). It remains constant regardless of the router's interface IP addresses.
Area ID	Enter an OSPF area identifier to which a router belongs. Routers exchange routing information only with other OSPF routers in the same area. It can be specified in decimal or IPv4 address format.
Interface	Select the network interface on which OSPF is enabled

Parameter	Description
Interface Authentication Type	Select the authentication method used to validate OSPF packets exchanged over the interface. Both neighboring routers must use same authentication type. Options are: • **None** • **Plain Text** • **MD5**
Hello Interval (in seconds)	Enter the time interval, in seconds, between OSPF hello packets sent on the interface to discover and maintain neighboring routers. Neighboring routers must use the same Hello interval
Dead Interval (in seconds)	Enter the time interval, in seconds, after which a neighboring router is considered unreachable if no Hello packets are received. Neighboring routers must use the same Dead interval
Interface Cost	The OSPF cost assigned to the interface which is used by the OSPF to calculate the shortest path to a destination. Lower costs are preferred
Network Type	Select the OSPF network type for the interface. It determines how neighbors are discovered and how OSPF operates on the network. Options are: • **Broadcast** • **Point to Point** • **Point to Multipoint**
Skip MTU Mismatch	Set to **ON** to enable. When enabled OSPF ignores MTU size mismatches during adjacency formation.

Redundancy (VRRP)

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

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

To access the Redundancy (VRRP) page, navigate to **Networking > Routing > Redundancy (VRRP)**.

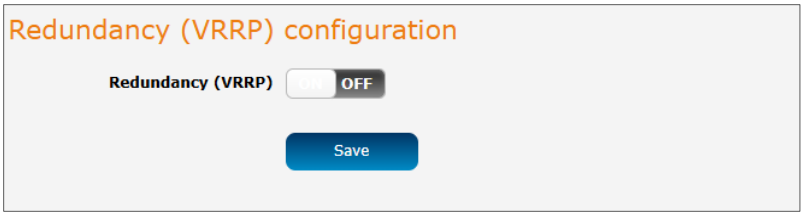


Figure 8-32 Redundancy (VRRP) page

Redundancy (VRRP) configuration

For Redundancy (VRRP) configuration, configure multiple devices and connect them all via an Ethernet network switch to downstream devices:

To configure Redundancy (VRP) on a device:

1. Set **Redundancy (VRRP)** to **ON**, the different settings display.

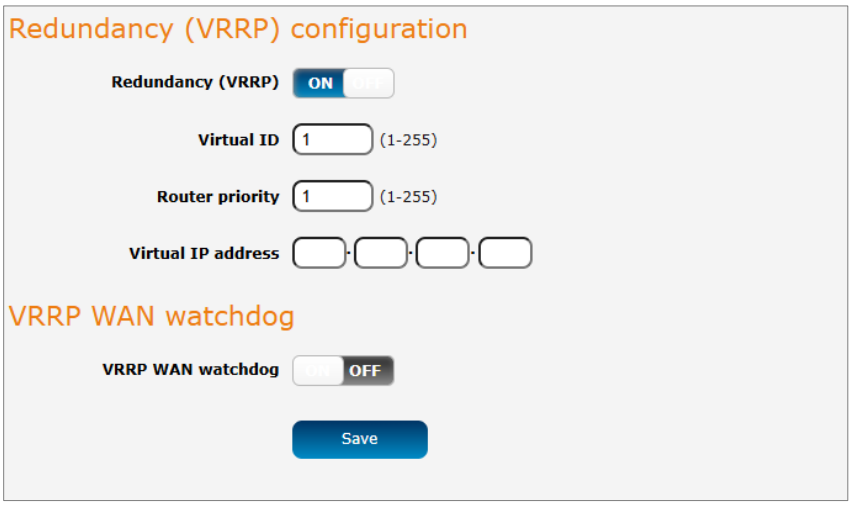


Figure 8-33 Redundancy (VRRP) settings

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. In the **Virtual IP address** field, enter VRRP IP address. This is the virtual IP address that both virtual routers share.
5. Click the **Save** to save and apply the settings.

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

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

VRRP WAN watchdog

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

Set **VRRP WAN watchdog** to **ON** to enable it. The different settings display.

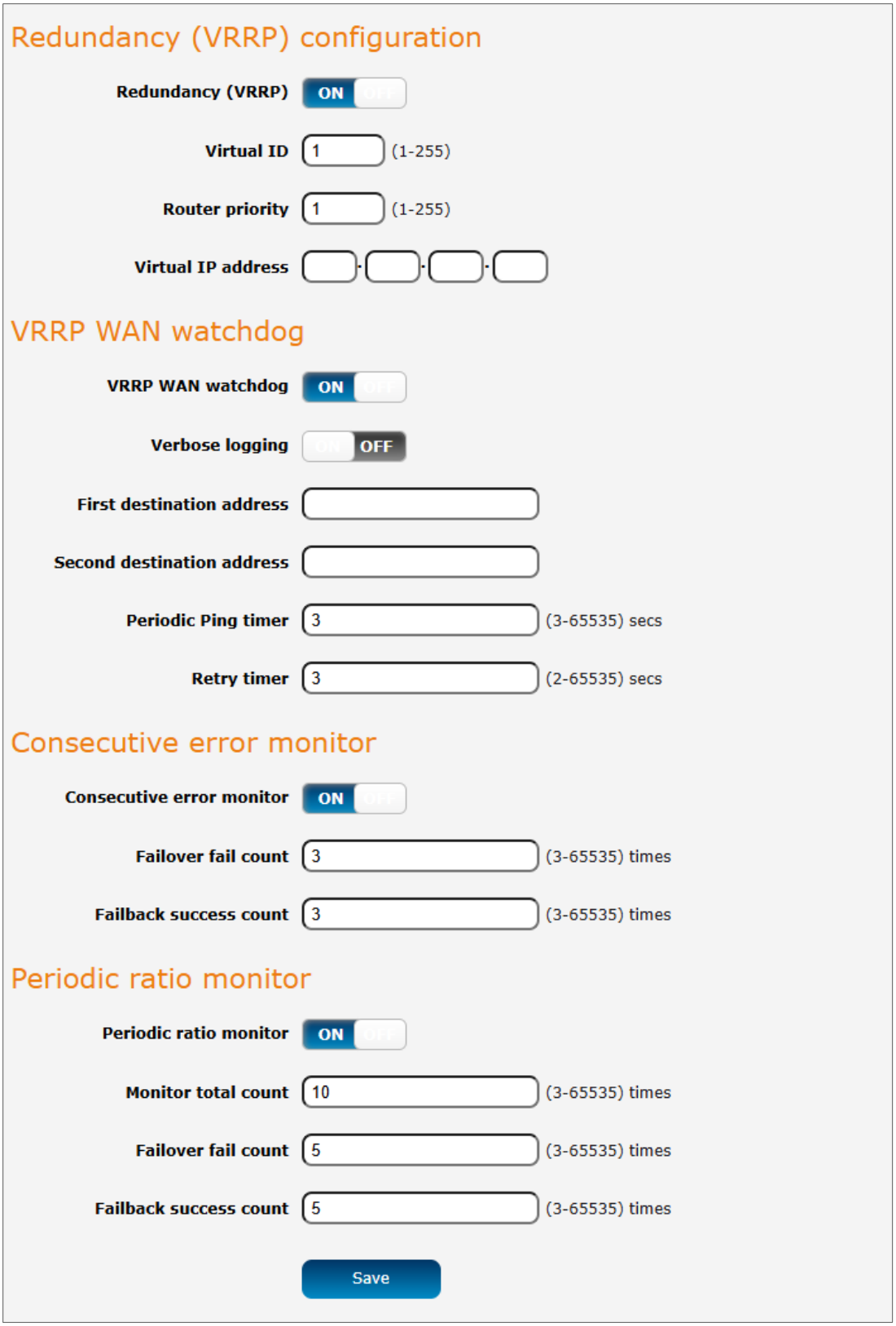


Figure 8-34 VRRP WAN watchdog, Consecutive error monitor, and Periodic ratio monitor settings

Table 8-9 VRRP WAN watchdog configuration details

Parameter	Description
VRRP WAN watchdog	Set to **ON** to enable.
Verbose logging	Set to **ON** to enable. When enabled, this logs verbose comments in the system log related to the failover monitoring.
First destination address	Enter the first address that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Second destination address	Enter the second address that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	Enter the time in seconds between ping attempts.
Retry timer	Entre the time in seconds between attempts when a ping failure occurs.

Consecutive error monitor

This method allows the router to determine the availability of an interface based on a set number of consecutive ping instance responses.

Table 8-10 Consecutive error monitor configuration details

Parameter	Description
Consecutive error monitor	Set to **ON** to enable.
Failover fail count	Enter the number of failed pings that must occur before the monitor fails the connection over to the next interface.
Failback success count	Entre the number of successful pings that must occur before the monitor fails the connection back to the higher priority interface.

Periodic ratio monitor

This method allows the router to determine the availability of an interface based on a set ratio of ping instance successes or failures to the number of attempts.

Table 8-11 Periodic ratio monitor configuration details

Parameter	Description
Periodic ratio monitor	Set to **ON** to enable.
Monitor total count	Enter the series of pings to consider when calculating whether to fail over or fail back. When the Series is completed, the router repeats the ping test and resets the Failover fail count/Failback success count. Therefore, for the failover or failback ratio to be met, the number of

Parameter	Description
	Failover fail counts/Failback success counts must occur within a particular series.
Failover fail count	Enter the number of failed ping results that must occur within the series of pings set in **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	Enter the number of ping successes that must be registered on a higher priority interface within the series of pings set in **Monitor total count**, before the router fails back to that interface.

Port forwarding

Port forwarding allows you to map inbound requests to a specific port on the WAN IP address to any connected device. The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the router. To access the Port forwarding page, navigate to **Networking > Routing > Port forwarding**

Figure 8-35 Port forwarding list

To add a new port forwarding rule, click **+Add** button for the Port forwarding list. The **Port forwarding** settings display.

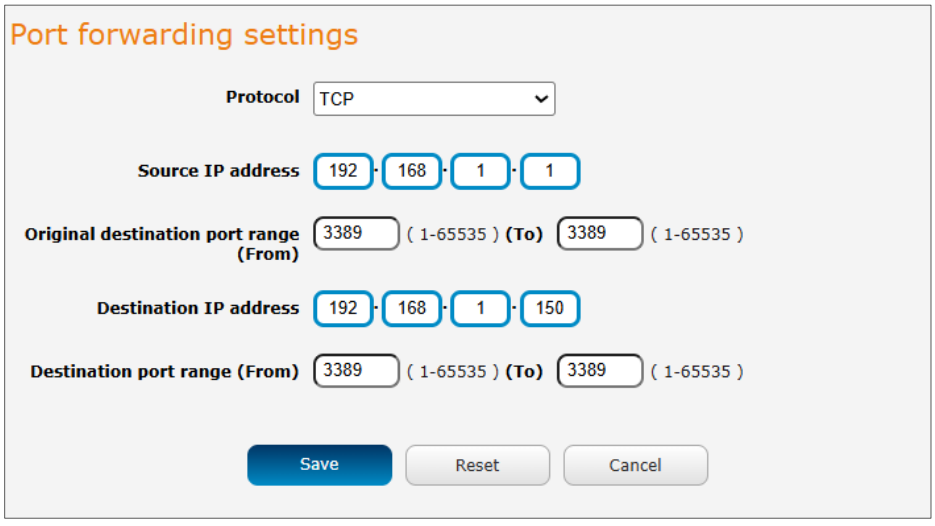
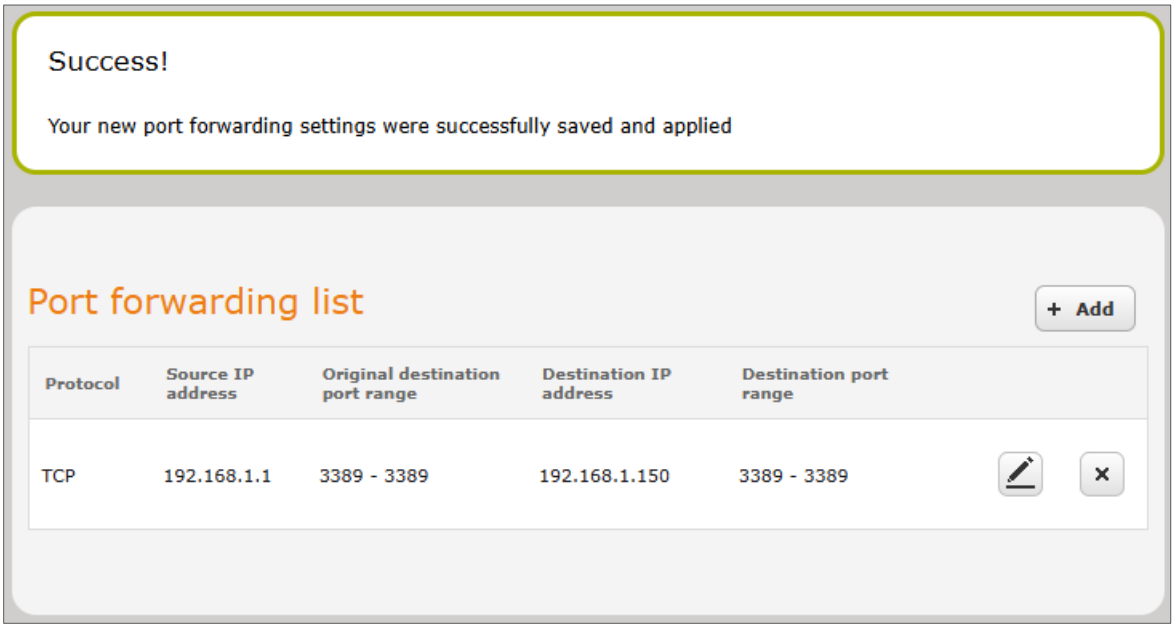


Figure 8-36 Port forwarding settings

Table 8-12 Port forwarding configuration details

Parameter	Description
Protocol	Select the type of protocol to use for the rule. Options are: • **TCP** • **UDP** • **ALL**
Source IP address	Enter a friendly IP address that is allowed to access the router or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the router.
Original destination port range (From) – (To)	Enter the port(s) on the destination side to which you want to apply port forwarding. Enter the first port in the range in **(From)** field and the last port in **(To)** field. To forward a single port, enter the port in **(From)** field and repeat it in **(To)** field.
Destination IP address	Enter the IP address of the destination client to which the traffic should be forwarded.
Destination port range (From) – (To)	Enter the port(s) on the destination side to which the traffic is routed after applying port forwarding. If the **Original destination port range** specifies a single port, then the **Destination port range** can be configured as any port. If the **Original destination port range** specifies a range of port numbers, then the same range of port numbers must be configured as **Destination port range**.

Click **Save** to save and apply the settings. The new rule displays in the Port forwarding list.



Click the icon for a rule to edit it, and the icon to delete it.

DMZ

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

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

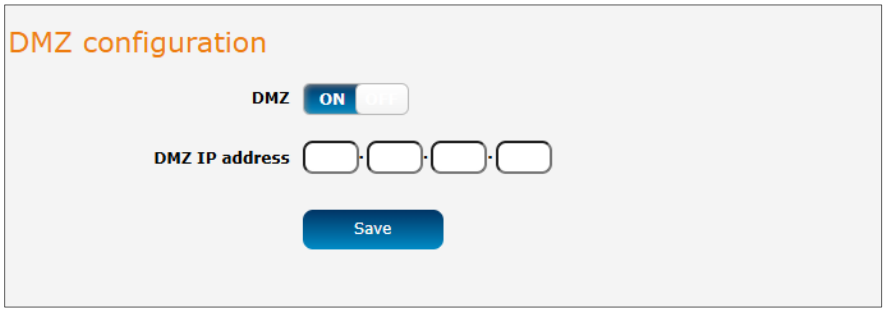


Figure 8-37 DMZ configuration

To configure DMZ:

1. Set **DMZ** to **ON** to enable it.
2. In the **DMZ IP address** field, enter the IP Address of the device of used as DMZ host.
3. Click the **Save** to save the settings.

Router firewall

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

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

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

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

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

Figure 8-38 Router firewall

Set **Enable router firewall** to **ON** to enable Router firewall. Click **Save** to save the setting.

MAC / IP / Port filtering

The MAC/IP/Port filtering feature allows you to apply a policy to the traffic that passes through the router, both inbound and outbound to control network access.

To access the MAC / IP / Port filtering page, navigate to **Networking > Routing > MAC / IP / Port filtering**

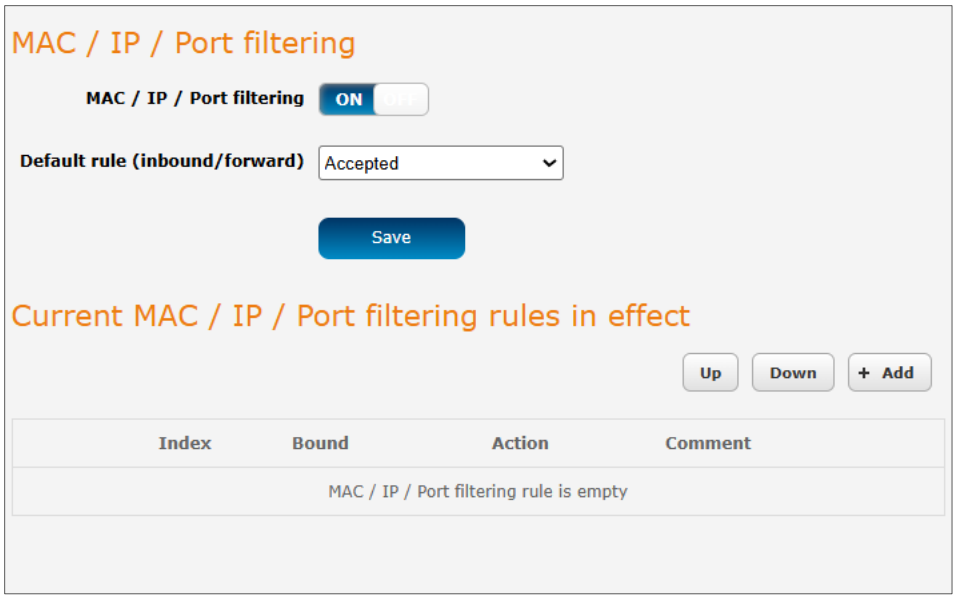


Figure 8-39 MAC / IP /Port filtering

Set **MAC / IP / Port filtering** to enable MAC / IP / Port filtering. When **Default rule (inbound/forward)** is set to **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 (inbound/forward)** is set to **Dropped**, all connections are denied except for those listed in the filtering rules list.

Click **Save** to save the settings.

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

To create MAC / IP / Port filtering a filtering rule, click **+Add** button in the Current MAC / IP / Port filtering rules in effect section. The MAC / IP / Port filter settings display:

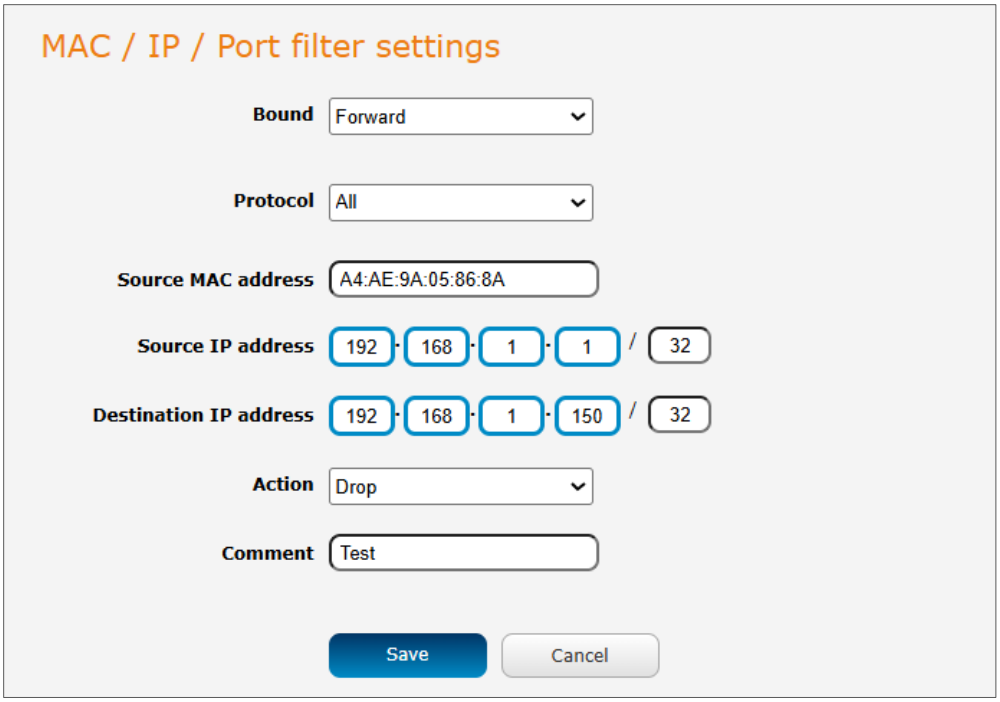


Figure 8-40 MAC / IP / Port filter settings

Table 8-13 MAC / IP / Port filter configuration details

Parameter	Description
Bound	Select the direction of the traffic for which you want to apply to the rule. Options are: • **Inbound/Forward** – Traffic entering the from WAN and LAN destined for a device behind the router • **Inbound** – Traffic entering the router including data entering from the WAN and the LAN • **Outbound** – Traffic exiting the router including traffic leaving in the direction of the WAN and LAN • **Forward** – Traffic entering from the LAN or WAN side and is forwarded to the opposite end.
Protocol	Select the protocol for the rule. Options are: • **All** • **UDP/TCP** • **TCP** • **UDP** • **ICMP-type8 (echo-request)** • **ICMP-type13 (timestamp-request)** • **ICMP-type14 (timestamp-reply)**
Source MAC Address	Enter the MAC address that the traffic originates from in six groups of two hexadecimal digits separated by colons (:). e.g., 00:40:F4:CE:FA:1E

Parameter	Description
Source IP Address	Enter the IPv4 address that the traffic originates from and the subnet mask using CIDR notation.
Destination IP Address	Enter the IPv4 address for the traffic destination and the subnet mask using CIDR notation.
Action	Select the action to take when the traffic meets the above criteria. Options are: • **Drop** • **Accept** You can choose to Accept or Drop packets. When the default rule is set to Accept, you cannot create a rule with an Accept action since the rule is redundant. Likewise, if the default rule is set to Dropped you cannot create a rule with a Drop action.
Comment	Optional. Use this field to enter a description of the rule.

Click **Save** to save and apply the settings. The new rule is displayed in the filtering rules list.

Figure 8-41 New MAC / IP /Port filtering rule

Click the icon for a rule to edit it, and the icon to delete it.

Click **Up** and **Down** to change the priority of a rule in the list.

VPN

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

The advantages of a VPN connection include:

- Data Protection
- Access Control
- Data Origin Authentication
- Data Integrity

Each VPN connection has different configuration requirements. The following VPN configurations are available:

- IPSec
- Open VPN

- PPTP client
- GRE tunnelling

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

IPSec

IPSec operates on Layer 3 of the OSI model and can protect higher layered protocols. IPSec is used for both site-to-site VPN and Remote Access VPN. The NTC-201 router supports IPsec end points and can be configured with site-to-site VPN tunnels with third party VPN routers.

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

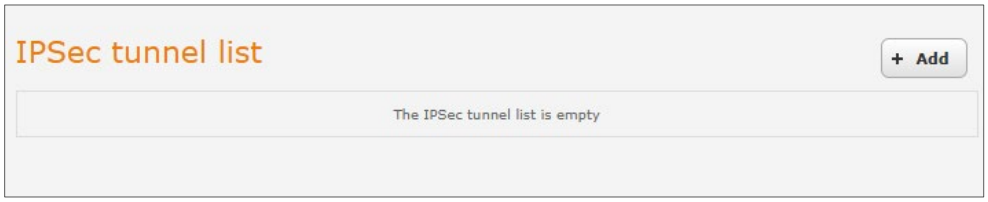


Figure 8-42 IPSec VPN List

To configure an IPSec tunnel, click the **+Add** button for IPSec tunnel list. The different settings display.

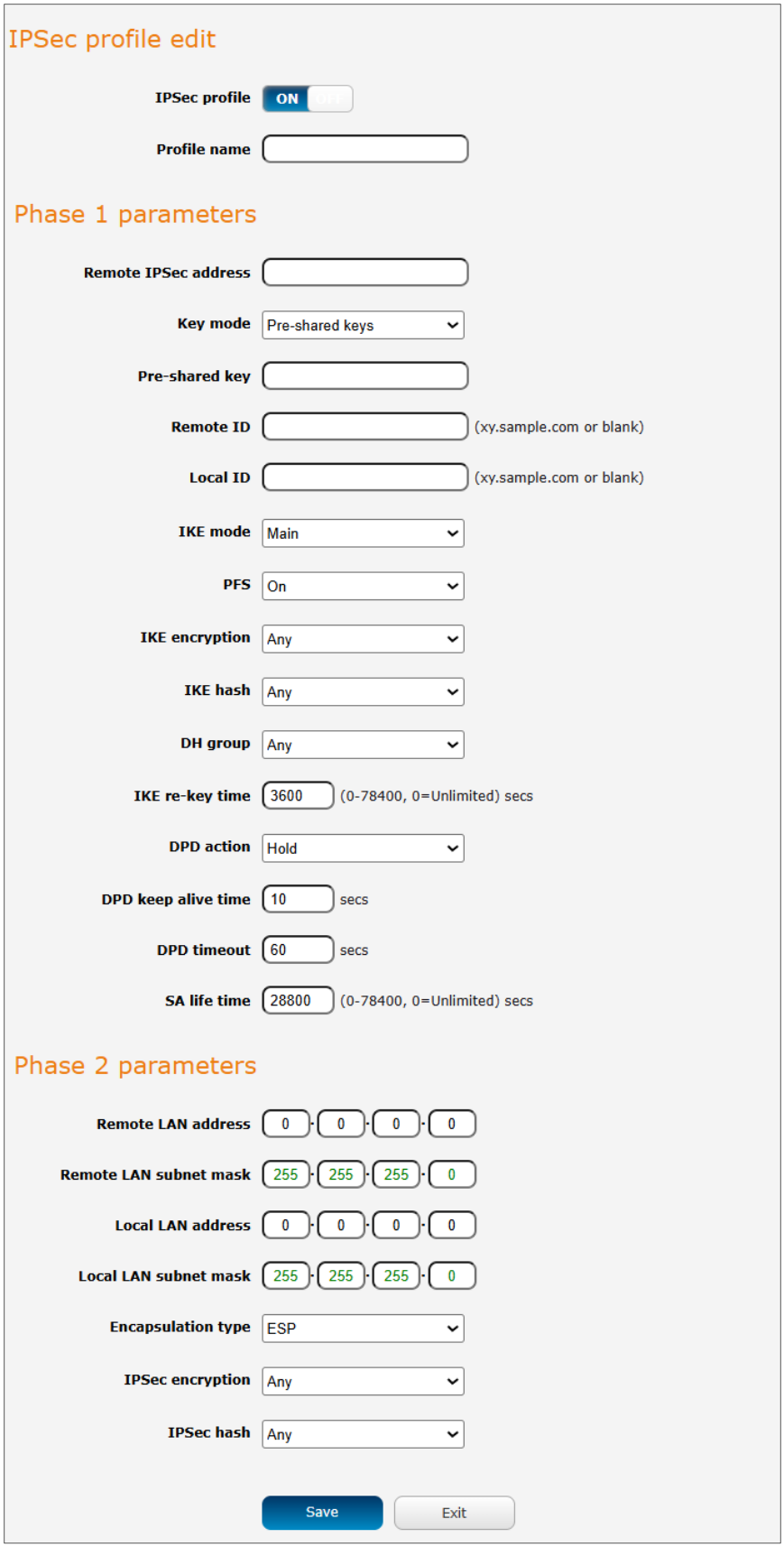


Figure 8-43 IPSec profile edit

Table 8-14 IPSec Configuration details

Parameter	Description
IPSec profile	Set to **ON** to enable.
Profile name	Enter a name to identify the VPN connection profile.
Phase 1 parameters	
Remote IPSec address	Enter the IP address or domain name of the IPSec server.
Key mode	Select the type of key mode to use for the VPN connection. Options are: • **Pre-shared Key** • **RSA keys** • **Certificates**
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.
Remote ID	Enter the domain name of the remote network.
Local ID	Enter the domain name of the local network.
IKE mode	Select the IKE mode to use with the VPN connection. Options are: • **Any** • **Main** • **Aggressive**
PFS	Set Perfect Forward Secrecy (PFS) to **ON** or **OFF**.
IKE encryption	Select the cipher type to use for the Internet Key Exchange. Options are: • **Any** • **AES** • **AES-128** • **AES-192** • **AES-256** • **3DES**
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. Options are: • **Any** • **MD5** • **SHA1** • **SHA256** • **SHA512**
DH group	Select the Diffie-Hellman group to use. Higher groups are more secure but require longer time to generate a key. Options are: • **Any**

Parameter	Description
	• **Group1(768)** • **Group2(1024)** • **Group5(1536)** • **Group14(2048)** • **Group15(3072)** • **Group16(4096)** • **Group17(6144)** • **Group18(8192)**
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 Dead Peer Detection action to take when a dead Internet Key Exchange Peer is detected. Options are: • **None** • **Clear** • **Hold** • **Restart**
DPD timeout	Enter the time in seconds for 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 to use on the VPN connection.
Remote LAN subnet mask	Enter the subnet mask to use on the remote network.
Local LAN address	Enter the IP address of the local network to use on the VPN connection.
Local LAN subnet mask	Enter the subnet mask to use on the local network.
Encapsulation type	Select the encapsulation protocol to use with the VPN connection. Options are: • **Any** • **ESP** • **AH**
IPSec encryption	Select the IPSec encryption type to use with the VPN connection. Options are: • **Any** • **AES** • **AES-128** • **AES-192** • **AES-256** • **3DES**

Parameter	Description
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. Options are: • **Any** • **MD5** • **SHA1** • **SHA256** • **SHA512**

Click **Save** to save and apply the settings. The new IPSec tunnel is added to the IPSec tunnel list.

Click the icon for a tunnel to edit it, and the icon to delete it.

OpenVPN

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

To access OpenVPN, navigate to **Networking > VPN > OpenVPN**.

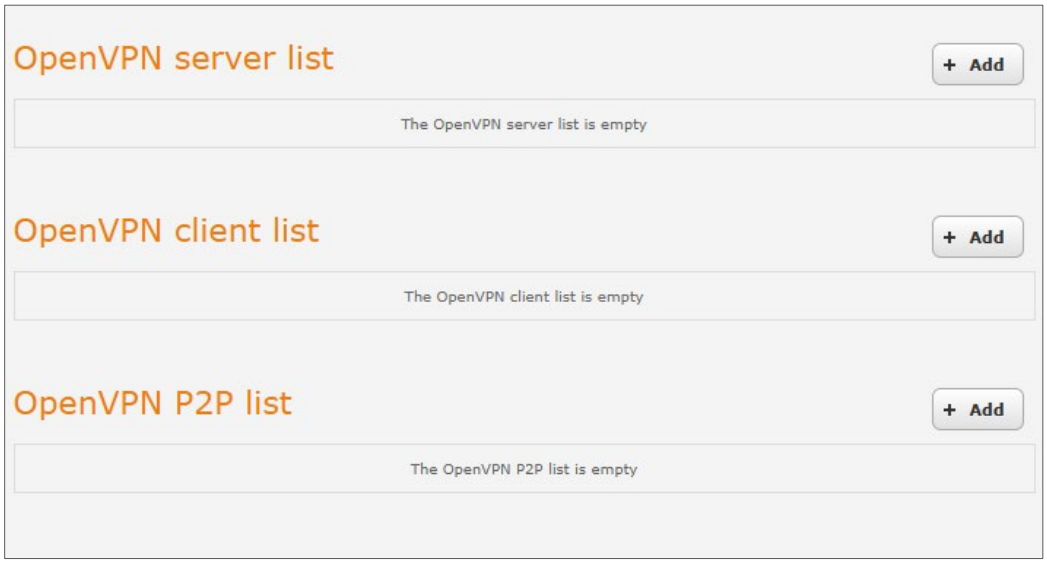
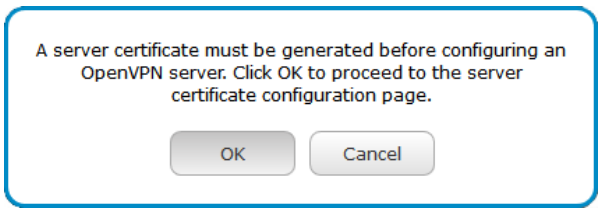


Figure 8-44 OpenVPN VPN List

OpenVPN server

To configure an OpenVPN server click **+Add** button for the OpenVPN server list. If no server certificate is found, you are prompted to generate a certificate before configuring the OpenVPN server.



Click **OK** button, you will be directed to the Server certificate page. For more information on generating server certificates, refer to the Server certificate section of this guide. After you have created the certificate, return to the OpenVPN server configuration page.

