Vodafone MachineLink 3G

User Guide

Vodafone
Power to you

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. NetComm Wireless and Vodafone accept no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Vodafone MachineLink 3G (NWL-10) to transmit or receive such data.

Safety and Hazards

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

Copyright

Copyright© 2017 NetComm Wireless Limited. All rights reserved.

Copyright© 2017 Vodafone Group Plc. All rights reserved.

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

Trademarks and registered trademarks are the property of NetComm Wireless Limited or Vodafone Group or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

Note – This document is subject to change without notice.

Save our environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with domestic waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Document History

This guide covers the following products:

Vodafone MachineLink 3G (NWL-10)

Ver.	Document Description	Date
v1.0	Initial document release	9 April 2013
v1.1	Cosmetic fixes	17 May 2013
v1.2	Aligned to firmware version 1.10.16.X. Added description of Data usage button and Ethernet port LED indicators	12 June 2013
v1.3	Aligned to firmware version 1.10.32.X. Added Vodafone GDSP roaming settings page, hostname description on LAN settings page and updated Administration settings screenshot and descriptions.	20 September 2013
v1.4	Updated “Setting timers for dial up and disconnection” and “Configuring a periodic reboot” descriptions	15 November 2013
v1.5	Updated LED signal strength table	28 February 2014
v1.6	Updated for Maintenance Release 2	10 November 2014
v2.0	Updated for Maintenance Release 3	16 February 2017
v2.1	Updated device weight	13 April 2017
v2.2	Corrected IPSec VPN with SCEP certificate description and an SCEP Client screenshot	26 June 2017

Table i. - Document Revision History

Note – Before performing the instructions in this guide, please ensure that you have the latest firmware version installed on your router.

Visit https://vodafone.netcommwireless.com to download the latest firmware.

Note – The functions described in this document require that the router is assigned with a publicly routable IP address.

Please ensure that your mobile carrier has provided you with a publicly routable IP address before performing the instructions in this document.

Table of contents

Overview **7**
- Introduction 7
- Target audience 7
- Prerequisites 7
- Notation 7

Product introduction **8**
- Product overview 8
- Package contents 8
- Product features 8

Physical dimensions and indicators **10**
- Physical dimensions 10
- LED indicators 11
- Ethernet port LED indicators 13
- Interfaces 15

Placement of the MachineLink 3G router **17**
- Mounting options 17

Installation and configuration of the Vodafone MachineLink 3G **24**
- Powering the router 24
- Power consumption 26
- Installing the router 26

Advanced configuration **28**
- Configuring a strong password 30

Status **31**

Networking **35**
- Wireless WAN 35
- LAN 62
- Routing 68
- VPN 83

Services **107**
- Dynamic DNS 107
- Network time (NTP) 109
- SNMP 111
- TR-069 115
- Event notification 117
- Email settings 123
- SMS messaging 125
- Network quality 147

System **148**
- Log 148
- Ping watchdog 154
- System configuration 157
- Administration 163

Appendix A: Tables 178

Appendix B: Device Mounting Dimensions 180

Appendix C: Mounting Bracket 181

Appendix D: Default Settings 182

Restoring factory default settings 183

Appendix E: Recovery mode 184

Accessing recovery mode 184

Status 185

Log 185

Application Installer 187

Settings 187

Reboot 188

Appendix F: HTTPS - Uploading a self-signed certificate 189

Appendix G: RJ-45 connector 192

Appendix H: Obtaining a list of RDB variables 193

Open Source Disclaimer 195

Safety and product care 195

Regulatory compliance 199

Overview

Introduction

This document provides you all the information you need to set up, configure and use the Vodafone MachineLink 3G (NWL-10) router.

Target audience

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

Prerequisites

Before continuing with the installation of your Vodafone MachineLink 3G (NWL-10) router, please confirm that you have the following:

- A device with a working Ethernet network adapter.
- A web browser such as Internet Explorer, Mozilla Firefox or Google Chrome.
- A working SIM card if your router was not shipped with one pre-inserted.
- A flathead screwdriver (No. 3) if field terminated power is required.

Notation

The following symbols are used in this user guide:

The following note requires attention.

The following note provides a warning.

The following note provides useful information.

Product introduction

Product overview

- HSPA+ up to 14.4Mbps downstream
- Penta-band 3G with quad-band 2G auto-fallback
- Internal diversity antennae with option for external main antenna (auto-sensing)
- Ethernet port with full passive Power over Ethernet (PoE) support (802.3af)
- Intelligent tri-colour LED display for clear, easy-to-read modem status information
- Integration with Vodafone GDSP back end
- Roaming algorithm with prioritisation for cost effective, flawless network connection across the globe
- Extensive device management with support for TR-069, web configuration and full feature management with SMS
- Optimised web configuration
- Flexible mounting suitable for in-home use or industrial applications with built-in wall mount, DIN and C-Rail mounting options

Package contents

The Vodafone MachineLink 3G package consists of:

- 1x Vodafone MachineLink 3G router
- 1x 1.5m yellow Ethernet cable 8P8C
- 1x DIN rail mounting bracket
- 1x quick start guide and safety manual

If any of these items are missing or damaged, please contact your Vodafone sales representative immediately.

Product features

The Vodafone MachineLink 3G is a feature-packed wireless M2M device designed by Vodafone to address the rapid growth in M2M deployments. The first M2M device of its kind, it is designed to deliver state of the art features, versatility and ease of use at an affordable price. Compatible with Vodafone networks worldwide, Vodafone MachineLink 3G is managed by Vodafone's global M2M platform enabling remote management and support wherever you are. The open management system also allows you to customise your own software applications for scalability, large scale compatibility and an easy path to large deployments across a broad range of industries.

The Vodafone MachineLink 3G meets the global demand for a reliable and cost-effective M2M device that successfully caters to mass deployment across businesses.

Physical dimensions and indicators

Physical dimensions

Below is a list of the physical dimensions of the Vodafone MachineLink 3G.

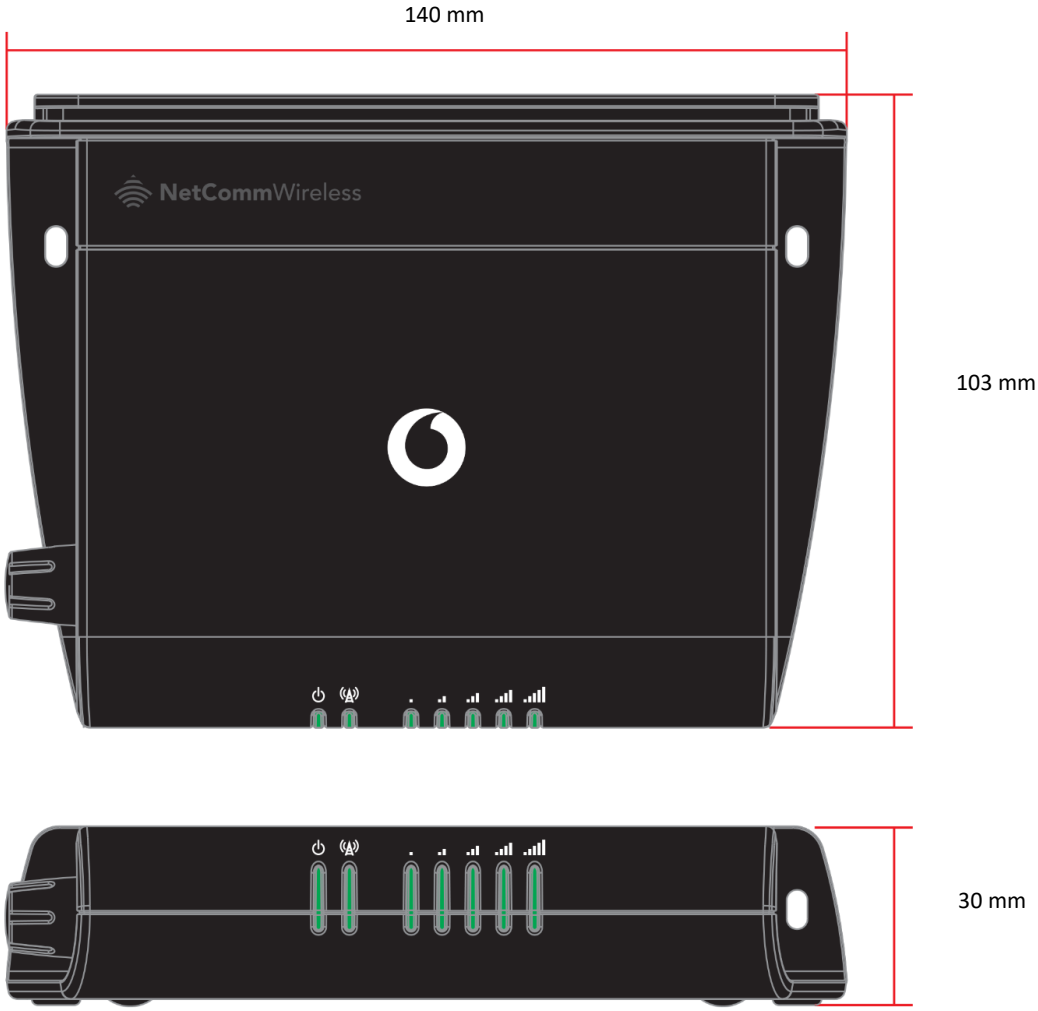


Figure 1 – Vodafone MachineLink 3G Dimensions

Vodafone MachineLink 3G (without external antenna attached)	
Length	140 mm
Depth	103 mm
Height	30 mm
Weight	187g

Table 1 - Device Dimensions

LED indicators

The Vodafone MachineLink 3G uses seven LEDs to display the current system and connection status.

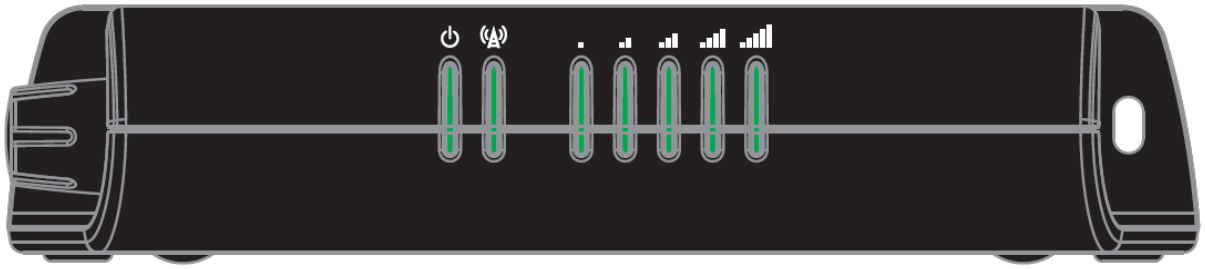


Figure 2 - Vodafone MachineLink 3G LED Indicators

LED Icon	Name	Colour	State	Description
	Power		Off	Power off
			Double flash	Powering up
			On	Power on
			On	Power on in recovery mode
			Slow flashing	Hardware error
	Network		On	Connected via WWAN
			Blinking[1]	Traffic via WWAN
			Slow flashing	Connecting PDP
			On	Registered network
			Slow flashing	Registering network
			Slow flashing	SIM PIN locked
			Fast flashing	SIM PUK locked
			On	Can't connect
	Signal strength		On	3G
			On	2G GPRS
			On	GSM only (no GPRS)

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

Table 2 - LED Indicators

Signal strength LEDs

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

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

Table 3 - Signal strength LED descriptions

LED update interval

The signal strength LEDs update within a few seconds with a rolling average signal strength reading. When selecting a location for the router or connecting 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 Vodafone MachineLink 3G router has two LED indicators on it.

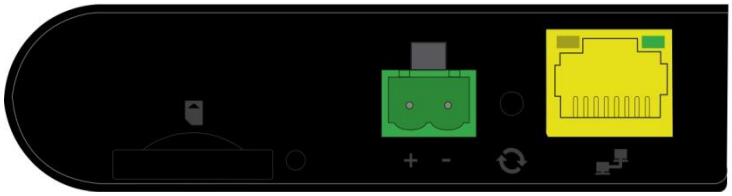


Figure 3 - Ethernet port LED indicators

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

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 10Mbps or no Ethernet cable is connected.

Table 4 - Ethernet port LED indicators description

Interfaces

The following interfaces are available on the Vodafone MachineLink 3G:

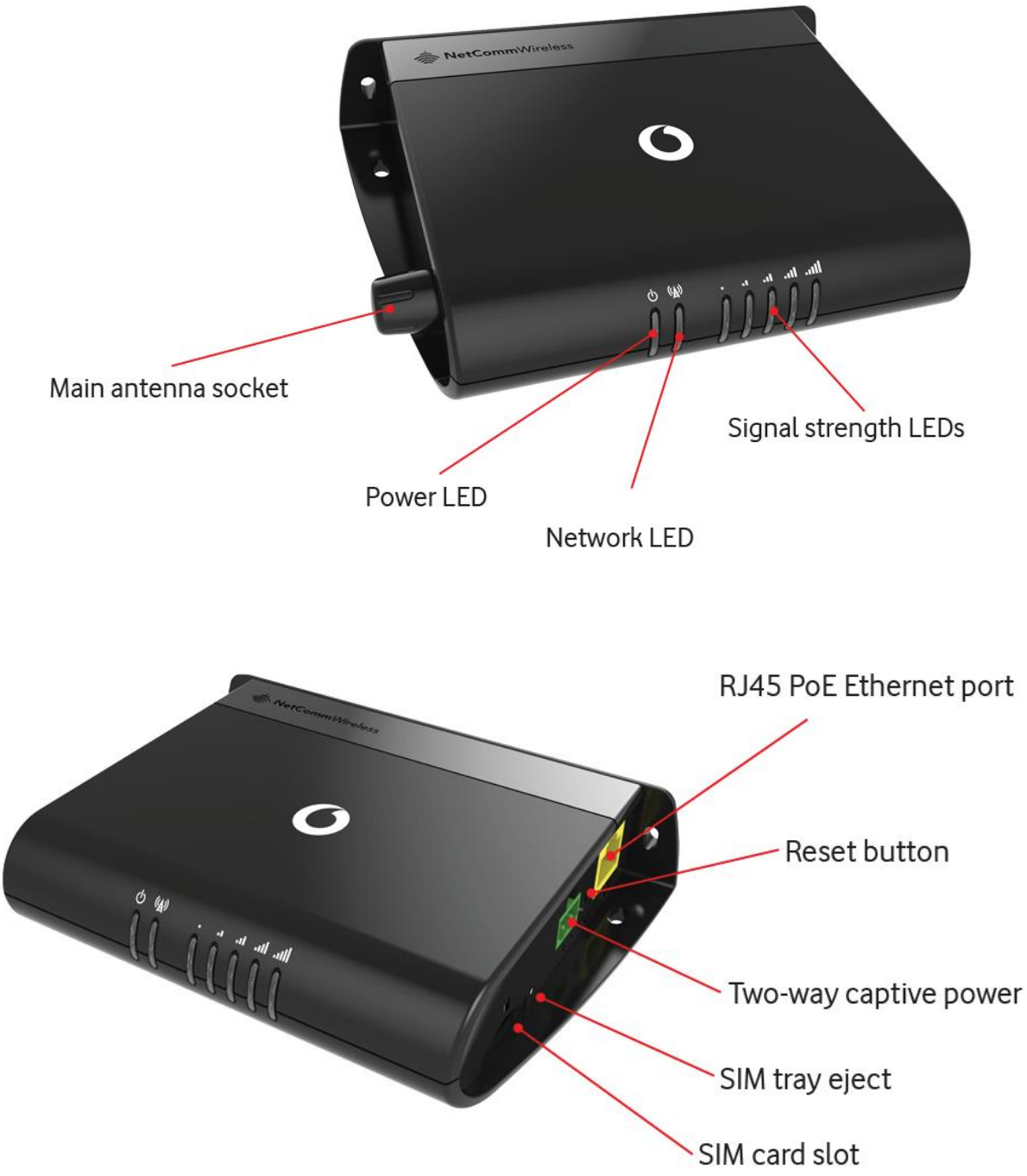


Figure 4 - Interfaces

Item	Description
External main antenna socket	SMA female connector for an optional external antenna (not supplied). The main internal antenna is disabled when an external antenna is connected but the auxiliary antenna remains active to provide (where possible) diversity assistance.
Power LED	Indicates the power status of the device and whether the device is in recovery mode.
Network LED	Indicates the network and SIM status.
Signal strength LEDs	Indicates the signal strength and network type.
RJ45 PoE Ethernet port	Connect one or several devices via a network switch here. This port can also optionally receive Power over Ethernet (802.3af PoE) in which case the DC power supply can serve as backup power source if required.
Reset button	Press and hold for less than 5 seconds to reboot to normal mode. The LEDs are green and extinguish in sequence to indicate that the router will reboot normally if the button is released during this period. Press and hold for 5 to 15 seconds to reboot to recovery mode. The LEDs are amber and extinguish in sequence to indicate that the router will reboot to recovery mode if the button is released during this period. Press and hold for 15 to 20 seconds to reset the router to factory default settings. The LEDs are red and extinguish in sequence to indicate that the router will reset to factory default settings if the button is released during this period.
Two-way captive power	Connect power source here. Power wires may be terminated on optional terminal block and connected to DC input jack. Operates in the 8-35V DC range.
SIM tray eject	Insert a pencil or paper clip here to eject the SIM card tray.
SIM card slot	Insert SIM card here.

Table 5 - Interfaces

Placement of the MachineLink 3G router

When selecting a location to mount the MachineLink 3G router, keep in mind that it houses two high performance internal antennas designed to provide optimum signal strength in a wide range of environments. If you find the signal strength is weak, try moving the router to a different place or mounting it differently. If signal strength doesn't improve, you may need to attach an external antenna (not included) to the router's female SMA connector.

Note: If you connect an external antenna to the female SMA connector, the main internal antenna disables automatically but the auxiliary internal antenna remains connected to provide (where possible) diversity assistance.

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 or connecting an external antenna.

Mounting options

The Vodafone MachineLink 3G router can be quickly and easily mounted in a variety of locations.

Mounted flat against the wall

When mounted flat against the wall, the MachineLink 3G router has a slimline form factor. Use appropriately sized screws in the mounting holes provided on the base of the unit.

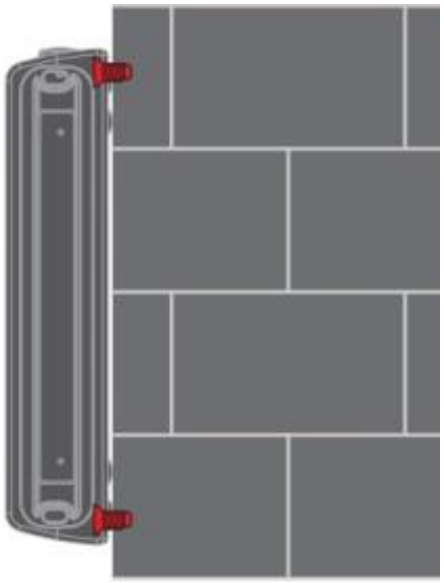


Figure 5 - Wall mount - Flat against the wall

Perpendicular to the wall

If a large surface area is not available, there is the option of mounting the router perpendicular to the wall. This gives the router a small wall footprint while remaining securely attached. Use appropriately sized screws in the mounting holes provided on the back of the unit.

Figure 6 - Wall mount - Perpendicular to the wall

C Section DIN Rail mount

The Vodafone MachineLink 3G router easily slides onto a C Section DIN rail so that it is horizontally mounted. The DIN Rail mounting bracket is not required for C Section DIN rail mounting.

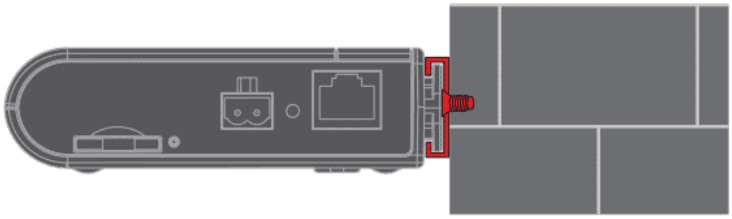


Figure 7 - C Section DIN rail mount

To mount the unit on a C-Section DIN rail, slide it on as illustrated below:

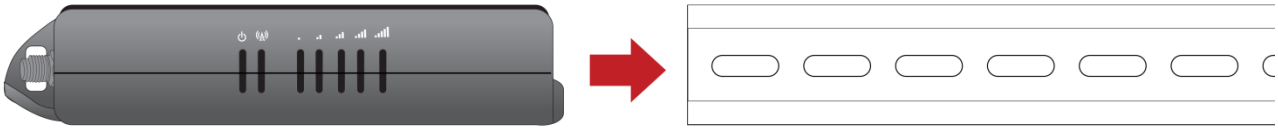


Figure 8 - Mounting the unit on a DIN rail

Mounting bracket

The provided mounting bracket provides additional methods of mounting the Vodafone MachineLink 3G Router.

To attach the mounting bracket, slide it onto the rear of the router as shown in the diagram below:

Figure 9 - Sliding on the mounting bracket

To remove the bracket, press the **PUSH** button and slide the router off the bracket:

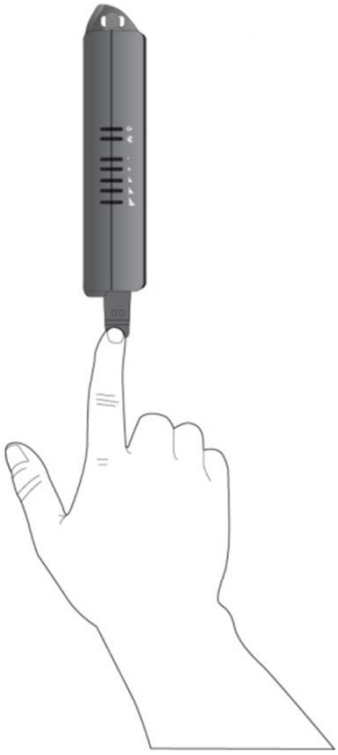


Figure 10 - Removing the mounting bracket

Using the mounting bracket for wall mounting

By first attaching the DIN rail bracket to the wall, the Vodafone MachineLink 3G can be easily attached and removed from the bracket.

Figure 11 – Wall mount - Mounted via DIN rail bracket

Using the mounting bracket for Top hat DIN rail mounting

The Vodafone MachineLink 3G Router may be vertically mounted to the wall with the bracket by sliding the bracket onto a top hat DIN rail.

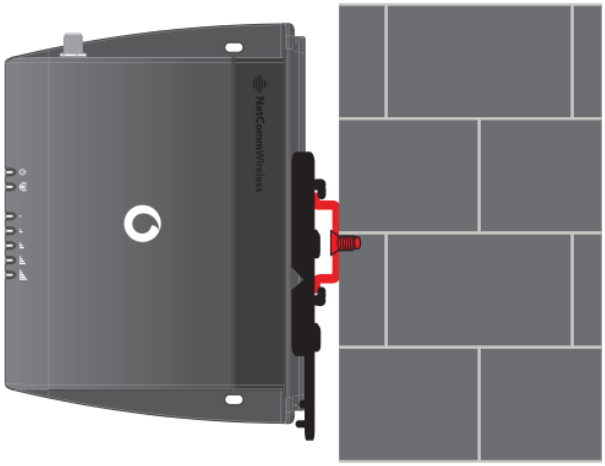


Figure 12 - Top hat DIN rail mount

Alternatively, you can attach it to the DIN Rail by using the V bend in the bracket as illustrated below:

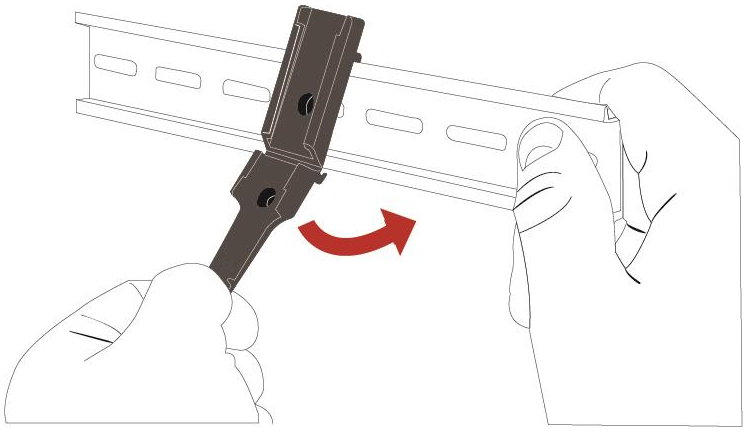


Figure 13 - Attaching the mounting bracket to the DIN rail using the V bend

Desk mount

In situations where wall mounts and DIN rails are not required, you can simply place the MachineLink 3G router on a desk using its rubber feet to prevent it from slipping.

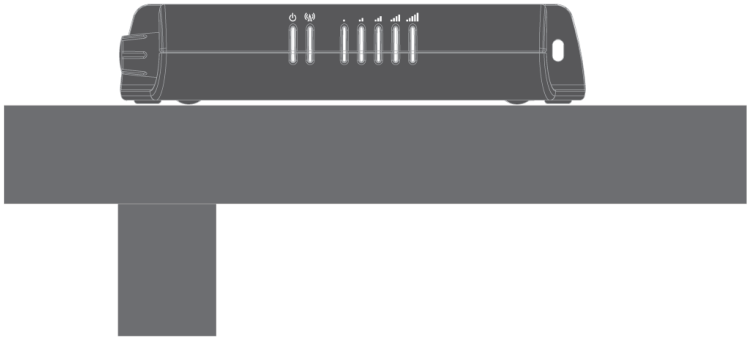


Figure 14 - Desk mount

Installation and configuration of the Vodafone MachineLink 3G

Powering the router

The MachineLink 3G Router can be powered in one of three ways:

1. Power over Ethernet (802.3af PoE)
2. DC power input via 2-pin connector (8-35V DC)
3. DC power input via field terminated power source (8-35V DC)

The green power LED on the router lights up when a power source is connected.

Power over Ethernet (802.3af PoE)

Power over Ethernet (PoE) is a method of connecting network devices through Ethernet cable where power and data are passed along a single cable. This may be a desirable method of powering the device if PoE is available, or if it's most convenient in the desired installation environment to only have a single cable running to the MachineLink 3G device.

There are 5 power classes defined in the IEEE 802.3-2005 standard, of which the Vodafone MachineLink 3G is a class 3 device.

Class	Classification current	Power range	Class description
3	26-30 mA	6.49 – 12.95 W	Mid power

Table 6 - PoE power classes

To use PoE to power the MachineLink 3G, simply connect your router to a PoE injector or PoE network switch using the bundled yellow Ethernet cable 8P8C.

DC power via 2-pin connector

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

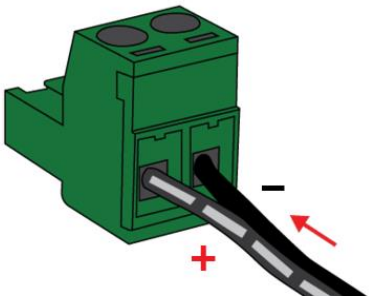


Figure 15 - Terminal block wiring diagram

DC power via field terminated power source

If an existing 8-35V DC power supply is available, you can insert the wires into the supplied terminal block to power your router. Use a No. 3 flathead screwdriver to tighten the terminal block screws and secure the power wires, making sure the polarity of the wires are correctly matched, as illustrated below.

Figure 16 - Locking Power Terminal Block

Pin	Signal	Description
+	V+	Voltage +
-	V-	Ground

Table 7 - Locking power block pin outs

Failover power support

The MachineLink 3G Router includes support for connection of two power sources at the same time. When a PoE Ethernet cable is connected and DC power is also supplied to the DC input jack of the router, the router will source power exclusively from the PoE source. In the event that power from the PoE cable is lost, the router will automatically switch to source power from the DC input jack, without affecting the router's operation. When PoE power is restored, the router automatically switches back to receive power from the PoE input source.

Viewing power source information

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

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

Power consumption

To assist with power consumption planning, the following table summarises average power consumption during the various states of the MachineLink 3G under normal usage conditions. It's important to note that this table serves as an indication only as the power consumed by the device is affected by many variables including signal strength, network type, and network activity.

Average power consumption figures

State	Power consumption
Powered on, idle and connected to packet data	1.2W
Powered on, connected to packet data with average load	2.0W
Powered on, connected to packet data with heavy traffic	4.0W
Peak power draw at maximum 3G module transmission power	5.0W

Table 8 - Average power consumption figures

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 MachineLink 3G. You can connect one device directly, or several devices using a network switch. If you're using PoE as the power source, you need to connect any devices via an available data Ethernet port on your PoE power source (be it a PoE network switch or PoE power injector).
2. If your router does not come with a SIM pre-installed, insert a SIM card into the SIM card slot by pressing the SIM Eject button to eject the SIM card tray. Place the SIM card in the tray and then insert the loaded tray into the SIM slot with the gold side facing up, as shown below.

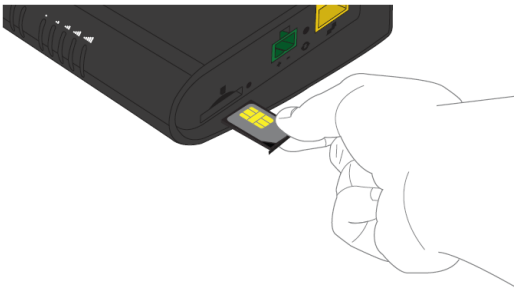


Figure 17 – Inserting the SIM card

3 Ensure the external power source is switched on and wait 2 minutes for your Vodafone MachineLink 3G to start up and connect to the mobile network. Your router arrives with preconfigured settings that should suit most customers. Your router is now connected. To check the status of your router, compare the LED indicators on the device with those listed in the LED indicators table.

Advanced configuration

The Vodafone MachineLink 3G Router comes with preconfigured settings that should suit most customers. For advanced configuration, login to the web-based user interface of the router.

To log in to the web-based user interface:

1 Open a web browser (e.g. Internet Explorer, Firefox, Safari), type https://192.168.1.1 into the address bar and press Enter. The web-based user interface login screen is displayed.

Note – The HTTP protocol is disabled by default, secure HTTP (HTTPS) is the default protocol.

HTTP access is available, but must be manually enabled.

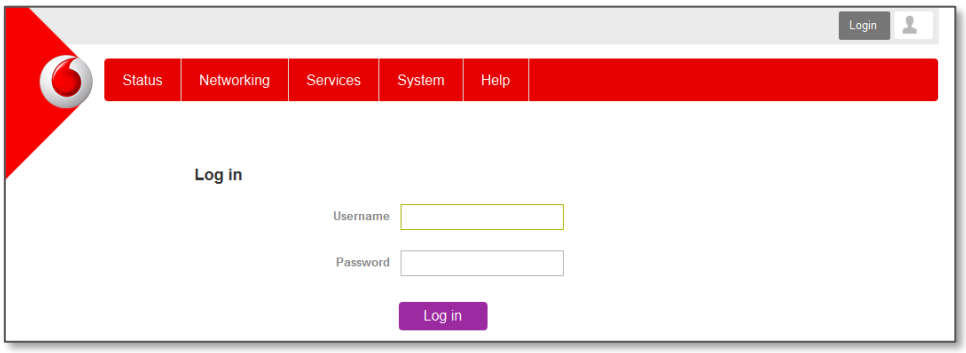


Figure 18 – Log in prompt for the web-based user interface

2 Enter the login username and password. If this is the first time you are logging in or you have not previously configured the password for the "root" or "user" accounts, you can use one of the default account details to log in.

Root manager account	
Username	root
Password	admin

Table 9 - Management account login details – Root manager account

User account	
Username	user
Password	admin

Table 10 - Management account login details –User account

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

For security reasons, we highly recommend that you change the passwords for the root and user accounts upon initial installation. You can do so by navigating to the **System** and then **Administration** page.

Whenever the root account logs in with the default password, the **Administration** page is displayed.

If the router is configured with the default password, each time that you log in to the web user interface, you are re-directed to the Administration settings page to set a secure password for the root account.

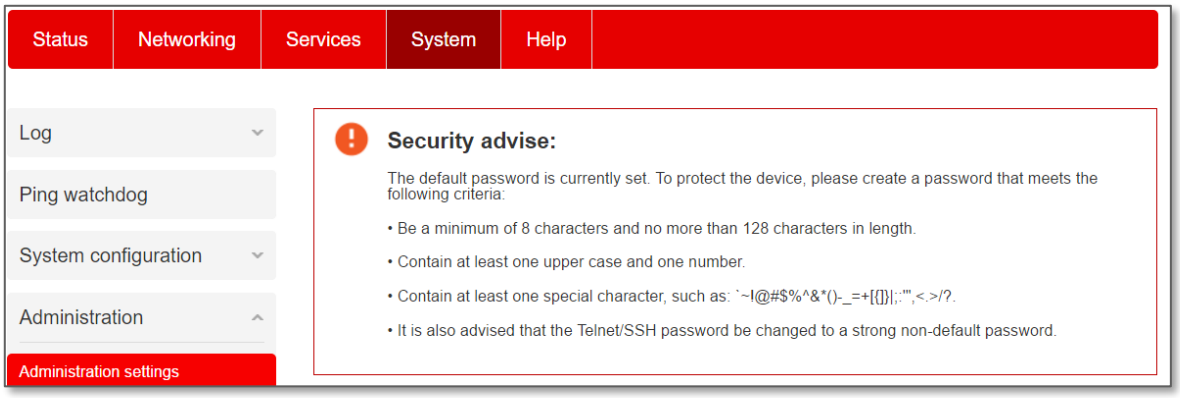


Figure 19 – Security advise at log in.

It is mandatory that a strong password be configured to use certain features of the router, such as Administration settings, IPSec VPN Pre-shared key and SMS Diagnostics. In any case, we highly recommend that you change the default password as soon as possible. After changing the default password, the **Status** page is displayed when you log in. See the next section for notes on setting a strong password.

Configuring a strong password

The root manager account, IPSec VPN Pre-shared key and SMS white list passwords must now meet the following criteria:

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

The password requirements for the SMS Diagnostics feature differ slightly due to the smaller supported character set. Refer to the White list for diagnostic or execution SMS section for more information.

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

Status

The status page of the web interface provides system related information and is displayed when you log in to the Vodafone MachineLink 3G management console. The status page shows System information, LAN details, Cellular connection status, Packet data connection status and Advanced status details. You can toggle the sections from view by clicking the or buttons to show or hide them.