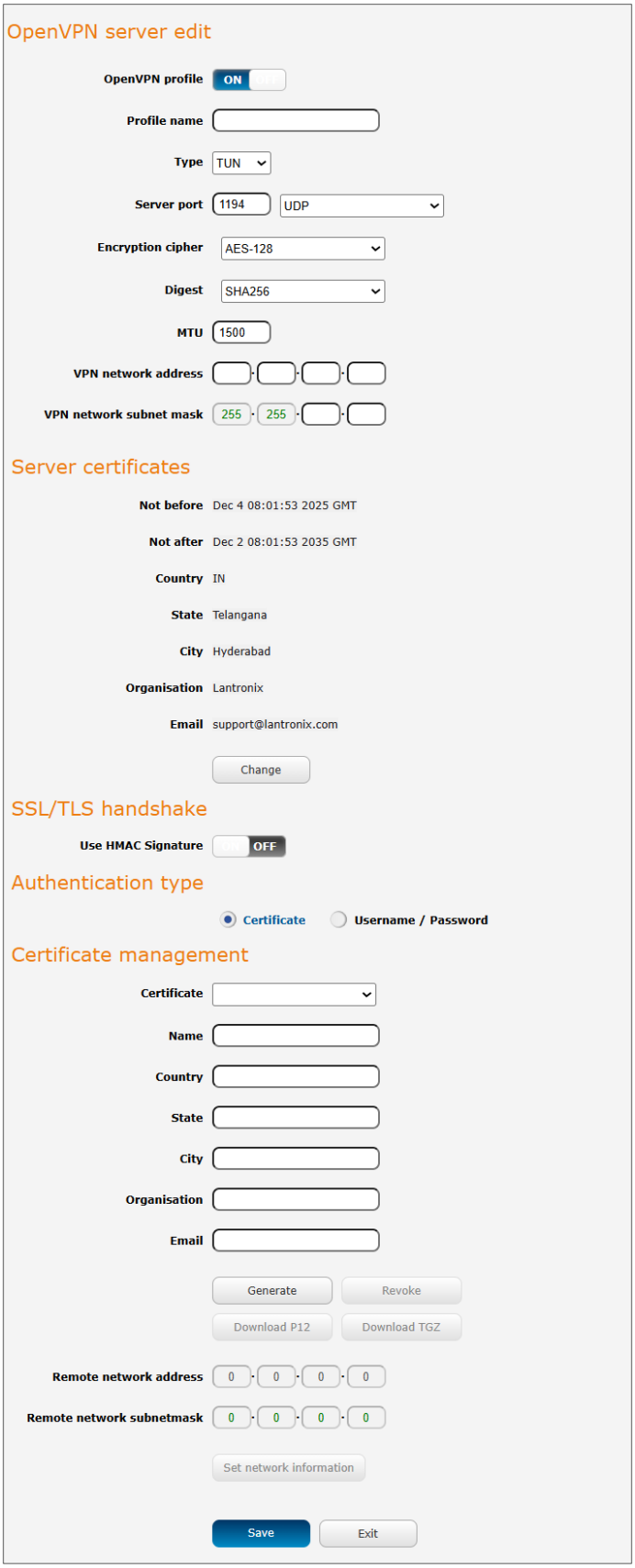


Figure 8-45 OpenVPN server configuration page

OpenVPN server edit

Table 8-15 OpenVPN server edit details

Parameter	Description
OpenVPN profile	Set to **ON** to enable.
Profile name	Enter a name for the OpenVPN server.
Type	Select the OpenVPN connection type. Options are: • **TUN** – Network Tunnel • **TAP** – Network TAP Default is **TUN**.
Server port	Enter the server port and select the packet type to use for your VPN server. Options are: • **UDP** • **TCP** Default port is 1194 and default packet type is **UDP**
Encryption cipher	Select the Encryption cipher type. Specifies the algorithm used to encrypt the data transmitted through the VPN tunnel. Options are: • **AES-256** • **AES-192** • **AES-128** • **None**
Digest	Select Digest type. It defines the message digest (hash) algorithm used for HMAC (Hash-based Message Authentication Code) to verify the integrity and authenticity of data packets. Options are: • **SHA1** • **SHA256** • **None**
MTU	Enter the Maximum Transmission Unit (MTU) size. It specifies the maximum size (in bytes) of a data packet that can be transmitted through the VPN tunnel without fragmentation.
VPN network address	Enter the IP address to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
VPN network subnet mask	Enter the subnet mask to assign to your VPN.

Server certificates

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

SSL/TLS handshake

HMAC or Hash-based Message Authentication Code is a method of calculating a message authentication code using a cryptographic hash function and a cryptographic key. To use the HMAC signature as an additional key and level of security, set the **Use HMAC Signature** to **ON** position and then click the **Generate**, the router will randomly generate the key. The **Server key timestamp** field is updated with the time when the key was generated. Click **Download** to download the key file so that it can be uploaded on the client.

Authentication type

Select an **Authentication type**. Options are:

- **Certificate**
- **Username / Password**

If you select **Certificate**, the **Certificate management** section displays. If you select **Username / Password** the **Username / Password** section displays.

Certificate management

In the Certificate Management section, enter the required details to create a client certificate. All fields are required. Once you enter the values for all the fields, click **Generate**.

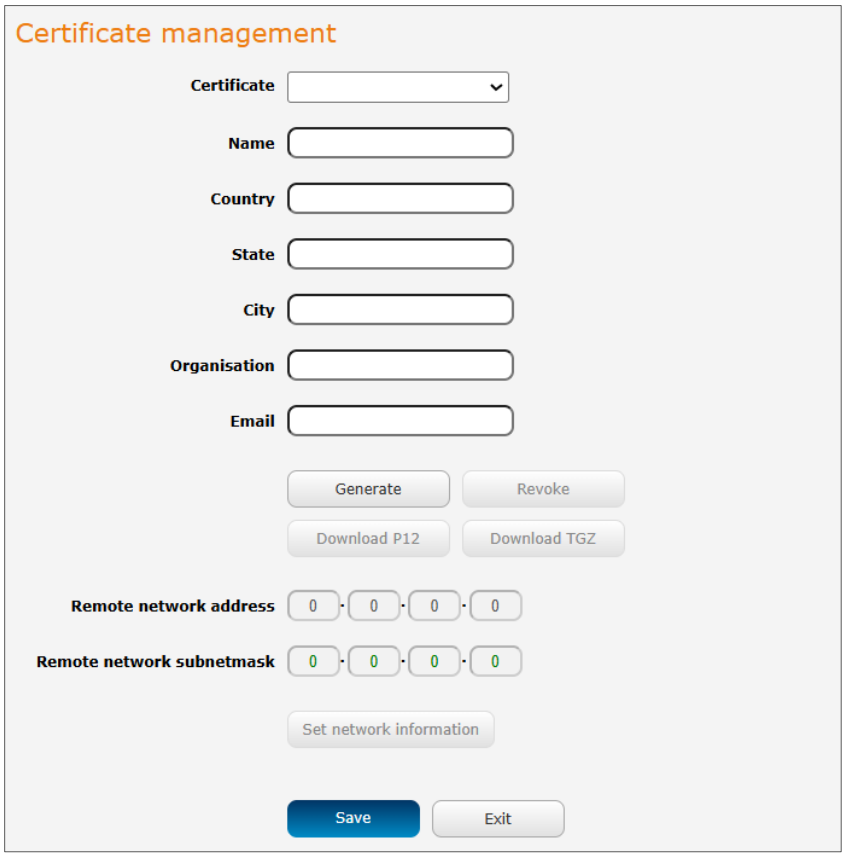


Figure 8-46 Certificate management

You can click the **Download P12** or **Download TGZ** to save the certificate in the corresponding format. If the integrity of your network has been compromised, you can return to this screen, use the **Certificate** drop-down list to select the certificate, and click **Revoke** to disable it.

Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the values for **Remote network address** and **Remote network subnetmask** fields and click **Set network information**. 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 as it is not aware of the remote client's subnet.

Username / Password Authentication

In the Username/Password section, enter the **Username** and **Password** to use for authentication on the OpenVPN Server. Click the **Download CA certificate** or **Download CA TGZ** to save the ca.crt file in the corresponding format. This file must be provided to the client.

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

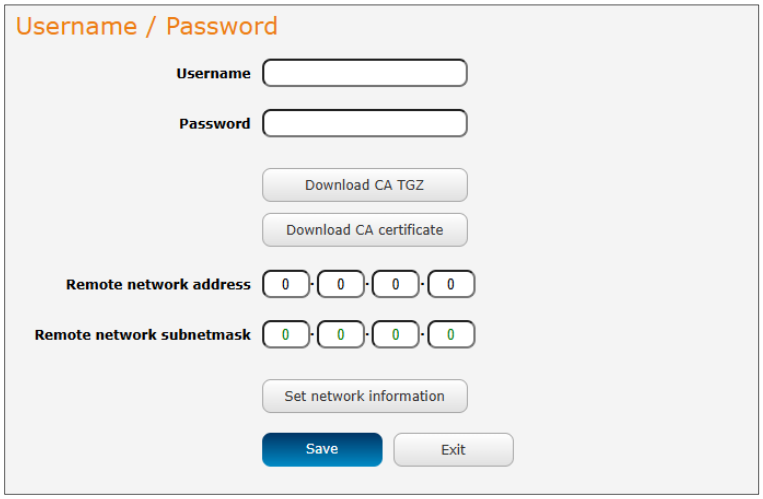


Figure 8-47 Username / Password section

Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the values for **Remote network address** and **Remote network subnetmask** and click the **Set Network Information**. 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.

Once you configure all the sections for the OpenVPN server click **Save** to the save the settings. The server is added to **OpenVPN server list**. Click the icon for a server to edit it, and the icon to delete it.

OpenVPN Client

To configure an OpenVPN client, click **+Add** button for the OpenVPN client list in the Open VPN page. The different settings display.

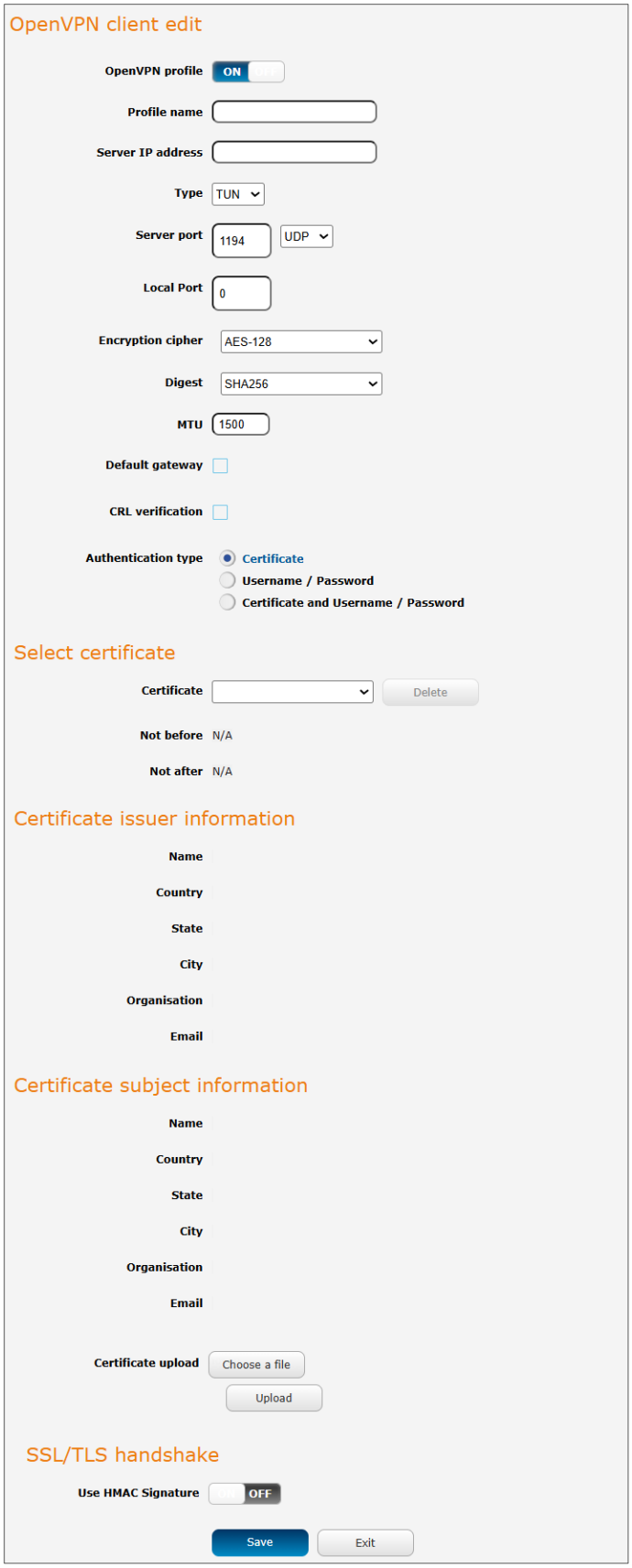


Figure 8-48 OpenVPN client configuration page

OpenVPN client edit

Table 8-16 OpenVPN client edit details

Parameter	Description
OpenVPN profile	Set to **ON** to enable.
Profile name	Enter a name for the OpenVPN client.
Server IP address	Enter the WAN IP address/host domain name of the OpenVPN server
Type	Select the OpenVPN connection type. Options are: • **TUN** – Network Tunnel • **TAP** – Network TAP Default is **TUN**.
Server port	Enter the server port and select the packet type to use for your VPN server. Options are: • **UDP** • **TCP** Default port is 1194 and default packet type is **UDP**
Local Port	Enter the port to use.
Encryption cipher	Select Encryption cipher type. Specifies the algorithm used to encrypt the data transmitted through the VPN tunnel. Options are: • **AES-256** • **AES-192** • **AES-128** • **None**
Digest	Select Digest type. It defines the message digest (hash) algorithm used for HMAC (Hash-based Message Authentication Code) to verify the integrity and authenticity of data packets. Options are: • **SHA1** • **SHA256** • **None**
MTU	Enter the Maximum Transmission Unit (MTU) size. It specifies the maximum size (in bytes) of a data packet that can be transmitted through the VPN tunnel without fragmentation.
Default gateway	If selected, all the outbound traffic (internet and private network) is sent through the VPN tunnel.
CRL verification	If selected, it enables you to check the Certificate Revocation List (CRL) to ensure that a server certificate has not been revoked and is still trustworthy.
Authentication type	Select and Authentication type. Options are: • **Certificate**

Parameter	Description
	• **Username / Password** • **Certificate and Username / Password**

Certificate Authentication

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

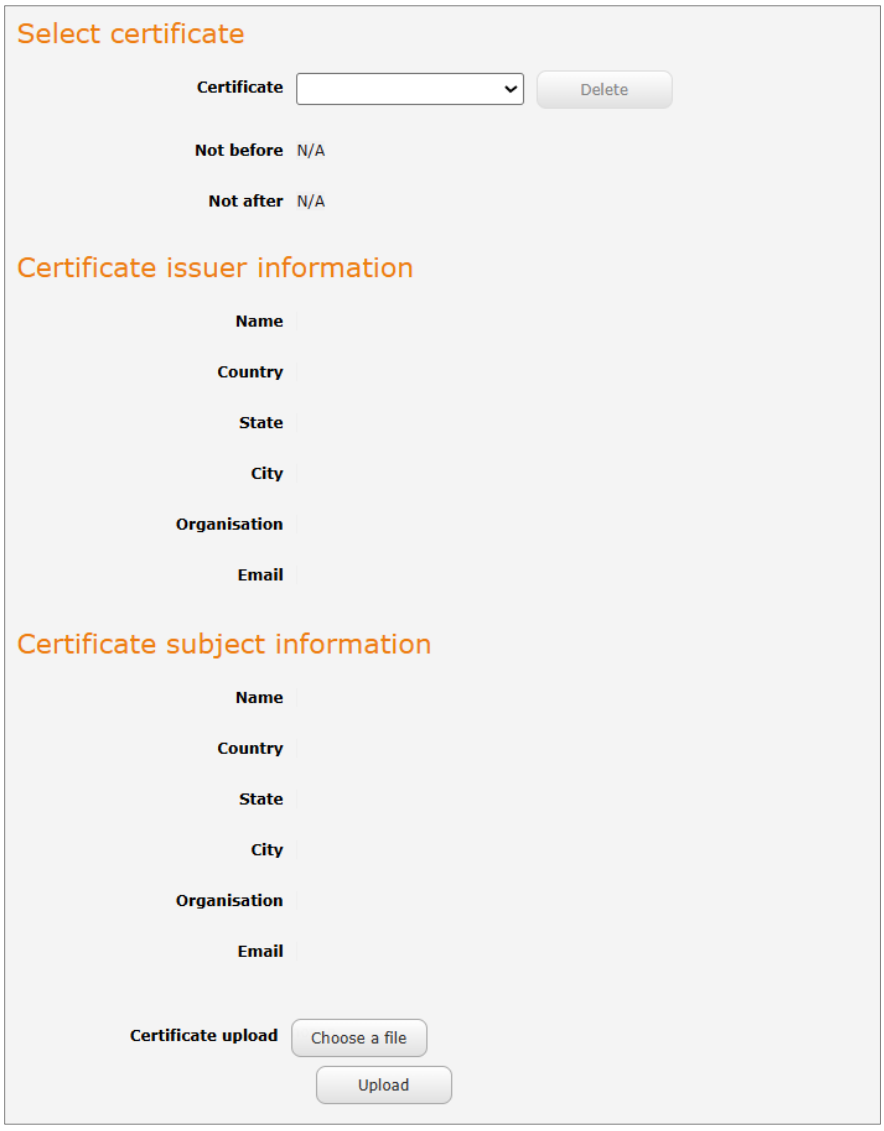


Figure 8-49 OpenVPN client certificate authentication settings

In the **Certificate upload** field at the bottom of the screen, click **Choose a file**, locate and select the certificate file saved during OpenVPN server configuration. Click the **Upload** to upload it to the router.

Username / Password Authentication

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

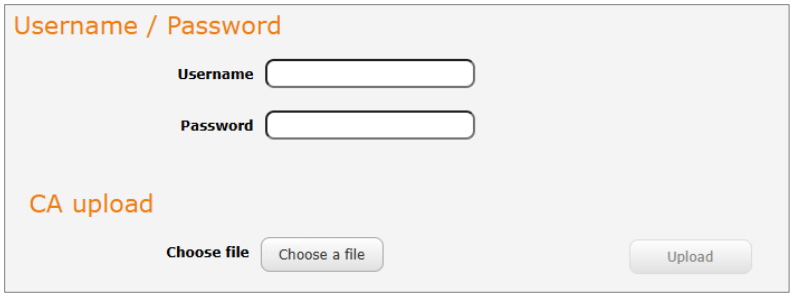


Figure 8-50 OpenVPN client username / password authentication settings

To configure:

1. Enter the **Username** and **Password** to authenticate with the OpenVPN server.
2. In the **Choose file** field click **Choose file**, locate and select the CA certificate file you had saved during OpenVPN server configuration .
3. Click **Upload** to send it to the router.

Certificate and Username / Password Authentication

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

SSL/TSL handshake

Once you select the required Authentication type and complete the configuration, proceed to the SSL/TLS handshake section if you have and additional SSL/TLS key created on the server.

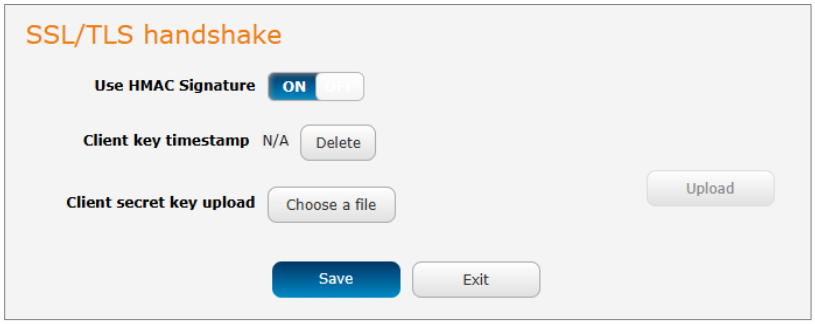


Figure 8-51 OpenVPN client SSL/TLS handshake section

To configure:

1. Set **Use HMAC Signature** to **ON**.
2. In the **Client secret key upload** field, click **Choose a file**, then locate and select the file.
3. Click **Upload** to upload the file.

Once you have completed the configuration of all the above sections, click **Save** to save and apply the settings. The client is added to the OpenVPN client list.

Click the icon for a client to edit it, and the icon to delete it.

OpenVPN P2P

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

To configure an Open VPN P2P profile, click **+Add** button for the OpenVPN P2P list. The different settings display.

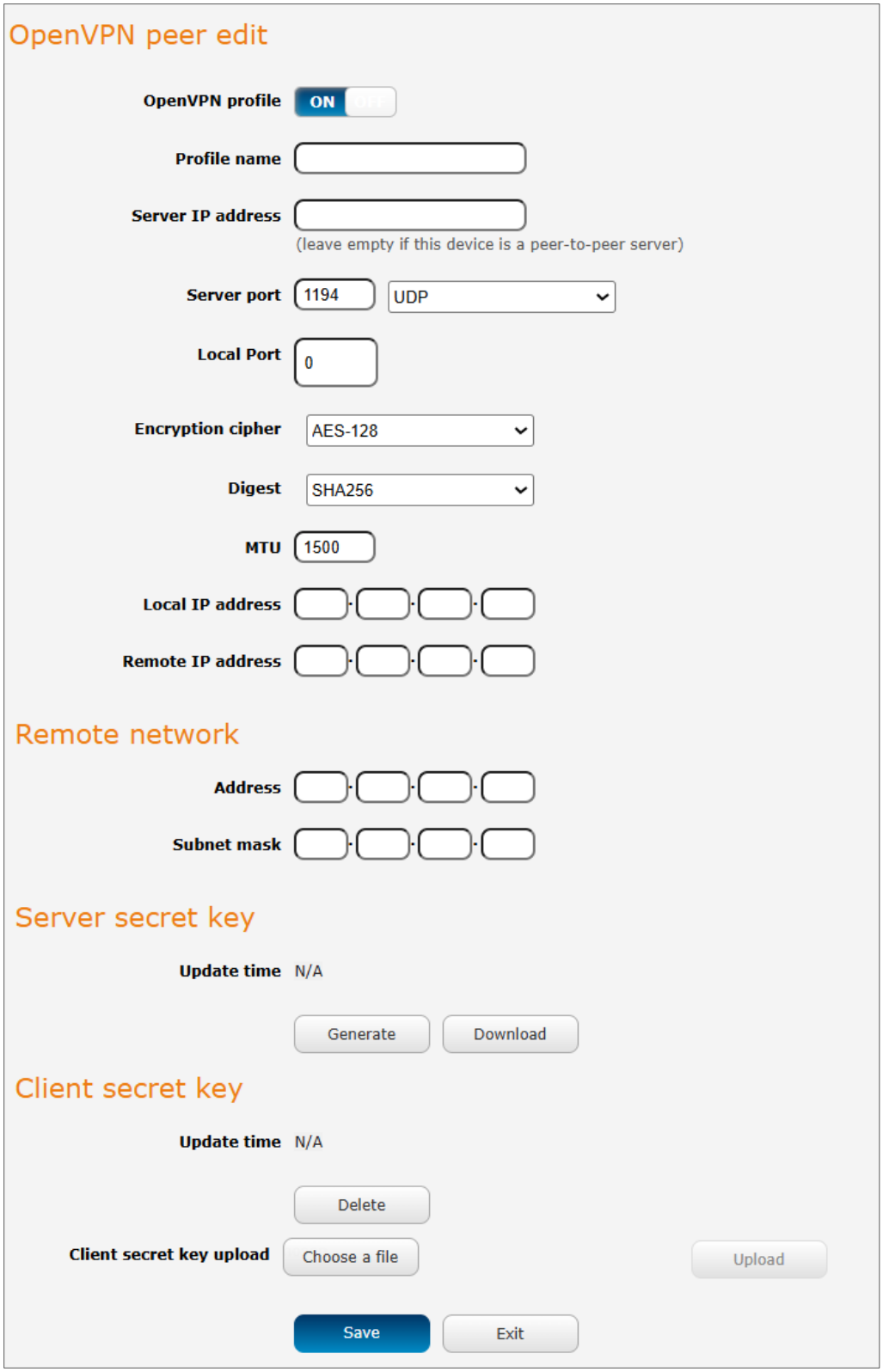


Figure 8-52 OpenVPN P2P settings

Table 8-17 OpenVPN P2P configuration details

Parameter	Description
OpenVPN peer edit	
OpenVPN profile	Set to **ON** to enable.
Profile name	Enter a name for OpenVPN P2P profile.
Server IP address	For the router designated as the server, leave this field empty. For the router designated as the client, enter the WAN IP address/host domain name of the server.
Server port	Enter a port number to use and select a packet type to use for the OpenVPN server. Options are: • **UDP** • **TCP** The default OpenVPN port is **1194** and default packet type is **UDP**.
Local port	Enter the port to use.
Encryption cipher	Select the Encryption cipher to use. Options are: • **AES-256** • **AES-192** • **AES-128** • **None**
Digest	Select the Digest to use: • **SHA1** • **SHA256** • **None**
MTU	Enter the Maximum Transmission Unit (MTU) size. It specifies the maximum size (in bytes) of a data packet that can be transmitted through the VPN tunnel without fragmentation.
Local IP address	Enter the Local IP address of the VPN tunnel.
Remote IP address	Enter the Remote IP address of the VPN tunnel.
Remote network (These fields inform the Master node of the LAN address scheme of the slave)	
Address	Enter the network address.
Subnet mask	Enter the network subnet mask
Server secret key	
Update time	Displays the timestamp for the generated key.

Parameter	Description
	Click **Generate** to create a secret key to be shared with the slave. When the timestamp displays, click **Download** to save the file that needs to be exchanged with the other router.
Client secret key	
Update time	Displays the timestamp for the generated key.
Client secret key upload	After you have saved the secret key file on each router, click **Choose a file**, locate and select the secret key file for the master, and then Click **Upload** to send it to the slave. Perform the same steps for the other router, to upload the slave's secret key file to master.

Click **Save** to save and apply the settings. The profile is added to the OpenVPN P2P list.

Click the icon for a profile to edit it, and the icon to delete it.

PPTP client

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

To access the PPTP client page, navigate to **Networking > VPN > PPTP client**.

Figure 8-53 PPTP client list

To configure a PPTP client, click **+Add** button for the PPTP client list. The PPTP client configuration settings display.

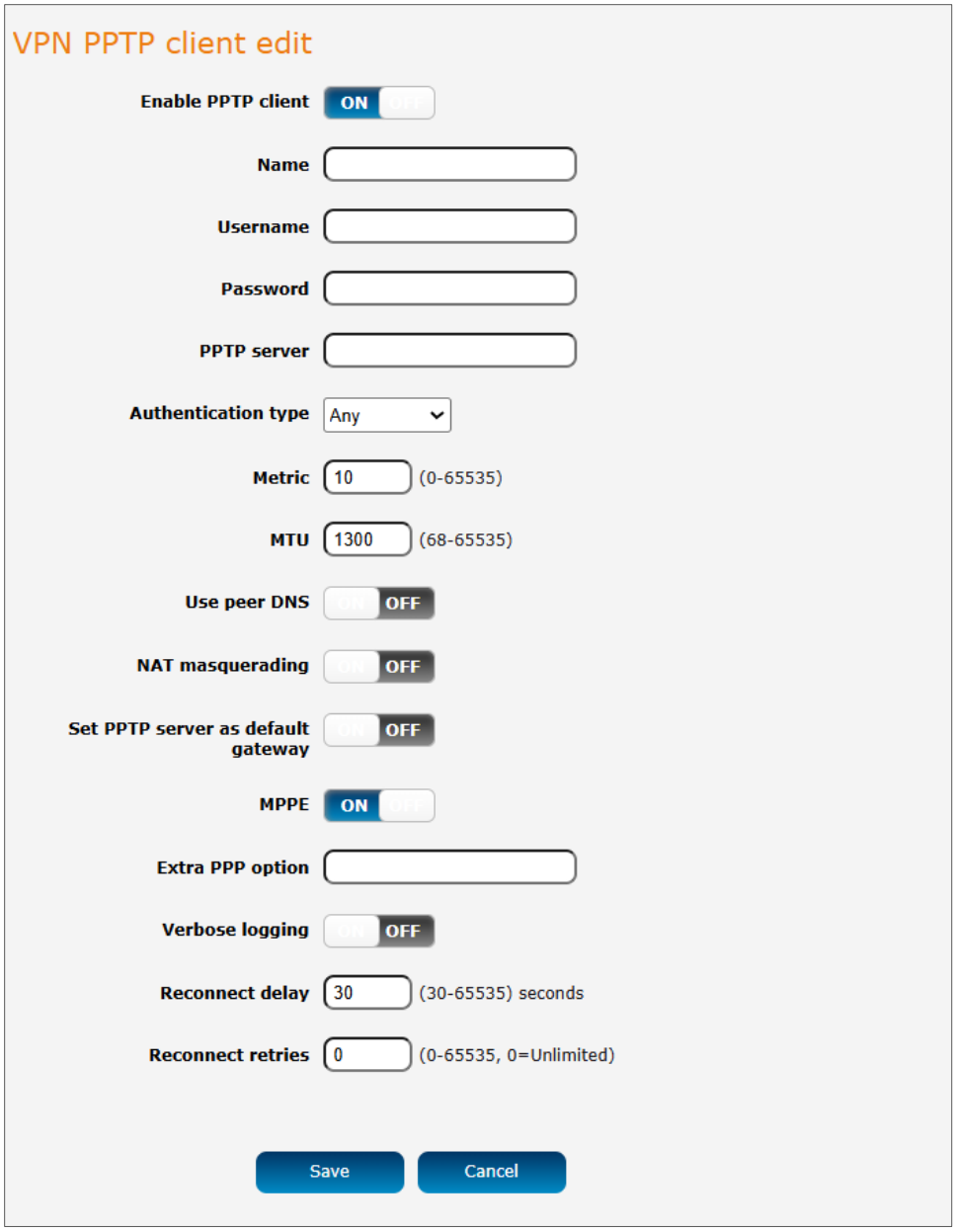


Figure 8-54 PPTP client settings

Table 8-18 PPTP client configuration details

Parameter	Description
Enable PPTP client	Set to **ON** to enable.
Name	Enter a profile name for the tunnel.
Username	Enter a username for the PPTP account.
Password	Enter a password for the PPTP account.
PPTP server	Enter the IP address/host domain name of the PPTP server
Authentication type	Select the authentication type to use. Options are:

Parameter	Description
	• **Any** – If you do not know the authentication method used, select any, and the router will attempt to determine the correct authentication type. • **ms-chap-v2** – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol which was introduced in Windows® NT 4.0 and is still supported today. • **ms-chap** – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista. • **CHAP** – Uses a three-way handshake to authenticate the identity of a client. • **EAP** – Extensible Authentication Protocol. An Authentication protocol commonly used in wireless networks. • **PAP** – The Password Authentication Protocol uses a password as a means of authentication and is commonly supported. PAP is not recommended because it transmits passwords unencrypted and is not secure.
Metric	Enter the metric value. It helps the router prioritize routes and must be a number between 0 and 65535. The default value is 10 and should not be modified unless you are aware of the effect your changes will have on the device.
MTU	Enter the size of the Maximum Transmission Unit (MTU). It specifies the maximum size (in bytes) of a data packet that can be transmitted through the VPN tunnel without fragmentation. Default value is 1300.
Use peer DNS	Set to **ON** to enable. It allows you to select whether the remote clients will use the Domain Name Server of the PPTP server.
NAT masquerading	Set to **ON** to enable. It allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router originated from the WAN IP address of the router's internal NAT IP address.
Set PPTP server as default gateway	Set to **ON** to enable. It allows all outbound data packets to go out through the PPTP tunnel.
MPPE	Set to **ON** to enable the Microsoft Point-to-Point Encryption feature. It is used to secure transmissions.
Extra PPP option	Specify any extra commands or parameters that you wish to use when the PPP connection is established.
Verbose logging	Set to **ON** to enable. It allows the router to output detailed logs regarding the PPTP connection in the System Log section of the router interface.
Reconnect delay	Enter the time in seconds that the router will wait before attempting to connect to the PPTP server if the connection is disconnected. The minimum

Parameter	Description
	time to wait is 30 seconds to not flood the PPTP server with connection requests, while the maximum time to wait is 65335 seconds.
Reconnect retries	Enter the number of connection attempts that the router should make when PPTP connection is disconnected. If set to 0, the router will retry the connection indefinitely. If you set a value other than 0 for the maximum number of retries, it cannot be greater than 65335.

Click **Save** to save and apply the settings, the PPTP client displays in the PPTP client list.

Click the icon for a PTP client to edit it, and the icon to delete it.

GRE tunnelling

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

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

Figure 8-55 GRE client list

To configure a GRE client, click **+Add** button for the GRE client list. The GRE client configuration settings display.

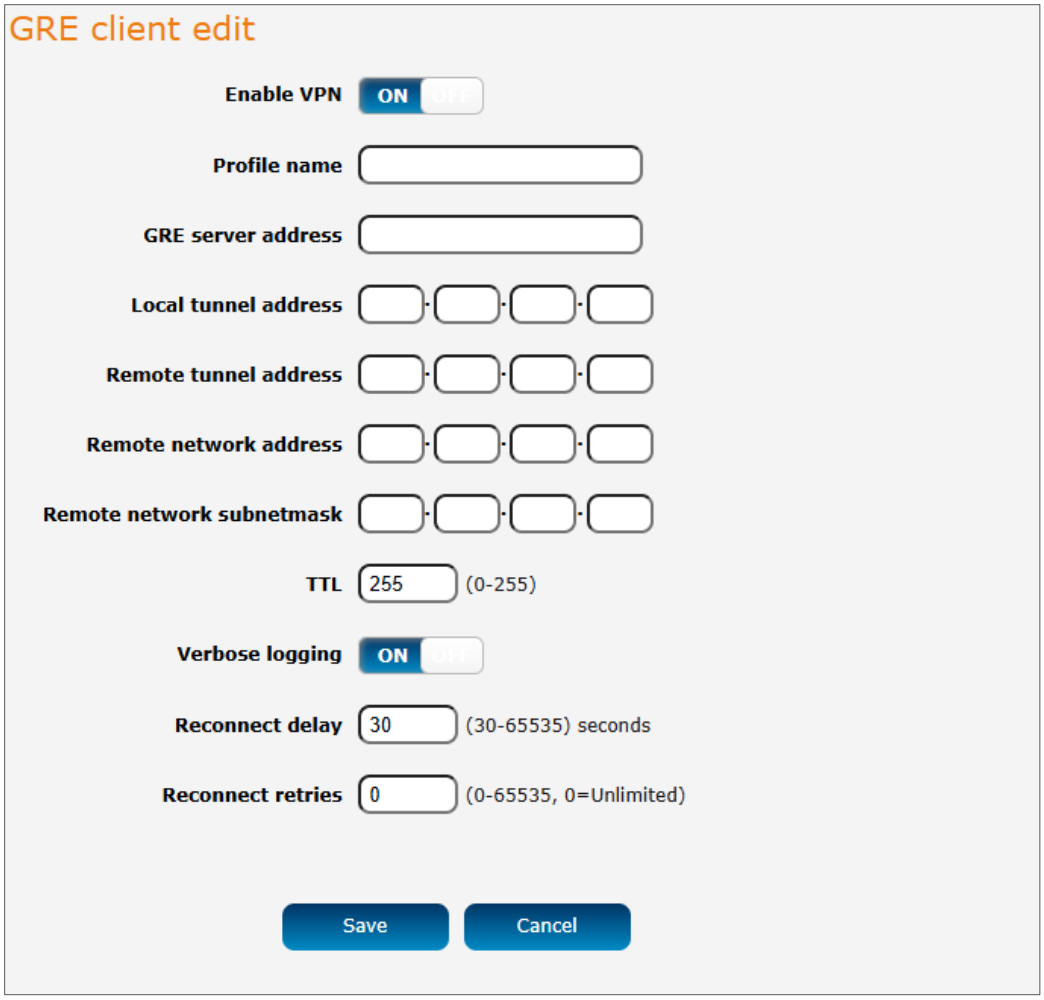


Figure 8-56 GRE client settings

Table 8-19 GRE client configuration details

Parameter	Description
Enable VPN	Set to **ON** to enable.
Profile name	Enter a profile name for the tunnel.
GRE server address	Enter the IP address or domain name of the GRE server.
Local tunnel address	Enter the IP address to assign the tunnel locally.
Remote network address	Enter the IP address to assign to the remote tunnel.
Remote network subnetmask	Enter the subnet mask of the remote network.
TTL	The Time to Live (TTL) 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 of the value that limits how long 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

Parameter	Description
	zero before the datagram reaches its destination the data packet is discarded, and an error message is sent to the sender.
Verbose logging	Set to **ON** to enable. It allows the router to output detailed logs regarding the GRE tunnel in the System Log section of the router interface.
Reconnect delay	Enter the time in seconds that the router will wait before attempting to connect to the GRE server if the connection is disconnected. The minimum time to wait is 30 seconds to not flood the PPTP server with connection requests, while the maximum time to wait is 65335 seconds.
Reconnect retries	Enter the number of connection attempts that the router should make when GRE connection is disconnected. If set to 0, the router will retry the connection indefinitely. If you set a value other than 0 for the maximum number of retries, it cannot be greater than 65335.