Extra status boxes will appear as additional software features are enabled (e.g. VPN connectivity)

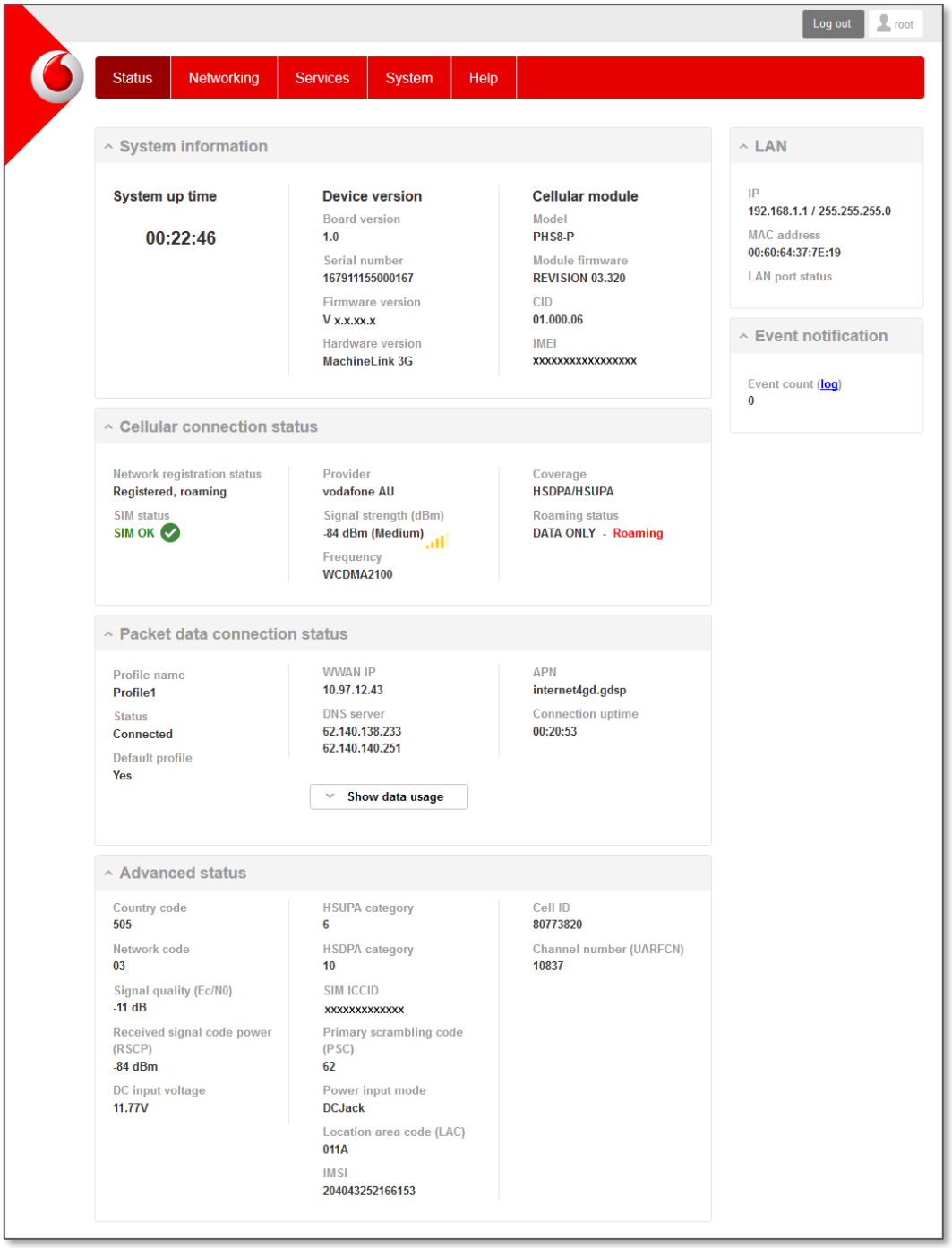


Figure 20 – NWL-10 Status page

Item	Definition
System information	
System up time	The current uptime of the router.
Board version	The hardware version of the router.
Serial Number	The serial number of the router.
Firmware version	The firmware version of the router
Model	The type of phone module and the firmware version of the module.
Module firmware	The firmware revision of the phone module.
CID	Cellular configuration ID.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
LAN	
IP	The IP address and subnet mask of the router.
MAC Address	The MAC address of the router.
Ethernet Port Status	Displays the current status of the Ethernet port and its operating speed.
Event notification	
Notification count	Displays the number of event notifications that have been triggered.
Cellular connection status	
SIM status	Displays the activation status of the router on the carrier network.
Signal strength (dBm)	The current signal strength measured in dBm
Network registration status	The status of the router's registration for the current network.
Provider	The current operator network in use.
Roaming status	The roaming status of the router.
Frequency	The current band being used by the router.
Coverage	The type of mobile coverage being received by the router.
Transparent bridge mode (If Transparent bridge is enabled)	
Status	The status of the bridged connection mode.
IP	The IP address and subnet mask of the bridged connection.
APN name	The Access Point Name you have selected for the bridged connection.
Service name	The optional service name you have chosen for the bridged connection.
Packet data connection status	
Profile name	The name of the active profile.
Status	The connection status of the active profile.
Default profile	Indicates whether the current profile in use is the default profile.
WWAN IP	The IP address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary DNS servers for the WWAN connection.
APN	The Access Point Name currently in use.
Connection uptime	The length of time of the current mobile connection session.
Advanced status	

Item	Definition
Mobile country code	The Mobile Country Code (MCC) of the network provider.
Mobile network code	The Mobile Network Code (MNC) of the network provider.
Signal quality (Ec/N0)	A measurement of the portion of the received signal that is usable. This is the signal strength minus the signal noise level.
Received signal code power (RSCP)	The power level of the signal on the current connection's particular channel.
Power input mode	Displays whether power is currently being sourced from the PoE Ethernet port or from the DC input jack.
HSUPA category	Displays the HSUPA category (1-6) for the current uplink
HSDPA category	Displays the HSDPA category (1-12) for the current downlink.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the router, a unique number up to 19 digits in length.
Primary scrambling code (PSC)	The Primary scrambling code for the current signal.
DC input voltage	Displays the current voltage of the power input source provided via the DC Input jack
Location area code (LAC)	The ID of the cell tower grouping the current signal is broadcasting from.
IMSI	The International Mobile Subscriber Identity is a unique identifier of the user of a cellular network.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile network signal.
Channel number (UARFCN)	The channel number of the current 3G/2G connection.

Table 11 - Status page item details

Networking

The Networking section provides configuration options for Wireless WAN, LAN, Routing and VPN connectivity.

Wireless WAN

Data connection

The data connection has two modes of operation:

Transparent bridge (PPPoE) ON

In this mode, the router does not manage the status of the connection to the packet data network. The status of the connection is instead managed by a client device connected behind the router via a PPPoE session. Certain functions of the router are unavailable when running in transparent bridge mode such as Connect on demand, Routing, VPN, TR-069, Router firewall and Remote access. As the responsibility of maintaining the connection is passed to a client machine, only that device will have network access.

Transparent bridge (PPPoE) OFF

This is the default mode of operation. When transparent bridging is turned off, the router manages the status of the connection allowing Connect on demand, Routing, VPN, TR-069, Router firewall and Remote access.

The data connection page allows you to configure and enable/disable up to six connection profiles or to alternatively bridge the data connection via a PPPoE session.

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

When the transparent bridge function is off, you can configure the connection profiles by clicking the **Edit** button to the right of each row.

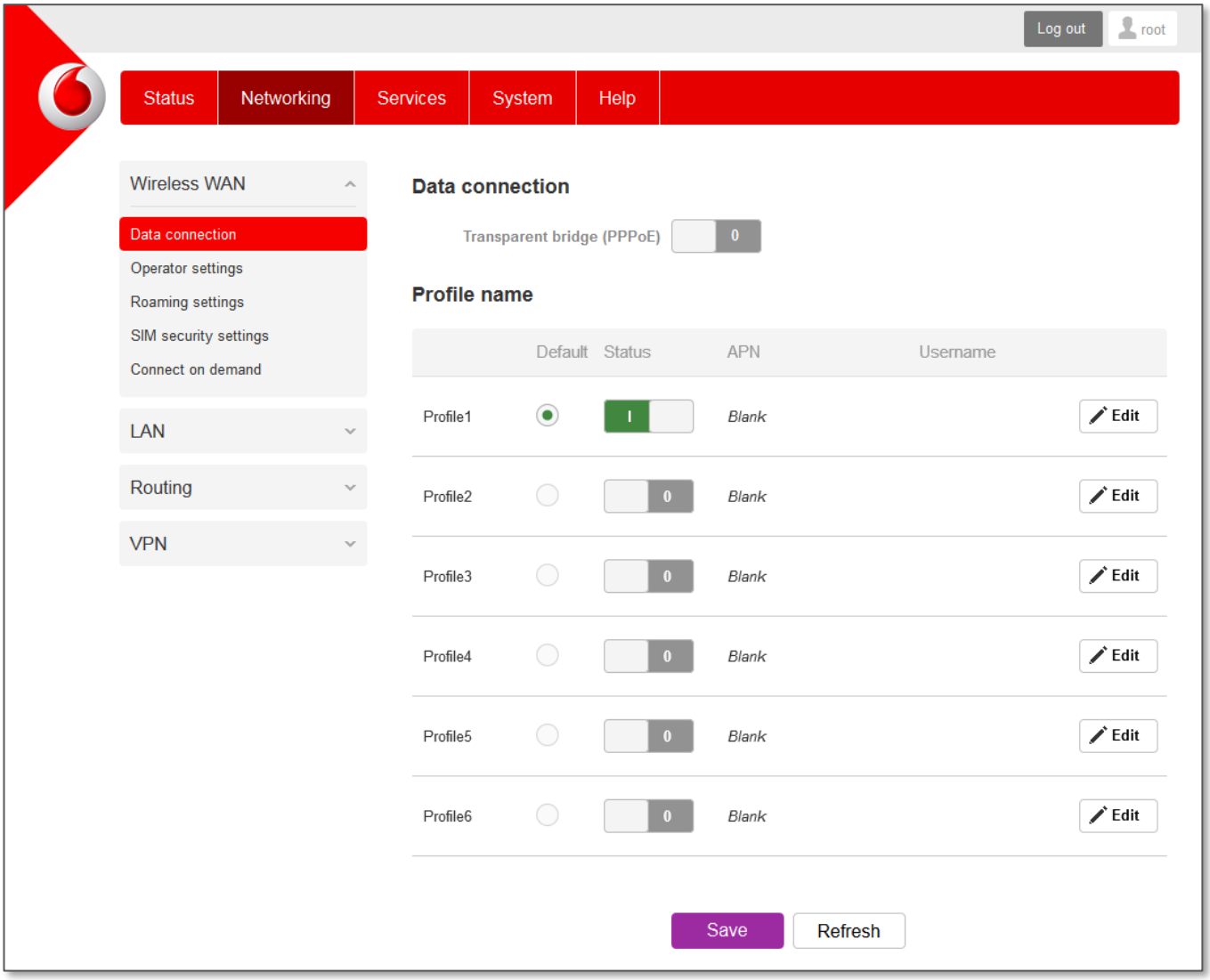


Figure 21 – Data connection settings (Transparent bridge off)

Item	Definition
Data connection	
Transparent Bridge (PPPoE)	Toggles the transparent bridge function on and off.
Profile name list	
Default	Sets the corresponding profile to be the default gateway for all outbound traffic except traffic for which there are configured static route rules or profile routing settings.
Status	Toggles the corresponding profile on and off. If your carrier supports it, two profiles may be turned on simultaneously.
APN	The APN configured for the corresponding profile.
Username	The username used to log on to the corresponding APN.

Table 12 - Data connection item details

Connecting to the mobile broadband network

The router supports the configuration of up to six APN profiles; these profiles allow you to configure the settings that the router will use to connect to the 2G/3G network and switch easily between different connection settings.

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

Using a Vodafone Global SIM

When using a Vodafone Global SIM, the router is pre-configured with the APN field blank. A blank APN setting allows the network to determine the correct APN.

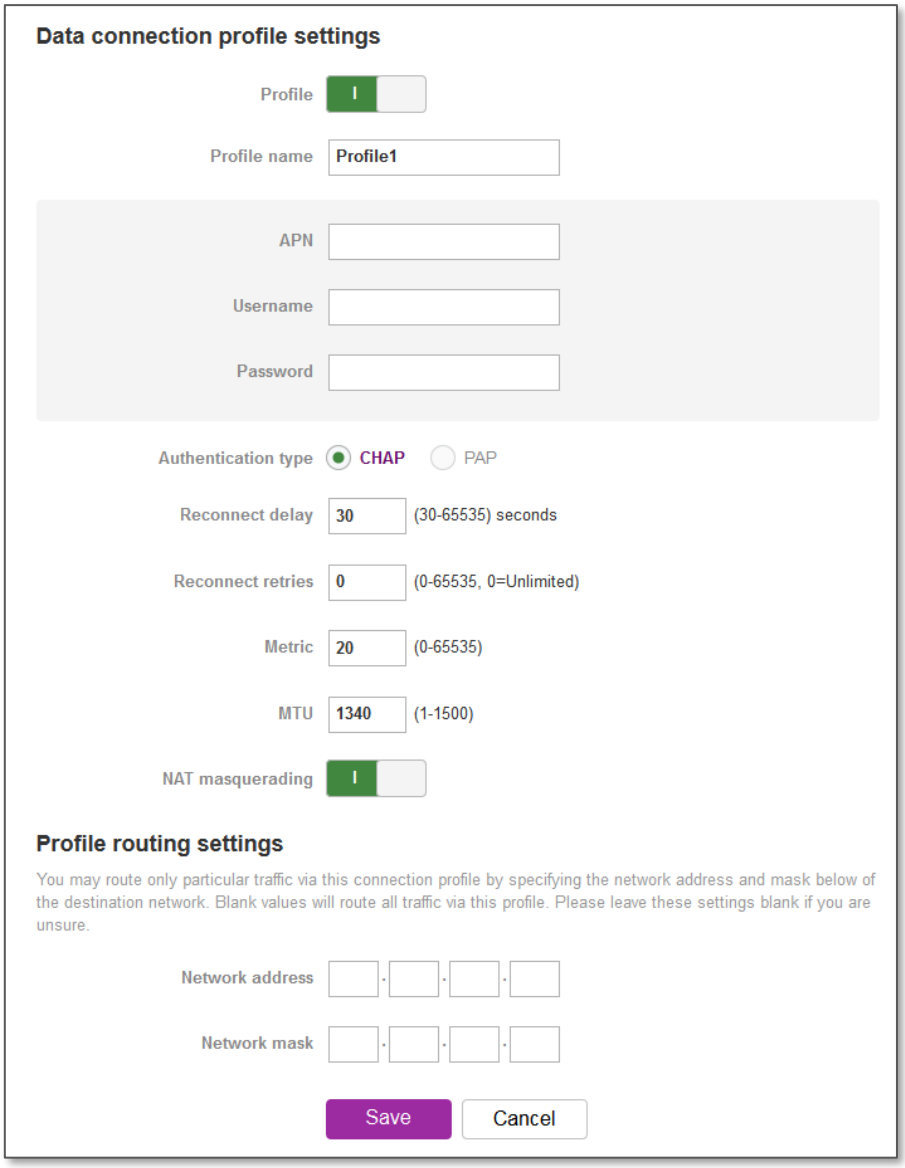


Figure 22 - Data connection profile settings - Vodafone Global SIM

Using a non-Vodafone Global SIM

When using a non-Vodafone Global SIM, the MachineLink 3G Router gives you the option of turning Automatic APN selection on or off. By default, Profile 1 is configured with Profile1 and Automatic APN set to ON.

When Automatic APN selection is turned on, the router selects an appropriate APN from an internal database of known APNs. If the SIM you have inserted into the router is not of a known carrier, you may need to manually enter an APN to obtain a network connection. See manually configuring a connection profile for details on entering an APN manually.

To see the automatically selected APN, view the Status page.

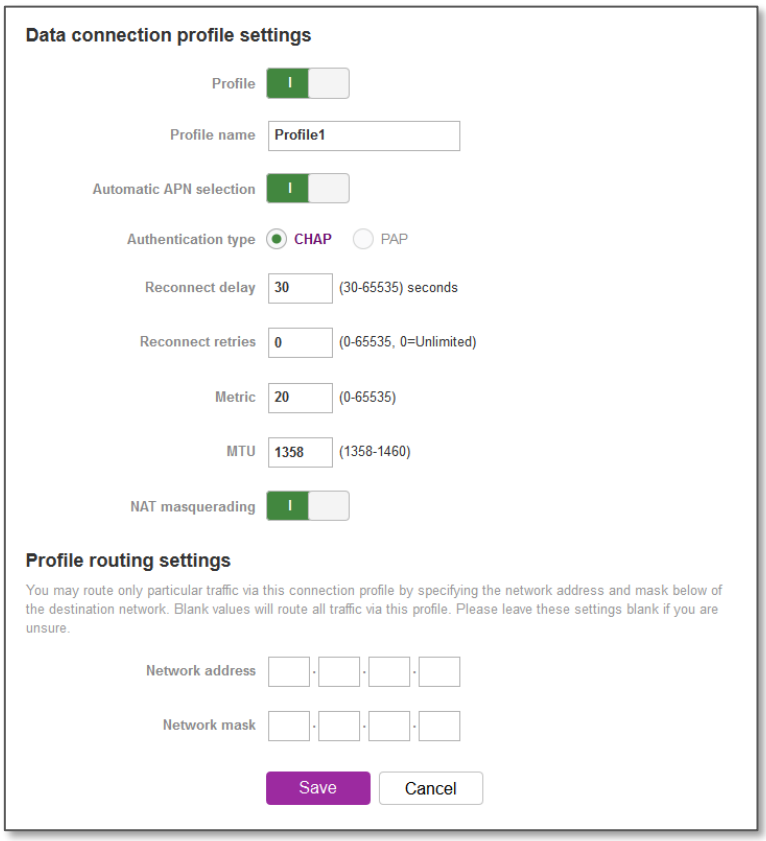


Figure 23 - Data connection profile settings –Non-Vodafone Global SIM - Automatic APN settings

Manually configuring a connection profile

To manually configure a connection profile:

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

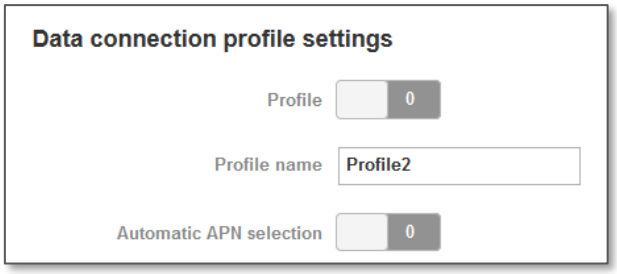


Figure 24 - Data connection profile settings

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

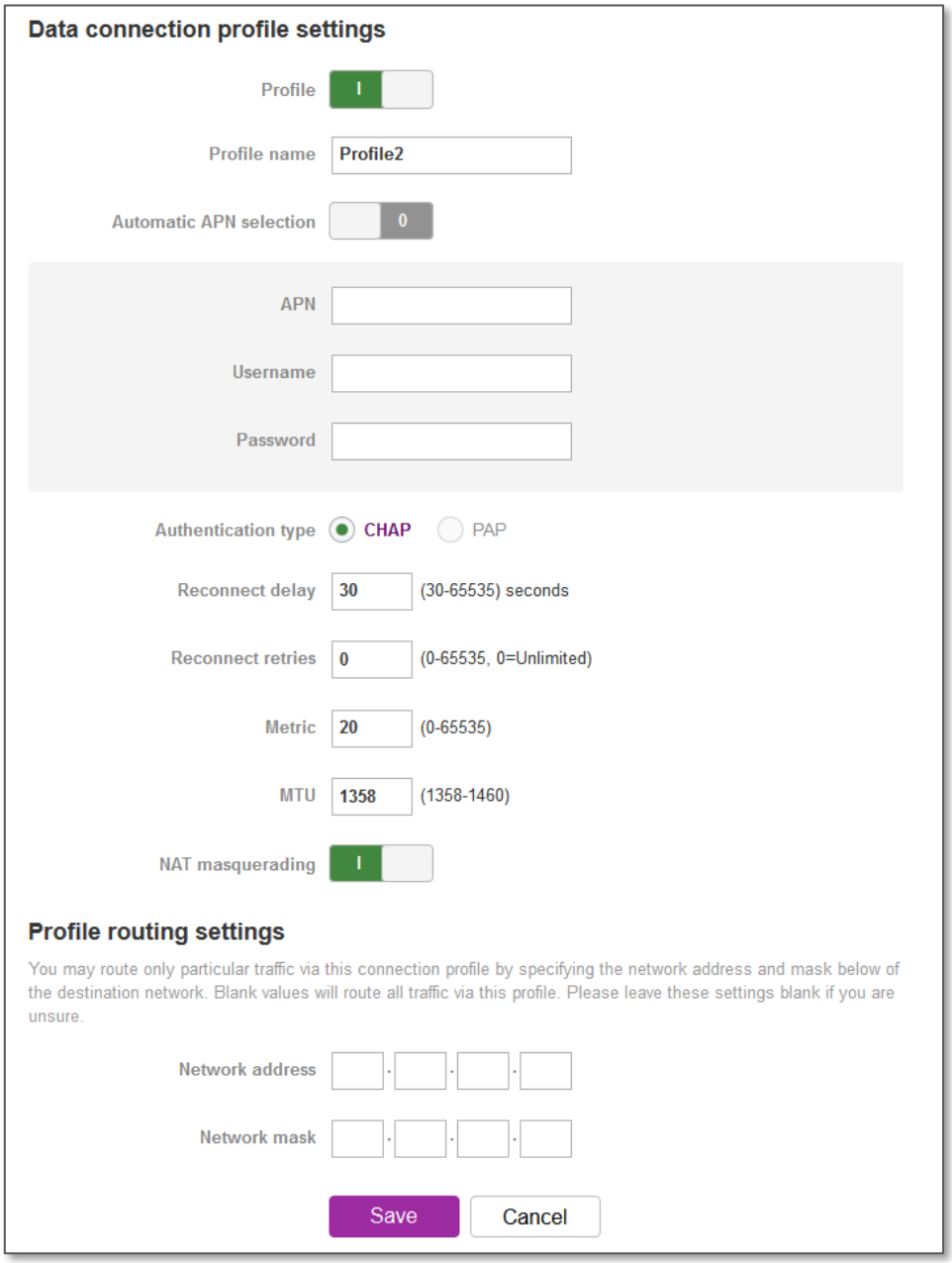


Figure 25 - Data connection settings - Profile turned on

Note: The Automatic APN toggle key is not available when using a Vodafone Global SIM.

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

4 When using a SIM other than a Vodafone Global SIM, ensure that the **Automatic APN selection** toggle key is set to off. If it is not, click it to toggle it to the off position.

5 In the **APN** field, enter the APN Name (Access Point Name) and if required, use the **Username** and **Password** fields to enter your login credentials (if required).

6 Next to **Authentication** type, select the either CHAP or PAP depending on the type of authentication used by your provider.

7 The **Reconnect delay** field specifies the number of seconds to wait between connection attempts. The default setting of 30 seconds is sufficient in most cases but you may modify it to wait up to 65535 seconds if you wish.

8 The **Reconnect retries** field specifies the number of times to attempt to connect to the network if the router fails to establish a connection. It is set to 0 by default which causes the router to attempt to reconnect indefinitely.

9 The **Metric** value is used by router to prioritise routes (if multiple are available) and is set to 20 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.

10 Use the **NAT masquerading** toggle key to turn NAT Masquerading on or off. NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses.

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

12 Click the **Save** button when you have finished entering the profile details.

Confirming a successful connection

After configuring a packet data session, and ensuring that one is enabled, click on the Status menu item at the top of the page to return to the Status page.

When there is a mobile broadband connection, the **Packet data connection status** section is expanded showing the details of the connection. To see details on each connected session, you can click **Show data usage** button.

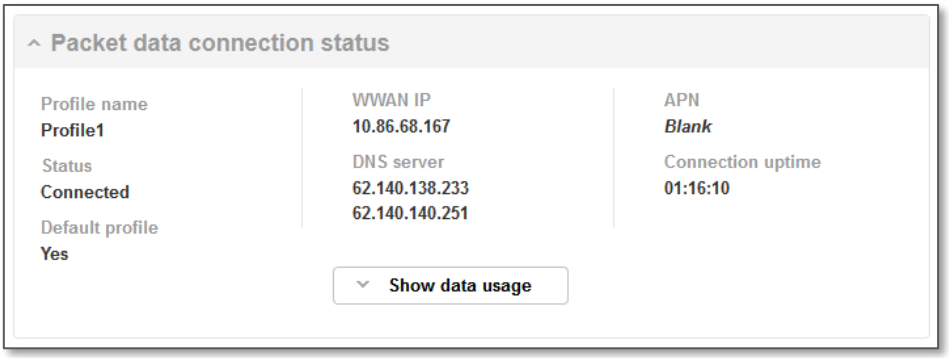


Figure 26 - Packet data connection status section

Checking data usage

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

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

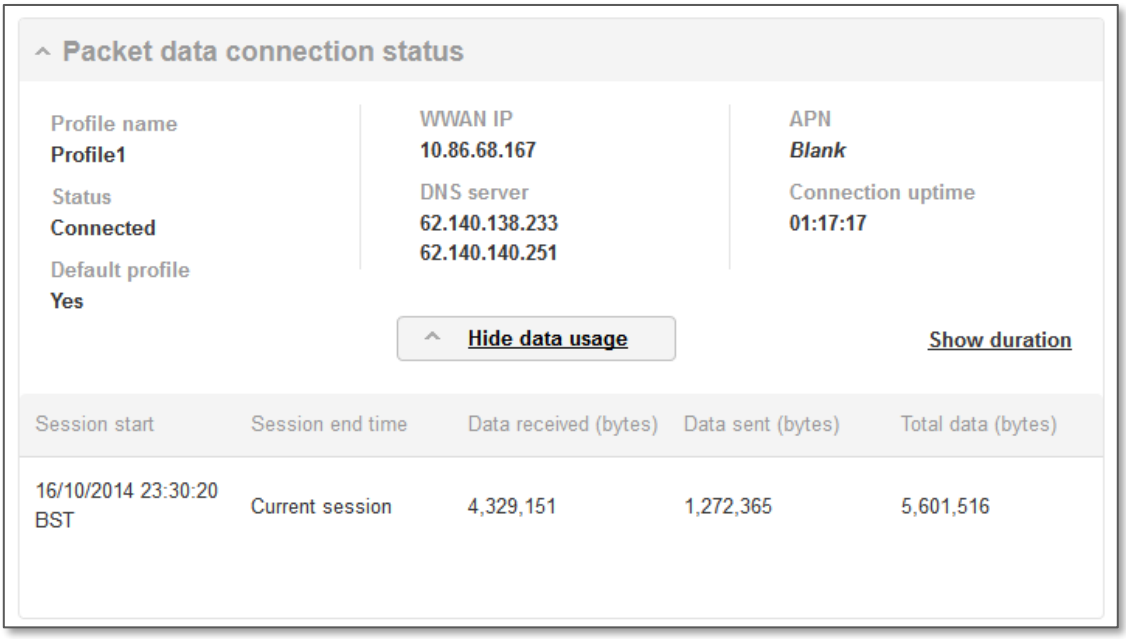


Figure 27 - Data usage

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

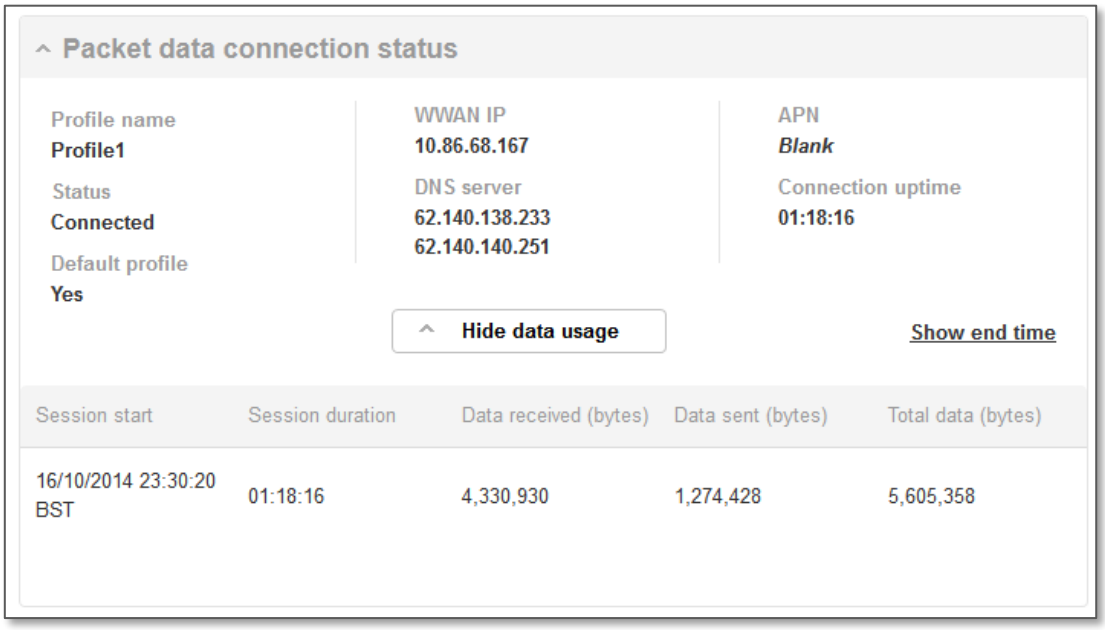


Figure 28 - Data usage with connection duration

Transparently bridging the mobile broadband connection via PPPoE

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

To enable transparent bridging via PPPoE:

1. Click the **Networking** menu item from the top menu bar.
2. On the **Data connection** page, click the **Transparent bridge (PPPoE)** toggle key so that it is **ON**.

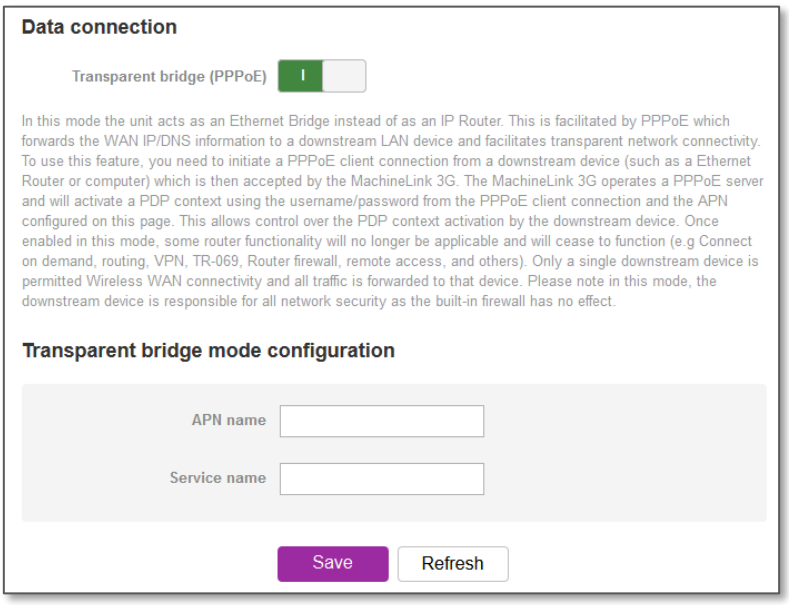


Figure 29 - Transparent bridge configuration

3. In the **APN name** field, enter the APN that you wish to use for the mobile broadband connection. If using a Vodafone Global SIM card, you may leave this blank or use any of the Vodafone assigned APNs.
4. (Optional) In the **Service name** field, enter a name that allows you to easily identify the connection.
5. Click the **Save** button to confirm the settings.
6. Click the **Status** menu item from the top menu bar to see the transparent bridging status.

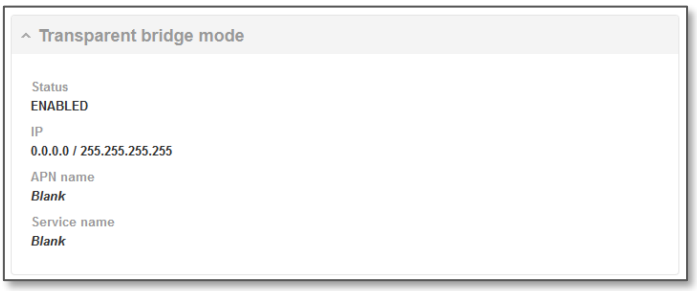


Figure 30 - Transparent bridge mode status

7 Next you must configure your downstream device connected via Ethernet to the MachineLink 3G to initiate a network connection a PPPoE client. The username and password used by the downstream device for the PPPoE session will be passed on and used by the MachineLink 3G as the packet data (PDP) context authentication settings.

Operator settings

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

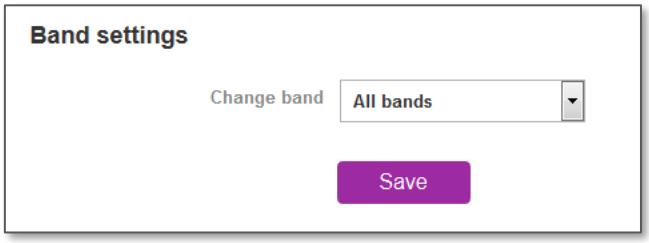


Figure 31 – Band settings

Note: Band settings and Operator settings do not take effect until you click the **Apply** button.

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

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

The following band settings options are available:

- All Bands
- GSM All
- WCDMA All
- GSM 850
- GSM 900
- GSM 1800
- GSM 1900
- WCMDA 850
- WCDMA 900
- WCDMA 800
- WCDMA 1900
- WCDMA 2100

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

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

The GSM All and the WCDMA all options allow you to force the device to lock to either 2G networks only, or 3G networks only.

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

Operator settings

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

Using a Vodafone GDSP SIM

When a GDSP SIM is inserted and the operator mode is set to **Automatic**, you are provided with further options to configure cost effective mode and network access technology preference. When **Cost effective mode** is turned on, the router selects the best carrier's 3G network (according to the PLMN list) and if that fails, it selects the 2G network of the same carrier. If connection to that network fails, the router then attempts to connect to the next best carrier's 3G network and so on.

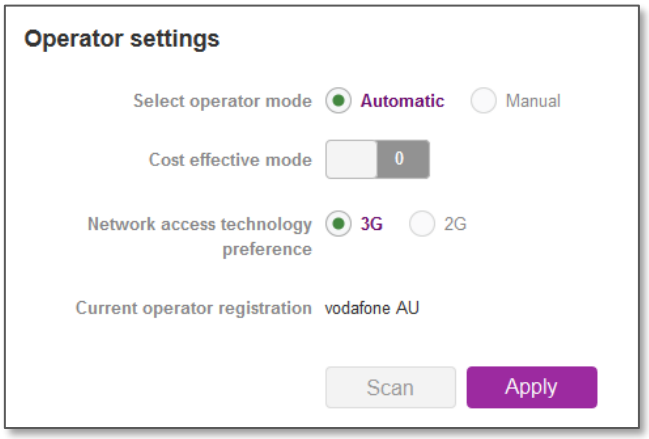


Figure 32 - Operator settings (using Vodafone GDSP SIM)

Using a non-Vodafone GDSP SIM

When a non-Vodafone GDSP SIM is inserted and operator mode is set to Automatic, the router attempts to connect to the best network (3G or 2G) of the carrier that provided the SIM

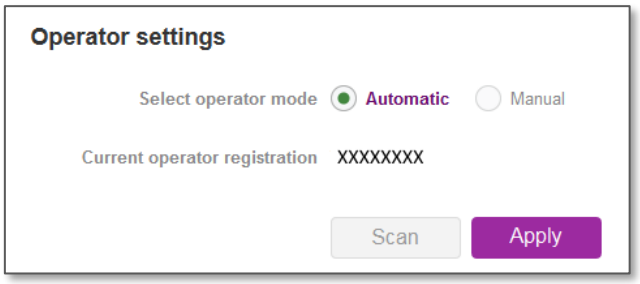
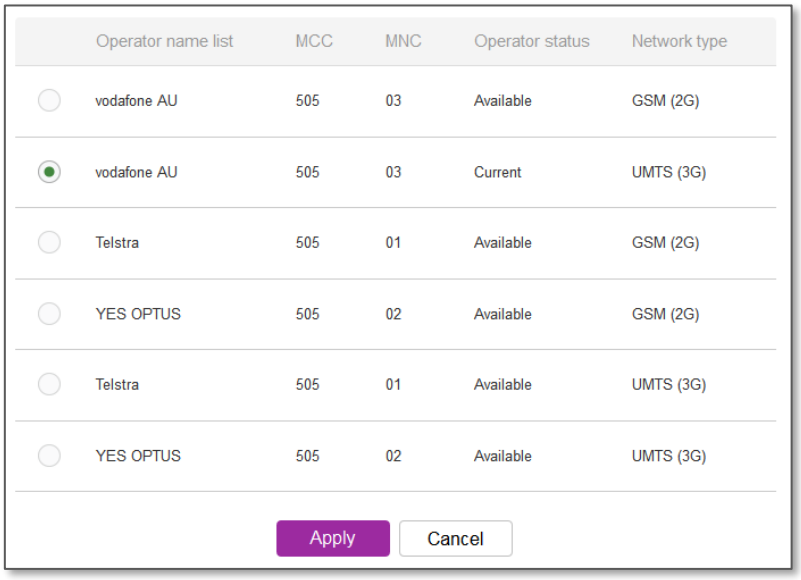


Figure 33 - Operator settings (using non-Vodafone GDSP SIM)

To scan for available networks, set the **Select operator mode** from **Automatic** to **Manual** then click the scan button. This operation can take a few minutes and requires that the packet data session be disconnected prior to scanning.

A list of the detected 3G service carriers in your area is displayed.



	Operator name list	MCC	MNC	Operator status	Network type
○	vodafone AU	505	03	Available	GSM (2G)
●	vodafone AU	505	03	Current	UMTS (3G)
○	Telstra	505	01	Available	GSM (2G)
○	YES OPTUS	505	02	Available	GSM (2G)
○	Telstra	505	01	Available	UMTS (3G)
○	YES OPTUS	505	02	Available	UMTS (3G)

Apply Cancel

Figure 34 - Detected operator list

Select the most appropriate 3G/2G service from the list shown and click **Apply**.

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

Roaming settings

When set the **Allow data roaming** toggle key is set to **ON**, the router will allow local devices to access the Wireless WAN network when it is roaming onto a foreign network. When set to **OFF**, the router will deny network access to data services when roaming onto a foreign network. This setting is **OFF** by default.

Roaming settings (Vodafone GDSP SIMs only)

The roaming settings page provides the ability to configure the Advanced Vodafone network (PLMN) selection feature. This feature provides a specialized algorithm which the router uses to select the best network to connect to from a prioritized list of networks which are stored on the router.