Click **Save** to save and apply the settings, the GRE client displays in the GRE client list.

Click the icon for a GRE client to edit it, and the icon to delete it.

9. Services

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

- Dynamic DNS
- Network Time (NTP)
- Data stream manager
- Remote management
- Event notification
- Email settings
- SMS messaging
- Network quality
- Percepxion

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

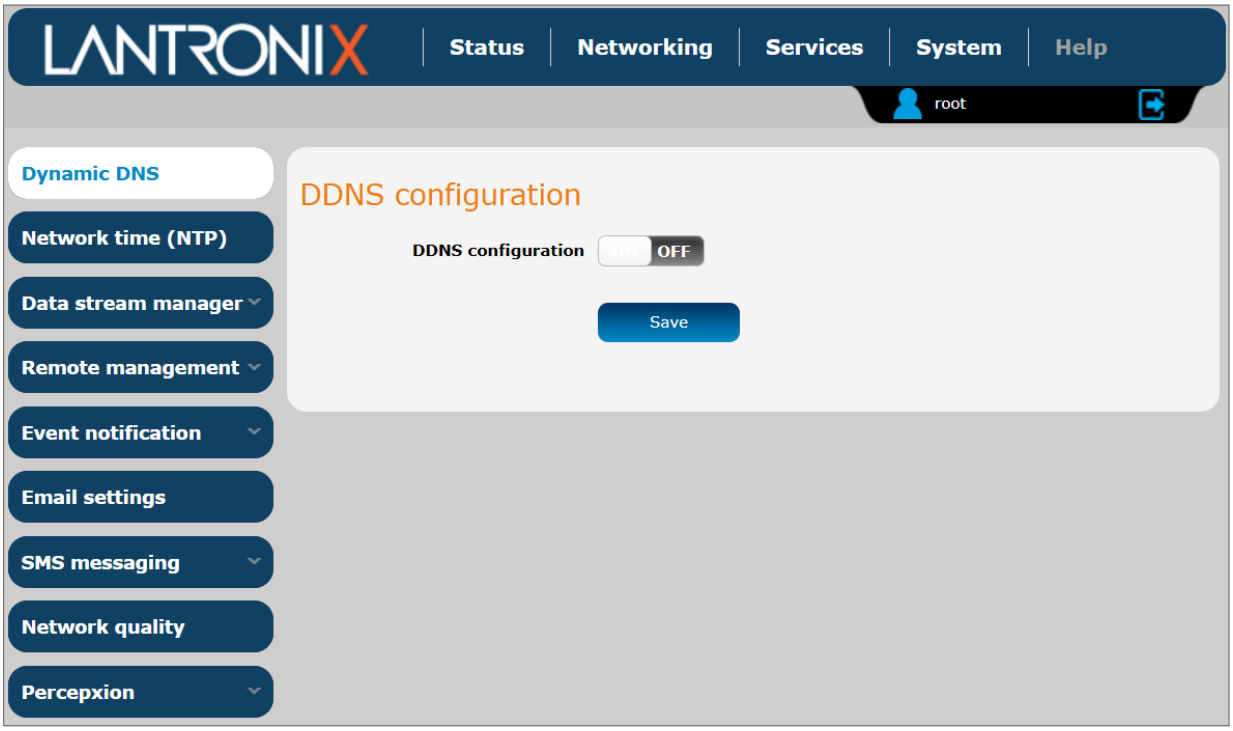


Figure 9-1 Services page

Dynamic DNS

Dynamic DNS provides a method for the router to update an external name server with the current WAN IP address. The Dynamic DNS (DDNS) page allows you to configure the Dynamic DNS feature of the router. Several Dynamic DNS hosts are available from which to select. To access the Dynamic DNS page, navigate to **Services > Dynamic DNS**.

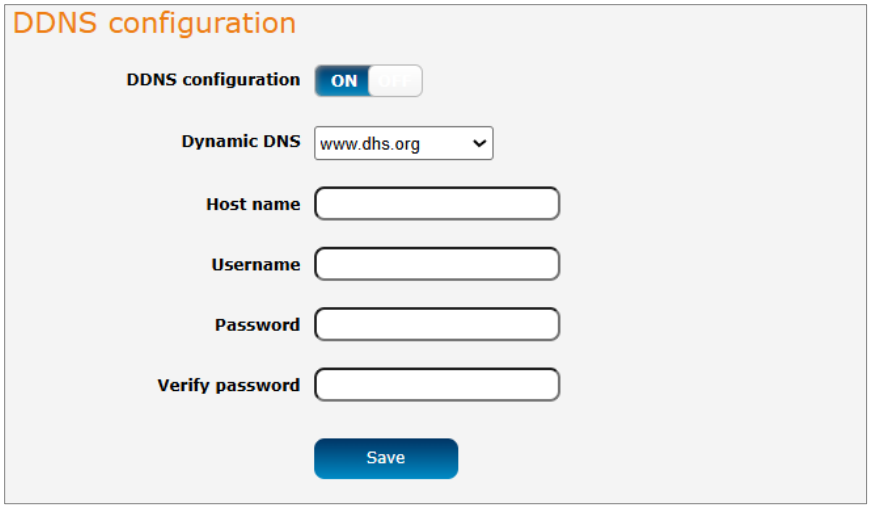


Figure 9-2 DDNS configuration settings

Table 9-1 DDNS configuration details

Parameter	Description
DDNS configuration	Set to **ON** to enable.
Dynamic DNS	Select the Dynamic DNS service to use. Options are: • **www.dhs.org** • **www.dyndns.org** • **www.easydns.com** • **www.no-ip.com** • **www.zoneedit.com**
Host name	Enter your hostname.
Username	Enter the username for your DDNS account.
Password	Enter the password for your DDNS account.
Verify password	Re-enter the password for your DDNS account.

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

Network time (NTP)

The Network Time Protocol (NTP) allows you to configure the NTC-201 router to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded. Any NTP server available publicly on the internet may be used.

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

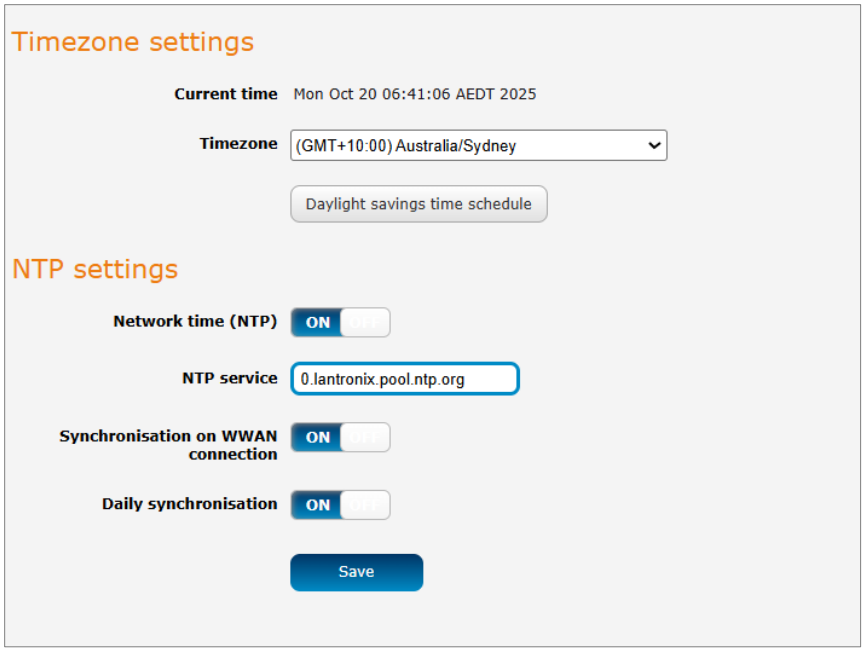


Figure 9-3 NTP settings

Table 9-2 NTP settings configuration details

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

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

Data stream manager

The data stream manager allows you to create mappings between two endpoints on the router. These endpoints may be physical or virtual. For example, you could configure a TCP Server as an endpoint. You can then configure a virtual data tunnel or stream between the endpoints.

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

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

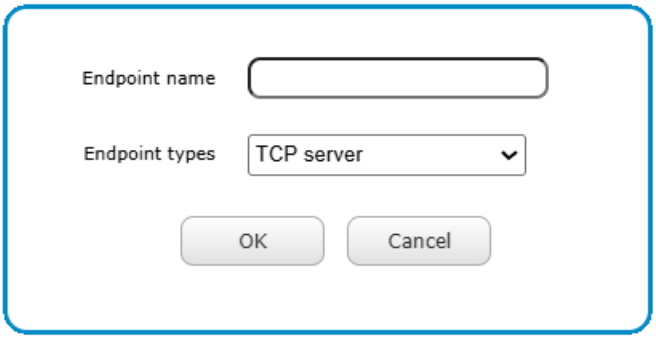
Endpoints

Endpoints need to be defined to create a data stream. The Endpoints page allows you to add datapoints. To access the endpoints page, navigate to **Services > Data stream manager > Endpoints**.

Figure 9-4 Endpoints page

To create an endpoint:

1. Click the **+Add** button for the Endpoints list, the below window displays.



2. In the **Endpoint name** field, type a name for the endpoint. The name can contain alphanumeric characters only i.e. A-Z, a-z, 0-9.
3. In the **Endpoint types** field, select the type of endpoint you want to create. Options are:
   - **TCP server**
   - **TCP client**
   - **UDP server**
   - **UDP client**
   - **User defined executable**
   - **TCP connect-on-demand**
4. Once you select the required Endpoint type, click **OK**. The configuration settings for that endpoint type display. See Endpoint configuration below for configuration details of all endpoint types.
5. Once you complete the configuration of an endpoint, click **Save** to save and apply the settings. The endpoint is added to the Endpoints list.

Click the icon for an endpoint to edit it, and the icon to delete it.

Endpoint configuration

TCP server

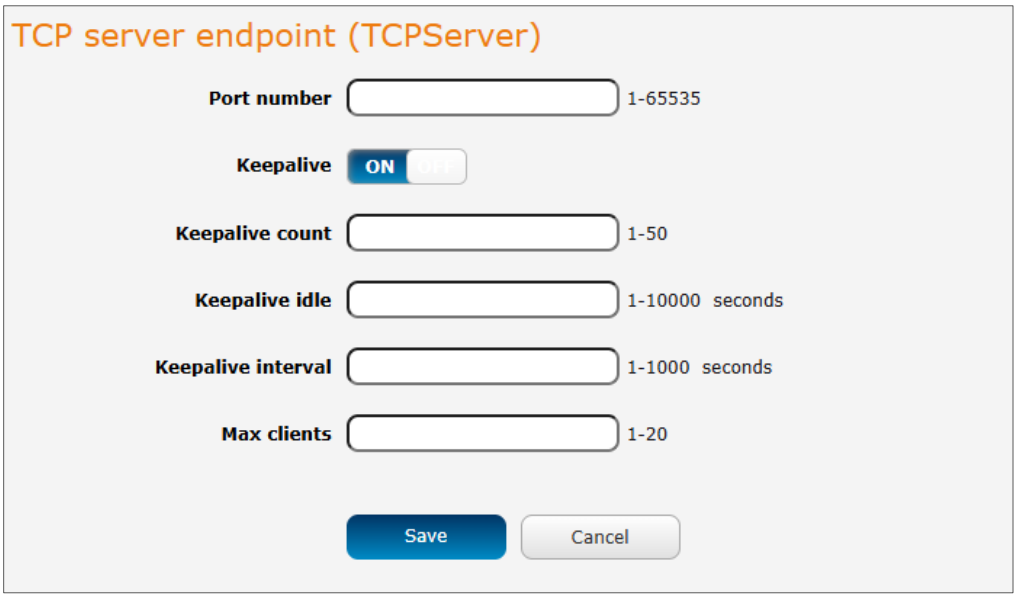


Figure 9-5 TCP server endpoint configuration

Table 9-3 TCP server endpoint configuration details

Parameter	Description
Port number	Enter the port number of the TCP server
Keepalive	Set to **ON** to enable. Keepalive sends a message to check that the link is still active or to keep it active.
Keepalive count	Enter the number of keepalive messages to send.
Keepalive idle	Enter the duration between two keepalive transmissions when in idle condition.
Keepalive interval	The duration between two successive keepalive retransmissions.
Max clients	The maximum number of clients a TCP server endpoint can handle.

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

TCP client

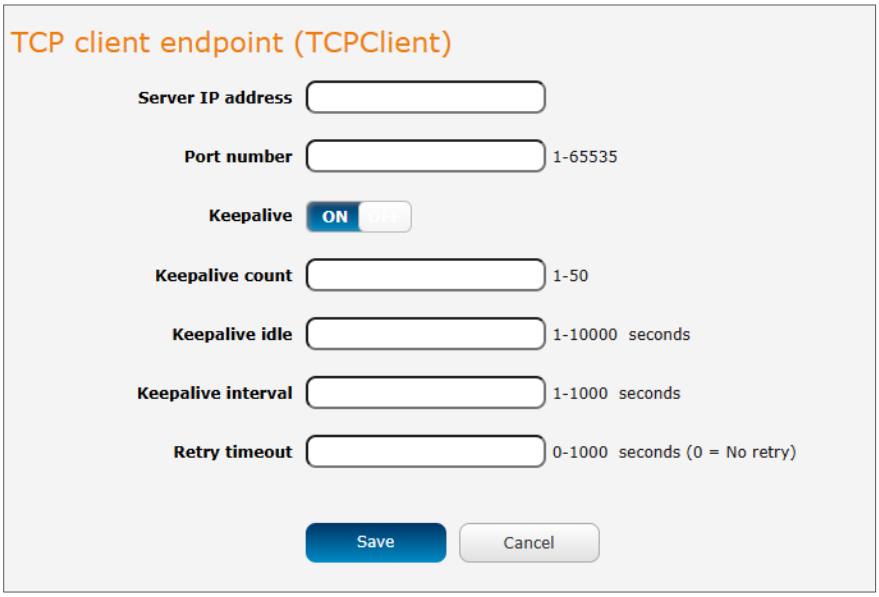


Figure 9-6 TCP client endpoint configuration

Table 9-4TCP client endpoint configuration details

Parameter	Description
Server IP address	Enter the IP address of the TCP client.
Port number	Enter the port number of the TCP client.
Keepalive	Set to **ON** to enable. Keepalive sends a message to check that the link is still active or to keep it active.
Keepalive count	Enter the number of keepalive messages to send.
Keepalive idle	Enter the duration between two keepalive transmissions when in idle condition.
Keepalive interval	The duration between two successive keepalive retransmissions.
Retry timeout	Enter the number of seconds to wait between attempts to re-establish a connection in the event that it is lost.

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

UDP server

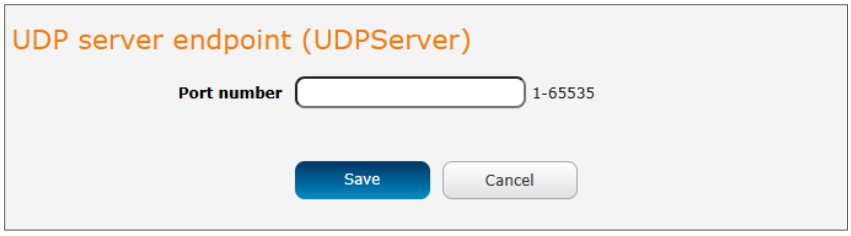


Figure 9-7 UDP server endpoint configuration

In the **Port number** field, enter the port number of the UDP server. Click **Save** to save and apply the settings and create the endpoint.

UDP client:

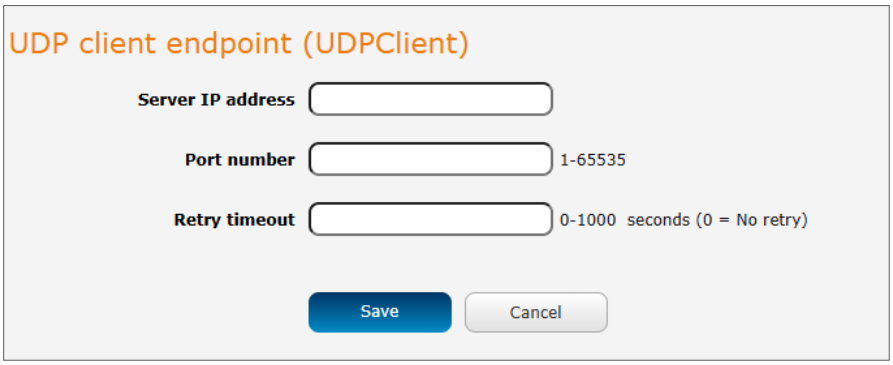


Figure 9-8 UDP client endpoint configuration

Table 9-5 UDP client endpoint configuration details

Parameter	Description
Server IP address	Enter the IP address of the UDP client.
Port number	Enter the port number of the UDP client.
Retry timeout	Enter the number of seconds to wait between attempts to re-establish a connection in the event that it is lost.

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

User defined executable

Allows you to specify an executable and parameters to be used as an endpoint.

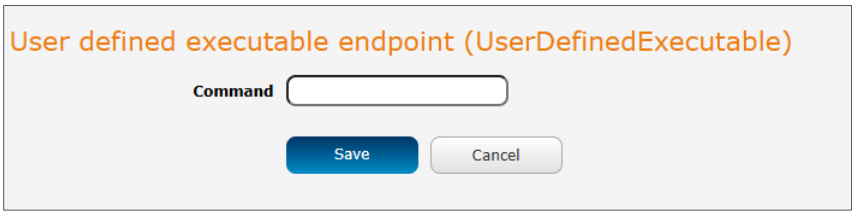


Figure 9-9 User defined executable endpoint configuration

For example, the following executable reads the phone module temperature every second.

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

The temperature can then be sent to another endpoint.

Once to enter the required command, click **Save** to save and apply the settings and create the endpoint.

TCP connect-on-demand endpoint

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

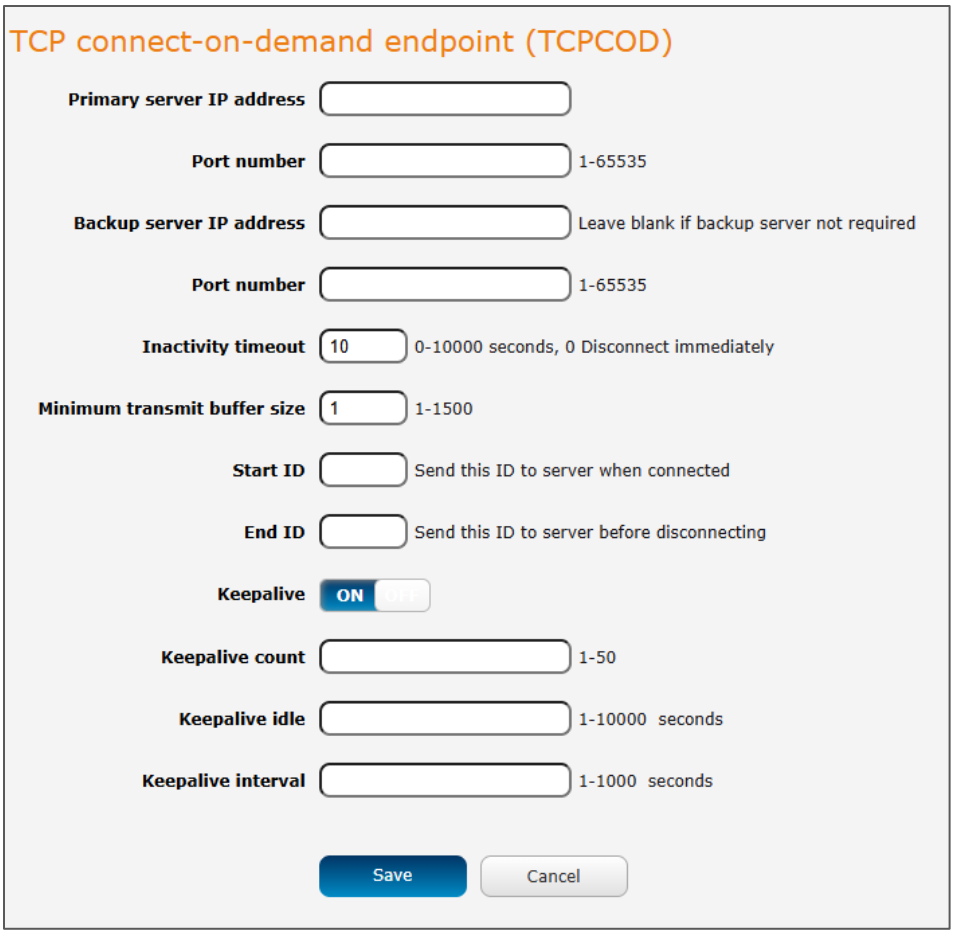


Figure 9-10 TCP connect-on-demand endpoint configuration

Table 9-6 TCP connect-on-demand endpoint configuration details

Parameter	Description
Primary server IP address	The IP address of the TCP server to which the router should attempt the initial connection.
Port number	The port number that the TCP server operates on.
Backup server IP address	If connection to the primary server fails, the router will attempt to connect to this address.
Port number	The port number that the backup TCP server operates on.
Inactivity timeout	The time in seconds that the socket is considered idle/inactive if no packets are sent. The timer begins at the end of the last sent packet. The valid range is 0-10000 seconds. If this field is set to 0, the client disconnects immediately after sending a packet.
Minimum transmit buffer size	The number of bytes that must be reached before the client decides to transmit.
Start ID	If configured, this string is sent before any serial data is sent, every time the client connects <START ID><SERIAL DATA>

Parameter	Description
End ID	If configured, this string is sent after all serial data, just before the client disconnects <START ID><SERIAL DATA><END ID>
Keepalive	Keepalive sends a message to check that the link is still active or to keep it active.
Keepalive count	The number of keepalive messages to send.
Keepalive idle	The duration between two keepalive transmissions when in idle condition.
Keepalive interval	The duration between two successive keepalive retransmissions.

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

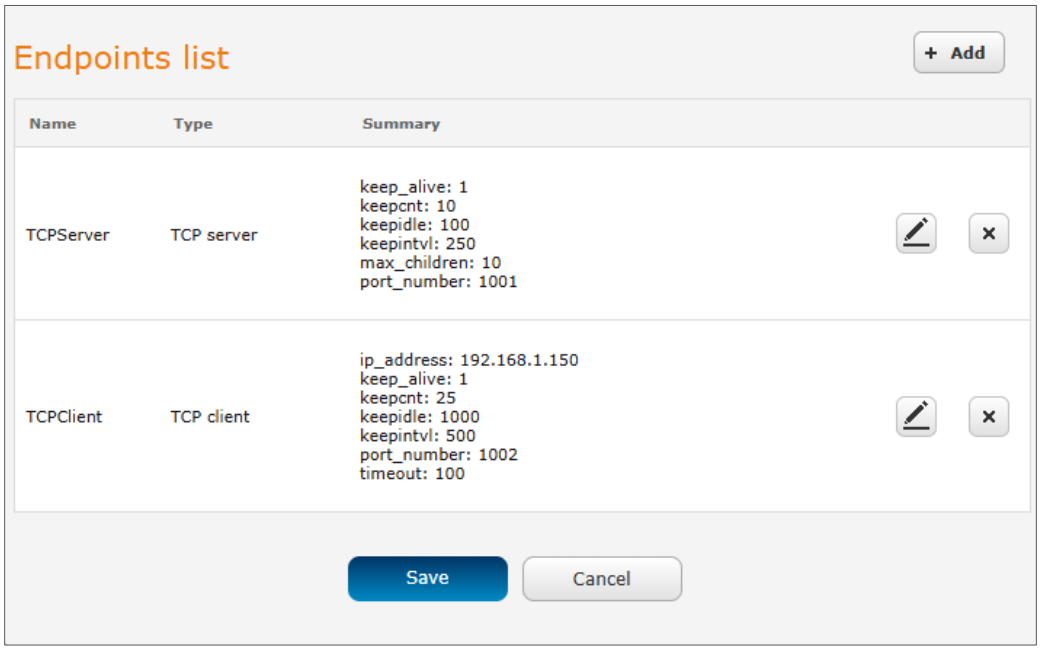


Figure 9-11 Endpoints list with created endpoints

Streams

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

To access the Streams page, navigate to **Services > Data stream manager > Streams**.

Figure 9-12 Streams page

Important: *When any changes to the Data stream manager configuration are detected, all data streams are stopped and restarted as per the new configuration.*

Multiple Modbus clients cannot connect simultaneously to Modbus serial slaves connected to the router.

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

To create a new data stream, click **+Add** button for the Data stream list, the different configuration settings display.

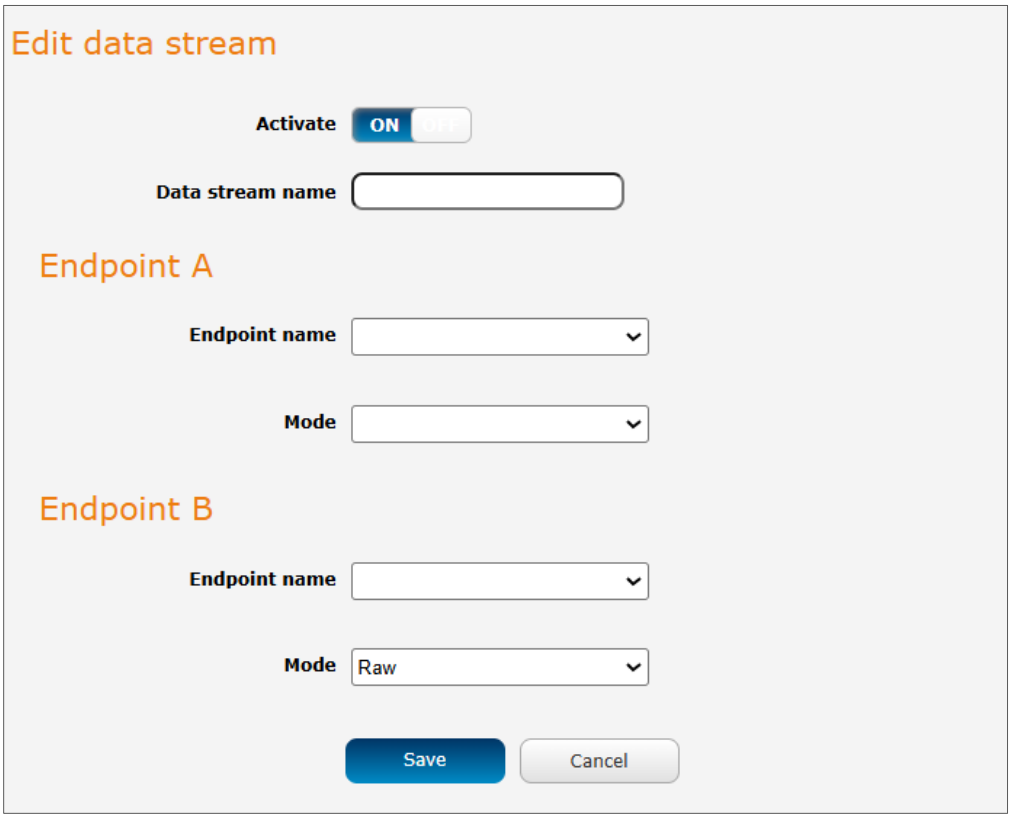


Figure 9-13 Data stream settings

Table 9-7 Data stream configuration details

Parameter	Description
Edit data stream	
Activate	Set to **ON** to enable the data stream.
Data stream name	Enter a name for the data stream.
Endpoint A	
Endpoint name	Select one of the endpoints you have created. This endpoint should be the starting point of the stream.

Parameter	Description
Mode	Select the mode of operation of the endpoint. The mode indicates the type of transformation of the data as it leaves this endpoint.
Endpoint B	
Endpoint name	Select one of the endpoints you have created. This endpoint should be the destination of the stream.
Mode	Select the mode of operation of the endpoint. The mode indicates the type of transformation of the data as it arrives at this endpoint.

Click **Save** to save and apply the settings. The data stream to added to the data stream list.

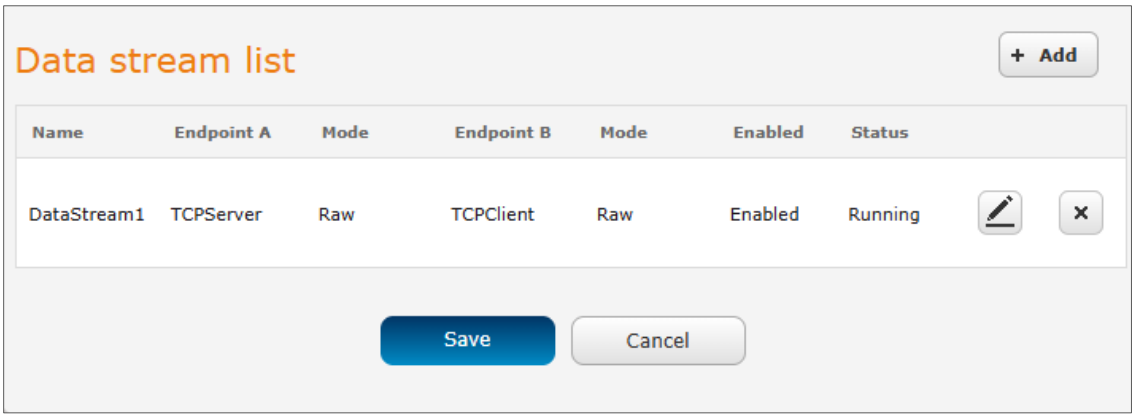


Figure 9-14 Enabled data stream

Click the icon for a data stream to edit it, and the icon to delete it.

Remote management

SNMP

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

SNMP traps are messages from the router to the Network Management System sent as UDP packets. They are often used to notify the management system of any significant event. For example, if the status of the link changes from up to down or vice versa.

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

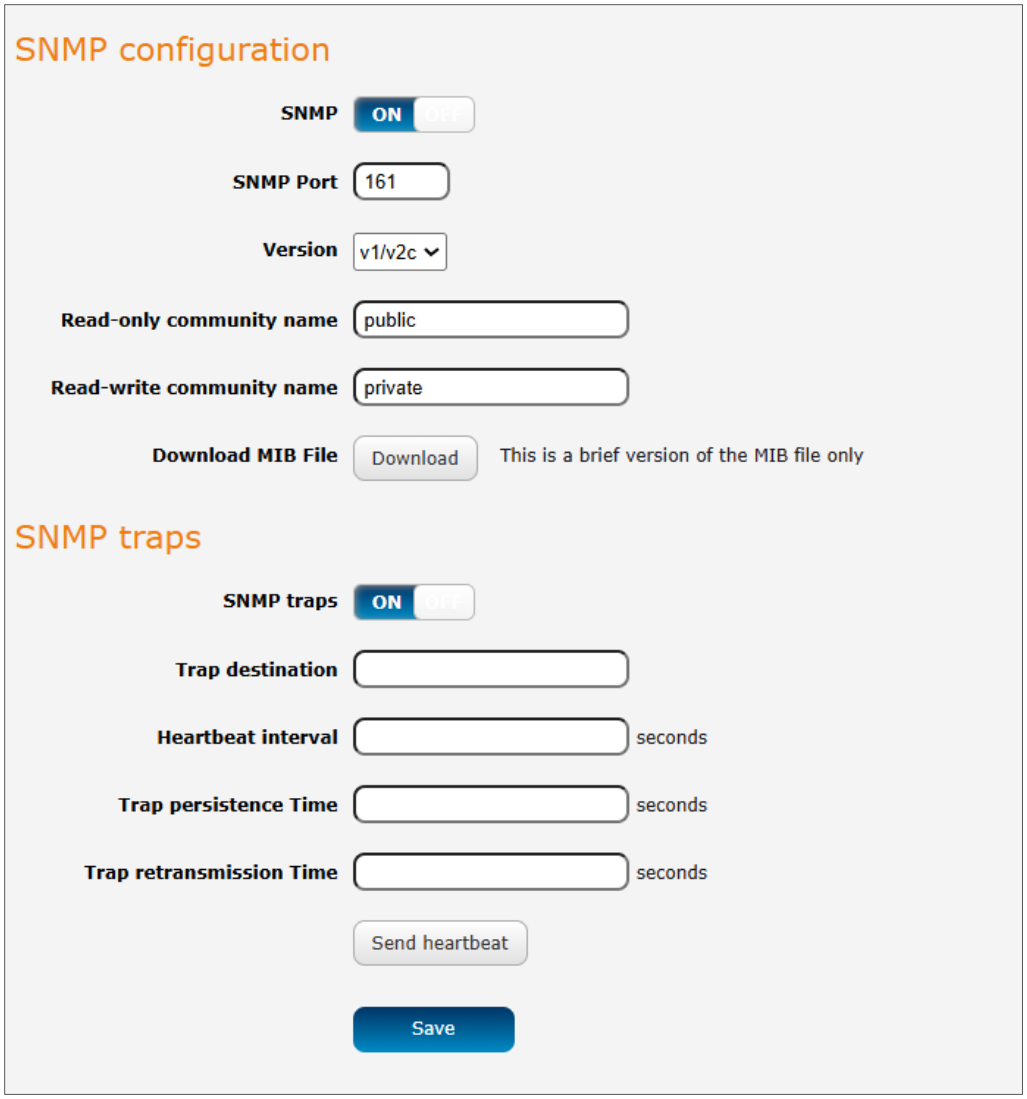


Figure 9-15 SNMP and SNMP trap configuration

Table 9-8 SNMP and SNMP trap configuration details

Parameter	Description
SNMP configuration	
SNMP	Set to **ON** to enable SNMP.
SNMP Port	Enter the port number to user for SNMP
Version	Select the SNMP version to use. Options are: • **v1/v2** • **v3** v1 and v2 are known to be insecure, therefore you should use v1 and v2 of SNMP with caution. If v1/v2 is selected, the below fields display:

Parameter	Description
	• **Read-only community name** – Enter Read-only community name used for client authentication. • **Read-write community name** – Enter the Read-write community name used for client authentication. ***Important:*** *Community names are used as a type of security to prevent access to reading and/or writing to the router's configuration. It is recommended that you change the Community names to something other than the default settings when using this feature.* If v3 is selected, the below fields display: • **Engine ID suffix** – Enter the Engine ID suffix generated by the SNMP server. • **Username** – Enter the SNMP username. • **Security level** – Select the required Security level. Options are: ○ **No authentication, no privacy –** No authentication or encryption methods used. ○ **Authentication, no privacy –** When selected, select **Authentication protocol** (**MD5** or **SHA**), and enter **Authentication passphrase** ○ **Authentication, privacy** – When selected, select **Authentication protocol** (**MD5** or **SHA**), enter **Authentication passphrase**, select **Privacy protocol** (**DES or AES**), and enter **Privacy passphrase**.
Download MIB file	Click **Download** to display the Management Information Base (MIB) of the router. The MIB displays all the objects of the router that can have their values set or report their status. The MIB is formatted in the SNMP-related standard RFC1155.
SNMP traps	
SNMP traps	Set to **ON** to enable.
Trap destination	Enter the IP address to which the SNMP data is to be sent.
Heartbeat interval	Enter the number of seconds between SNMP heartbeats.
Trap persistence Time	Enter the number of seconds that an SNMP trap persists.
Trap retransmission time	Enter the number of seconds between SNMP trap retransmissions.
Send Heartbeat	Click to send a manual SNMP Heartbeat.

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

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

TR-069

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

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

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

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

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

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

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

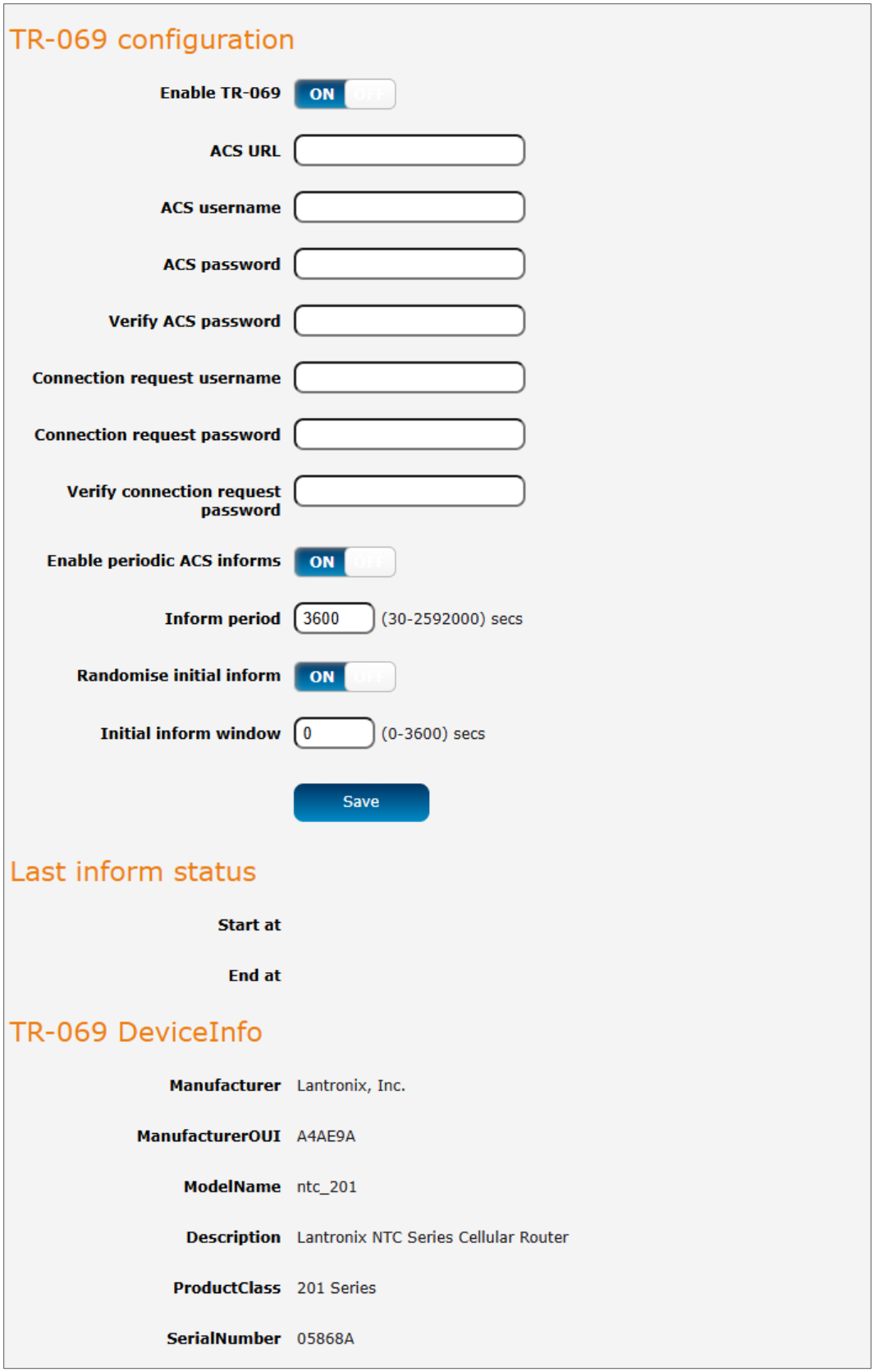


Figure 9-16 TR-069 page

Table 9-9 TR-069 configuration details

Parameter	Description
TR-069 configuration	
Enable TR-069	Set to **ON** to enable.
ACS URL	Enter the full domain name or IP address of the Auto Configuration Server.
ACS username	Enter a username that the server should use to authenticate the CPE when it sends an inform message.
ACS password	Enter a password that the server should use to authenticate the CPE when it sends an inform message.
Verify ACS password	Re-enter the above password.
Connection request username	Enter a username that the CPE should use to authenticate the Auto Configuration Server during a connection request to the CPE.
Connection request password	Enter a password that the CPE should use to authenticate the Auto Configuration Server during a connection request to the CPE.
Verify connection request password	Re-enter the above password.
Enable periodic ACS informs	Set to **ON** to enable the periodic ACS inform messages. The inform message acts as a beacon to inform the ACS of the existence of the router.
Inform period	Enter the number of seconds between inform messages.
Randomize initial inform	Set to **ON** to enable. This allows the CPE to wait for a random delay within a configured time window before sending the first Inform. It is helpful where many CPE devices contact the AC at the exact same time after reboot or power-up.
Initial inform window	Enter the number of seconds for initial inform window.

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

OMA-LWM2M

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

It provides:

- Firmware upgrades
- Device monitoring and configuration
- Server provisioning

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

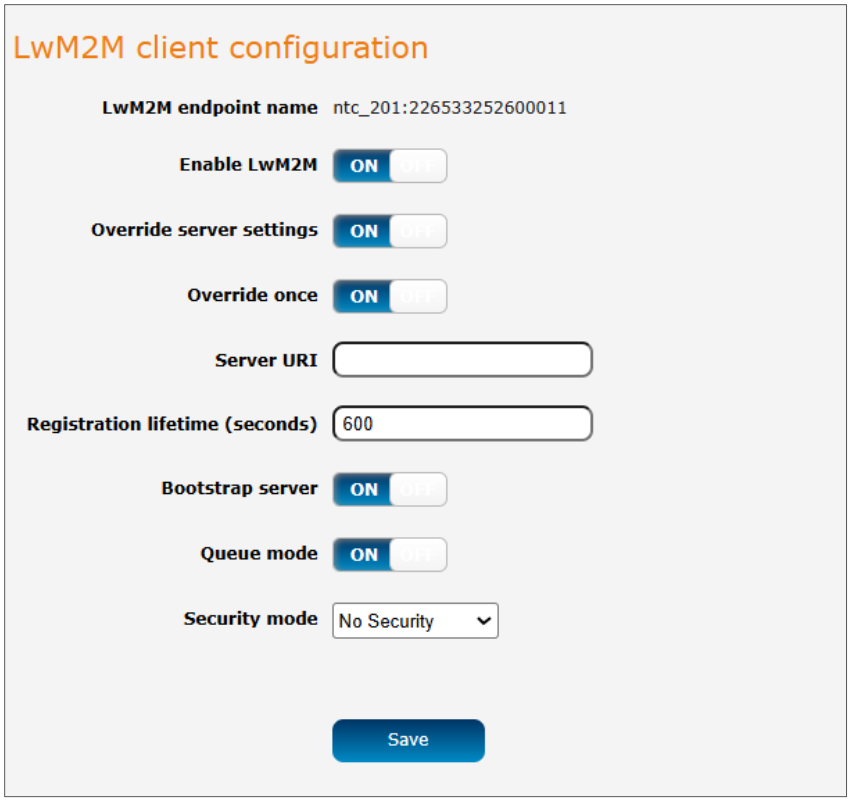


Figure 9-17 OMA-LWM2M page

Table 9-10 LwM2M client configuration details

Parameter	Description
LwM2M Endpoint Name	This is the unique ID the device will use to identify itself with LwM2M servers.
Enable LwM2M	Set to **ON** to enable.
Override server settings	Set to **ON** to enable. 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 the current settings of the client.
Override Once	Set to **ON** to enable. It allows you to specify whether the new server details you provide will be applied once when the client restarts (normal flow for configuring/reconfiguring the client) or when disabled, applied every time the client restarts (used for debugging/troubleshooting.)
Server URI	Specify the URI of the LwM2M server to connect to. It must be a fully specified CoAP or CoAPS URI, including port number, e.g. coap://server.com:5683 or coaps://server.com:5864.
Registration Lifetime (seconds)	Specify the interval (in seconds) at which the LwM2M client will send registration updates (i.e. heartbeat messages) to the server.
Bootstrap Server	Set to **ON** to enable. It allows you to specify whether the new server is a LwM2M bootstrap server.

Queue Mode	Set to **ON** to enable. It 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	It allows you to choose the security mode that will be used to connect to the LwM2M server. Options are: • **Pre-Shared key** • **No security**
Client Identity	Displays when Pre-Shared key is selected as security mode. Specify the identity string associated with your pre-shared key.
Client Pre-Shared Key PSK coding	Displays when Pre-Shared key is selected as security mode. Select the required coding type. Options are: • **Hexadecimal** • **Plain text**
PSK key	Enter the PSK key.

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

The table below lists the supported object IDs on the NTC-201 router. For further information on the objects, refer to the Open Mobile Alliance LWM2M registry.

Table 9-11 Supported LWM2M objects

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

Event notification

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

Notification configuration

The Notification configuration page allows you to select the event types, methods of notification and the destinations for the notifications.

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

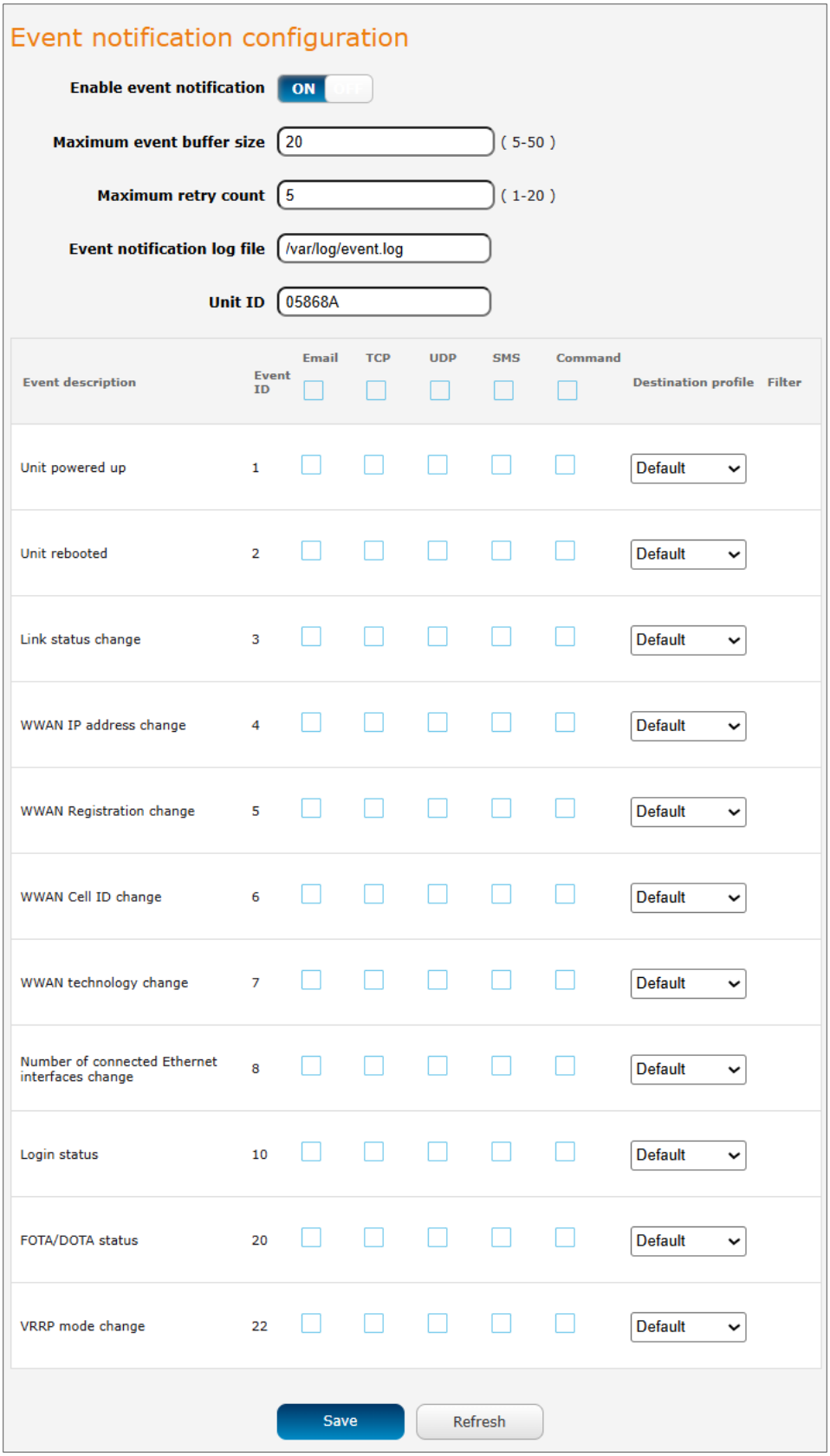


Figure 9-18 Event notification configuration page

Table 9-12 Event notification configuration details

Parameter	Description
Enable event notification	Set to **ON** to enable.
Maximum event buffer size	Enter the buffer size for event notifications which fail to be delivered or are yet to be sent.
Maximum retry count	Enter the maximum number of attempts that the router should make to deliver an event notification. The range is between 1 and 20.
Event notification log file	Enter the name and location of the file used to log the event notification activity.
Unit ID	Enter an ID for the router that is specified in the event notifications, to identify which router has an event.

For each event select the type of notification to be sent and the destination profile (see Destination configuration). If the Destination profile does not contain the required contact details, a pop-up warns you to enter the required details in the Destination profile. Hovering the mouse over the event description provides more details of event notification type.

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

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

The table below lists the different event types and their description.

Table 9-13 Event types and description

Event	Event ID	Description	Example message
Unit powered up	1	Notification is sent when the unit is powered up by a power source or after a soft reset.	Power is up
Unit rebooted	2	Notification is sent when the unit is rebooted via Web UI, SMS diagnostics or via command line/telnet session.	Rebooting triggered by internal application
Link status change	3	Notification is sent if the status of the data connection profile or any IPSec/OpenVPN/PPTP/GRE tunnel endpoint changes i.e. the link goes up or down.	Profile 1 WWAN status changed : down -> up
WWAN IP address change	4	Notification is sent if an active data connection profile's WWAN IP address changes.	WWAN IP address changed : N/A --> 10.103.4.149

Event	Event ID	Description	Example message
WWAN Registration change	5	Notification is sent if the network registration status changed between “registered”, “unregistered” or “roaming”.	WWAN registration status changed : Not registered --> Registered to home network
WWAN Cell ID change	6	Notification is sent if the router connects to a different cell, marked by a changed in the Cell ID.	Cell ID changed : --> 15224145 Cell ID changed : 15224148 --> 15224145
WWAN technology change	7	Notification is sent if the router connects to a different network technology, e.g. 3G/2G.	WWAN network changed : N/A() --> 3G(UMTS) WWAN network changed : 3G(UMTS) --> 2G(GSM)
Number of connected Ethernet interfaces change	8	Notification is sent if there is a change to the number of directly connected Ethernet interfaces.	Ethernet device number changed : 0 --> 1
Login status	10	Notification is sent if there was a failure to log into the router via the Web UI.	WEBUI login failed, username root, password
FOTA/DOTA status	20	Notification is sent with the result of the Firmware Over-the-air via SMS or TR-069.	FOTA/DOTA: upgrading firmware successful
VRRP mode change	22	Notification is sent if a device configured as a slave becomes a master router or returns to slave status.	VRRP is in backup mode

Destination configuration

A Destination profile on the router contains the different contact details of a recipient of event notification alerts. A destination profile must contain the at least one type of contact detail, to be able to use it.

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

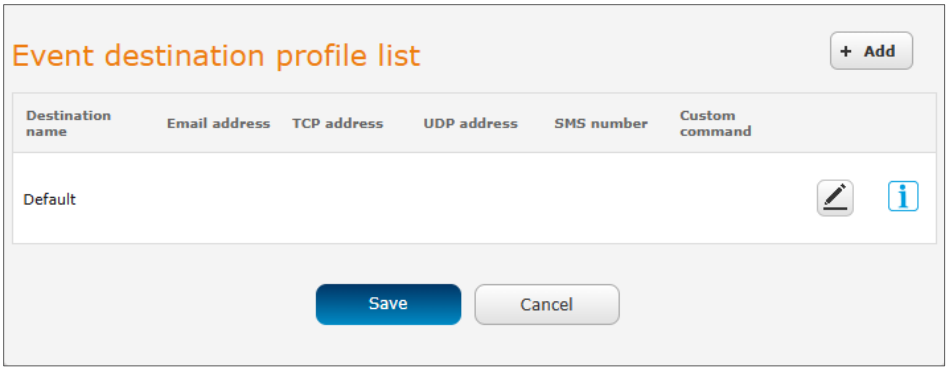


Figure 9-19 Event destination profile list

To create a Destination profile, click +**Add** button for the Event destination profile list, the configuration settings display.

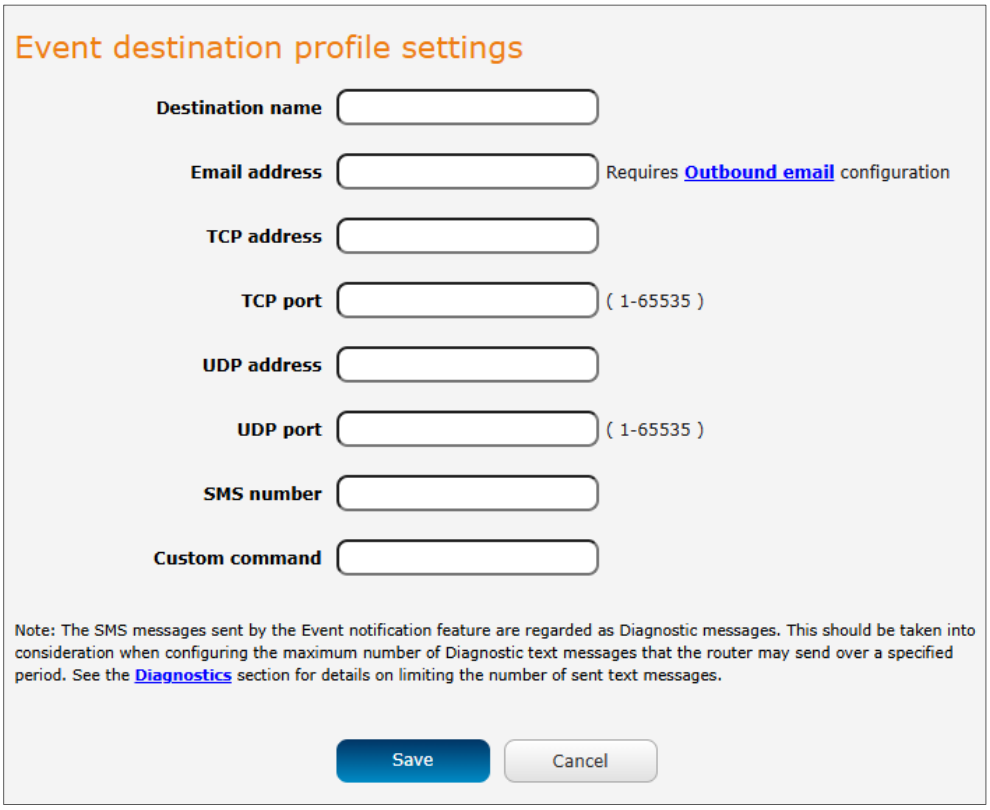


Figure 9-20 Event destination profile settings

Table 9-14 Event destination configuration details

Parameter	Description
Destination name	Enter a name for the destination profile.
Email address	Enter Email address of the recipient.
TCP address	Enter TCP address of the recipient
TCP port	Enter the TCP port of the recipient.

UDP address	Enter the UDP address of the recipient.
UDP port	Enter the UDP port of the recipient
SMS number	Enter the SMS number of the recipient
Custom command	Enter a custom command to perform certain tasks when an event is triggered. Any command or script that can be executed from a terminal command prompt can be entered in the Custom command field.

Click **Save** to save and apply the details. The Destination profile is added to the Event destination profile list.

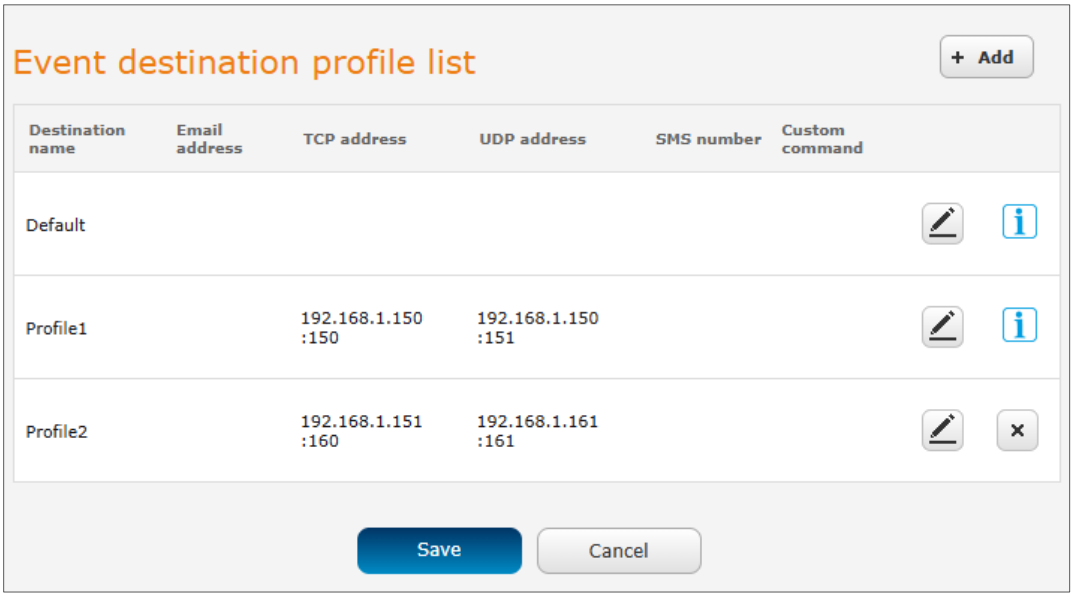


Figure 9-21 Event destination profile list with newly added profiles

Click the icon for a destination profile to edit it, and the icon to delete it. If the destination profile is linked to an event notification type, the icon is displayed instead of the delete button. To delete such a destination profile, you must go to the Event notification configuration page, remove check marks for all the notification types for each event for which the destination profile is configured. Then, return to the Event destination profile list and select the delete button. Click **Save** to save and apply the changes.

Email settings

The Email settings page allows you to configure the email account that is used to send outbound emails in features such as Event notification.

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

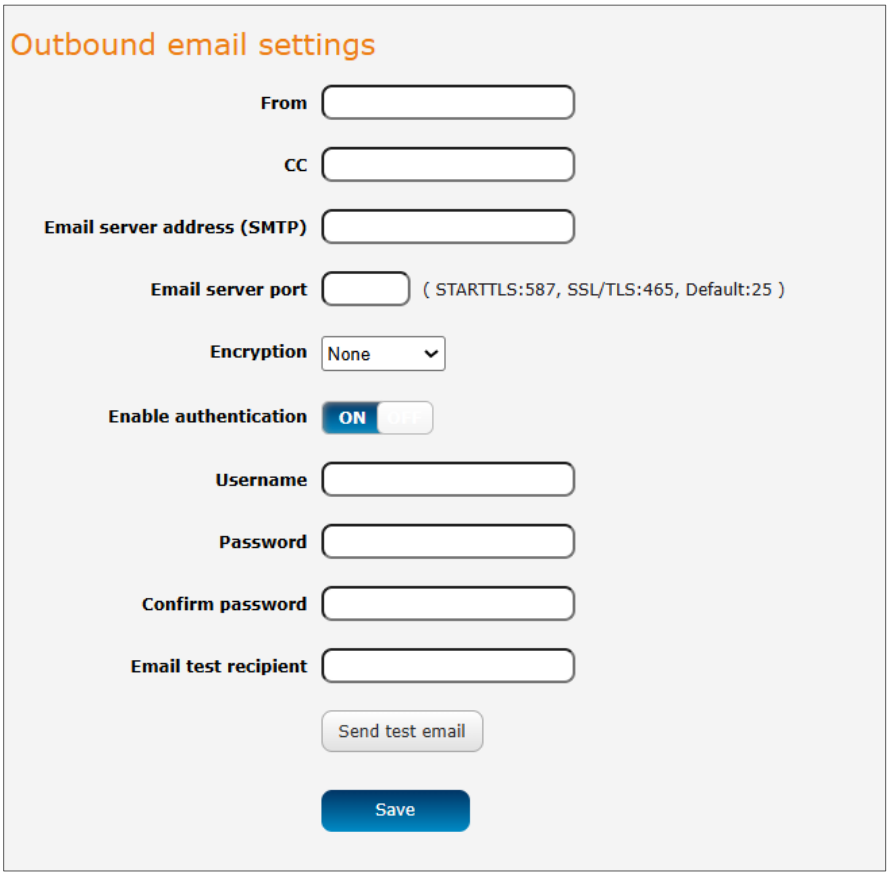


Figure 9-22 Email settings page

Table 9-15 Email settings configuration details

Parameter	Description
From	Enter the email address of the account you will use to send emails.
CC	(Optional) Enter an email address which will be copied on all messages sent.
Email server address (SMTP)	Enter the SMTP server address of the email server. This may be an IP address or a hostname.
Email server port	Enter the Email server's SMTP port.
Encryption	Select the encryptions type. Options are: • **None** – No encryption • **SSL/TLS** – Opens a secure connection first, and then begins the SMTP transaction.

	• **STARTTLS** – Starts the SMTP transaction and then looks for support for TLS in the response message.
Username	Enter the username of the account used for sending emails.
Password	Enter the password of the account used for sending emails.
Confirm password	Re-enter the above password.
Email test recipient	Enter an email address to which you want to send a test mail
Send test mail	Click to send test mail

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

SMS messaging

The NTC-201 router offers an advanced SMS feature set, that includes including sending messages, receiving messages, redirecting incoming messages to another destination, as well as supporting remote commands and diagnostics messages.

Some of the supported functions are:

- Sending a text message via a cellular network and store it in permanent storage
- Receiving a text message via a cellular network and store it in permanent storage
- Forwarding incoming text messages via a cellular network to another remote destination which may be a TCP/UDP server or other mobile devices
- Receiving run-time variables from the device, on request (e.g. uptime)
- Changing live configuration on the device (e.g. network username)
- Executing supported commands (e.g. reboot) via SMS
- Triggering the NTC-201 router to download and install a firmware upgrade
- Triggering the NTC-201 router to download and apply a configuration file

Setup

The Setup page allows you to configure General SMS and SMS forwarding. SMS forwarding allows you store incoming text messages on the router and forward them to another mobile device, TCP, or UDP server. SMS messaging is enabled by default.

To access the Setup page, navigate to **Services > SMS messaging > Setup**.

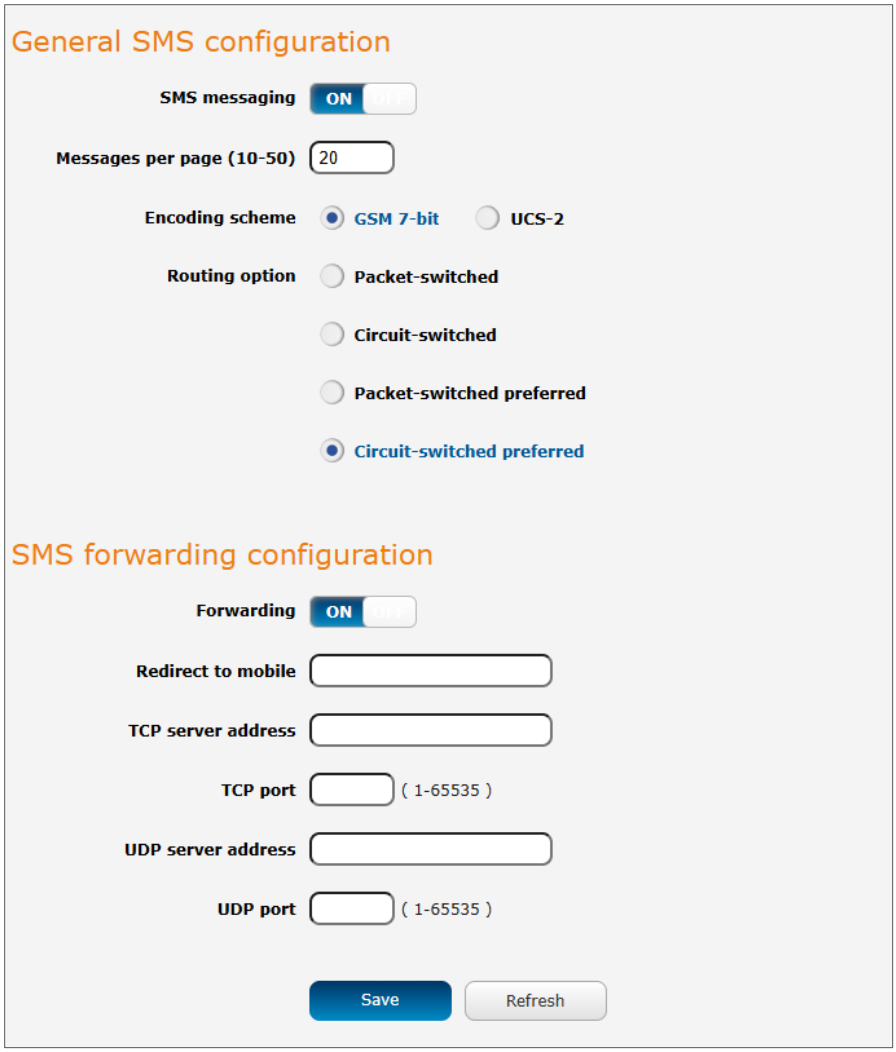


Figure 9-23 SMS Setup page

Table 9-16 SMS Setup configuration details

Parameter	Description
General SMS configuration	
SMS messaging	Set to **ON** to enable.
Messages per page (10-50)	Enter the number of SMS messages to display per page.
Encoding scheme	Select the encoding scheme. Options are: • **GSM 7-bit** – Permits up to 160 characters per message but drops to 50 characters if the message includes special characters • **UCS-2** – Allows Unicode characters and permits a message to be up to 50 characters in length.
Routing option	Select Routing option. Options are: • **Packet-switched** – Use packet-switched service only • **Circuit-switched** – Use circuit-switched service only

Parameter	Description
	• **Packet-switched preferred** – Use packet-switched service if available • **Circuit-switched preferred** – Use circuit-switched service if available
SMS forwarding configuration	
Forwarding	Set to **ON** to enable.
Redirect to mobile	Enter a mobile number of the destination.
TCP server address	Enter the IP address or domain name of the destination TCP server.
TCP port	Enter the port of the destination TCP server to use.
UDP server address	Enter the IP address or domain name of the destination UDP server.
UDP port	Enter the port of the destination UDP server to use.

New message

The New message page allows you to send SMS text messages to a single or multiple recipients.