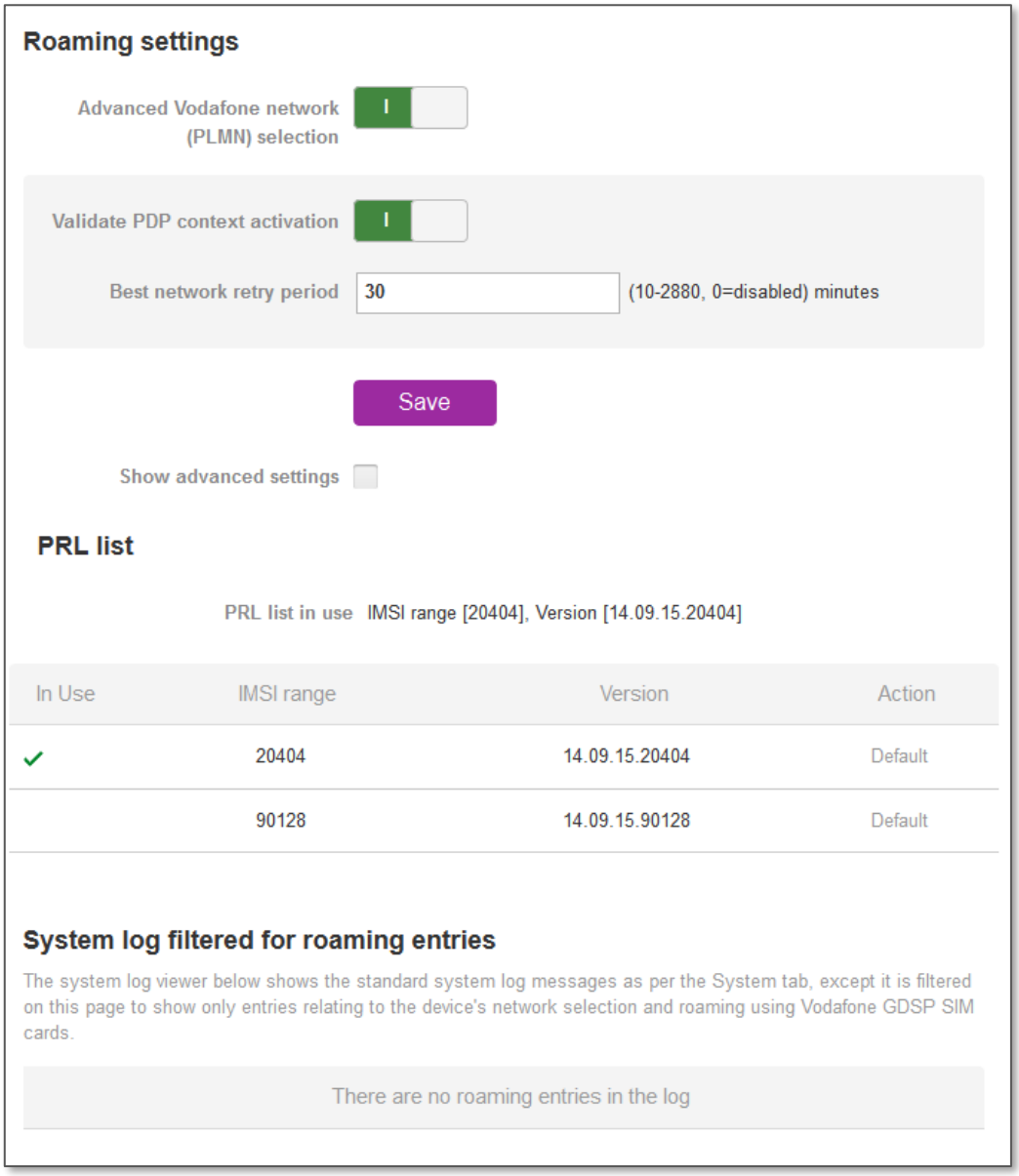


Figure 35 - Roaming settings

Item	Definition
Advanced Vodafone network (PLMN) selection	Switches the advanced network selection on or off. When on, the router will follow the advanced network selection algorithm designed by Vodafone to connect to the best network according to a priority ranked list stored on the router. If this is switched off, the router will revert to a standard connection methodology following the PLMN list stored on the SIM Card. It is recommended to leave advanced network selection enabled, unless there is a particular reason to disable it.
Validate PDP context activation	When this is turned on, the router verifies the default profile's username and password entered on the Profile settings page by activating a PDP context with each scanned network during advanced network selection process. This helps the router to avoid connecting to networks that are inaccessible by only allowing registration to a network if a PDP context was able to be established successfully. When this option is turned off, the router does not perform any validation of the PDP context activation and will register to a network even if it then cannot establish a PDP context.
Best network retry period	Sets the period for which the router will attempt to establish a connection to the best network listed in the preferred roaming list. This only takes place if the router is not already connected to the best network. By default this is set to 30 minutes. The best network retry period must be a value in minutes between 10 and 2880. Setting this option to 0 disables the router from retrying a connection to the best network.

Table 13 - Roaming settings options

The **PRL list** displays the Preferred Roaming Lists that are loaded on the router. The PRL lists are labelled according to the first 5 digits of the range of IMSI numbers that they cover. The list also indicates which list is in use, the version number of the list and an option to delete custom lists.

Important: Vodafone in The Netherlands uses IMSI range 20404, therefore regular Vodafone (non-GDSP) SIMs issued by Vodafone Netherlands may be detected as Vodafone GDSP SIMs. If using a Vodafone Netherlands issued SIM, please disable the **Advanced Vodafone network (PLMN) selection** option to avoid any problems.

Advanced settings

When the **Show advanced settings** option is selected, you are presented with the ability to customise the RSSI threshold.

Figure 36 – Advanced roaming settings

The Received Signal Strength Indicator (RSSI) threshold specifies the value in decibel-milliwatts that the signal strength must fall below for a total of 15 seconds without any traffic passing through before the router attempts to connect to the next network in the PRL list. RSSI values on cellular networks typically range between -113dBm (weak) and -51dBm (strong). As the RSSI approaches 0, the signal strength becomes stronger. The value that you enter into this field should be expressed as a positive integer but the router will process it as a negative value. The default RSSI threshold is -105dBm.

Important: Adjusting the RSSI roaming threshold incorrectly or without proper testing and validation may adversely affect network acquisition. Establishing a value different from the default, 105 (-105 dBm), will eliminate network registration attempts with any network observed to have a signal lower than the established threshold. Selecting a higher threshold may also eliminate available low cost networks resulting in higher data costs. It is recommended to consult your Vodafone technical contact prior to adjusting this parameter.

When you have made the desired change, click the **Apply** button. The router displays the above warning message. If you are sure you wish to proceed, select the "**I have read and understand the risk"** checkbox then click the **OK** button. The new RSSI threshold is applied immediately.

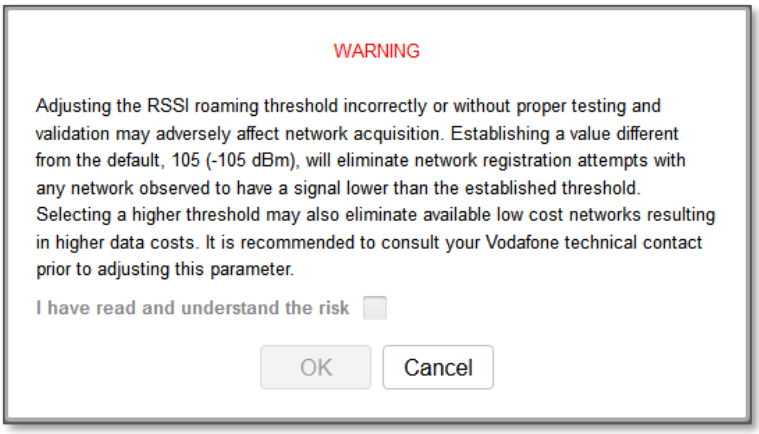


Figure 37 - RSSI threshold warning

The **System log filtered for roaming entries** section displays system log messages as per the System tab, except they are filtered to show only the entries related to the device's network selection and roaming using Vodafone GDSP SIM cards. You may use the **Download** button to download a filtered log file containing only messages related to the advanced network selection algorithm. The **Clear** button removes all System log records, including those records unrelated to the advanced network selection.

SIM security settings

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

Unlocking a PIN locked SIM

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

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

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

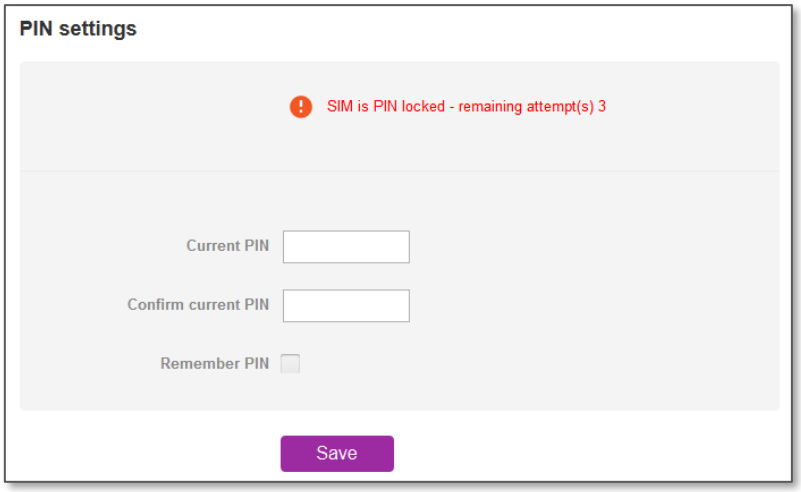


Figure 38 - SIM security settings - SIM PIN locked

2 Enter the PIN in the **Current PIN** field and then enter it again in the **Confirm current PIN** field to confirm the PIN.

3 If you are placing the router in a remote, unattended location, you may wish to check the **Remember PIN** option. This feature allows the router to automatically send the PIN to the SIM each time the SIM asks for it (usually at power up). This enables the SIM to be PIN locked (to prevent unauthorised re-use of the SIM elsewhere), while still allowing the router to connect to the cellular service.

When this feature is enabled, the PIN you enter when setting the **Remember PIN** feature is encrypted and stored locally on the router. The next time the SIM asks the router for the PIN, the router decrypts the PIN and automatically sends it to the SIM without user intervention.

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

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

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

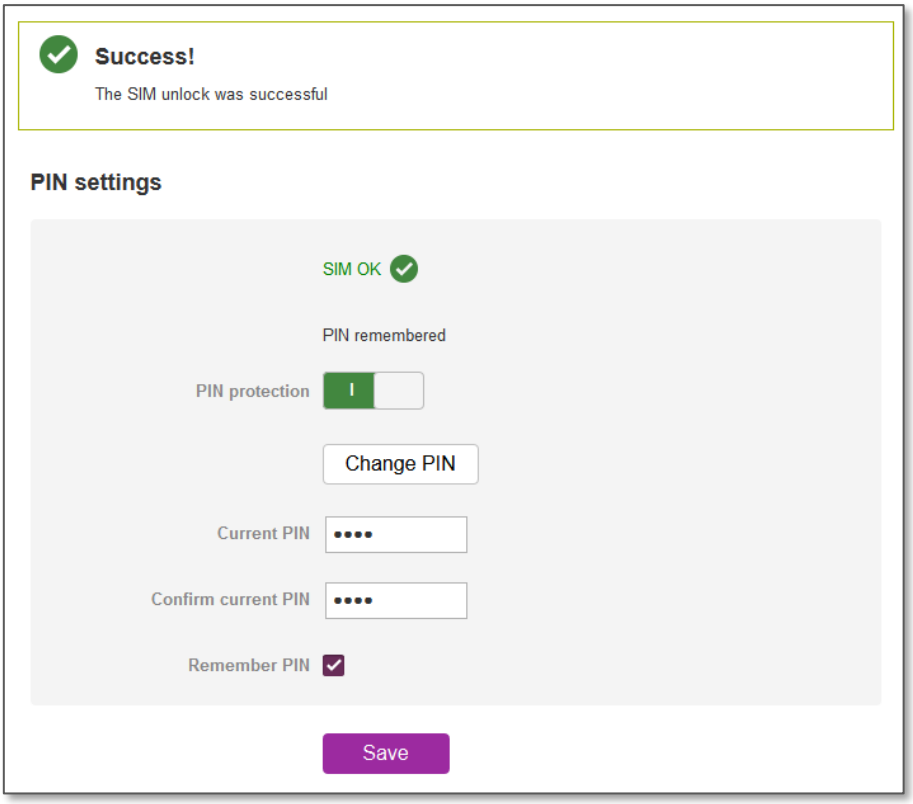


Figure 39 - SIM security settings - SIM unlock successful

Enabling/Disabling SIM PIN protection

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

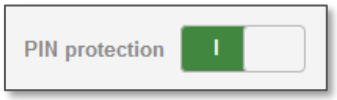


Figure 40 - PIN protection toggle key

Changing the SIM PIN code

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

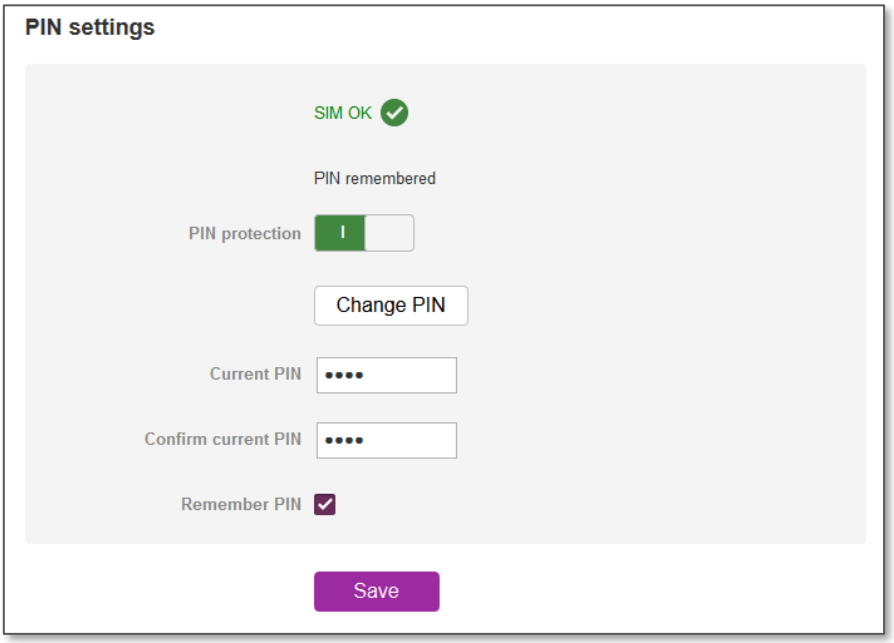


Figure 41 - PIN settings - Change PIN

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

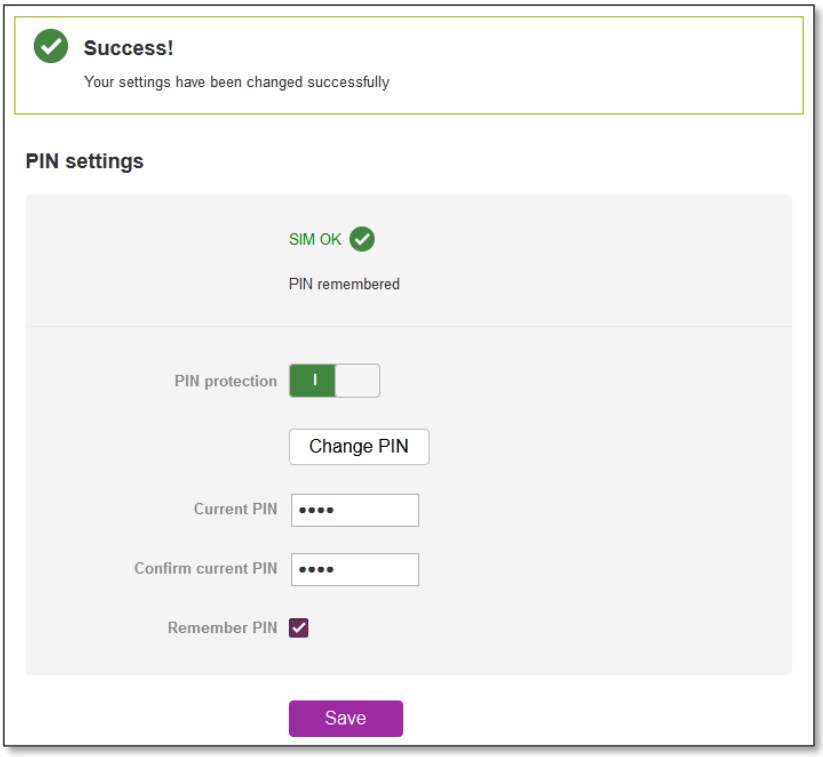


Figure 42 - SIM security settings – PIN change successful

Unlocking a PUK locked SIM

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

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

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

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

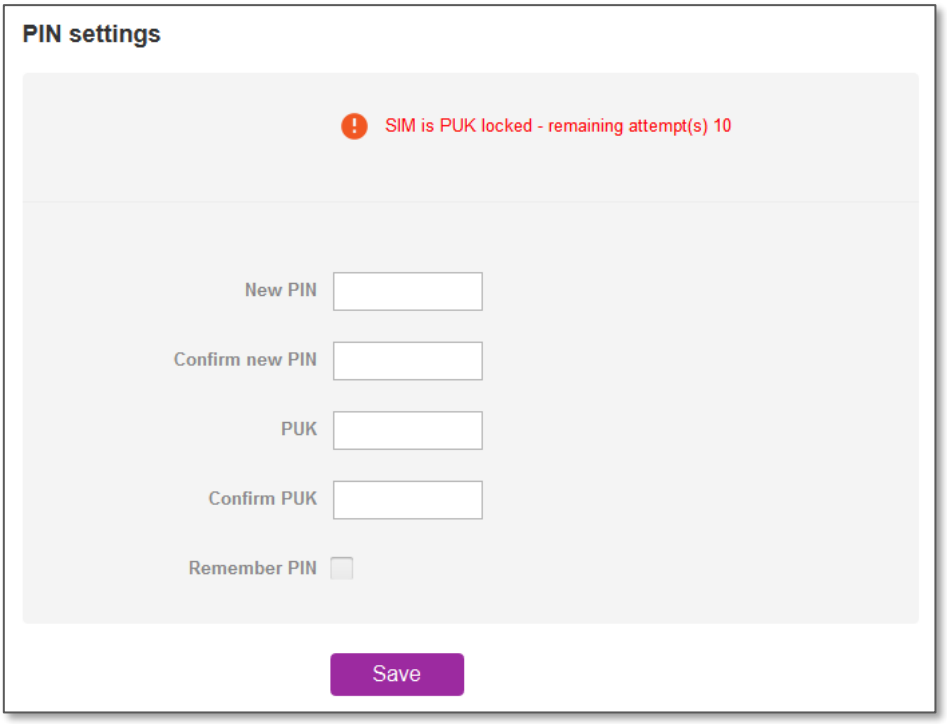


Figure 43 - SIM security - SIM PUK locked

Connect on demand

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

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

Configuring connect on demand

To configure Connect on demand:

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

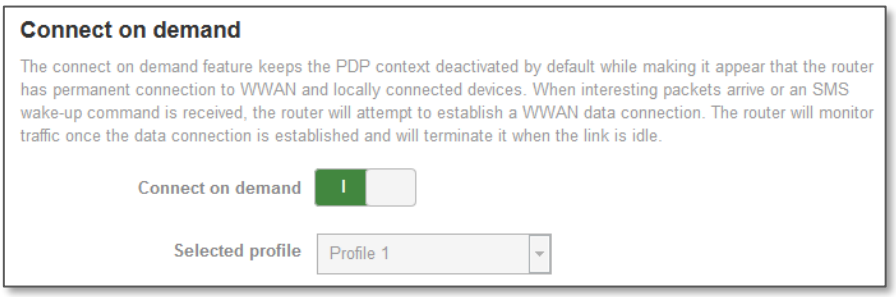


Figure 44 - Connect on demand configuration options

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

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

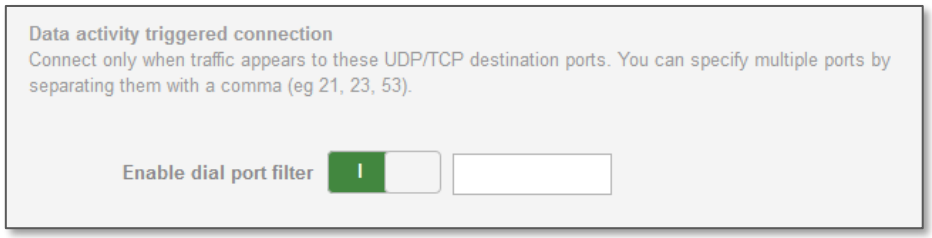


Figure 45 - Connect on demand - Data activity triggered connection

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

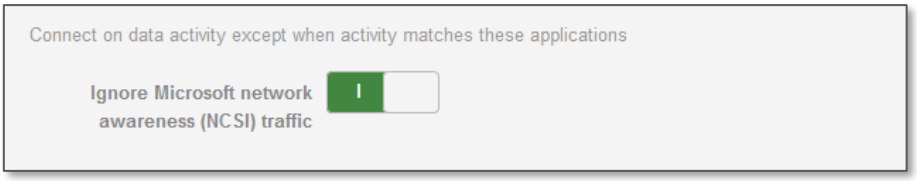


Figure 46 - Connect on demand - Ignore NCSI traffic

Excluding certain packet types from triggering the connection to dial

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

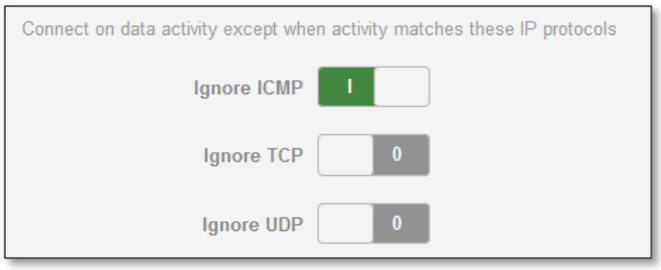


Figure 47 - Connect on demand - Excluding IP protocols

Excluding certain application types from triggering the connection to dial

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

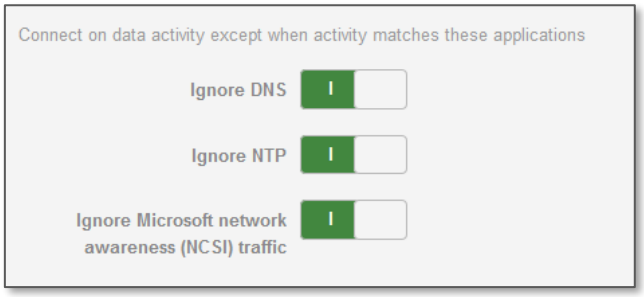


Figure 48 - Connect on demand - Excluding application types

Setting timers for dial-up and disconnection

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

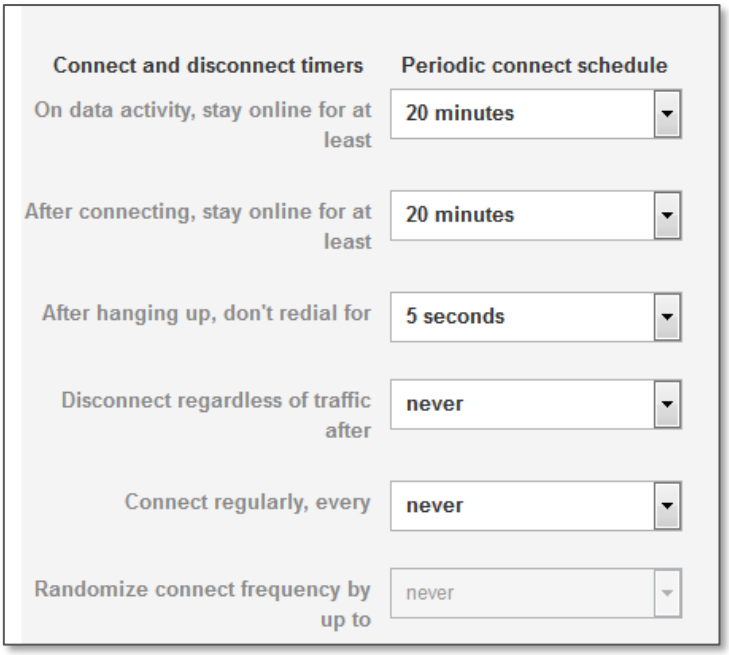


Figure 49 - Connect on demand - Connect and disconnect timers

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

Table 14 - Connect on demand - Connect and disconnect timers descriptions

Verbose logging

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

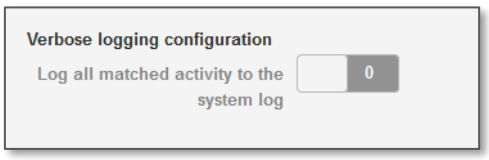


Figure 50 - Connect on demand - Verbose logging configuration

Manually connecting/disconnecting

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

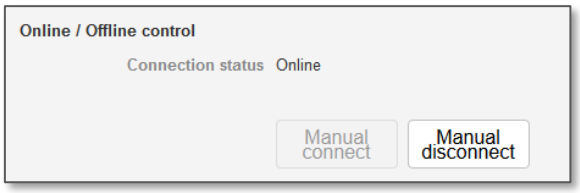


Figure 51 - Connect on demand - Online/Offline control

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

SMS Wake up

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

LAN

LAN configuration

The LAN configuration page is used to configure the LAN settings of the router and to enable or disable DNS Masquerading.

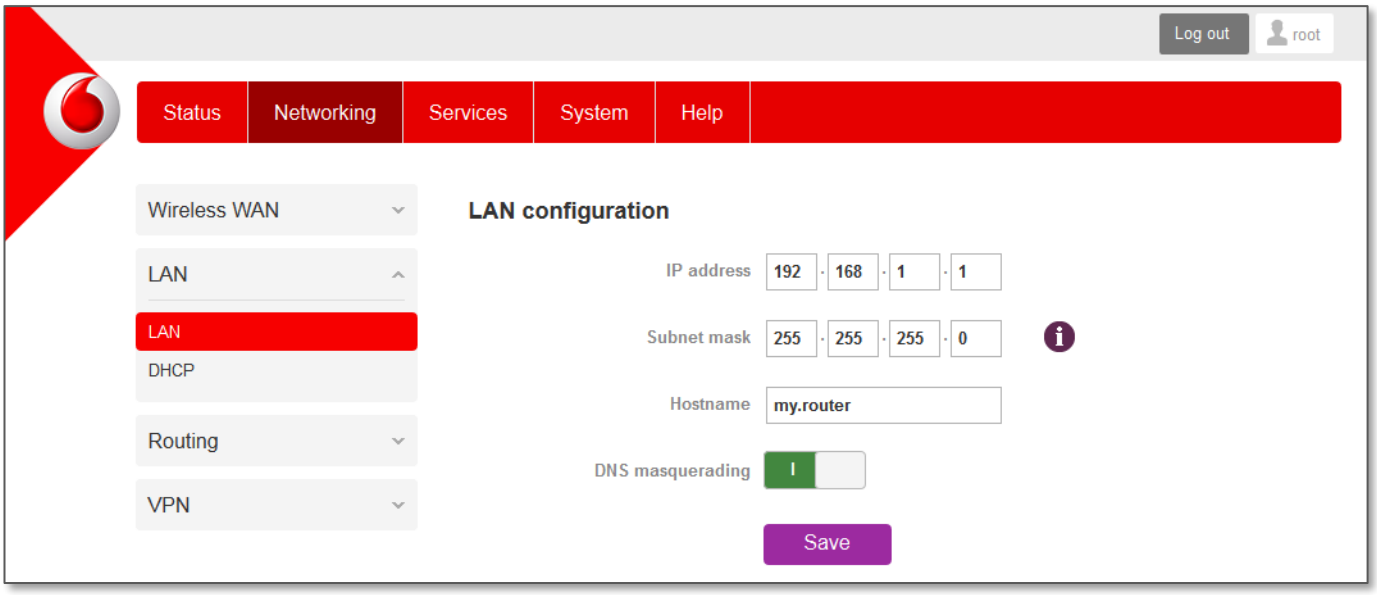


Figure 52 – LAN configuration settings

The default IP of the Ethernet port is 192.168.1.1 with subnet mask 255.255.255.0 and a Host name of "my.router". To change the IP address, Subnet mask or Host name, enter them in the appropriate fields and click the **Save** button.

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

DNS masquerading

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

With DNS masquerading **ON**, the DHCP server embedded in the MachineLink 3G 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 MachineLink which proxies them to the upstream DNS servers.

With DNS masquerading **OFF**, the DHCP server hands out the upstream DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the MachineLink 3G.

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

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

DHCP

The DHCP page is used to adjust the settings used by the router's built in DHPC Server which assigns IP addresses to locally connected devices.

DHCP relay configuration

In advanced networks configurations where the MachineLink 3G Router should not be responsible for DHCP assignment, but instead an existing DHCP server is located on the Wireless WAN connection, the clients behind the MachineLink 3G are able to communicate with the DHCP server when DHCP relay is enabled. This enables the MachineLink 3G to accept client broadcast messages and to forward them onto another subnet.

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

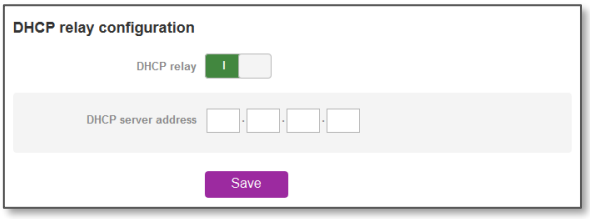


Figure 53 – DHCP relay configuration

DHCP configuration

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

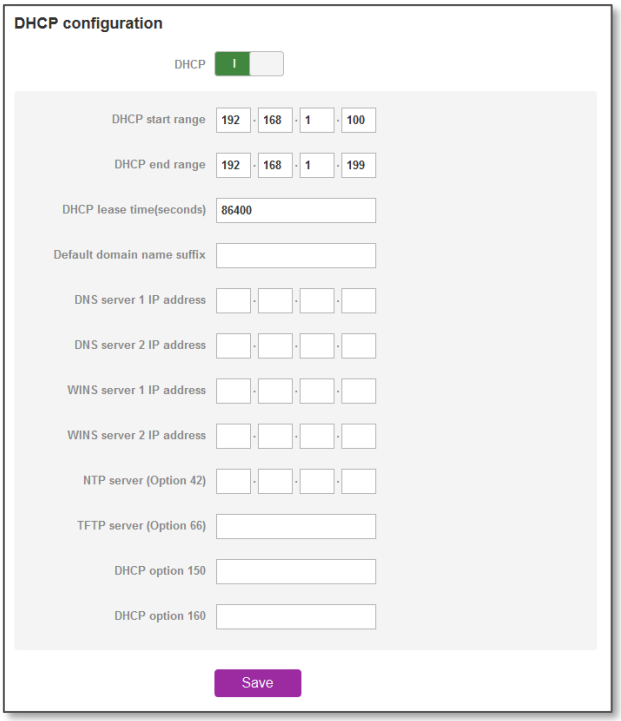


Figure 54 - DHCP configuration

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

Enter the desired DHCP options and click the **Save** button.

Address reservation list

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

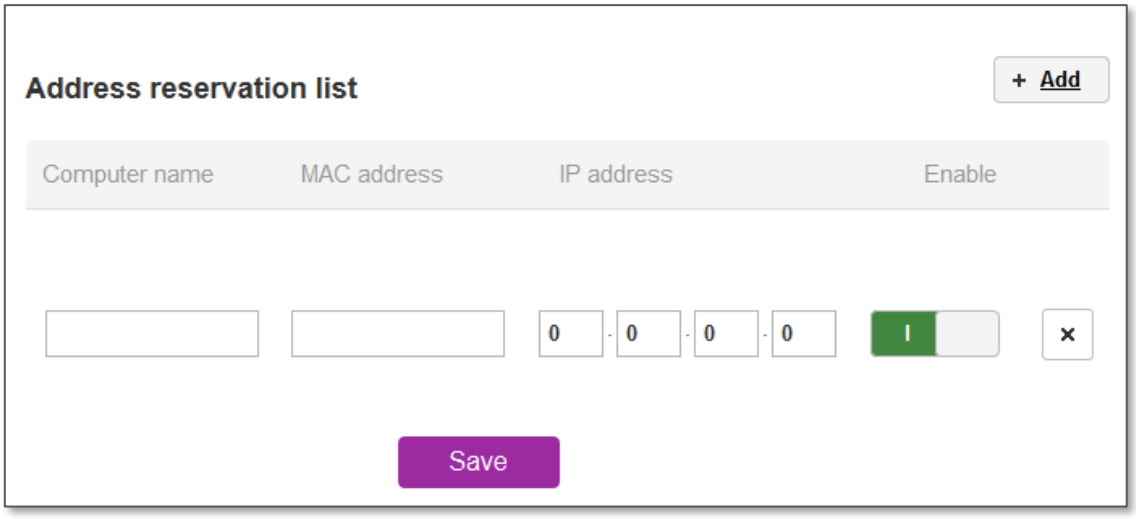


Figure 55 – DHCP – Address reservation list

To add a device to the address reservation list:

1. Click the **+Add** button.
2. In the **Computer name** field enter a name for the device.
3. In the **MAC address** field, enter the device's MAC address.
4. In the **IP address** fields, enter the IP address that you wish to reserve for the device.
5. If the **Enable** toggle key is not set to **ON**, click it to switch it to the **ON** position.
6. Click the **Save** button to save the settings.

Dynamic DHCP client list

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

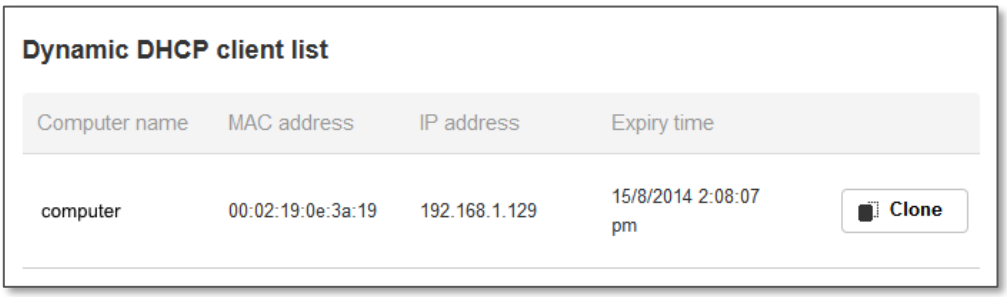


Figure 56 - Dynamic DHCP client list

Routing

Static

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

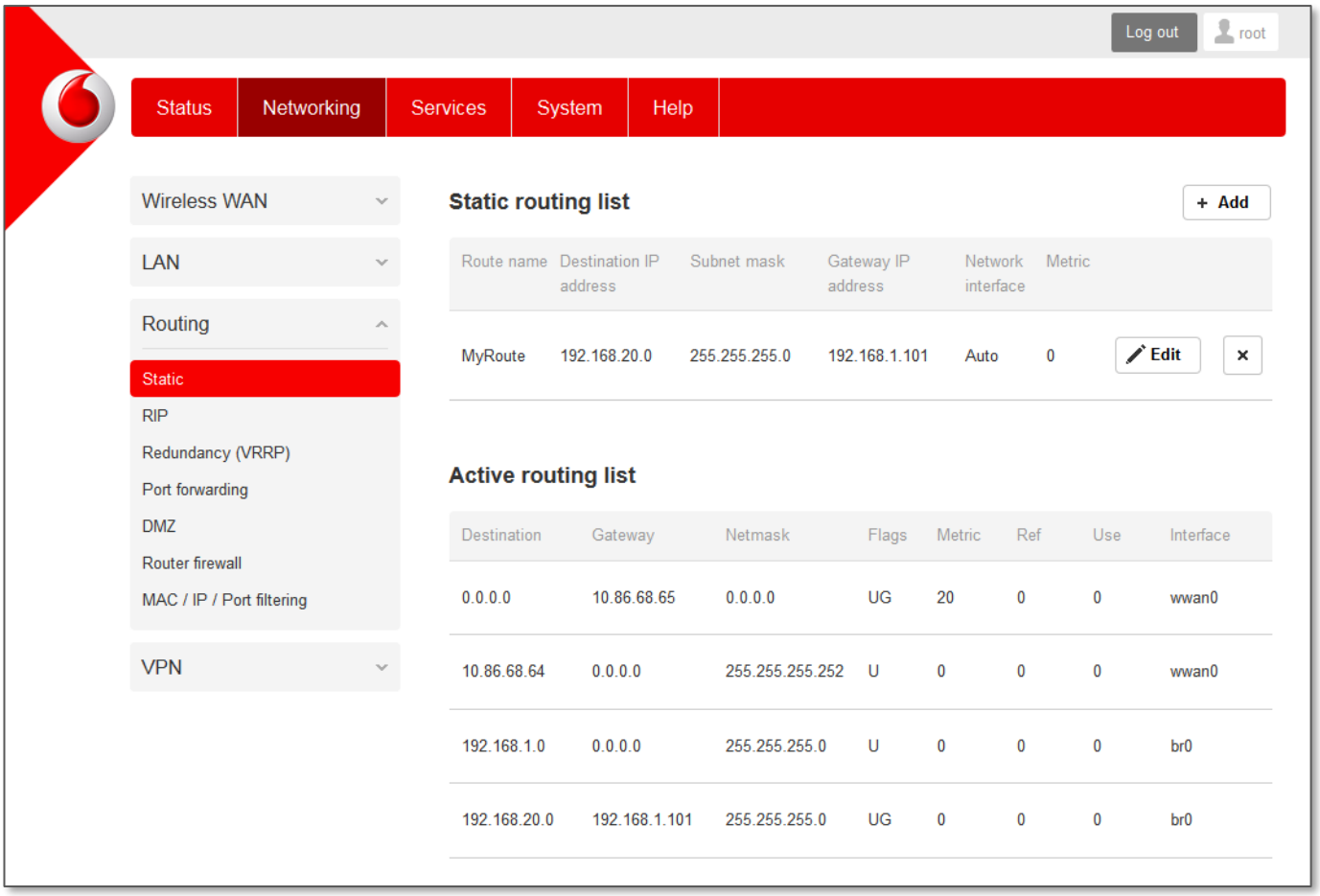


Figure 57 - Static routing list

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

Adding Static Routes

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

1. In the **Route name** field, type a name for the route so that it can be identified in the static routing list.
2. From the **Network interface** drop down list, select the interface for which you would like to create a static route.
3. In the **Destination IP address** field, enter the IP address of the destination of the route.