To access the New message page, navigate to **Services > SMS messaging > New message**.

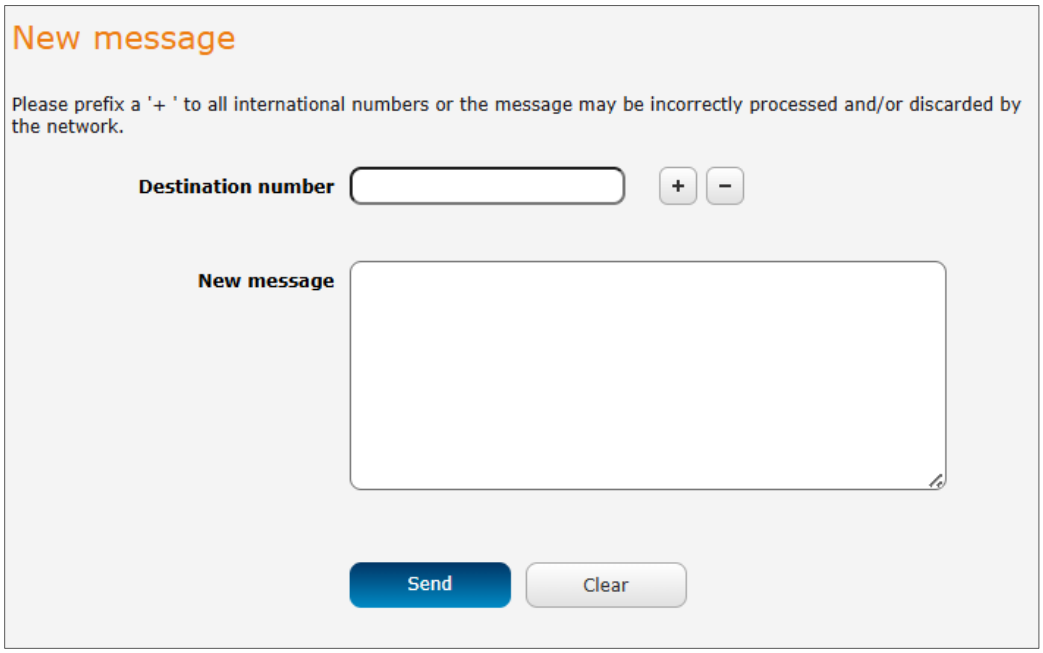


Figure 9-24 New message page

To send a new message:

1. In the **Destination number field** enter the mobile number of the recipient. Destination numbers should begin with the "+" symbol followed by the country calling code.
2. Click + icon to add a recipient and – icon to remove a recipient. A maximum of 9 recipients can be added and sent a message at the same time.
3. In the **New message** field, type your message. 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.

4. Click **Send**, to send the message. The result is displayed next to the destination number as Success or Failure.

Inbox

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

To access the Inbox page, navigate to **Services > SMS messaging > Inbox**.

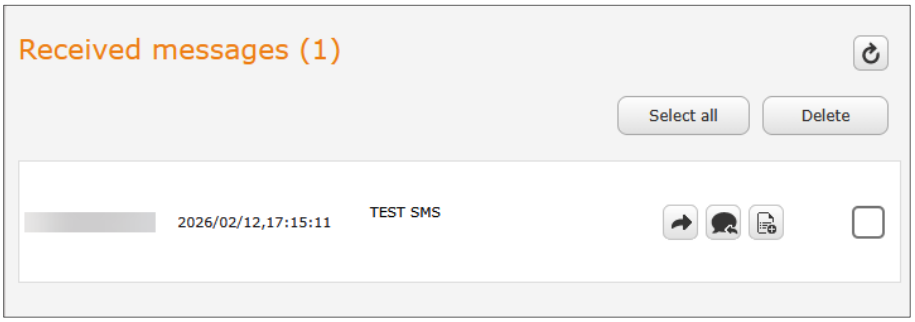


Figure 9-25 Inbox page

Sent items

The Sent items page displays all the sent messages.

To access the Sent items page, navigate to **Services > SMS messaging > Sent items**.

Figure 9-26 Sent items page

Table 9-17 Inbox/Sent items icons

Icon	Name	Description
	Forward	Click to open a new message window to forward the corresponding message to another recipient.
	Reply	Click to open a new message window to reply to the sender.
	Add to Whitelist	Click to add the sender's mobile number to the Whitelist on the router.
	Checkbox	Click to select the corresponding message.
	Refresh	Click this to refresh the inbox or outbox to see new messages.

Click **Select All** to select all messages. Click **Delete** to delete selected messages.

Diagnostics

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

To access the Diagnostics page, navigate to **Services > SMS messaging > Diagnostics**.

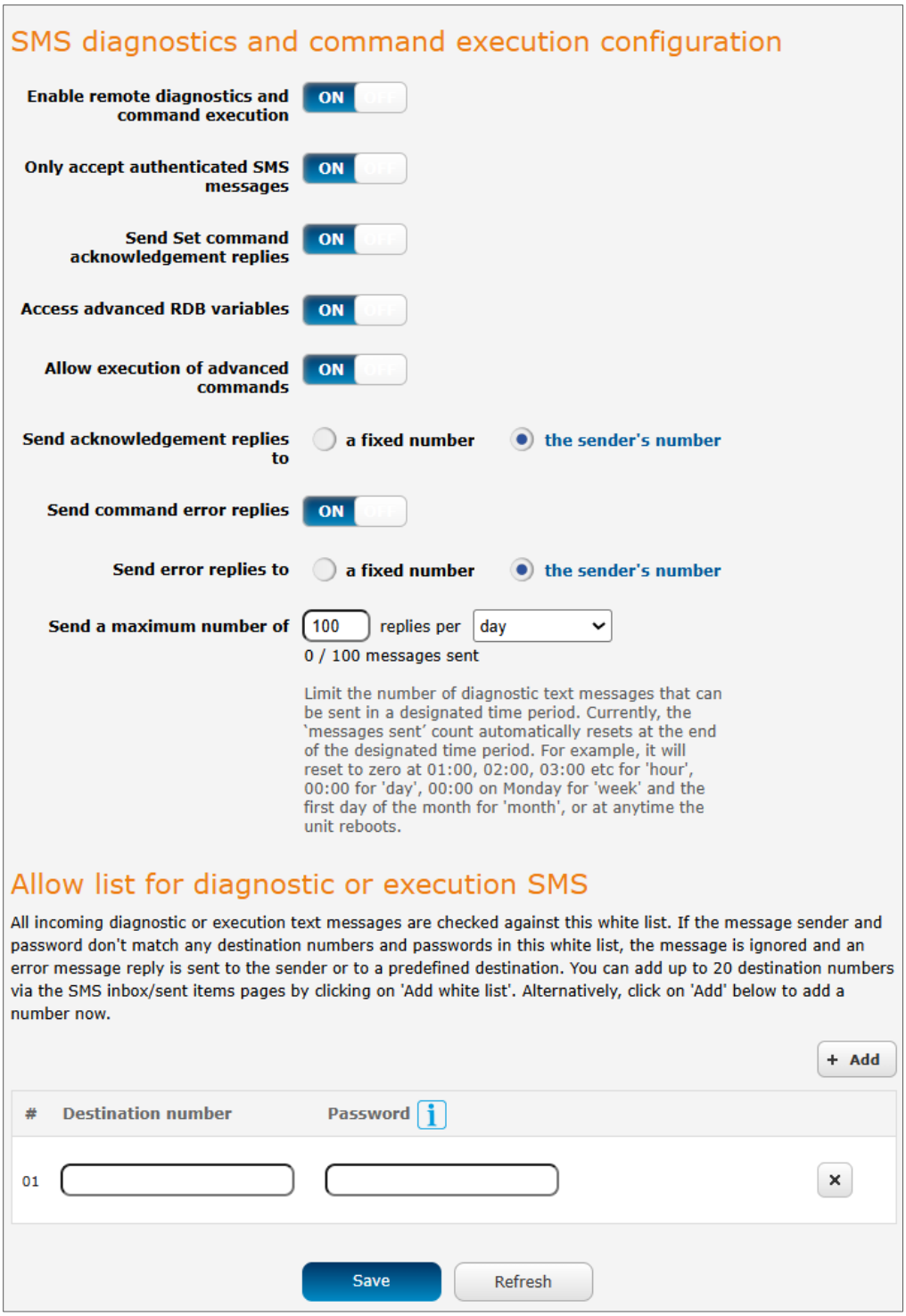


Figure 9-27 SMS diagnostics page

Table 9-18 SMS diagnostics and command execution configuration

Parameter	Description
SMS diagnostics and command execution configuration	
Enable remote diagnostics and command execution	Set to **ON** to enable. Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands. If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox. ***Note:*** *It is possible to adjust settings and prevent your router from functioning correctly using remote diagnostics. If this occurs, you will need to perform a factory reset to restore normal operation.* ***Important:*** *We highly recommend that you use the whitelist and a password when utilizing this feature to prevent unauthorized access. See the whitelist description for more information*.
Only accept authenticated SMS messages	Set to **ON** to enable. Enables or disables checking the sender's phone number against the allowed sender Allow 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 Allow list. If it exists, the router then checks the password (if configured) in the incoming message against the password in the Allow list for the corresponding number. If they match, the diagnostic or command is executed. If the number does not exist in the Allow list or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message. This is enabled by default, and it is strongly advised that you leave this feature enabled to maintain security.
Send Set command acknowledgement replies	Set to **ON** to enable. The NTC-201 router will automatically reply to certain types of commands received, such as get commands, or execute commands. However, acknowledgement replies from the NTC-201 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

Parameter	Description
	have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.
Access advanced RDB variables	Set to **ON** to enable. When enabled, it allows access to the full list of RDB variables via SMS. When disabled, it only allows access the basic RDB variables listed later in this guide.
Allow execution of advanced commands	Set to **ON** to enable. When enabled, it 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 `/usr/bin/sms` folder on the router. When disabled, it allows execution of only the basic commands listed later in this guide.
Send acknowledgement replies to	Set to **ON** to enable. 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 **Fixed number to send replies to** field displays. Enter the required number. 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 the sender's number.
Send command error replies	Set to **ON** to enable. Enables or disables the sending of an error message resulting from the execution of a get, set, or exec command. All error replies are stored in the Outbox after they have been sent.
Send error replies to	If a **fixed number** is selected, the **Fixed number to send error replies to** field displays. Enter the required number. The error 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 error message will be sent to the number that the SMS diagnostic or command message originated from. The default setting is the sender's number.
Send a maximum number of	Enter the maximum number of acknowledgement and error messages sent when an SMS diagnostic or command is executed. The maximum number of replies can be set per **hour**, **day**, **week** or **month**. The router will send a maximum of 100 replies per day by default.

Parameter	Description
	The number of messages sent is shown displayed. The total transmitted message count resets after a reboot or at the beginning of the time frame specified.
Allow list for diagnostic or execution SMS	
+Add	Click to add a number to the allow list, the different display. The Allow list is a list of mobile numbers that you can add 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 Allow list to give an additional level of security. Up to 20 numbers can be added to Allow list.
Destination number	Enter a number.
Password	Enter a password for the number. Click the icon next to password to display the password criteria.
×	Click to remove the number from Allow list.

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

Types of SMS diagnostic commands

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

```
execute COMMAND
get VARIABLE
set VARIABLE=VALUE
```

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

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

The following are some examples of SMS diagnostic commands:

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

SMS acknowledgment replies

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

SMS command format

Generic Format for reading variables:

```
get VARIABLE
PASSWORD get VARIABLE
```

Generic Format for writing to variables:

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

Generic Format for executing a command:

```
Execute COMMAND
PASSWORD execute COMMAND
```

Replies

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

Table 9-19 SMS Diagnostic Command Syntax

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

Where VARIABLE is the name of the value to be read

Where 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)

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 Allow 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 WWAN profile list page of the Web-UI.

Table 9-20 List of basic SMS diagnostic commands

Command	Definition
reboot	Immediately performs a soft reboot.
pdpcycle	Disconnects (if connected) and reconnects the data connection. If a profile number is added in the command, it disconnects/reconnects the specified profile in case the profile is active. If no profile number is added, it disconnects/reconnects the current active profile. Reports an error if no profile number is selected and there is no active profile.
pdpdown	Disconnects the PDP. If a profile number is added in the command, the router disconnects the specified profile in case the profile is active. If no profile number is added, it disconnects the current active profile. Reports an error if no profile number is added and there is no active profile.
pdpup	Reconnects the PDP. If a profile number is added in the command, the router connects to the specified profile. If no profile number is added, it connects to the last active profile. The gateway will check the currently active profile and disconnect this profile before executing the command. The router reports an error if no profile number is added and there is no stored last active profile number.
factorydefaults	Performs a factory reset on the router. Be aware that this command also clears the SMS Allow list on the router.
download	Downloads and installs a Firmware Upgrade (.cdi) file, Config (.tar.gz) file 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 .tar.gz 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*
codconnect	Causes the router to activate the PDP context when the Connect on demand feature is enabled.
coddisconnect	Causes the router to de-activate the PDP context when the Connect on demand feature is enabled.
ssh.genkeys	Instructs the router to generate new public SSH keys.
ssh.clearkeys	Instructs the router to clear the client public SSH key files.

List of get/set commands

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

Table 9-21 List of get/set commands

Command name	Example	Description
get status	`get status`	Returns the Module firmware version, LAN IP Address, Network State, Network operator and Signal strength.
get sessionhistory	`get sessionhistory`	Returns the time and date of recent sessions along with the total amount of data sent and received for each session.
set syslogserver	`set syslogserver=123.45.67.89:514`	Sets a remote syslog server IP or hostname and port.
set cod	`set cod=1`	Enables or disables Connect on demand.
get cod	`get cod`	Returns the enable/disable status of the Connect on demand feature.

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

set codignore.icmp	**set codignore.icmp=1**	Sets the router to ignore ICMP packets triggering data activity detection.
get codignore.icmp	**get codignore.icmp**	Returns the status of the Ignore ICMP option.
set codignore.tcp	**set codignore.tcp=1**	Sets the router to ignore TCP packets triggering data activity detection.
get codignore.tcp	**get codignore.tcp**	Returns the status of the Ignore TCP option.
set codignore.udp	**set codignore.udp=1**	Sets the router to ignore UDP packets triggering data activity detection.
get codignore.udp	**get codignore.udp**	Returns the status of the Ignore UDP option.
set codignore.dns	**set codignore.dns=1**	Sets the router to ignore DNS traffic triggering data activity detection.
get codignore.dns	**get codignore.dns**	Returns the status of the Ignore DNS option.
set codignore.ntp	**set codignore.ntp=1**	Sets the router to ignore NTP traffic triggering data activity detection.
get codignore.ntp	**get codignore.ntp**	Returns the status of the Ignore NTP option.
set codignore.ncsi	**set codignore.ncsi=1**	Sets the router to ignore NCSI traffic triggering data activity detection.
get codignore.ncsi	**get codignore.ncsi**	Returns the status of the Ignore NCSI option.
get plmnscan	**get plmnscan**	Instructs the router to perform a network scan and returns the results by SMS.
set forceplmn	**set forceplmn=505,3**	Sets the operator to a manual selection made by the user where “505” is the Mobile Country Code for Australia. As no network type (e.g., LTE/3G/2G) is specified, it is selected automatically.
get forceplmn	**get forceplmn**	Returns the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values
get pppoe	**get pppoe**	Returns the PPPoE status, currently configured dial string and service name
set pppoe	**set pppoe=1,1,1,test**	Sets PPPoE on, debug logging on, Forward WAN IP on, and service name to “test”.
get ledmode	**get ledmode**	Returns the status of the LED operation mode.
set ledmode	**set ledmode=10**	Sets the LED operation mode to be always on or to turn off after the specified number of minutes.

get ssh.proto	**get ssh.proto**	Returns the SSH protocol in use.
set ssh.proto	**set ssh.proto=1,2**	Sets the SSH Protocol to protocol 1, 2 or both (1,2).
get ssh.passauth	**get ssh.passauth**	Returns the status of the SSH Enable password authentication option.
set ssh.passauth	**set ssh.passauth=1**	Sets the SSH Enable password authentication option on or off.
get ssh.keyauth	**get ssh.keyauth**	Returns the status of the SSH Enable key authentication option.
set ssh.keyauth	**Set ssh.keyauth=1**	Sets the SSH Enable key authentication option on or off.
get download.timeout	**get download.timeout**	Returns the time in minutes that the router waits before a download times out.
set download.timeout	**set download.timeout=20**	Sets the time in minutes that the router waits before a download times out. This is set to 10 minutes by default. Supported range is 10 – 1440 minutes.
get install.timeout	**get install.timeout**	Returns the time in minutes that the router waits before a file that is being installed times out.
set install.timeout	**set install.timeout=5**	Sets the time in minutes that the router waits before a file that is being installed times out. This is set to 3 minutes by default. Supported range is 3 – 300 minutes.
get sw.version	**get sw.version**	Returns the software version of the router.

List of basic RDB variables

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

Table 9-22 List of basic SMS diagnostics RDB variables

RDB variable name	SMS variable name	Read/ Write	Description	Example VALUE
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
link.profile.1.user	username	RW	Cellular broadband username	Guest, could also return null
link.profile.1.pass	password	RW	Cellular broadband password	Guest, could also return null
link.profile.1.auth_type	authtype	RW	Cellular broadband Authentication type	pap or chap
link.profile.1.iplocal	wanip	R	WAN IP address	202.44.185.111
wwan.0.radio.information.signal_strength	rssi	R	Cellular signal strength	-65 dBm
wwan.0.imei	imei	R	IMEI number	357347940022876
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
statistics.usage_current	wanuptime	R	Up time of current cellular	1 days 02:30:12 or 0 days 00:00:00 when wwan down

			broadband session	
/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
wwan.0.system_network_status.current_band	band	R	Current band	LTE Band 3 – 1800 MHz

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.

It returns the following information each network in range, separated by a semi-coclon:

- MCC
- MNC
- Network Type (LTE, 3G, 2G)
- Provider's Name
- Operator Status (available, forbidden, current)

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

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

Table 9-23 Network types returned by get plmnscan SMS command

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

Table 9-24 Operator status codes returned by get plmnscan SMS command

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

Note: *If the connection status is Up and connection mode is Always on, the get plmnscan SMS will cause the connection to disconnect, perform the scan, send the result through SMS and then bring the connection back up again.*

If the connection status is Down, the router will perform the PLMN scan, send the result and keep the connection status down.

If the connection status is Waiting and connection mode is Connect on demand, the get plmnscan SMS will change the connection status to Down, perform the scan, send the result through SMS and then restore the connection status to the Waiting state.

If the connection status is Up and connection mode is Connect on demand, the get plmnscan SMS will cause the connection to disconnect, perform the scan, send the result through SMS, and then restore the connection status to the Waiting state unless there is a traffic which triggers a connection in which case the connection status will be set to Up.

Setting the router to connect to a network

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

Command format:

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

For example:

```
set forceplmn=0
```

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

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

Sets the operator to a manual selection made by the user where 505 is the Mobile Country Code for Australia and 1 is the Mobile Network Code for Telstra. As no network type (e.g. LTE/3G/2G) is specified, it is selected automatically.

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

Sets the operator and network type to a manual selection made by the user where “505” is the Mobile Country Code for Australia, 1 is the Mobile Network Code for Telstra and 7 is the 3G network type.

Table 9-25 Mobile Network Provider codes (Australia)

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

Table 9-26 Network types

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

Notes:

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

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

Confirming the currently configured operator and network type

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

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

```
Automatic,505,1
```

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

SMS diagnostics examples

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

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

If authentication required:

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

If authentication not required:

```
set username=’username’
```

Table 9-27 SMS diagnostics example commands

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

Send SMS to Disconnect (if connected) and reconnect the data connection	**execute pdpcycle**
Send SMS to disconnect the data connection	**execute pdpdown**
Send SMS to connect the data connection	**execute pdpup**
Send multiple get command	**get wanip; get rssi**
Send multiple set command	**set ssh.genkeys=1; set username=test; set auth=pap**
Send SMS to reset to factory default settings	**execute factorydefaults**
Send SMS to retrieve status of router	**get status**
Send SMS to retrieve the history of the session, including start time, end time and total data usage	**get sessionhistory**
Send SMS to configure the router to send syslog to a remote syslog server	**set syslogserver=123.209.56.78**
Send SMS to wake up the router, turn on the default gateway and trigger the connect on demand profile if in waiting state.	**A zero-byte class 1 flash SMS**
Send SMS to perform firmware upgrade when firmware is located on HTTP server	**execute download http://download.com:8080/firmware_image.cdi** **execute download http://download.com:8080/firmware_image_r.cdi**
Send SMS to perform firmware upgrade when firmware is located on FTP server	**execute download ftp://username:password@download.com/firmware_image.cdi** **execute download ftp://username:password@ download.com/firmware_image_r.cdi**
Send SMS to download and install IPK package located on HTTP server	**execute download http://download.com:8080/package.ipk**
Send SMS to download and install IPK package located on FTP server	**execute download ftp://username:password@ download.com:8080/package.ipk**
Send SMS to turn off PPPoE	**set pppoe=0**
Send SMS to retrieve the PPPoE status, currently configured dial string and service name	**get pppoe**
Send SMS to set the LED mode timeout to 10 minutes	**set ledmode=10**

Send SMS to retrieve the current LED mode	`get ledmode`
Retrieve current SSH protocol	`get ssh.proto`
Select SSH protocol	`set ssh.proto=1`
Retrieve password authentication status	`get ssh.passauth`
Enable/disable password authentication on host	`set ssh.passauth=1 or set ssh.passauth=0`
Generate set of public/private keys on the host	`execute ssh.genkeys`
Clear client public keys stored on host	`execute ssh.clearkeys`
Send SMS to initiate a Network Quality test	`get networkquality`

Network Quality

The Network Quality page displays the network performance metrics. To access the Network Quality page, navigate to **Services > Network Quality**.

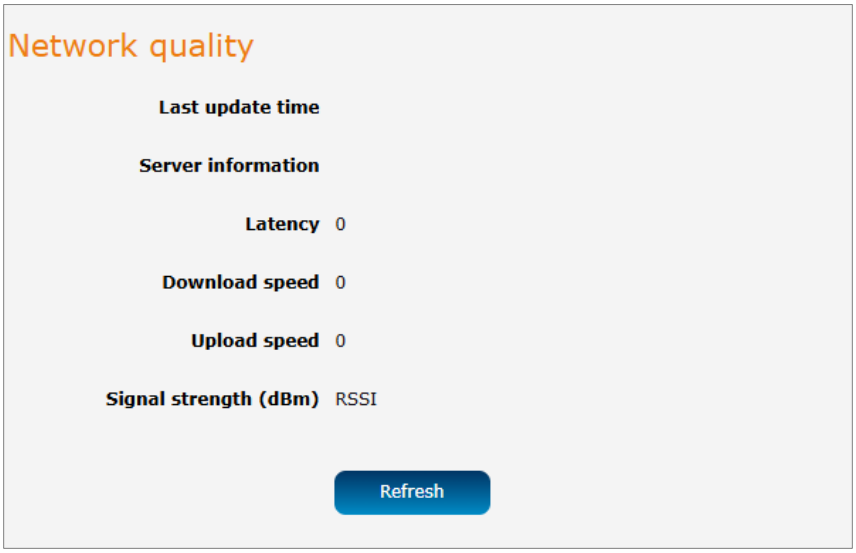


Figure 9-28 Network quality

Table 9-28 Network quality details

Parameter	Description
Last update time	Date and time of the last successful refresh
Server information	Includes details of the server used to conduct the network quality test. The distance to the particular server accessed by the software is displayed in kilometres.

Parameter	Description
Latency	Latency limits the maximum rate in milliseconds (ms), that information can be transmitted. This network test measures round trip latency and excludes the amount of time that a destination system spends processing the packet.
Download speed	Average download speed achieved between the server and the router, measured in megabits per second (Mbit/s).
Upload speed	Average upload speed achieved between the router and the server, measured in megabits per second (Mbit/s)
Signal strength (dBm)	The method used to measure signal strength depends on the network technology: • 4G uses RSRP (Reference Signal Received Power) • 3G uses RSCP (Received Signal Code Power) • 2G uses RSSI (Received Signal Strength Indication) All methods express the signal strength as a ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
Refresh	Click **Refresh** for the router to perform a network test to the address listed in the Server information field. This process may take a few minutes depending on the speed of your network.

Percepxion

The NTC-201 router comes integrated with Percepxion cloud platform to allow for remote management of devices.

Configuration

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

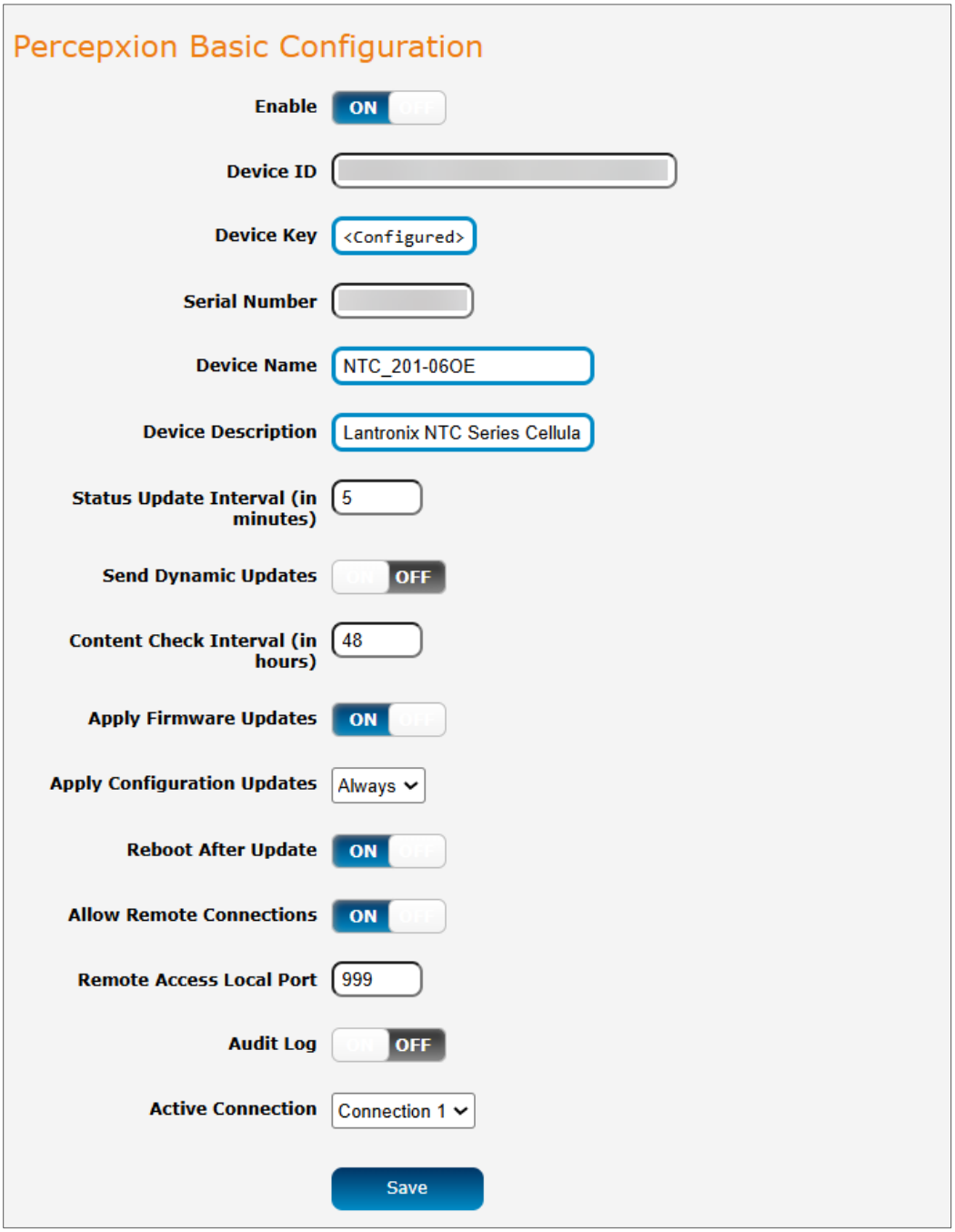


Figure 9-29 Percepxion configuration settings

Table 9-29 Percepxion configuration details

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

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

Connection 1

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

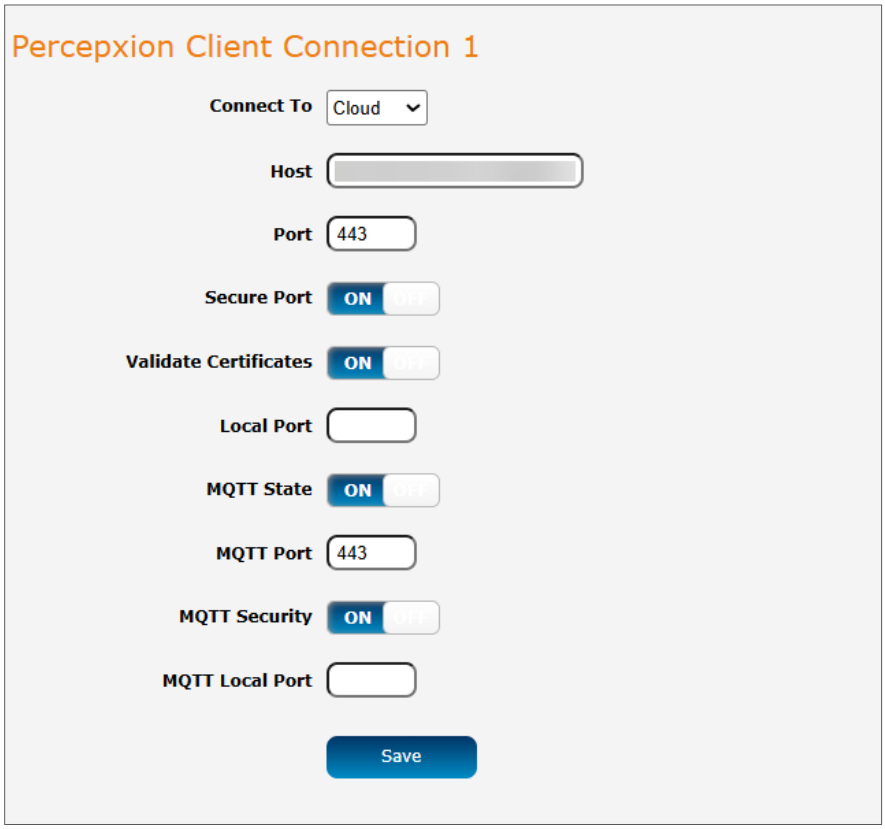


Figure 9-30 Connection 1 configuration settings

Table 9-30 Connection1/Connection2 configuration details

Item	Description
Connect To	Select the type of Percepxion connection. Options are: • **Cloud** • **Premise**
Host	Enter the host name or IP address of the Percepxion server, used to register the device.
Port	Enter the Percepxion port. Default port is 443.
Secure Port	Set to **ON** to enable the Percepxion client secure port 443.
Validate Certificates	Set to **ON** to enable the validation of the Percepxion server certificates. To validate certificates, both MQTT Security and Secure Port must be enabled.
Local Port	Enter local port for the Percepxion client. When configured, a total of 32 consecutive ports will be reserved.
MQTT State	Set to **ON** to enable MQTT.

MQTT Port	Enter the port number of the Percepxion MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Set to **ON** to enable SSL for MQTT.
MQTT Local Port	Enter the local port for Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.

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

Connection 2

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

See Table 9-29 for configuration details.

10. System

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

- Log
- System configuration
- Administration
- Watchdogs
- Power management
- Reboot

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

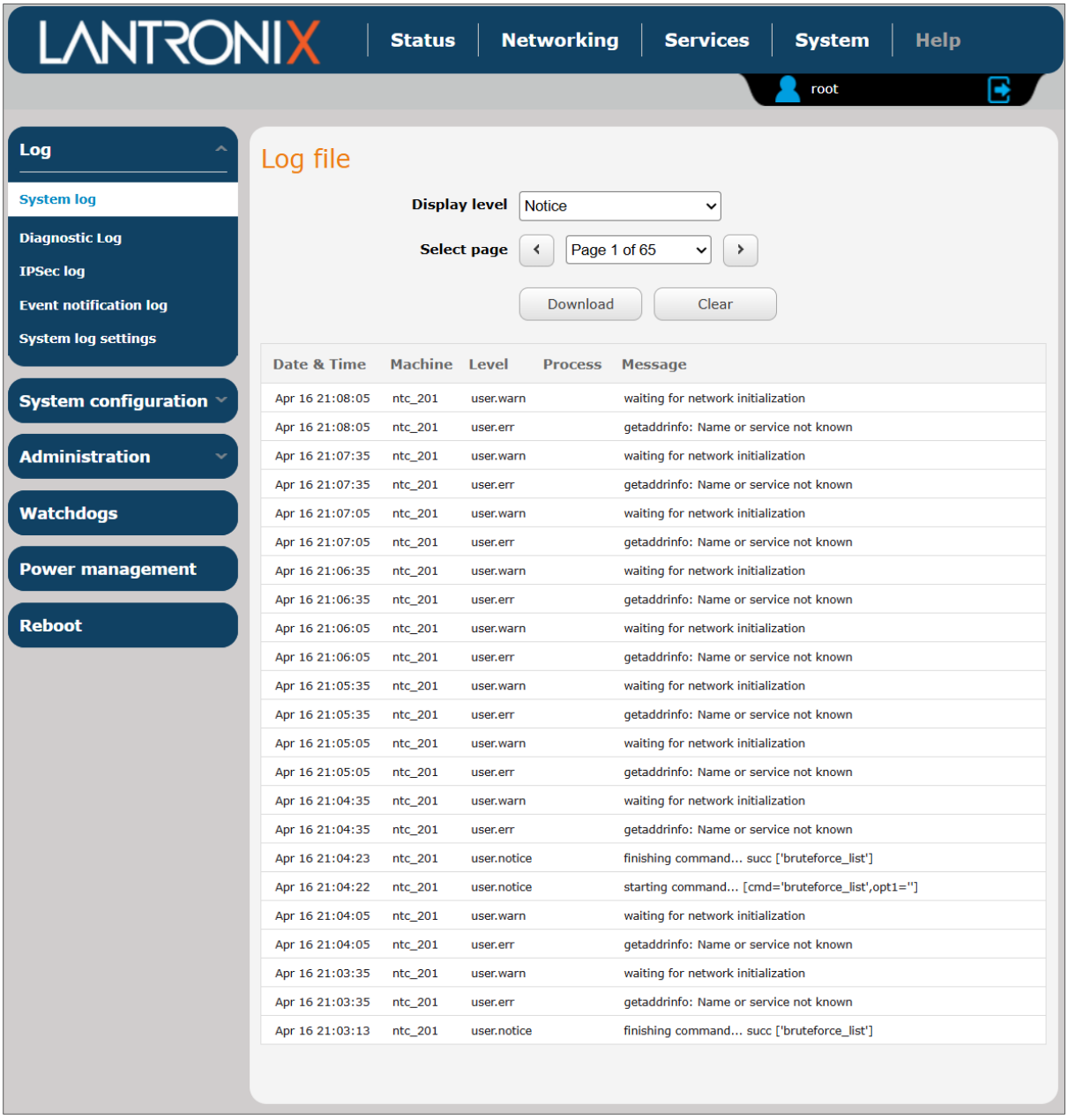


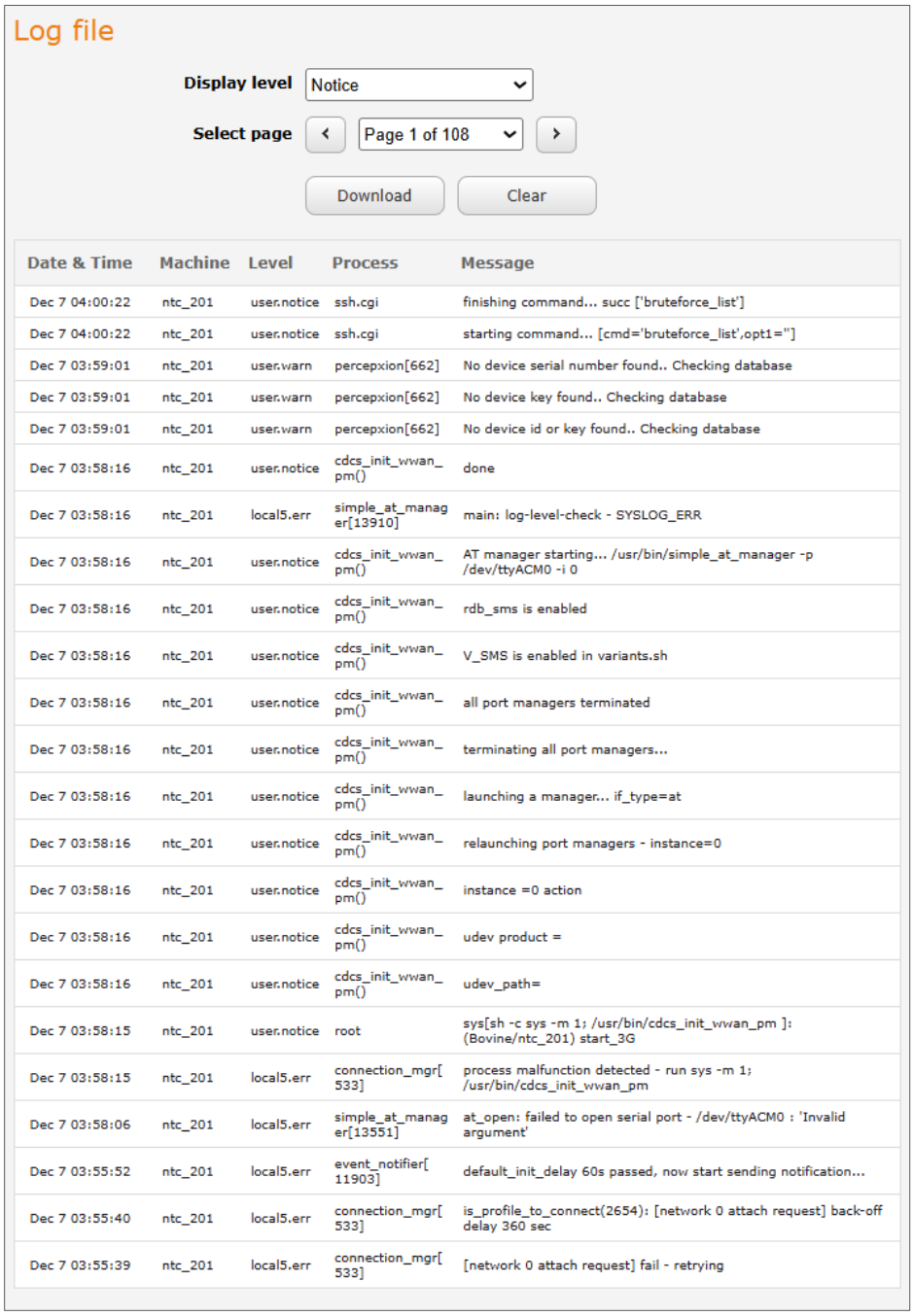
Figure 10-1 System page

Log

The Log section provides the different types logs generated by the router. You can view and download the logs and configure the log settings as required.

System log

The System log page allows you to view and download the System logs. You can use these logs to troubleshoot any issues that you experience with your NTC-201 router. To access the System log page, navigate to **System > Log > System log**.



Date & Time	Machine	Level	Process	Message
Dec 7 04:00:22	ntc_201	user.notice	ssh.cgi	finishing command... succ ['bruteforce_list']
Dec 7 04:00:22	ntc_201	user.notice	ssh.cgi	starting command... [cmd='bruteforce_list',opt1='']
Dec 7 03:59:01	ntc_201	user.warn	percepxion[662]	No device serial number found.. Checking database
Dec 7 03:59:01	ntc_201	user.warn	percepxion[662]	No device key found.. Checking database
Dec 7 03:59:01	ntc_201	user.warn	percepxion[662]	No device id or key found.. Checking database
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	done
Dec 7 03:58:16	ntc_201	local5.err	simple_at_manager[13910]	main: log-level-check - SYSLOG_ERR
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	AT manager starting... /usr/bin/simple_at_manager -p /dev/ttyACM0 -i 0
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	rdb_sms is enabled
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	V_SMS is enabled in variants.sh
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	all port managers terminated
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	terminating all port managers...
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	launching a manager... if_type=at
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	relaunching port managers - instance=0
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	instance =0 action
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	udev product =
Dec 7 03:58:16	ntc_201	user.notice	cdcs_init_wwan_pm()	udev_path=
Dec 7 03:58:15	ntc_201	user.notice	root	sys[sh -c sys -m 1; /usr/bin/cdcs_init_wwan_pm]: (Bovine/ntc_201) start_3G
Dec 7 03:58:15	ntc_201	local5.err	connection_mgr[533]	process malfunction detected - run sys -m 1; /usr/bin/cdcs_init_wwan_pm
Dec 7 03:58:06	ntc_201	local5.err	simple_at_manager[13551]	at_open: failed to open serial port - /dev/ttyACM0 : 'Invalid argument'
Dec 7 03:55:52	ntc_201	local5.err	event_notifier[11903]	default_init_delay 60s passed, now start sending notification...
Dec 7 03:55:40	ntc_201	local5.err	connection_mgr[533]	is_profile_to_connect(2654): [network 0 attach request] back-off delay 360 sec
Dec 7 03:55:39	ntc_201	local5.err	connection_mgr[533]	[network 0 attach request] fail - retrying

Figure 10-2 System log page

In the **Display level** field, select the log type, to filter and display only related logs.

Table 10-1 System log type details

Parameter	Description
Debug	Displays extended system log messages with full debugging level details.
Info	Displays informational messages only.
Notice	Displays normal system logging information.
Warning	Display warning messages only.
Error	Displays error messages only.

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

Click the **Clear** button to clear the System log.

Diagnostic log

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

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

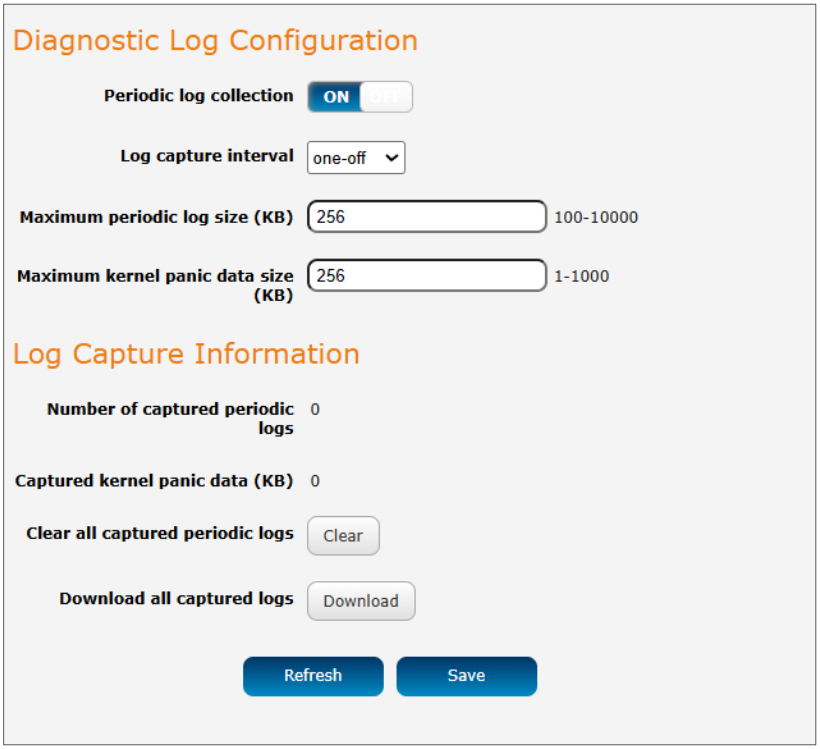


Figure 10-3 Diagnostic log page

Table 10-2 Diagnostic log configuration details

Parameter	Description
Diagnostic log configuration	
Periodic log collection	Set to **ON**, to enable diagnostic log collection.
Log capture interval	Select the interval at which the router should collect diagnostic log data. Options are: • **one-off** • **1 hour** • **2 hours** • **4 hours** • **6 hours** • **12 hours**
Maximum periodic log size (KB)	Enter the maximum size of the log file in kilobytes.
Maximum kernel panic data size (KB)	Enter the maximum size of the kernel panic data file in kilobytes.
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	Click **Clear**, to clear all captured periodic logs.
Download all captured logs	Click **Download**, to download all captured logs.

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

IPSec log

The IPSec log page allows you to view and download the logs for the IPSec VPN function. This can assist you in troubleshooting any problems you have with the IPSec VPN. To access the IPSec log page, navigate to **System > Log > IPSec log**.

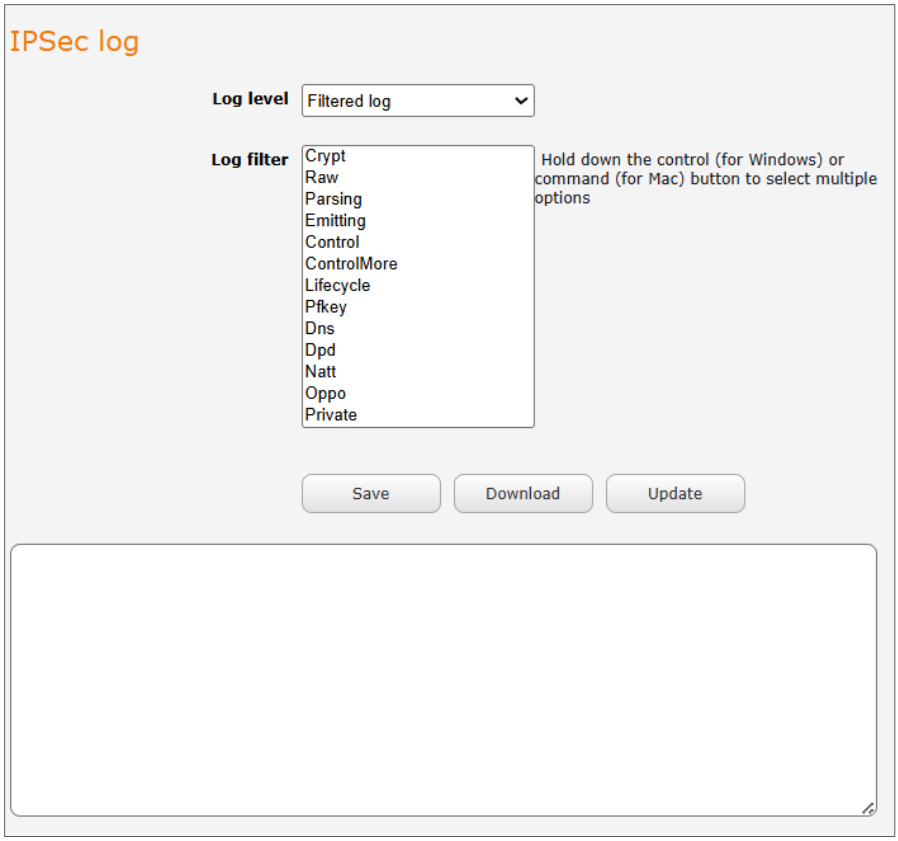


Figure 10-4 IPSec log page

In **Log level** field select the level of the logs you want to capture, then click **Save** button. When you change the Log level, any active IPSec VPN tunnels will be disconnected as a change in logging level requires the IPSec service to be restarted. Options for Log level are:

- **None**
- **All**
- **Filtered log**

When the **Log level** is set to **Filtered log**, the **Log filter** field displays. Select one or multiple Log filters (hold down **Ctrl** and select for Windows, **Cmd** and select for Mac). Click **Save** to save and apply the filter(s).

Click **Update** to force a refresh of the display to show any new entries since the display was last loaded. Click **Download** to download the log file.

Event notification log

The Event notification log page allows you to view and download the logs for the Event notification function. This can assist you to troubleshoot any problems you have with the Event notification feature. To access the Event notification log page, navigate to **System > Log > Event notification log**.

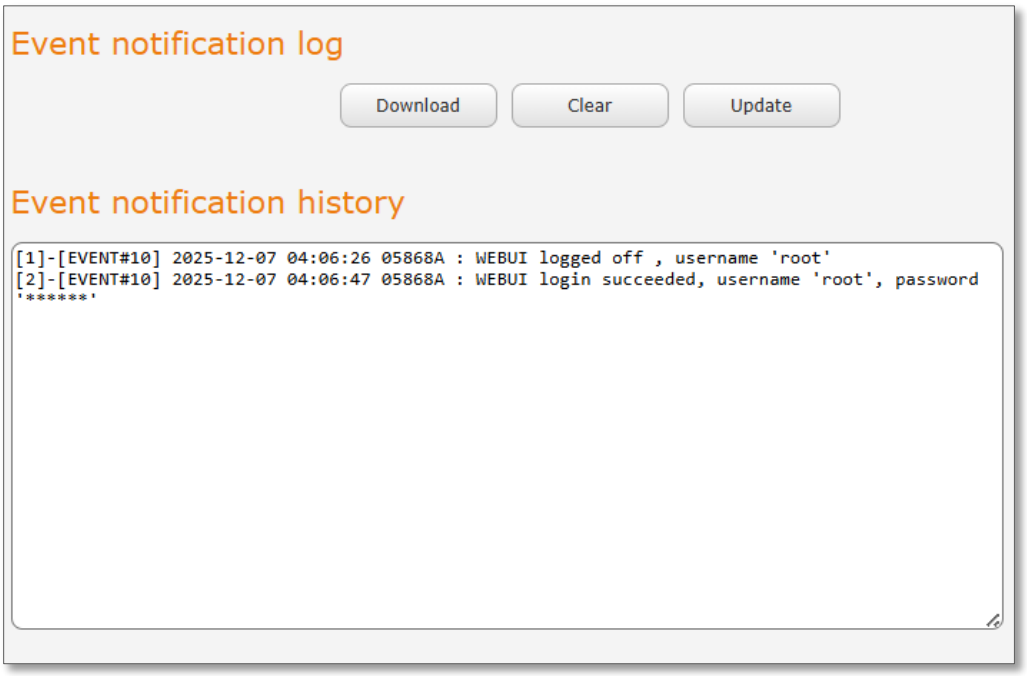


Figure 10-5 Event notification log page

Click **Download** to download the log file, click **Clear** to clear the display, and click **Update** to force a refresh of the log display.

System log settings

The System log settings page allows you to configure settings related to the capture of system log To access the System log settings page, navigate to **System > Log > System log settings**.

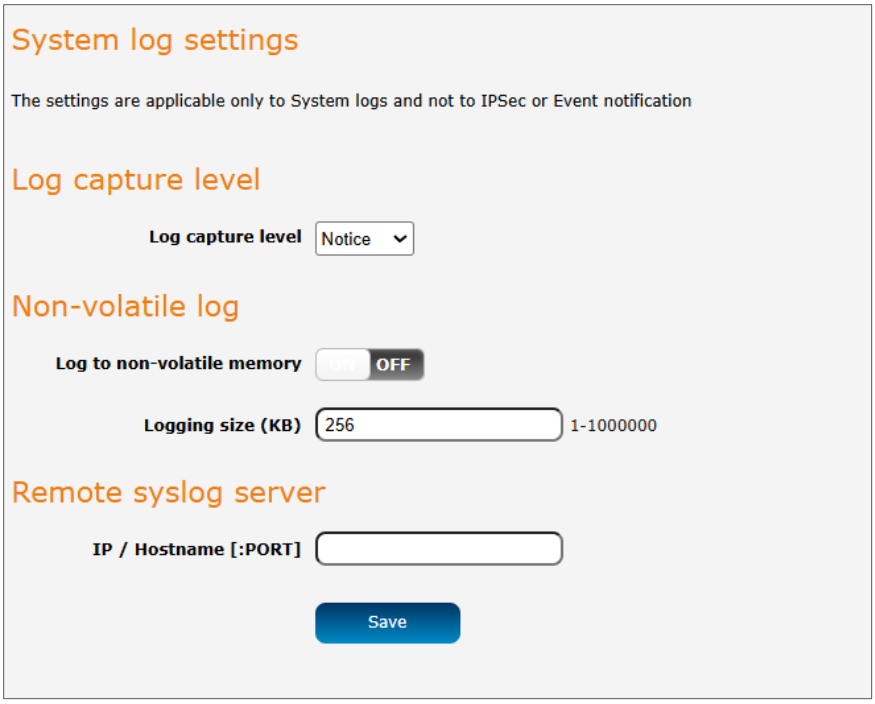


Figure 10-6 System log settings

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

- Enable Non-volatile log
- Use a Remote syslog server

Table 10-3 System Log settings configuration details

Parameter	Description
Log capture level	
Log capture level	Select the log capture level. Options are: • **Debug** – Displays extended system log messages with full debugging level details • **Info** – Displays informational messages only • **Notice** – Displays normal system logging information • **Warning** – Displays warning messages only • **Error** – Displays error messages only
Non-volatile log	
Log to non-volatile memory	Set to **ON** to enable. The log data is stored in flash memory, making it accessible after a reboot of the router. Up to 512 KB 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.

Parameter	Description
	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.
Logging size (KB)	Enter the maximum size of log file in kilobytes
Remote syslog server	
IP / Hostname [:PORT]	Enter the IP address or hostname of the Remote syslog server, and port number, e.g., 192.168.1.102:2356 If you do not specify a port number, the router will use the default UDP port 514.

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

System configuration

Settings backup and restore

The Settings backup and restore page allows you to backup or restore the router's configuration or reset to factory defaults. You can configure the settings for many NTC-201 routers by configuring one router with the required settings, backing them up to a file and then restoring that file to multiple NTC-201 router.

To access the Settings backup and restore page, you must be logged into the web user interface as root using the password admin, then navigate to **System > System configuration > Settings backup and restore**.

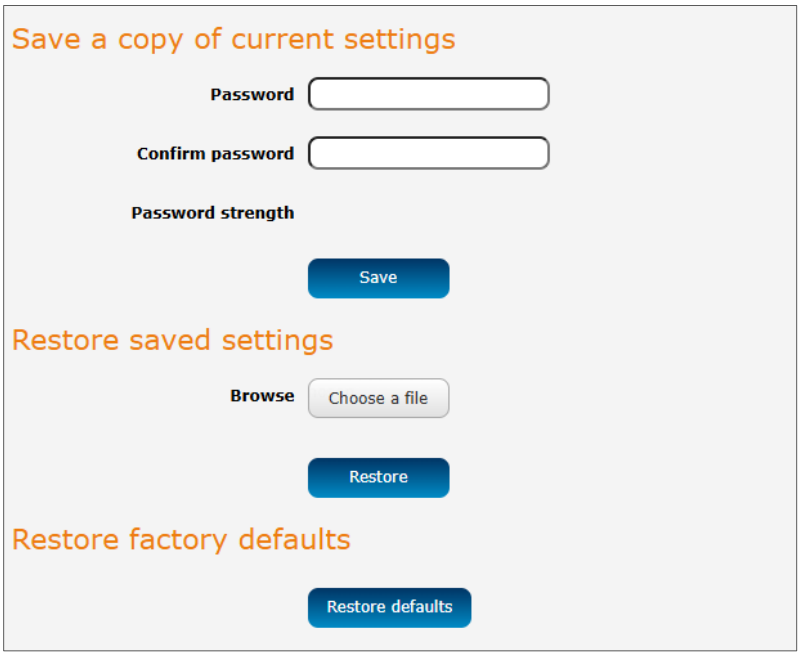


Figure 10-7 Settings backup and restore page

Table 10-4 Settings backup and restore configuration details

Parameter	Description
Save a copy of current settings	
Password	Enter a password to protect the settings backup file.
Confirm password	Re-enter the above password.
Save	Click to apply the password and save the settings file. Right click and select **Save as**, to choose a location for your file. If you do not require password protection for your file, then click **Save** without entering the password details. ***Note:*** *You should not edit the contents of the downloaded file. If you modify the contents of the file in any way you will not be able to restore it later.* *You may change the name of the file if you wish but the filename extension must remain as* ***.cfg****.*

Parameter	Description
Restore saved settings	
Browse	Click **Choose a file** and select the backup configuration file on your computer.
Restore	Click to save and apply the backup configuration settings to your router. The router will apply these settings and prompt to reboot. Click **OK**.
Restore factory defaults	
Restore defaults	Click to restore the factory default configuration. The router prompts you to confirm. Click **OK** to continue.

Upload

The Upload page allows you to upload firmware files, HTTPS certificates, and user-created application packages to the NTC-201 router. When firmware files have been uploaded, they can also be installed from this page. PDF files such as this user guide may also be uploaded for access from the router's help page.

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

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

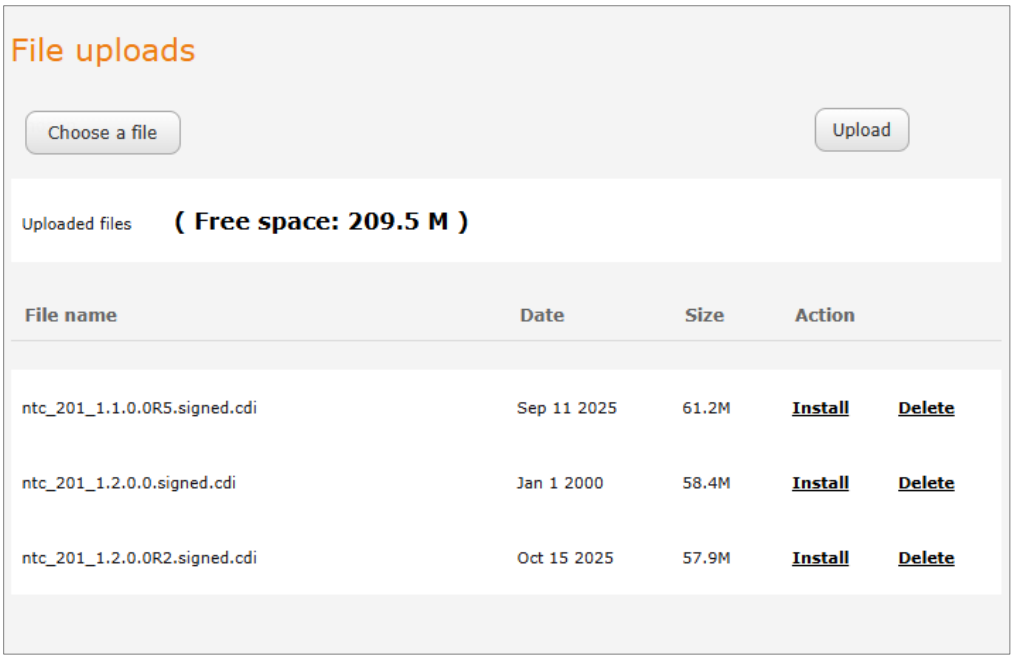


Figure 10-8 Upload page

To upload a file:

1. Click **Choose a file**, then locate and the file on your computer and select it. The file name displays next to **Choose a file** button.
2. Click **Upload** to upload the file. The file displays in the Uploaded files section.
3. Click **Install** action for a file to install it and **Delete** action to delete it.

Updating the Firmware

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

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

To update the NTC-201 router's firmware:

1. Log in to the router with the root user account (See the Advanced configuration section for details)
2. Navigate to **System > System configuration > Upload**. The File uploads page displays.

Figure 10-9 Upload page with selected file

3. Click **Choose a file** button, locate the firmware image file on your computer and click **Open**. The name of the image file is displayed next to **Choose a file** button. The firmware image is named **ntc_200_x.xx.xx.x.cdi** where the 'x' characters represent the version number and is displayed next to **Choose a file** button.
4. Click the **Upload** button. The firmware image is uploaded to the router.
5. The uploaded firmware is listed in the Uploaded files section.

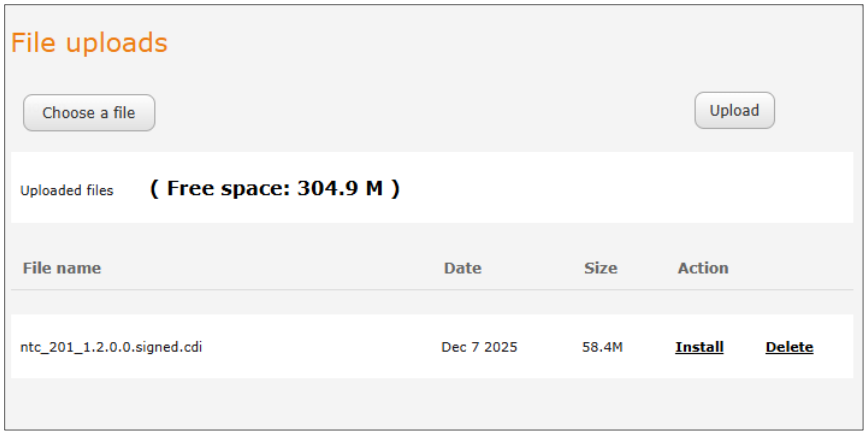


Figure 10-10 Upload page with uploaded file

6. Click the **Install** to install the firmware and then click **OK** in the confirmation window.
7. The firmware is flashed and when it is complete, the router displays **The firmware update was successful** and returns to the main Upload screen.

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

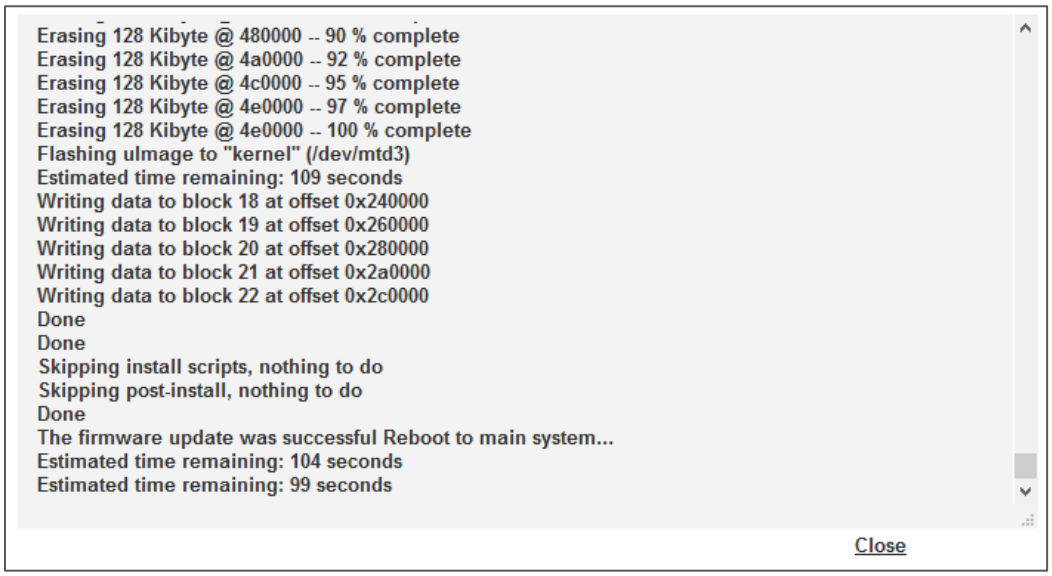


Figure 10-11 Firmware flash process complete

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

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

Figure 10-12 Installation process complete

Package manager

The Package manager page displays the list of the user installed packages on the router. To access the Package manager page, navigate to **System > System configuration > Package manager**.

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

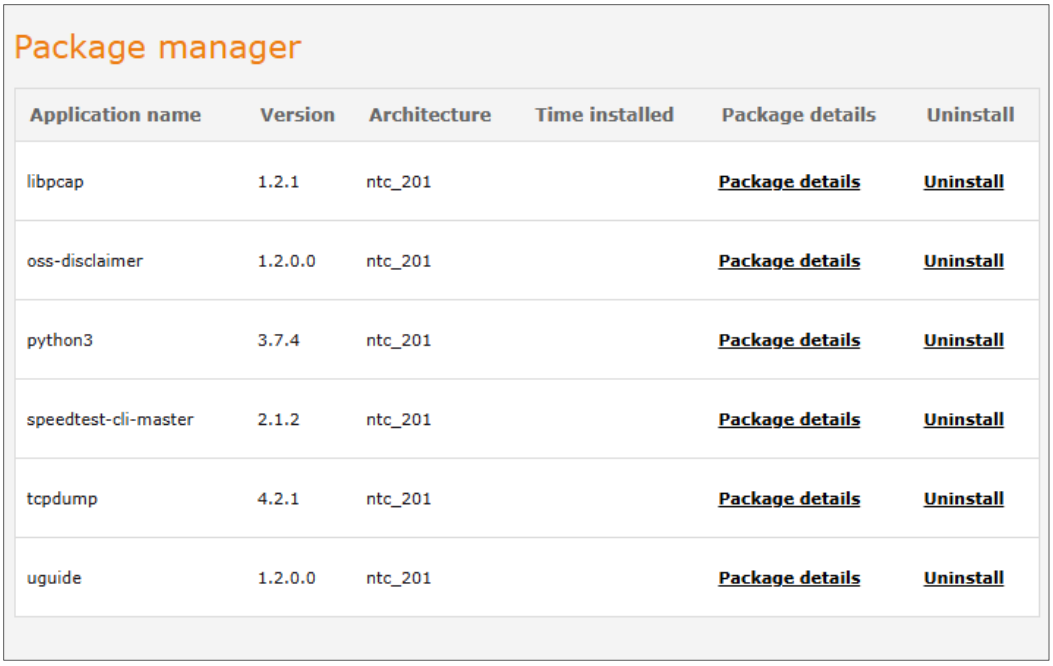


Figure 10-13 Package manger page

Click **Package details** for a package, a pop-up window displays with details about the package.

Click **Uninstall** for a package to uninstall it.

Signature public keys

The Signature public keys page displays the Public key list which contains the public keys used to validate firmware signatures. To access this page, navigate to **System > System configuration > Signature public keys**.

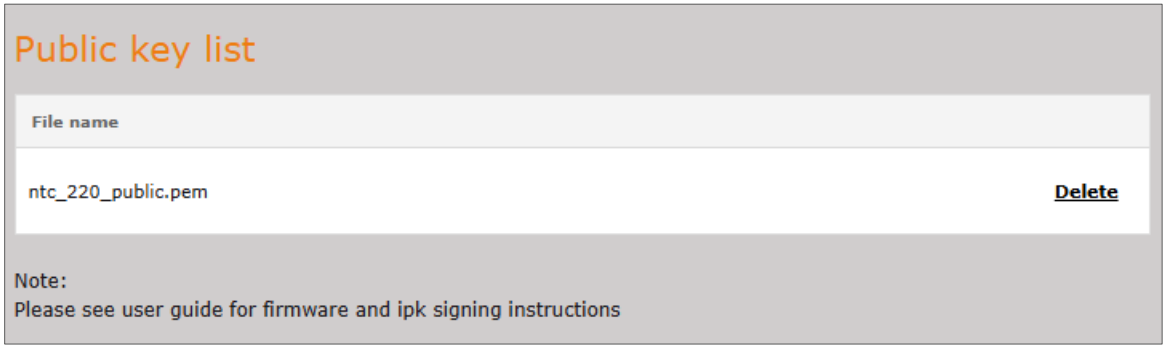


Figure 10-14 Public key list

Administration

Administration settings

The Administration settings page allows you to manage protocols used for remote access to the router and configure the passwords for the different user accounts available to log into to the router.