4 In the **Destination subnet mask** field, enter the subnet mask of the route.

5 In the **Gateway IP address** field, enter the IP address of the gateway that will facilitate the route.

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

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

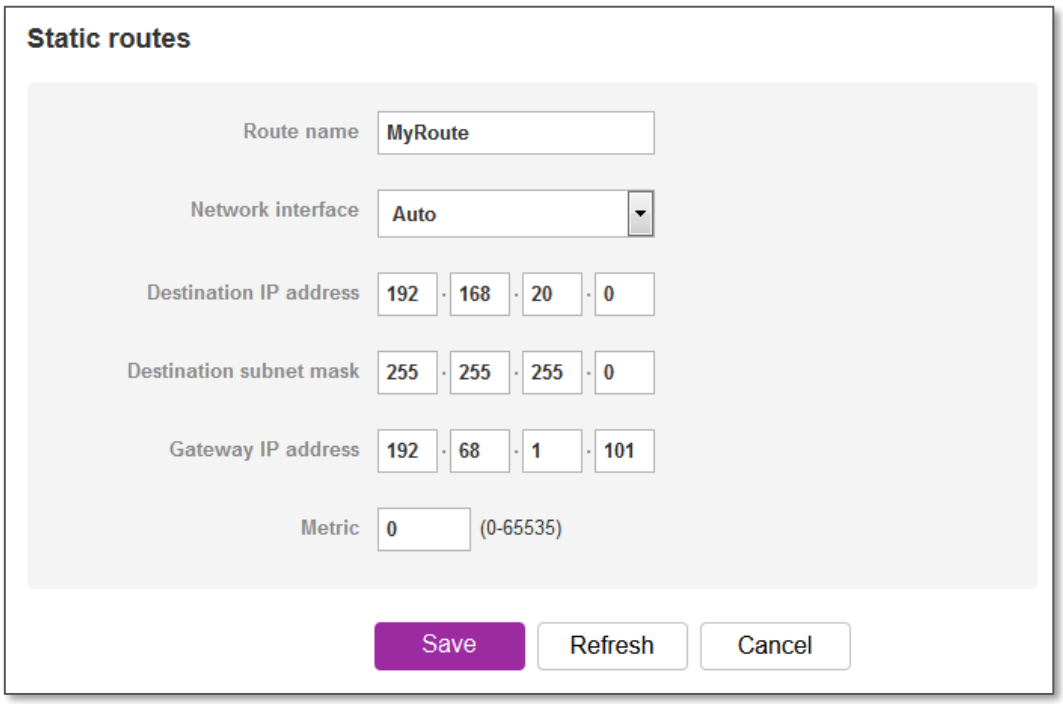


Figure 58 - Adding a static route

Setting a default gateway with two active connection profiles

When two connection profiles are active, all outbound traffic will be sent via the profile configured as the default gateway (See Data connection). If you wish to configure traffic to a network to go through a particular gateway, there are two methods available:

1 Use the static routing method described above.

2 Add the details of the remote network to the connection profile configuration.

For example:

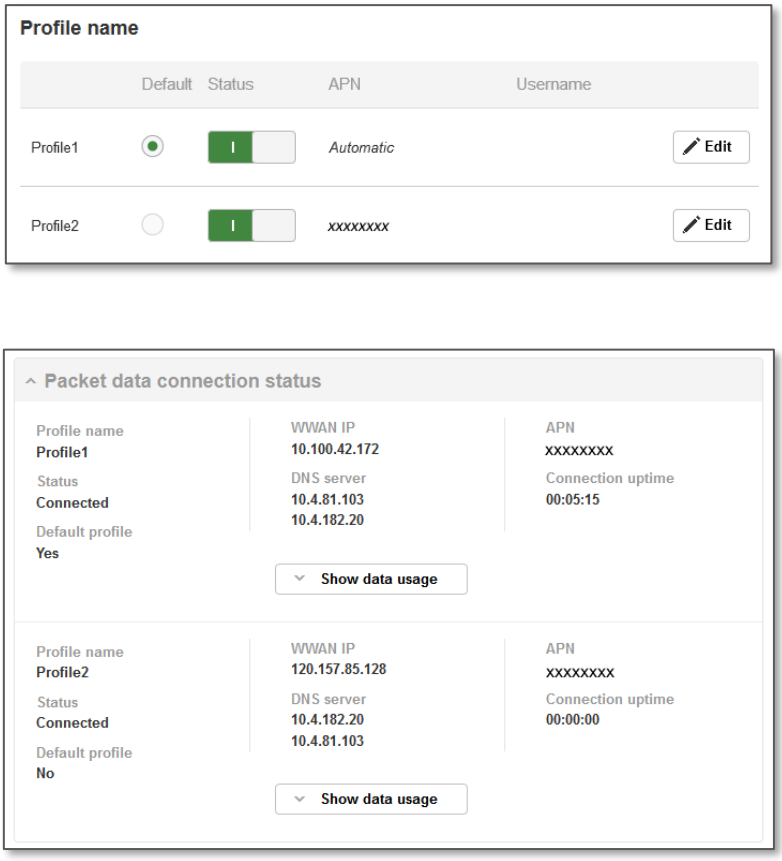


Figure 59 – Routing - Default gateway with two active connection profiles

In the example configuration above, Profile 1 and Profile 2 are both active and Profile 1 is configured as the default gateway. All outbound traffic is sent via Profile 1.

To specify that outbound traffic to remote network 123.121.120.X goes via Profile 2:

1 Click the **Networking** menu at the top of the screen and then click the **Edit** button next to Profile 2.

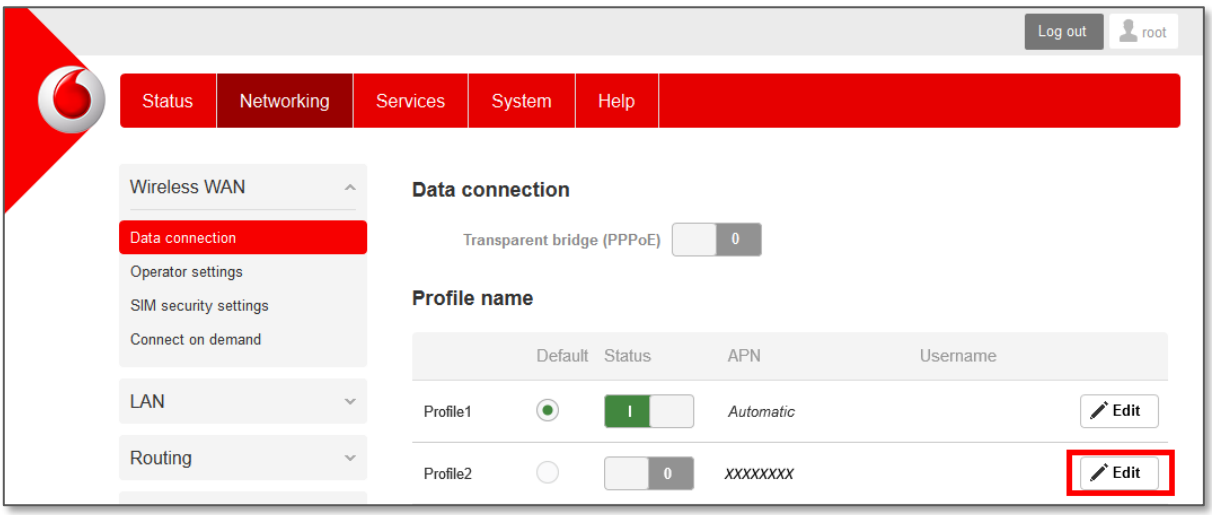


Figure 60 – Routing - Edit Profile 2

2 Scroll to the bottom of the window and in the **Profile routing settings** section, enter the address of the remote network and the subnet mask. A subnet is an identifiably separate part of a network and a subnet mask is the notation used to denote the subnet. Take care when configuring the subnet mask that the internal IP address of the router is in a different subnet than the remote network.

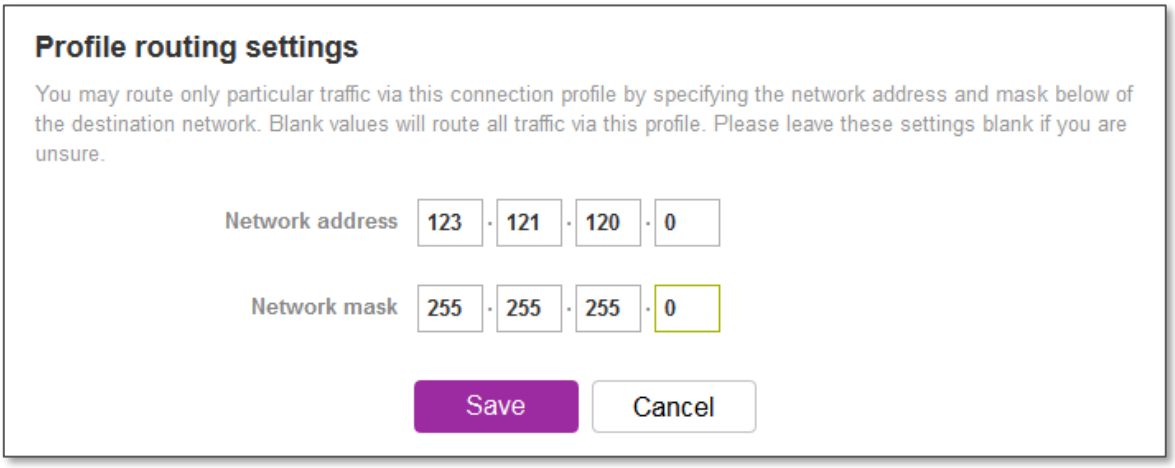
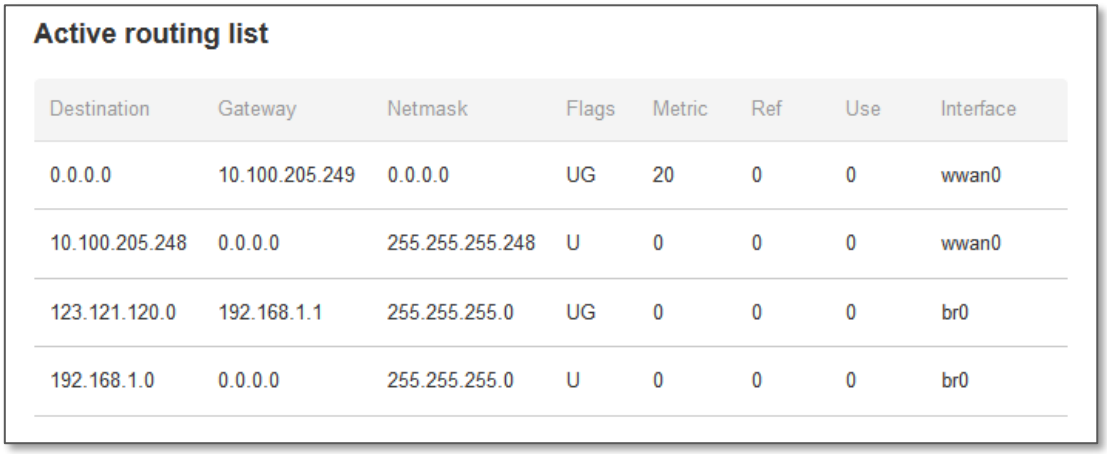


Figure 61 - Routing - adding remote network address and mask

3 Click the **Save** button to save the settings. All outbound traffic to 123.121.120.X addresses are now routed through Profile 2.

Active routing list

Static routes are displayed in the Active routing list.



Active routing list

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	10.100.205.249	0.0.0.0	UG	20	0	0	wwan0
10.100.205.248	0.0.0.0	255.255.255.248	U	0	0	0	wwan0
123.121.120.0	192.168.1.1	255.255.255.0	UG	0	0	0	br0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0

Figure 62 - Active routing list

Deleting static routes

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

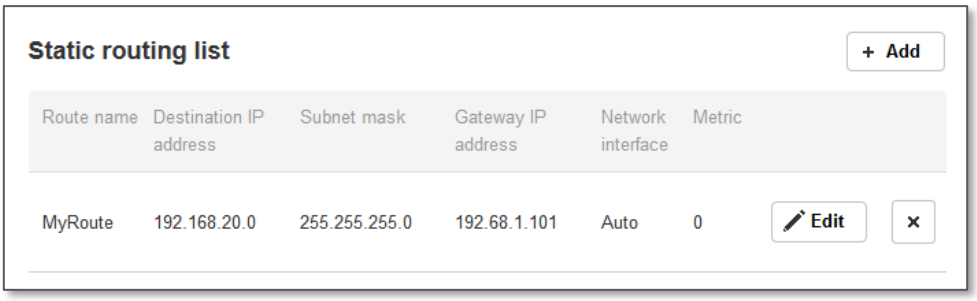


Figure 63 - Deleting a static route

RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. Thus all the routes in the router's routing table will be advertised to other nearby routers. For example, the route for the router's Ethernet subnet could be advertised to a router on the WAN 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.

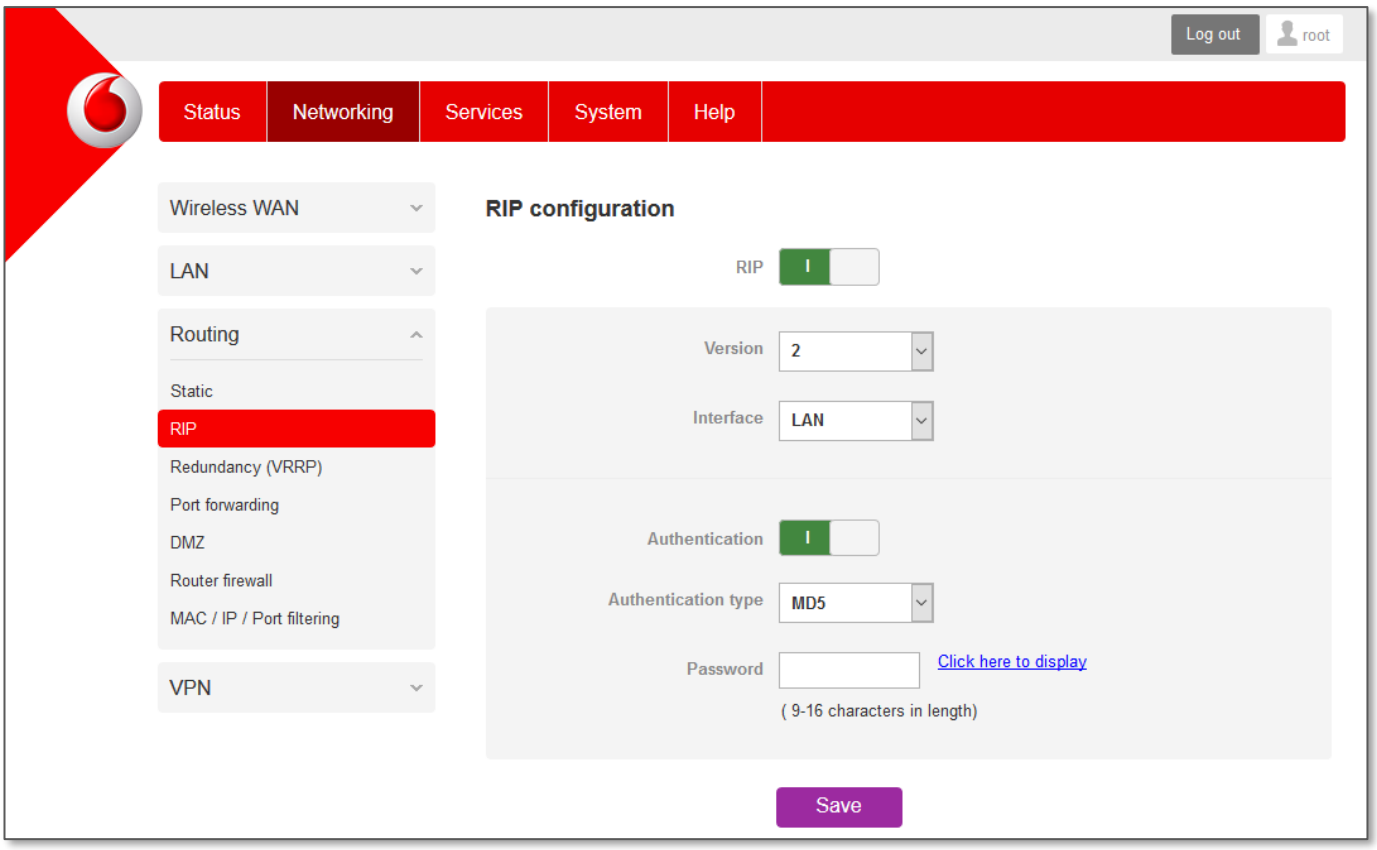


Figure 64 - RIP configuration

To enable Routing Information Protocol (RIP)

1. Click the **RIP** toggle key to switch it to the **ON** position.
2. Using the **Version** drop down list, select the version of RIP that you would like to use.
3. Select the interface for which you want RIP to apply. You can choose the **LAN** interface, the **WWAN** interface or **Both.**
4. If you wish to turn on authentication, toggle the **Authentication** toggle key to the **ON** position, use the **Authentication type** drop down list to select the method of authentication then enter password in the **Password** field.
5. Click the **Save** button to confirm your settings.