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

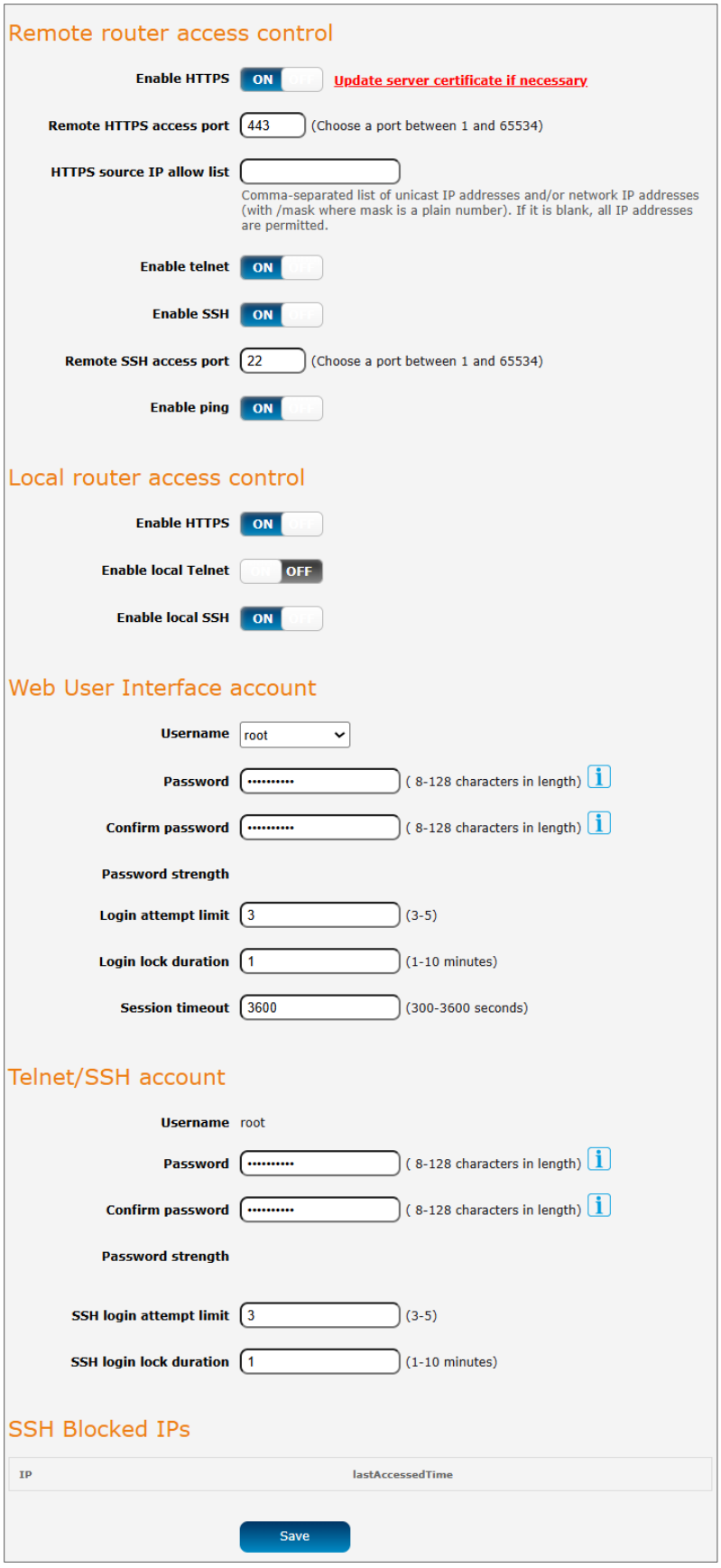


Figure 10-15 Administration settings page

Table 10-5 Administration settings configuration details

Parameter	Description
Remote router access control All remote router access control settings are disabled by default.	
Enable HTTPS	Set to **ON** to enable.
Remote HTTPS access port	Displays when HTTPS is enabled. Enter a port number between 1 and 65534, for HTTPS access.
HTTPS source IP allow list	Displays when HTTPS is enabled. Enter a list of IP addresses that will be permitted to access the router. Enter a list of comma-separated unicast IP addresses. You may also enter IP addresses in CIDR notation. However, no spaces are permitted. Note that if this field is left blank, all IP addresses will be permitted to access the router.
Enable Telnet	Set to **ON** to enable.
Enable SSH	Set to **ON** to enable.
Remote SSH Access Port	Displays when SSH is enabled. Enter the port number between 1 and 65534, for remote SSH access.
Enable Ping	Set to **ON** to enable.
Local router access control	
Enable HTTPS	Set to **ON** to enable.
Enable local Telnet	Set to **ON** to enable.
Enable local SSH	Set to **ON** to enable.
Web User Interface account	
Username	Select the account for which you want to configure the login settings, **root** or **admin**.
Password	Enter a password for the account. Click  icon to display password criteria.
Confirm password	Re-enter the above password.
Password strength	Displays the strength of the entered password.
Login attempt limit	Enter the number of unsuccessful login attempts that are allowed before the login lock applies.

Parameter	Description
Login lock duration	Enter the time in minutes that users must wait before they can re-attempt to login after reaching the **Login attempt limit** set above.
Session timeout	Enter the time in seconds that the system can remain idle before the sessions logs out.
Telnet/SSH account	
Username	Displays the Telnet/SSH username. This cannot be changed.
Password	Enter a password for the account. Click icon to display password criteria.
Confirm password	Re-enter the above password.
Password strength	Displays the strength of the entered password.
SSH login attempt limit	Enter the number of unsuccessful login attempts that are allowed before the login lock applies.
SSH login lock duration	Enter the time in minutes that users must wait before they can re-attempt to login after reaching the **Login attempt limit** set above.
SSH Blocked IPs	
IP	The host IP address for which SSH access has been blocked.
LastAccessedTime	The duration in seconds for which SSH access has been blocked. Once it reaches the value configured for **SSH login lock duration**, the SSH access is unblocked.

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

To access the router's configuration pages remotely:

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

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

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

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

Server certificate

HTTP Secure or HTTPS is the use of the HTTP protocol over an SSL/TLS security layer. It is used primarily to secure communication between a web browser and the web site to which it is connected and prevent eavesdropping and data theft. This is important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured with certificates issued by trusted certificate

authorities such as VeriSign. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.

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

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

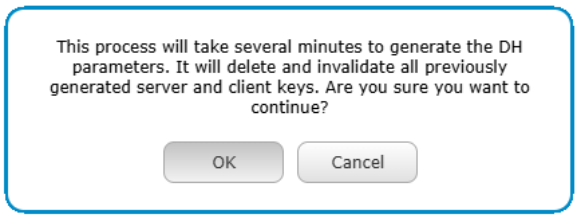
The encryption is achieved by using a pair of public and private keys on both sides of the connection. In cryptography, a key refers to a numerical value used by an algorithm to alter information (encrypt it), making the information secure and visible only to those who have the corresponding key to recover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

Each NTC-201 router contains a self-signed digital certificate which is identical on all NTC-201 routers. For a greater level of security, the router also supports generating your own unique key. Additionally, you may use third party software to generate your own self-signed digital certificate or purchase a signed certificate from a trusted certificate authority and then upload those certificates to the router.

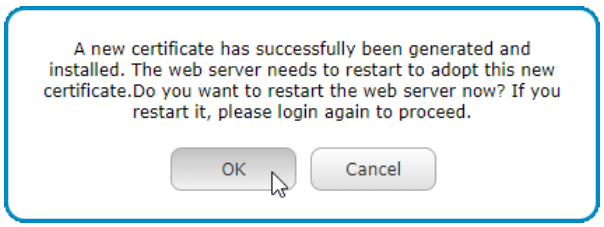
To generate your own self-signed certificate, navigate to **System > Administration > Server certificate**.

Figure 10-16 Server certificate page

Table 10-6 Server certificate configuration details

Parameter	Description
Server key size	Select the required Server key size. A larger key size takes more time to generate but provides better security
Diffie-Hellman parameters	Click **Generate** to generate Diffie-Hellman parameters. The below prompt displays.  Click **Ok**.
Certificate serial number	
Not before	Displays the date and time the certificate is generated.
Not after	Displays the date and time the certificate is set to expire.
Country	Enter the Country code. See Table 10-7 – Country codes for the applicable country code.
State	Enter the State name.
City	Enter the City name.
Organization	Enter the Organization name.
Email	Enter the Email address.

Click **Generate** to generate the certificate. Once the certificate has been successfully generated the below prompt displays.



Click **OK** to continue.

Table 10-7 Country codes

Code	Country	Code	Country	Code	Country	Code	Country
AX	Åland Islands	**ER**	Eritrea	**LS**	Lesotho	**SA**	Saudi Arabia
AD	Andorra	**ES**	Spain	**LT**	Lithuania	**SB**	Solomon Islands

Code	Country	Code	Country	Code	Country	Code	Country
AE	United Arab Emirates	**ET**	Ethiopia	**LU**	Luxembourg	**SC**	Seychelles
AF	Afghanistan	**FI**	Finland	**LV**	Latvia	**SE**	Sweden
AG	Antigua and Barbuda	**FJ**	Fiji	**LY**	Libya	**SG**	Singapore
AI	Anguilla	**FK**	Falkland Islands (Malvinas)	**MA**	Morocco	**SH**	St. Helena
AL	Albania	**FM**	Micronesia	**MC**	Monaco	**SI**	Slovenia
AM	Armenia	**FO**	Faroe Islands	**MD**	Moldova	**SJ**	Svalbard and Jan Mayen Islands
AN	Netherlands Antilles	**FR**	France	**ME**	Montenegro	**SK**	Slovak Republic
AO	Angola	**FX**	France, Metropolitan	**MG**	Madagascar	**SL**	Sierra Leone
AQ	Antarctica	**GA**	Gabon	**MH**	Marshall Islands	**SM**	San Marino
AR	Argentina	**GB**	Great Britain (UK)	**MK**	Macedonia	**SN**	Senegal
AS	American Samoa	**GD**	Grenada	**ML**	Mali	**SR**	Suriname
AT	Austria	**GE**	Georgia	**MM**	Myanmar	**ST**	Sao Tome and Principe
AU	Australia	**GF**	French Guiana	**MN**	Mongolia	**SU**	USSR (former)
AW	Aruba	**GG**	Guernsey	**MO**	Macau	**SV**	El Salvador
AZ	Azerbaijan	**GH**	Ghana	**MP**	Northern Mariana Islands	**SZ**	Swaziland
BA	Bosnia and Herzegovina	**GI**	Gibraltar	**MQ**	Martinique	**TC**	Turks and Caicos Islands
BB	Barbados	**GL**	Greenland	**MR**	Mauritania	**TD**	Chad
BD	Bangladesh	**GM**	Gambia	**MS**	Montserrat	**TF**	French Southern Territories
BE	Belgium	**GN**	Guinea	**MT**	Malta	**TG**	Togo

Code	Country	Code	Country	Code	Country	Code	Country
BF	Burkina Faso	**GP**	Guadeloupe	**MU**	Mauritius	**TH**	Thailand
BG	Bulgaria	**GQ**	Equatorial Guinea	**MV**	Maldives	**TJ**	Tajikistan
BH	Bahrain	**GR**	Greece	**MW**	Malawi	**TK**	Tokelau
BI	Burundi	**GS**	S. Georgia and S. Sandwich Isls.	**MX**	Mexico	**TM**	Turkmenistan
BJ	Benin	**GT**	Guatemala	**MY**	Malaysia	**TN**	Tunisia
BM	Bermuda	**GU**	Guam	**MZ**	Mozambique	**TO**	Tonga
BN	Brunei Darussalam	**GW**	Guinea-Bissau	**NA**	Namibia	**TP**	East Timor
BO	Bolivia	**GY**	Guyana	**NC**	New Caledonia	**TR**	Turkey
BR	Brazil	**HK**	Hong Kong	**NE**	Niger	**TT**	Trinidad and Tobago
BS	Bahamas	**HM**	Heard and McDonald Islands	**NF**	Norfolk Island	**TV**	Tuvalu
BT	Bhutan	**HN**	Honduras	**NG**	Nigeria	**TW**	Taiwan
BV	Bouvet Island	**HR**	Croatia (Hrvatska)	**NI**	Nicaragua	**TZ**	Tanzania
BW	Botswana	**HT**	Haiti	**NL**	Netherlands	**UA**	Ukraine
BZ	Belize	**HU**	Hungary	**NO**	Norway	**UG**	Uganda
CA	Canada	**ID**	Indonesia	**NP**	Nepal	**UM**	US Minor Outlying Islands
CC	Cocos (Keeling) Islands	**IE**	Ireland	**NR**	Nauru	**US**	United States
CF	Central African Republic	**IL**	Israel	**NT**	Neutral Zone	**UY**	Uruguay
CH	Switzerland	**IM**	Isle of Man	**NU**	Niue	**UZ**	Uzbekistan
CI	Cote D'Ivoire (Ivory Coast)	**IN**	India	**NZ**	New Zealand (Aotearoa)	**VA**	Vatican City State (Holy See)

Code	Country	Code	Country	Code	Country	Code	Country
CK	Cook Islands	**IO**	British Indian Ocean Territory	**OM**	Oman	**VC**	Saint Vincent and the Grenadines
CL	Chile	**IS**	Iceland	**PA**	Panama	**VE**	Venezuela
CM	Cameroon	**IT**	Italy	**PE**	Peru	**VG**	Virgin Islands (British)
CN	China	**JE**	Jersey	**PF**	French Polynesia	**VI**	Virgin Islands (U.S.)
CO	Colombia	**JM**	Jamaica	**PG**	Papua New Guinea	**VN**	Viet Nam
CR	Costa Rica	**JO**	Jordan	**PH**	Philippines	**VU**	Vanuatu
CS	Czechoslovakia (former)	**JP**	Japan	**PK**	Pakistan	**WF**	Wallis and Futuna Islands
CV	Cape Verde	**KE**	Kenya	**PL**	Poland	**WS**	Samoa
CX	Christmas Island	**KG**	Kyrgyzstan	**PM**	St. Pierre and Miquelon	**YE**	Yemen
CY	Cyprus	**KH**	Cambodia	**PN**	Pitcairn	**YT**	Mayotte
CZ	Czech Republic	**KI**	Kiribati	**PR**	Puerto Rico	**ZA**	South Africa
DE	Germany	**KM**	Comoros	**PS**	Palestinian Territory	**ZM**	Zambia
DJ	Djibouti	**KN**	Saint Kitts and Nevis	**PT**	Portugal	**COM**	US Commercial
DK	Denmark	**KR**	Korea (South)	**PW**	Palau	**EDU**	US Educational
DM	Dominica	**KW**	Kuwait	**PY**	Paraguay	**GOV**	US Government
DO	Dominican Republic	**KY**	Cayman Islands	**QA**	Qatar	**INT**	International
DZ	Algeria	**KZ**	Kazakhstan	**RE**	Reunion	**MIL**	US Military
EC	Ecuador	**LA**	Laos	**RO**	Romania	**NET**	Network
EE	Estonia	**LC**	Saint Lucia	**RS**	Serbia	**ORG**	Non-Profit Organization
EG	Egypt	**LI**	Liechtenstein	**RU**	Russian Federation	**ARPA**	Old style Arpanet

Code	Country	Code	Country	Code	Country	Code	Country
EH	Western Sahara	**LK**	Sri Lanka	**RW**	Rwanda		

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, and 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:

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

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

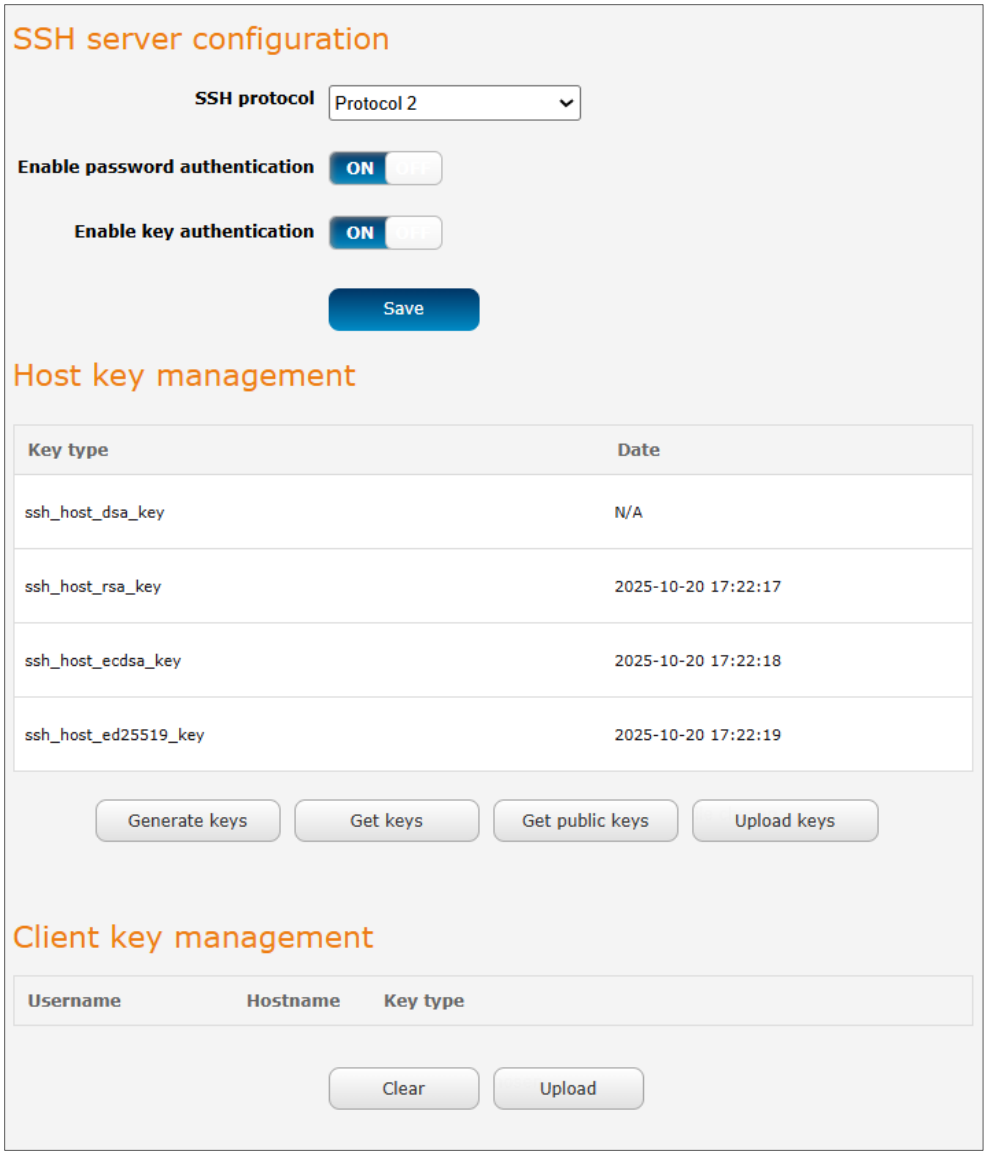


Figure 10-17 SSH key management page

SSH server configuration

Table 10-8 SSH server configuration details

Parameter	Description
SSH protocol	Select the SSH protocol to use. Options are: • **Protocol 1** • **Protocol 2** • **Protocol 1, 2** Protocol 2 is more recent and is considered more secure.
Enable password authentication	Set to **ON** to enable password authentication.
Enable key authentication	Set to **ON** to enable key authentication.

Note: *You can enable both authentication methods but cannot disable both. At least one authentication method must be enabled.*

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

Host key management

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

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

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

Figure 10-18 Host key management details

Parameter	Description
Generate keys	Click to generate the complete set of keys. This key generation process takes approximately 30 seconds to complete.
Get keys	Click to download the complete set of public and private keys
Get public keys	Click to download only the set of public keys.

Upload keys	You can generate your own SSH keys and upload them to the router. To generate keys on a Linux-based machine, use the following commands:
	`mkdir keys`
	`cd keys`
	`ssh-keygen -t rsa1 -f ssh_host_key -N ""`
	`ssh-keygen -t dsa -f ssh_host_dsa_key -N ""`
	`ssh-keygen -t rsa -f ssh_host_rsa_key -N ""`
	`ssh-keygen -t ecdsa -f ssh_host_ecdsa_key -N ""`
	`zip -e -P "PASSWORDHERE" -j keys.zip *`
	Click **Upload keys** to locate the keys and upload them to the router.

Client key management

The Client key management section allows you to upload the public key file of clients.

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

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

LED operation mode

The seven LED indicators may be turned off after a timeout period for aesthetic or power saving reasons. To access the LED Operation Mode page, navigate to **System > Administration > LED operation mode**.

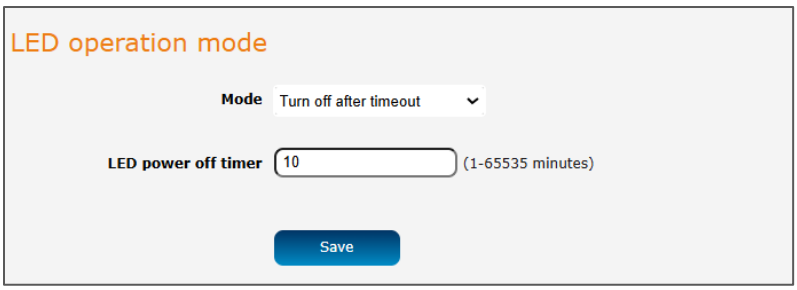


Figure 10-19 LED Operation Mode page

To configure LED operation mode:

1. Select Mode. Options are:
   - **Always on** – Sets the lights to operate at all times
   - **Turn off after timeout** – Sets the lights to turn off after a specific period**.** When selected the **LED power off timer** field displays. Enter the time in minutes to wait before turning off the LED indicators.
2. Click **Save** to save and apply the settings.

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

Site settings

The Site settings page allows you to set the Site name and location for the router. These details are displayed in the Status page, in System information section. To access the Site settings page, navigate to **System > Administration > Site settings**.

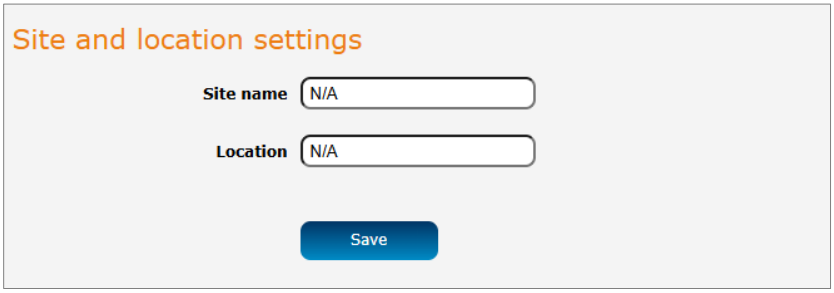


Figure 10-20 Site settings page

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

Watchdogs

The Watchdogs page allows you to configure the behaviour of the Periodic Ping monitor function.

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

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

It is due to the nature of the ping watchdog being a last resort standalone backup mechanism that it will continue to do its job and reboot the device even when the Connect on demand session is idle, or the PDP context is disabled by the user. Therefore, it is recommended to disable this feature if Connect on demand is configured, or if the PDP context will be intentionally disconnected on the occasion.

The feature operates as follows:

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

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

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

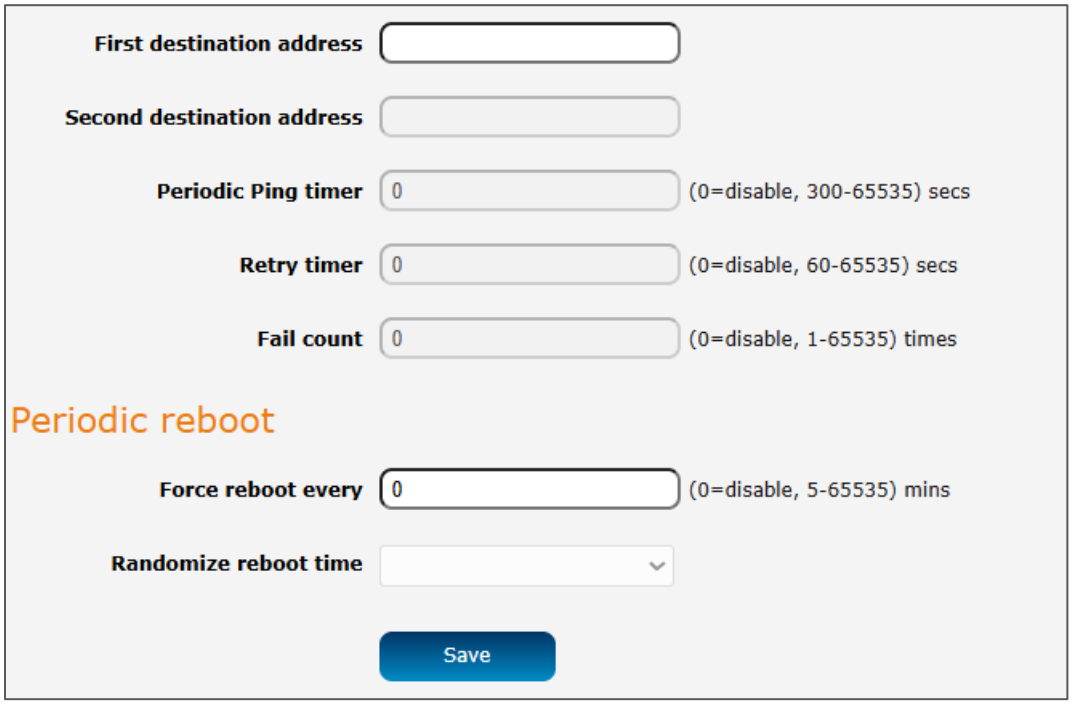


Figure 10-21 Watchdogs settings page

Table 10-9 Watchdogs settings configuration details

Parameter	Description
Watchdogs settings	
First destination address	Enter website address or IP address to which the router will send the first round of ping requests.
Second destination address	Enter website address or IP address to which the router will send the second round of ping requests.
Periodic Ping timer	Enter the time in seconds the router should wait between ping attempts. Setting this to 0 disables the Watchdog function.
Retry timer	Enter the time in seconds the router should wait to retry ping attempts i.e. pings to the second destination address. Setting this to 0 disables the watchdog function.
Fail count	Enter number of times an accelerated ping should fail before the router reboots. Setting this to 0 disables the watchdog function.
Periodic reboot	
Force reboot every	Enter the time in minutes between forced reboots. Setting this to 0 disables the Periodic reboot function.
Randomize reboot time	If you have set a value for **Force reboot every**, you can select a value for **Randomize reboot time**. Randomizing the reboot time is useful for preventing many devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured **Force reboot every** time and then randomly selects a time that is less than or equal to the Randomize reboot time setting. After that randomly selected time has elapsed, the router reboots.

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

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

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

Power management

The Power management page allows you to configure a power profile for the device. To access the Power management page, navigate to **System > Power management**.

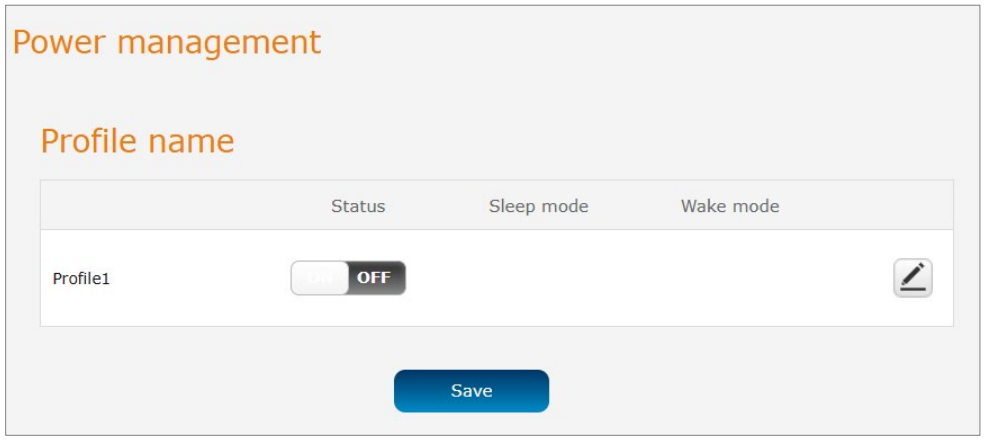


Figure 10-22 Power management page

The **Status** column indicates whether the profile is active, while the **Sleep mode** and **Wake mode** columns display the sleep and wake modes configured for the profile.

Click the icon to configure or edit the profile, the different configuration settings display.

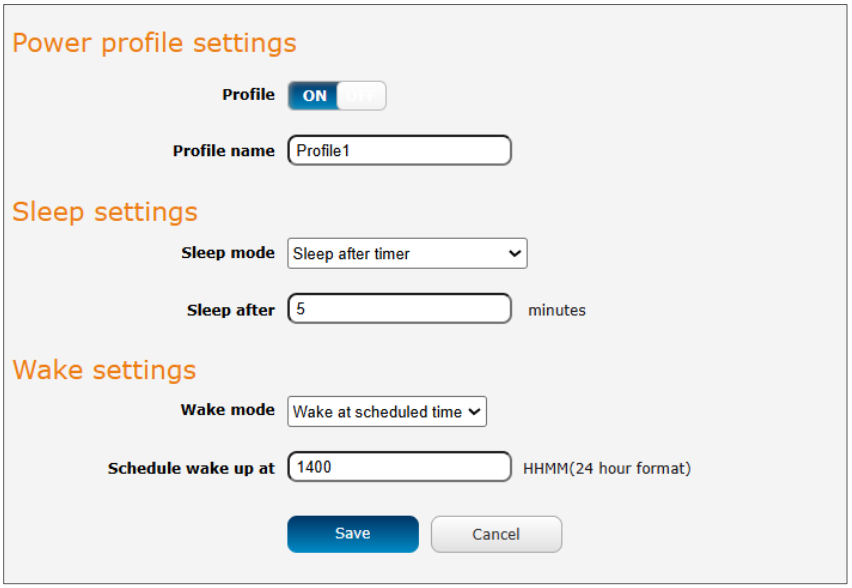


Figure 10-23 Power management configuration settings

Table 10-10 Power management configuration details

Parameter	Description
Power profile settings	
Profile	Set to **ON** to enable.
Profile name	Enter a name for the profile.

Parameter	Description
Sleep settings	
Sleep mode	Select a condition for which the router should enter the sleep state. Options are: • **Sleep after timer** – The router will enter the sleep state after the time in minutes specified in the **Sleep after** field. • **Sleep at scheduled time** – The router goes to sleep at the time specified in the **Schedule sleep at** field.
Sleep after	Displays when Sleep after timer is selected as Sleep mode. Enter the time in minutes.
Schedule sleep at	Displays when Sleep at scheduled time is selected as Sleep mode. Enter the time in 24-hour format without semi-colon.
Wake settings	
Wake mode	**Wake at scheduled time** – Sets the router to wake up at the time specified in the **Schedule wake up at** field.
Schedule wake up at	Displays when Sleep at scheduled time is selected as Wake mode. Enter the time in 24-hour format without semi-colon.

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

Reboot

The Reboot page allows you to perform soft reboot of the router. This is useful if you have made configuration changes you want to implement.

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

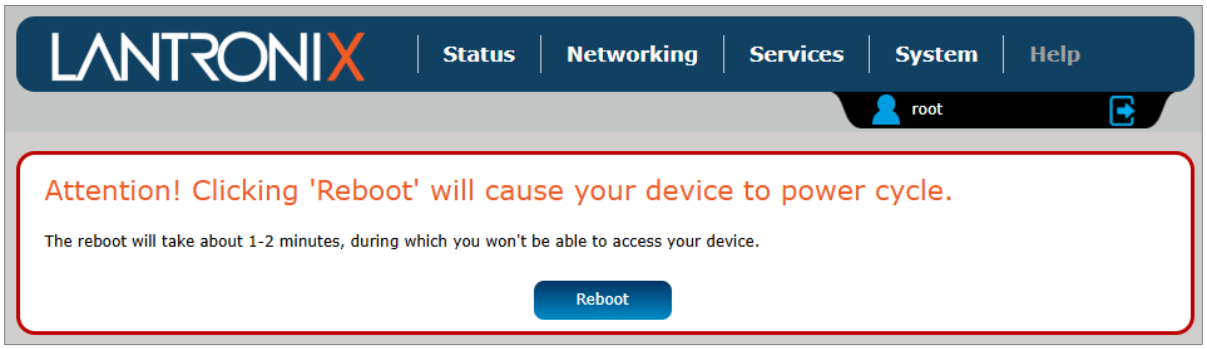
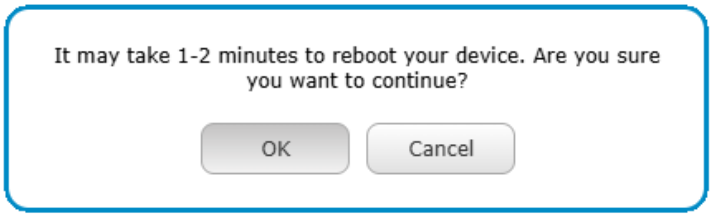


Figure 10-24 Reboot page

Click **Reboot** to reboot the router, the below prompt displays.



Click **OK** to continue.

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

11. Help

The Help page provides links to access the NTC-201 User Guide and Lantronix Support Portal. To access the Help page, click the **Help** tab on the top menu bar.

Figure 11-1 Help page

12. Open-source disclaimer

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

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

13. Safety and product care

Electrical safety

Accessories

Only use approved accessories.

Do not connect with incompatible products or accessories.

Distraction

Operating machinery

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

Product handling

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

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

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

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

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

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

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

Do not paint your device or its accessories.

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

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

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

Do not use your device in an enclosed environment or where heat dissipation is poor. Prolonged use in such space may cause excessive heat and raise ambient temperature, which will lead to automatic shutdown of your device or the disconnection of the mobile network connection for your safety. To use your device normally again after such shutdown, cool it in a well-ventilated place before turning it on.

Please check local regulations for disposal of electronic products.

Do not operate the device where ventilation is restricted

Installation and configuration should be performed by trained personnel only.

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

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

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

Small children

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

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

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

Demagnetisation

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

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

Electrostatic discharge (ESD)

Do not touch the SIM card's metal connectors.

Emergency & other situations requiring continuous connectivity

This device, like any wireless device, operates using radio signals, which cannot guarantee connection in all conditions. Therefore, you must never rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss.

Device heating

Your device may become warm during normal use.

Faulty and Damaged Products

Do not attempt to disassemble the device or its accessory.

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

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

Interference

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

Pacemakers

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

Hearing aids

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

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

Medical devices

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

Hospitals

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

Aircraft

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

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

Explosive environments

Petrol stations and explosive atmospheres

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

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

Blasting caps and areas

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

Appendix A. Compliance

Manufacturer's Name & Address:

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

Product Family:

NTC-201
Conforms to the following standards or other normative documents:

Country	Specification
Australia – RCM	Supplier's declaration of conformity
Canada – IC	Contains: IC: 5131A-LE910Q1WW
Europe – CE	EU Declaration of Conformity (see *Figure A-1*)
UK - UKCA	UK Declaration of Conformity (see *Figure A-2*)
USA – FCC	Contains: FCC ID: RI7LE910Q1WW
Cellular Certification	PTCRB, AT&T, and Verizon

FCC Compliance

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

FCC Regulations

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

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

RF Exposure

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

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

External Antenna

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

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

IC regulations

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

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

(1) this device may not cause interference, and

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

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

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

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

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

RF Exposure Information (MPE)

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

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

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

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

External antenna

RSS-Gen 8.3 (transmitters equipped with detachable antennas)

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

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

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

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

EU Declaration of Conformity

Figure A-1 EU Declaration of Conformity

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 US
Model Number: NTC-201
SW Version: 1.2.0.0

Manufacturer's Quality System:

TÜVRheinland

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

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)

- **EN IEC 62368-1:2023**

EMC Directive (2014/30/EU)

- **EN 301 489-1 V2.2.3 (2019-11)**
- **EN 301 489-52 V1.3.1 (2024-11**
- **EN 55032:2015+A11:2020**
- **EN55035:2017+A11:2020**

RF Radio Directive (2014 / 53 / EU)

- **EN 301 908-1 V15.2.1**
- **EN 301 908-13 V13.2.1**

Health & Safety Directive (2014 / 53 / EU)

- **EN 50663:2017, EN 62479:2010**
- **EN 50665:2017, EN IEC 62311:2020**

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

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

EU Directive 2011/65/EU for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I

- **EN IEC 63000:2018**

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

Signature: _____ Date: 11 December 2025

Name: Steve Burrington Title: Vice President RnD

CERT-00548 rev A

EU Statements

Table A-1 EU Statements

Code	Language	Statement
bg	Bulgarian	Lantronix, Inc., декларира, че този NTC-201 device отговаря на основните изисквания и други приложими разпоредби на Директива 2014/53/EU. Пълният текст на декларацията на ЕС за съответствие е достъпен на следния интернет адрес: http://www.lantronix.com/products/ntc-201-series/ Известие на ЕС за ограничения при употреба: Това устройство е ограничено само за вътрешна употреба. Може да не се работи наоткрито.
cs	Česky [Czech]	Lantronix, Inc. tímto prohlašuje, že tento NTC-201 device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. Úplné znění ES prohlášení o shodě je k dispozici na této internetové adrese: http://www.lantronix.com/products/ntc-201-series/ Oznámení EU o omezení používání: Toto zařízení je omezeno pouze na použití uvnitř. Nesmí být provozován venku.
da	Dansk [Danish]	Undertegnede Lantronix, Inc. erklærer herved, at følgende udstyr NTC-201 device overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. Den fulde tekst til EU-overensstemmelseserklæringen er tilgængelig på følgende internetadresse: http://www.lantronix.com/products/ntc-201-series/ EU-meddelelse om begrænsninger i brug: Denne enhed er kun begrænset til indendørs brug. Det betjenes måske ikke udendørs.
de	Deutsch [German]	Hiermit erklärt Lantronix, Inc., dass sich das Gerät NTC-201 device in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EUbefindet. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse abrufbar: http://www.lantronix.com/products/ntc-201-series/ EU-Hinweis zu Nutzungsbeschränkungen: Dieses Gerät darf nur in Innenräumen verwendet werden. Es darf nicht im Freien betriebenwerden.
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix, Inc. seadme NTC-201 device vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. EL-i vastavusdeklaratsiooni täielik tekst on saadaval järgmisel Interneti-aadressil: http://www.lantronix.com/products/ntc-201-series/ EL-i teade kasutuspiirangute kohta: seda seadet saab kasutada ainult siseruumides. Seda ei tohi õues kasutada.

Code	Language	Statement
en	English	Hereby, Lantronix, Inc., declares that this NTC-201 device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: http://www.lantronix.com/products/ntc-201-series/ EU Notice of Restrictions on Use: This device is limited to indoor use only. It may not be operated outdoors.
es	Español [Spanish]	Por medio de la presente Lantronix, Inc. declara que el NTC-201 device module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: http://www.lantronix.com/products/ntc-201-series/ Aviso de restricciones de uso de la UE: este dispositivo está limitado solo para uso en interiores. No puede ser operado al aire libre.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix, Inc. ΔΗΛΩΝΕΙ ΟΤΙ NTC-201 device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ διατίθεται στην ακόλουθη διεύθυνση διαδικτύου: http://www.lantronix.com/products/ntc-201-series/ Ειδοποίηση της ΕΕ για περιορισμούς χρήσης: Η συσκευή αυτή περιορίζεται μόνο σε εσωτερικούς χώρους χρήσης. Μπορεί να μην λειτουργεί σε εξωτερικούς χώρους.
fr	Français [French]	Par la présente Lantronix, Inc. déclare que l'appareil NTC-201 device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante: http://www.lantronix.com/products/ntc-201-series/ Avis de restrictions d'utilisation de l'UE: Cet appareil est limité à une utilisation en intérieur uniquement. Il ne doit pas être utilisé àl'extérieur
is	Icelandic	Hér með lýsir Lantronix, Inc. því yfir að NTC-201 device sé í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53 / ESB. Í heildartexta ESB-samræmisyfirlýsingarinnar er að finna á eftirfarandi internetfangi: http://www.lantronix.com/products/ntc-201-series/ Tilkynning ESB um takmarkanir á notkun: Þetta tæki er eingöngutakmarkað við notkun innanhúss. Það má ekki nota það úti.
it	Italiano [Italian]	Con la presente Lantronix, Inc. dichiara che questo NTC-201 device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.

Code	Language	Statement
		Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: http://www.lantronix.com/products/ntc-201-series/ Avviso di restrizioni d'uso dell'UE: questo dispositivo è limitato esclusivamente all'uso in interni. Potrebbe non essere utilizzatoall'aperto.
lv	Latviski [Latvian]	Ar šo Lantronix, Inc. deklarē, ka NTC-201 device atbilst Direktīvas 2014/ 53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā tīmekļa vietnē: http://www.lantronix.com/products/ntc-201-series/ ES paziņojums par lietošanas ierobežojumiem: šo ierīci var izmantot tikai iekštelpās. To nedrīkst darbināt ārpus telpām.
lt	Lietuvių [Lithuanian]	Šiuo Lantronix, Inc. deklaruoja, kad šis NTC-201 device atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. Visą ES atitikties deklaracijos tekstą galite rasti šiuo interneto adresu: http://www.lantronix.com/products/ntc-201-series/ ES pranešimas apie naudojimo apribojimus: Šis prietaisas skirtas naudoti tik patalpose. Jo negalima naudoti lauke.
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix, Inc. dat het toestel NTC-201 device overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: http://www.lantronix.com/products/ntc-201-series/ EU kennisgeving van gebruiksbeperkingen: dit apparaat is beperkt tot gebruik binnenshuis. Het mag niet buitenshuis worden gebruikt.
mt	Malti [Maltese]	Hawnhekk, Lantronix, Inc., jiddikjara li dan NTC-201 device jikkonforma mal‧tiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU. It-test sħiħ tad-dikjarazzjoni ta ’konformità tal-UE huwa disponibbli flindirizz tal-internet li ġej: http://www.lantronix.com/products/ntc-201-series/ Avviż tal-UE dwar Restrizzjonijiet fuq l-Użu: Dan l-apparat huwa limitat għal użu ġewwa biss. Ma jistax jitħaddem barra.
hu	Magyar [Hungarian]	Alulírott, Lantronix, Inc. nyilatkozom, hogy a NTC-201 device megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. Az EU-megfelelőségi nyilatkozat teljes szövege a következő internetes címen érhető el: http://www.lantronix.com/products/ntc-201-series/ EU értesítés a korlátozásokról: Ez az eszköz csak beltéri használatra korlátozódik. Lehet, hogy szabadban nem üzemeltethető.
no	Norwegian	Lantronix, Inc. erklærer herved at denne NTC-201 device er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53 / EU.

Code	Language	Statement
		Den fullstendige teksten til EU-samsvarserklæringen er tilgjengelig på følgende internettadresse: http://www.lantronix.com/products/ntc-201-series/ EUs merknad om bruksbegrensninger: Denne enheten er bare begrenset til innendørs bruk. Det kan hende at den ikke brukesutendørs.
pl	Polski [Polish]	Niniejszym Lantronix, Inc. oświadcza, że NTC-201 device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. Pełny tekst deklaracji zgodności EU jest dostępny pod następującym adresem internetowym: http://www.lantronix.com/products/ntc-201-series/ Zawiadomienie UE o ograniczeniach użytkowania: To urządzenie jest przeznaczone wyłącznie do użytku w pomieszczeniach. Nie można go obsługiwać na zewnątrz.
pt	Português [Portuguese]	Lantronix, Inc. declara que este NTC-201 device está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. O texto completo da declaração UE de conformidade está disponível no seguinte endereço na Internet: http://www.lantronix.com/products/ntc-201-series/ Aviso da UE de restrições de uso: Este dispositivo está limitado apenas ao uso interno. Não pode ser operado ao ar livre.
ro	Romanian	Prin prezenta, Lantronix, Inc., declară că acest NTC-201 device respect cerințele esențiale și alte dispoziții relevante din Directiva 2014/53 / UE. Textul complet al declarației de conformitate a UE este disponibil la următoarea adresă de internet: http://www.lantronix.com/products/ntc-201-series/ Notificarea UE privind restricțiile de utilizare: Acest dispozitiv este limitat numai la uz interior. Este posibil să nu funcționeze în aer liber.
sr	Serbian	Овиме, Лантроник, Инц., изјављује да је овај NTC-201 device у складу са суштинским захтевима и осталим релевантним одредбама Директиве 2014/53 / ЕУ. Комплетан текст ЕУ изјаве о усаглашености доступан је на следећој Интернет адреси: http://www.lantronix.com/products/ntc-201-series/ Обавештење ЕУ о ограничењима употребе: Овај уређај је ограничен само на унутрашњу употребу. Можда се не користи на отвореном.
sl	Slovensko [Slovenian]	Lantronix, Inc. izjavlja, da je ta NTC-201 device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu: http://www.lantronix.com/products/ntc-201-series/ Obvestilo EU o omejitvah uporabe: Ta naprava je omejena samo na notranjo uporabo. Morda ga ne uporabljate na prostem.
sk	Slovensky [Slovak]	Lantronix, Inc. týmto vyhlasuje, že NTC-201 device enterprise Wi-Fi IoT module spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU. Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: http://www.lantronix.com/products/ntc-201-series/

Code	Language	Statement
		Oznámenie EÚ o obmedzeniach pri používaní: Toto zariadenie je obmedzené iba na použitie v interiéri. Nesmie sa používať vonku.
fi	Suomi [Finnish]	Lantronix, Inc. vakuuttaa täten että NTC-201 device tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavana seuraavassa Internet-osoitteessa: http://www.lantronix.com/products/ntc-201-series/ EU: n ilmoitus käyttörajoituksista: Tämä laite on rajoitettu vain sisäkäyttöön. Sitä ei saa käyttää ulkona.
sv	Svenska [Swedish]	Härmed intygar Lantronix, Inc. att denna NTC-201 device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: http://www.lantronix.com/products/ntc-201-series/ EU-meddelande om begränsningar för användning: Den här enheten är endast begränsad till inomhusbruk. Det får inte användas utomhus.

UK Declaration of Conformity

Figure A-2 UK Declaration of Conformity

LANTRONIX®

UK CA

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 US
Model Number: NTC-201
SW Version: 1.2.0.0

Manufacturer's Quality System:

TÜVRheinland

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

Applicable EU Directives:

Electrical Equipment Regulations 2016

- **EN IEC 62368-1:2023**
- **BS EN 50663:2017, BS EN 62479:2010**
- **BS EN 50665:2017, BS EN IEC 62311:2020**

Electromagnetic Compatibility Regulations 2016

- **EN 301 489-1 V2.2.3 (2019-11)**
- **EN 301 489-52 V1.3.1 (2024-11**
- **EN 55032:2015+A11:2020**
- **EN55035:2017+A11:2020**

Radio Equipment Regulations 2017

- **EN 301 908-1 V15.2.1**
- **EN 301 908-13 V13.2.1**

UK SI 2012 No. 3032 for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and 6(c).

1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU[7(c)-I] and 2018/741/EU[6(c)]
BS EN IEC 63000 2018

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

Signature: _____ Date: 11 December 2025

Name: Steve Burrington Title: Vice President R&D

CERT-00549 rev A

Appendix B. Default Settings

The following tables list the default settings for the NTC-201 router.

Table A- 2 LAN Management Default Settings

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

Default root and admin passwords are printed on the label on the bottom of the router.

Restoring factory default settings

Restoring factory defaults will reset the NTC-201 router to its factory default configuration. You may encounter situations where you need to restore the factory defaults on your NTC-201 router, such as:

- Login credentials are lost and you are unable to login to the web configuration page.
- A factory reset is requested by support staff for troubleshooting purposes.

There are two methods you can use to restore factory default settings on your NTC-201 router:

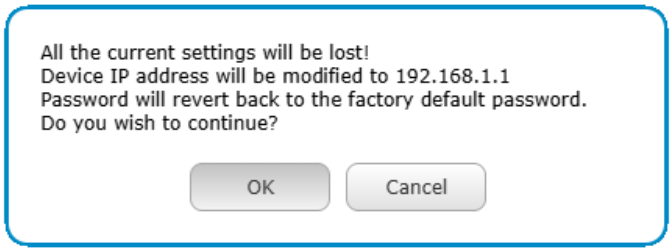
- Using the web-based user interface
- Using the reset button on the interface panel of the router (if the button is enabled)

Using the web-based user interface

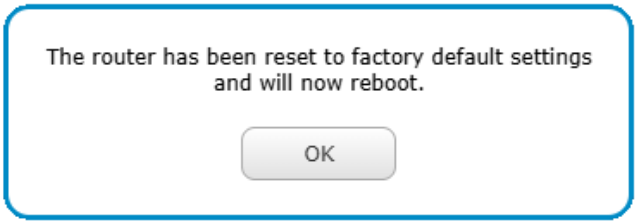
To restore your router to its factory default settings, please follow these steps:

1. Open a browser window and navigate to the IP address of the router (default address is https://192.168.1.1). Log into the router as root user.
2. Navigate to **System > System configuration > Settings backup and restore**.
3. In Restore factory defaults section, click **Restore defaults**, you are prompted to enter root password. Enter the root password and click **OK**.

4. You are prompted to confirm the reset. Click **OK** to continue.



5. Once the router is reset to factory default settings, click **OK** to reboot the router.



6. Once the router reboots, it enters configuration mode. Click **Next** to continue. See Initialization section to complete the initial configuration.

Using the reset button on the interface panel of the router

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

Appendix C. Recovery mode

The NTC-201 router features two independent operating systems, each with its own file system. These two systems are referred to as Main and Recovery. It is possible to use one to restore the other if one system becomes damaged or corrupted (such as during a firmware upgrade failure). The recovery console provides limited functionality and is typically used to restore the main firmware image in the case of a problem.

Accessing recovery mode

Both systems have web interfaces that can be used to manipulate the other inactive system. The NTC-201 router starts up by default in the Main system mode, however the router may be triggered to start in recovery mode if desired.

To start the router in recovery mode:

1. Press and hold the physical reset button on the interface panel of the router for 5 to 15 seconds. All LEDs turn green and start to extinguish in sequence. Then, the LEDs turn amber and start to extinguish in sequence. When the last amber LED extinguishes, release the reset button. The router then boots into recovery mode.
2. In your browser, navigate to **http://192.168.1.1**. The router's recovery mode is hardcoded to use this address regardless of the IP address that was configured in the main system. The router's recovery console displays.

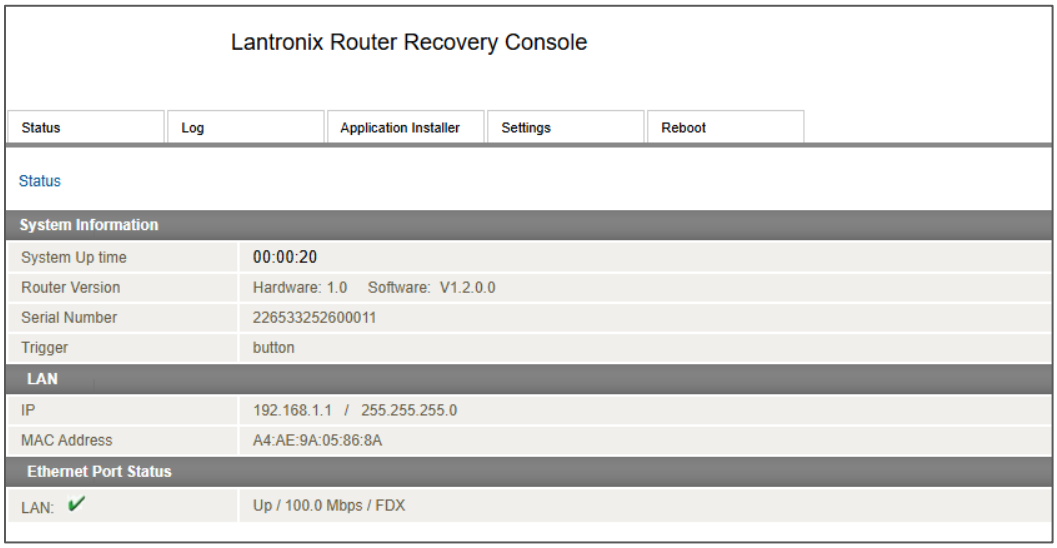


Figure C-1 Recovery console

Status

The status page provides System Information, LAN details, and the Ethernet Port Status as shown in image below. When you access the recovery mode, the Status page of Recovery Console displays.

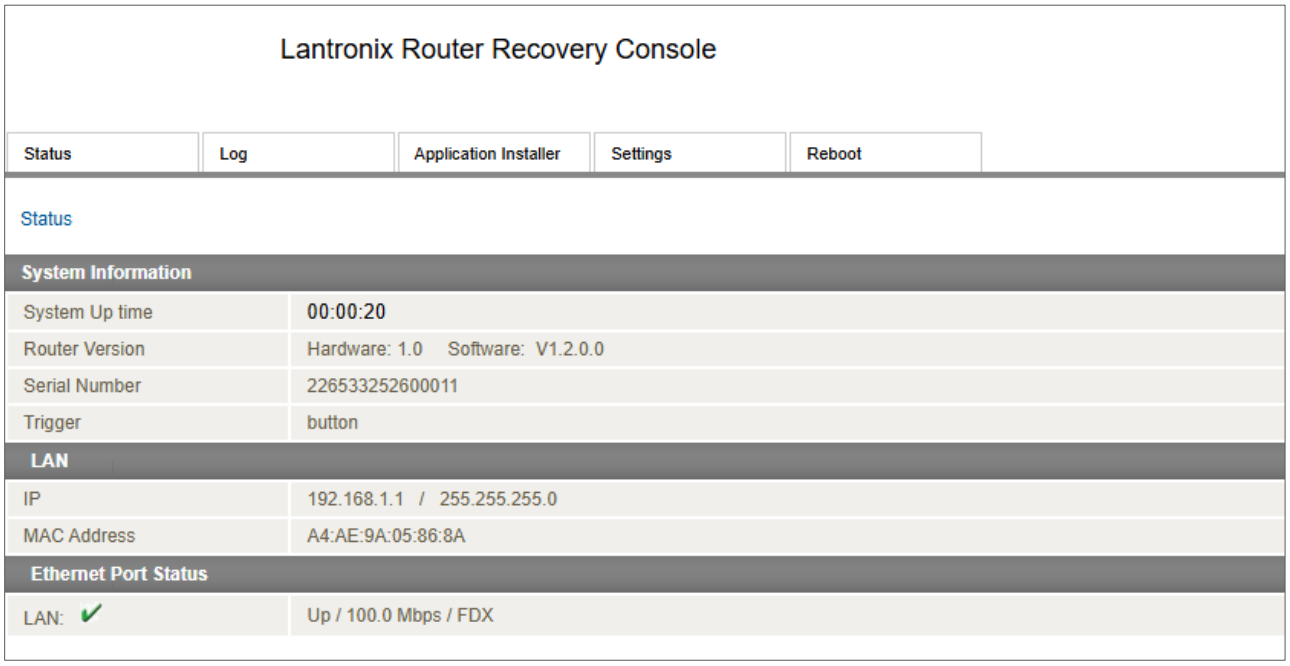
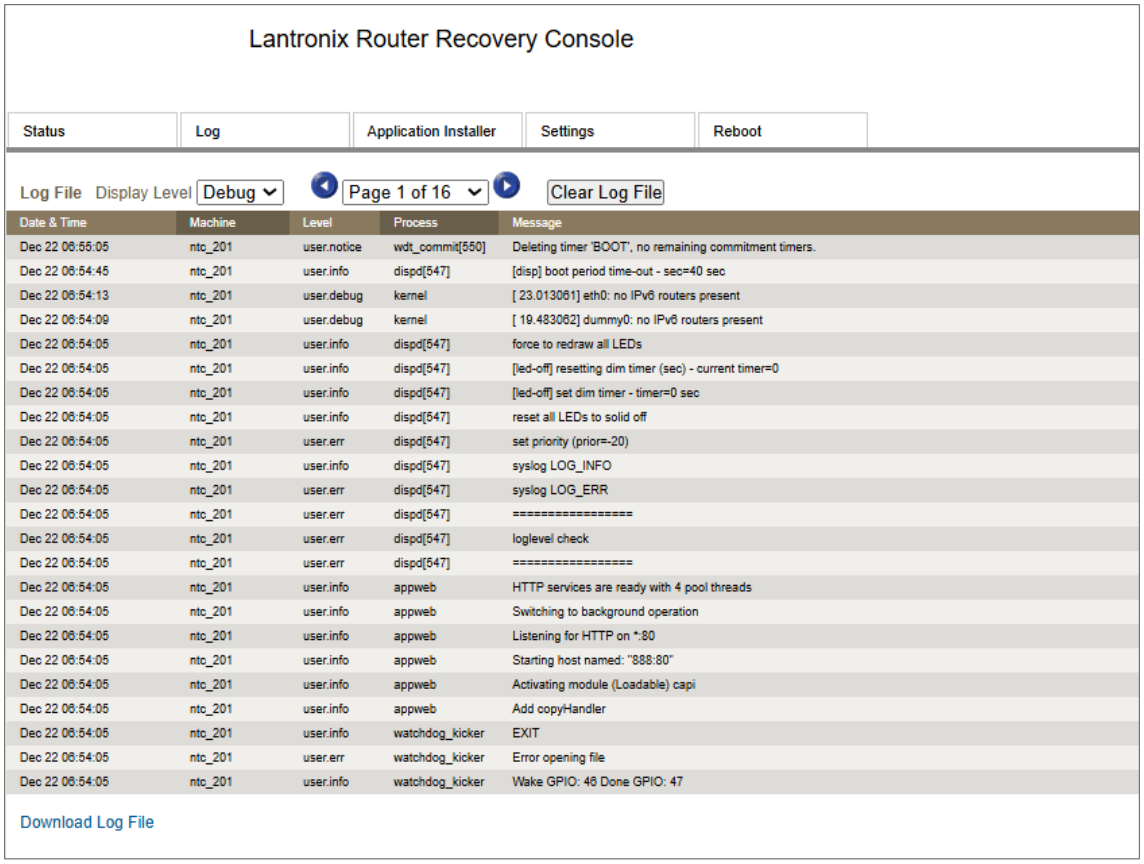


Figure C-2 Recovery mode – Status

Log

The log page displays the system log which is useful in troubleshooting problems which may have led to the router booting up in recovery mode. To access the Log page, click the Log tab in the top menu bar of the Recovery Console.



Date & Time	Machine	Level	Process	Message
Dec 22 06:55:05	ntc_201	user.notice	wdt_commit[550]	Deleting timer 'BOOT', no remaining commitment timers.
Dec 22 06:54:45	ntc_201	user.info	dispd[547]	[disp] boot period time-out - sec=40 sec
Dec 22 06:54:13	ntc_201	user.debug	kernel	[23.013061] eth0: no IPv6 routers present
Dec 22 06:54:09	ntc_201	user.debug	kernel	[19.483062] dummy0: no IPv6 routers present
Dec 22 06:54:05	ntc_201	user.info	dispd[547]	force to redraw all LEDs
Dec 22 06:54:05	ntc_201	user.info	dispd[547]	[led-off] resetting dim timer (sec) - current timer=0
Dec 22 06:54:05	ntc_201	user.info	dispd[547]	[led-off] set dim timer - timer=0 sec
Dec 22 06:54:05	ntc_201	user.info	dispd[547]	reset all LEDs to solid off
Dec 22 06:54:05	ntc_201	user.err	dispd[547]	set priority (prior=-20)
Dec 22 06:54:05	ntc_201	user.info	dispd[547]	syslog LOG_INFO
Dec 22 06:54:05	ntc_201	user.err	dispd[547]	syslog LOG_ERR
Dec 22 06:54:05	ntc_201	user.err	dispd[547]	================
Dec 22 06:54:05	ntc_201	user.err	dispd[547]	loglevel check
Dec 22 06:54:05	ntc_201	user.err	dispd[547]	================
Dec 22 06:54:05	ntc_201	user.info	appweb	HTTP services are ready with 4 pool threads
Dec 22 06:54:05	ntc_201	user.info	appweb	Switching to background operation
Dec 22 06:54:05	ntc_201	user.info	appweb	Listening for HTTP on *:80
Dec 22 06:54:05	ntc_201	user.info	appweb	Starting host named: "888:80"
Dec 22 06:54:05	ntc_201	user.info	appweb	Activating module (Loadable) capi
Dec 22 06:54:05	ntc_201	user.info	appweb	Add copyHandler
Dec 22 06:54:05	ntc_201	user.info	watchdog_kicker	EXIT
Dec 22 06:54:05	ntc_201	user.err	watchdog_kicker	Error opening file
Dec 22 06:54:05	ntc_201	user.info	watchdog_kicker	Wake GPIO: 46 Done GPIO: 47

Figure C-3 Recovery mode – Log

You can filter the log by setting the **Display Level** to any one of the following options:

- Debug
- Info
- Notice
- Error

Click **Clear Log File** to clear the log and **Download Log File** to download the log.

Application Installer

The Application Installer page allows you to perform the following functions:

- Upload and install main firmware images
- Upload and install recovery firmware images
- Upload and install custom applications and HTTPS certificates.

To access the Application Installer page, click the Application installer tab in the top menu bar of the recovery console.

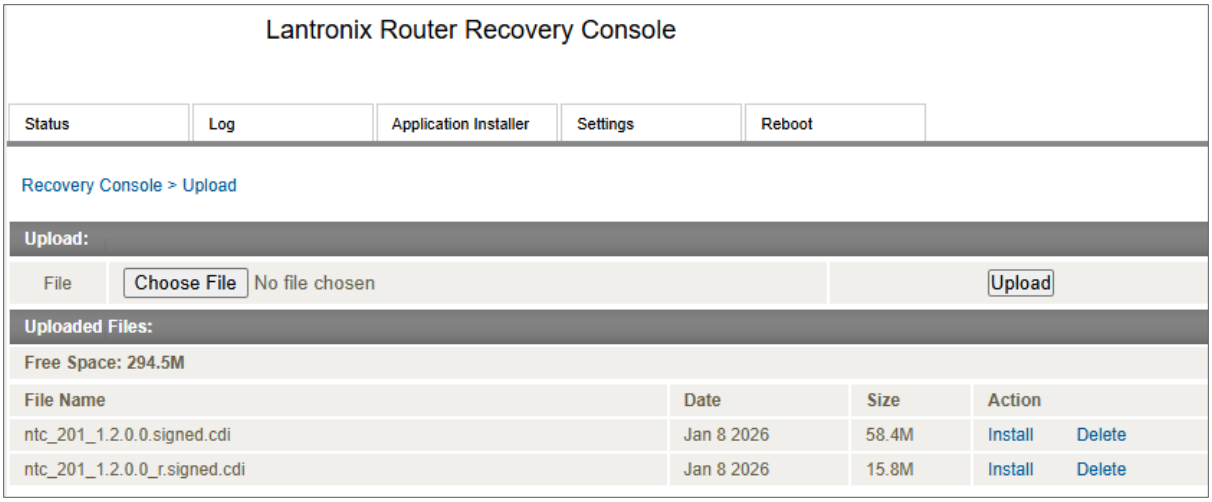


Figure C-4 Recovery mode – Application Installer

To upload and install a file:

1. Click **Choose File** to select the file to be uploaded to the router.
2. Click **Upload** to upload the file
3. Once the file is uploaded, it displays in the Uploaded Files list.
4. Click **Install** to install the file.

Click **Delete** to remove the file from the list.

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

Settings

The Settings page allows you to restore the router to factory default settings. To access the Settings page, click the **Settings** tab in the top menu bar of the Recovery Console. Click **Restore** to set the router to the original factory settings.

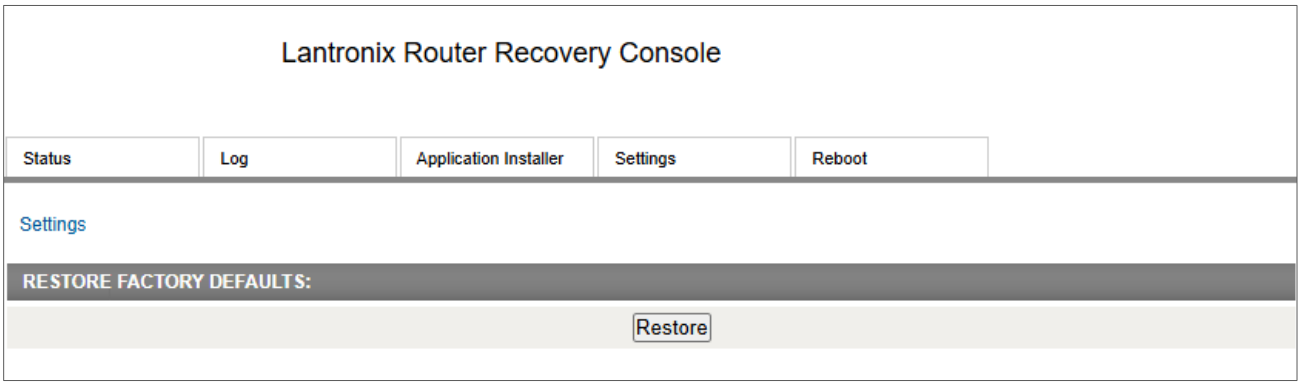


Figure C-5 Recovery mode – Settings

Reboot

The Reboot page allows you to reboot the router when you have finished using recovery mode. When rebooting the router from recovery mode, the router boots into the main firmware image unless there is some fault preventing it from doing so, in which case the recovery console will be loaded. To access the Reboot page, click the **Reboot** tab in the top menu bar of the Recovery Console.

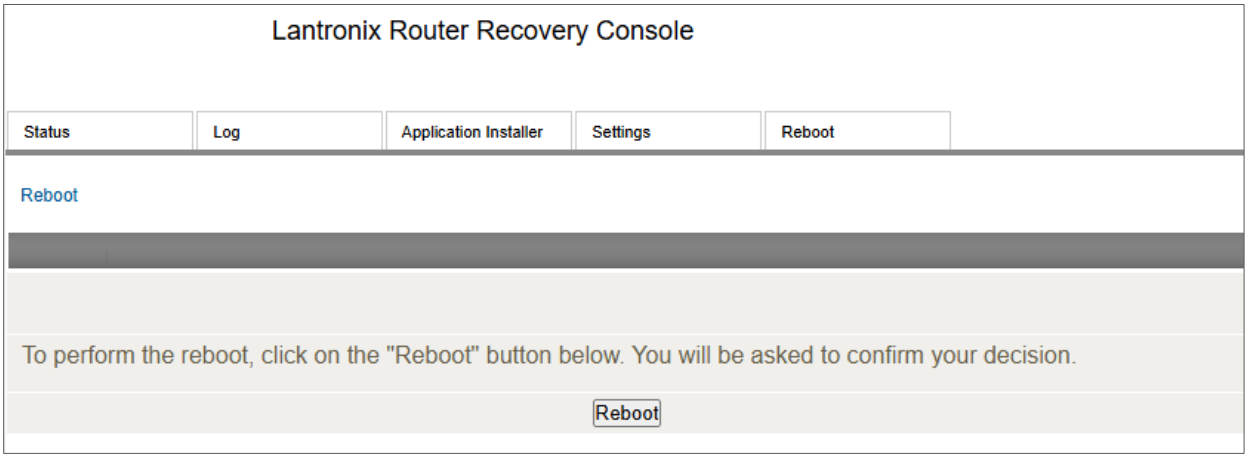


Figure C-6 Recovery mode – Reboot

Click the **Reboot** to reboot the router.

Appendix D. Obtaining a list of RDB variables

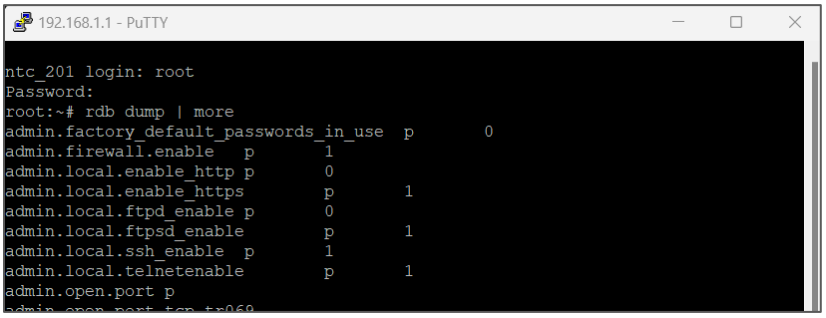
Important: *Modifying the RDB can cause your device to malfunction if you are not aware of the specific functions of each variable. Please take care whenever making changes to any RDB variable. These instructions are provided for your information only. Lantronix shall not be liable for any loss that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

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

1. Log into the web user interface of the router.
2. Navigate to **System > Administration > Administration settings**.
3. Set **Enable local Telnet** to **ON**.

4. In the **Telnet/SSH account** section, configure the password for the Telnet/SSH account if you had not configured it during the initial configuration of the router or you want to change the password.
5. Click the **Save** at the bottom of the screen.
6. Open a terminal client such as PuTTY and telnet to the router using its IP address.

7. At the login prompt, type root and press **Enter**.
8. At the password prompt, type the Telnet password and press **Enter.**
9. At the root prompt, enter the command **`rdb dump | more`**. The list of all the rdb variables is displayed.



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