Redundancy (VRRP)

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.

Master routers have a priority of 255 and backup router(s) can have a priority between 1 and 254. A virtual router must use 00-00-5E-00-01-XX as its (MAC) address. The last byte of the address (XX) is the Virtual Router Identifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time, and is the only way that other physical routers can identify the master router within a virtual router.

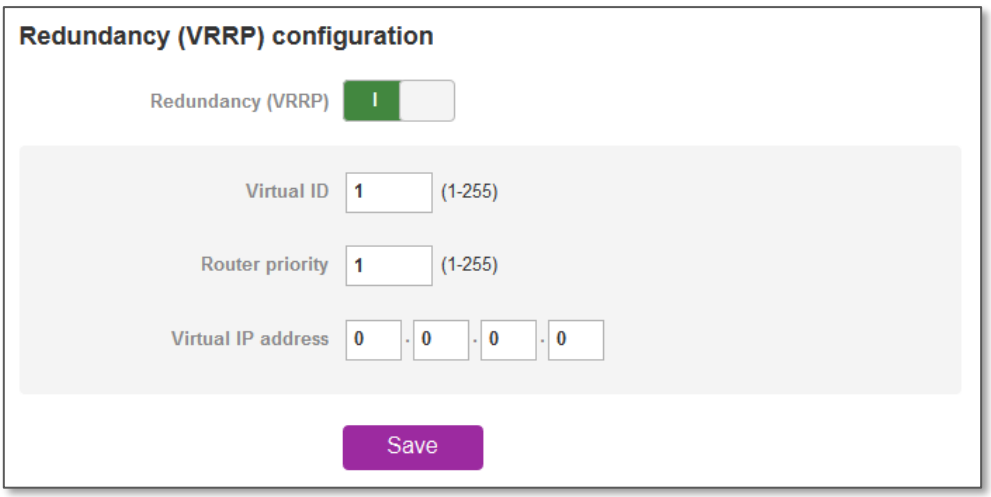


Figure 65 - VRRP configuration

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

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

Note: Configuring VRRP changes the MAC address of the Ethernet port and therefore if you want to resume with the web configuration you must use the new IP address (VRRP IP) or on a command prompt type:
`arp -d <ip address>` (i.e. `arp -d 192.168.1.1`) to clear the arp cache. (Old MAC address).

Port forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the router.

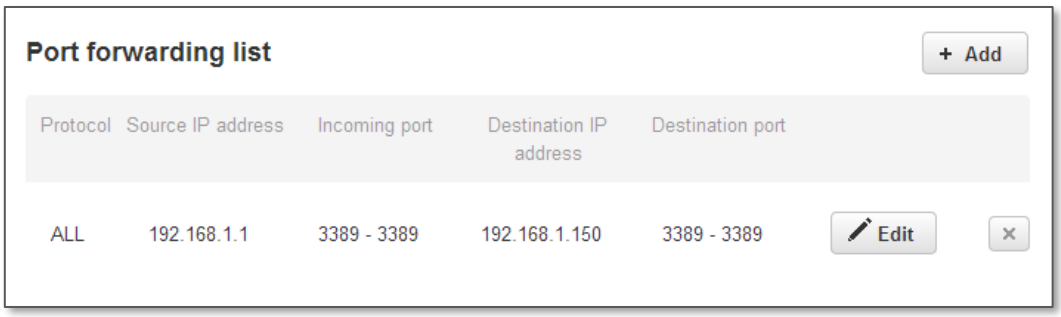


Figure 66 – Port forwarding list

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

Adding a port forwarding rule

To create a new port forwarding rule:

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

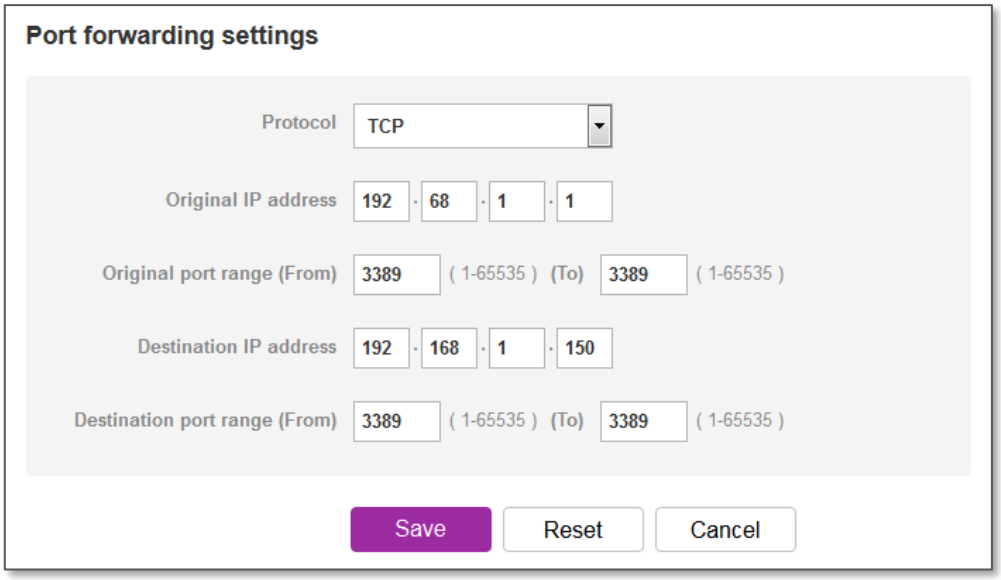


Figure 67 - Port forwarding settings

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

DMZ

The Demilitarised 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.

Figure 68 - DMZ configuration

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

Router firewall

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

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

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

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

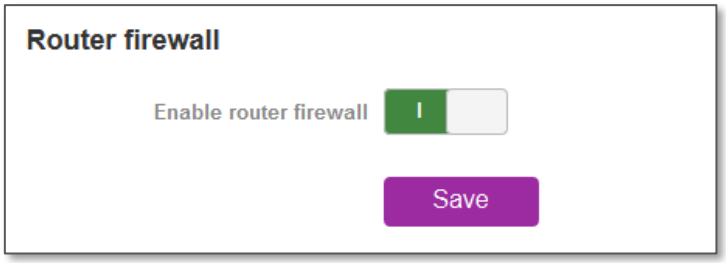


Figure 69 - Router firewall toggle key

MAC / IP / Port filtering

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

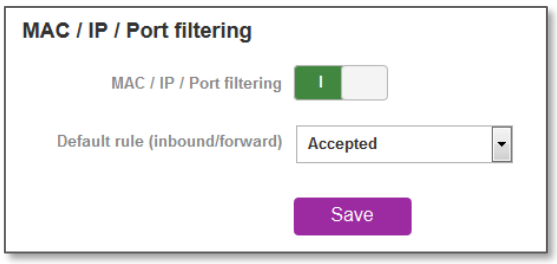


Figure 70 - MAC / IP / Port filtering

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

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

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

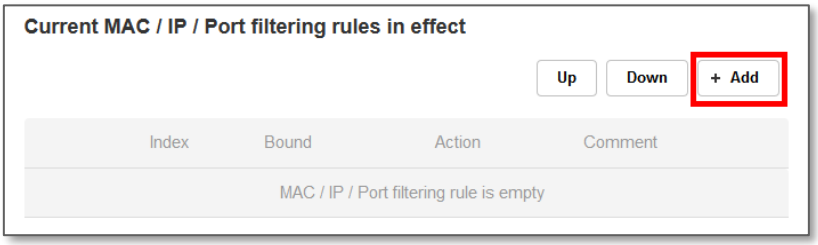


Figure 71 - Current MAC / IP/ Port filtering rules in effect

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

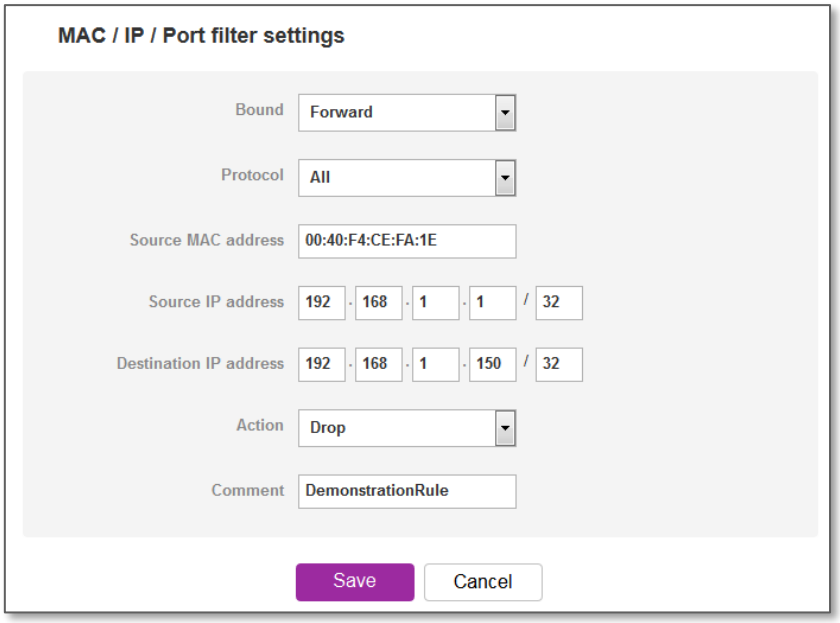


Figure 72 - MAC / IP / Port filtering settings

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

Table 15 - Current MAC / IP / Port filtering rules in effect

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

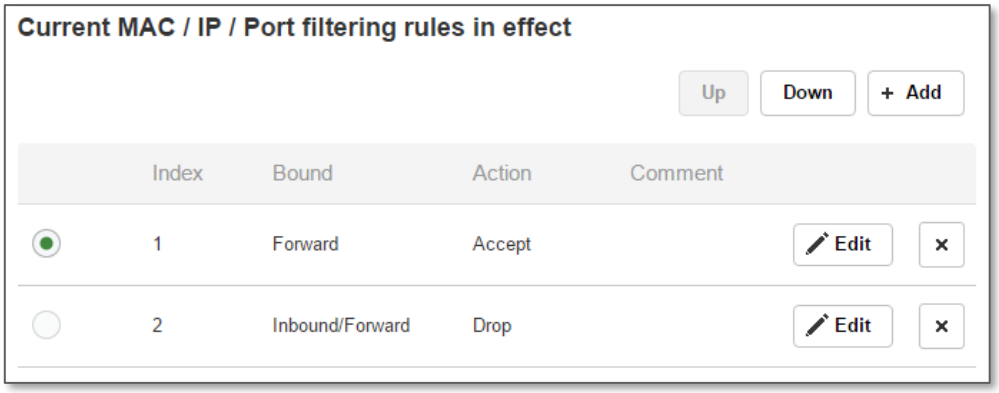


Figure 73 - Completed filtering rules and sequence

Option	Description
Selection button	Click the round button to select the rule that you want to promote/demote, edit or delete. When selected, the round button will display a green circle in its center
Index	The current order in which the filtering rules are applied. Can be changed by selecting the rule and applying the Up or Down buttons, see below.
Bound	Can be Inbound, Outbound, Forward or Inbound/Forward. For a more complete explanation, refer to Creating MAC / IP / Port filtering rules above.
Action	Can be Accept or Drop. For a more complete explanation, refer to Creating MAC / IP / Port filtering rules above.
Comment	Describes the effect of the rule.
Up / Down buttons	Select a rule and then click the Up or Down button to promote it in the indexed order in which it is applied to packets. Example: When a narrow rule accepts and another broader rule drops, the narrow rule must be indexed above the broader rule or it will not have any affect.
+Add button	Opens a blank MAC / IP / Port filter setting dialog, refer to Creating MAC / IP / Port filtering rules above.
Edit button	Select a rule and click the **Edit** button to change its properties.
Delete	Select a rule and click the **Delete** button to permanently remove it from the list.

Table 16 - Current MAC / IP / Port filtering rules in effect list

VPN

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

The advantages of a VPN connection include:

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

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

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

IPSec

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

Configuring an IPSec VPN

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

Figure 74 - IPSec VPN List

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

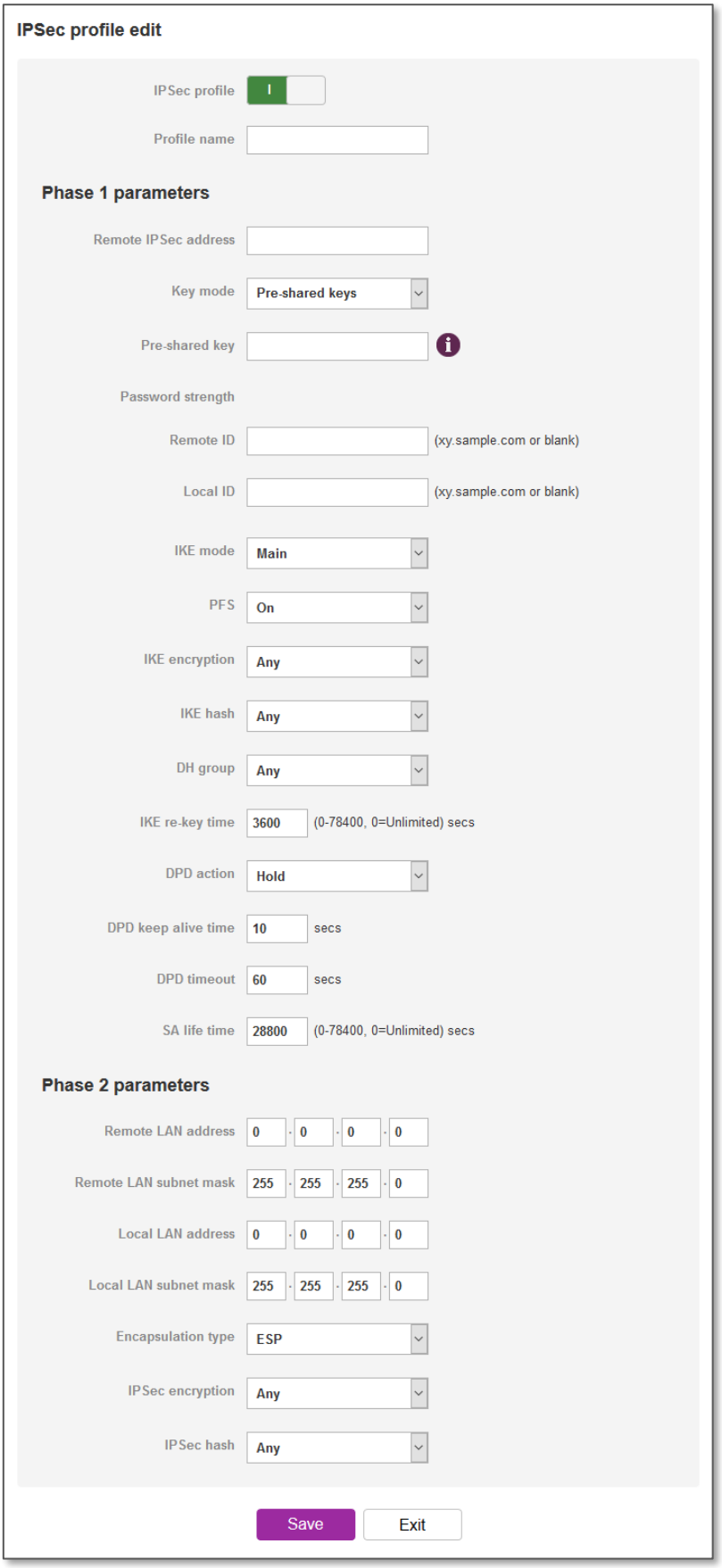


Figure 75 – IPSec profile edit

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

Item	Definition
IPSec profile	Enables or disables the VPN profile.
Profile name	A name used to identify the VPN connection profile.
Phase 1 parameters	
Remote IPSec address	The IP address or domain name of the IPSec server.
Key mode	Select the type of key mode in use for the VPN connection. You can select from: • Pre Shared Key • RSA keys • Certificates • SCEP client
Pre-shared key	The pre-shared key is the key that peers used to authenticate each other for Internet Key Exchange. The pre-shared key must meet the requirements for a strong password. See the Configuring a strong password section.
Update Time	Displays the last time the key was updated.
Local RSA Key Upload	Select the RSA key file for the local router here by clicking the **Browse** button.
Remote RSA Key Upload	Select the RSA key file for the remote router here by clicking the **Browse** button.
Private key Passphrase	The Private key passphrase of the router is the passphrase used when generating the router's private key using OpenSSL CA.
Key / Certificate	Select the type of key or certificate to use for authentication. You can select **Local private key**, **Local public certificate**, **Remote public certificate**, **CA certificate**, **CRL certificate**.
IPSec Certificate Upload	Select the IPSec certificate to upload by clicking the **Browse** button.
Remote ID	Specifies the domain name of the remote network.
Local ID	Specifies the domain name of the local network.
IKE mode	Select the IKE mode to use with the VPN connection. You can choose **Main**, **Aggressive** or **Any**.
PFS	Choose whether Perfect Forward Secrecy is ON or OFF for the VPN connection.
IKE encryption	Select the cipher type to use for the Internet Key Exchange.
IKE hash	Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.
DH group	Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.
IKE re-key time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.
DPD action	Select the desired Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.

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

Table 17 - IPSec Configuration Items

Configuring IPSec using an SCEP certificate

When adding or editing an IPSec profile, use the **Key mode** drop down list to select **SCEP client** and then enter the Distinguished Name details of the remote peer's certificate in the **Remote ID** field. They should be entered in the following format:

C=<Two-digit country code>, ST=<State>, L=<Locality>, O=<Organisation>, OU=<Organisational Unit>, CN=<Common Name>.

For example:

C=AU, ST=NSW2, L=LaneCove2, O=NetComm2, OU=SW2, CN=nwl222222999

See the below screenshot for an example configuration.

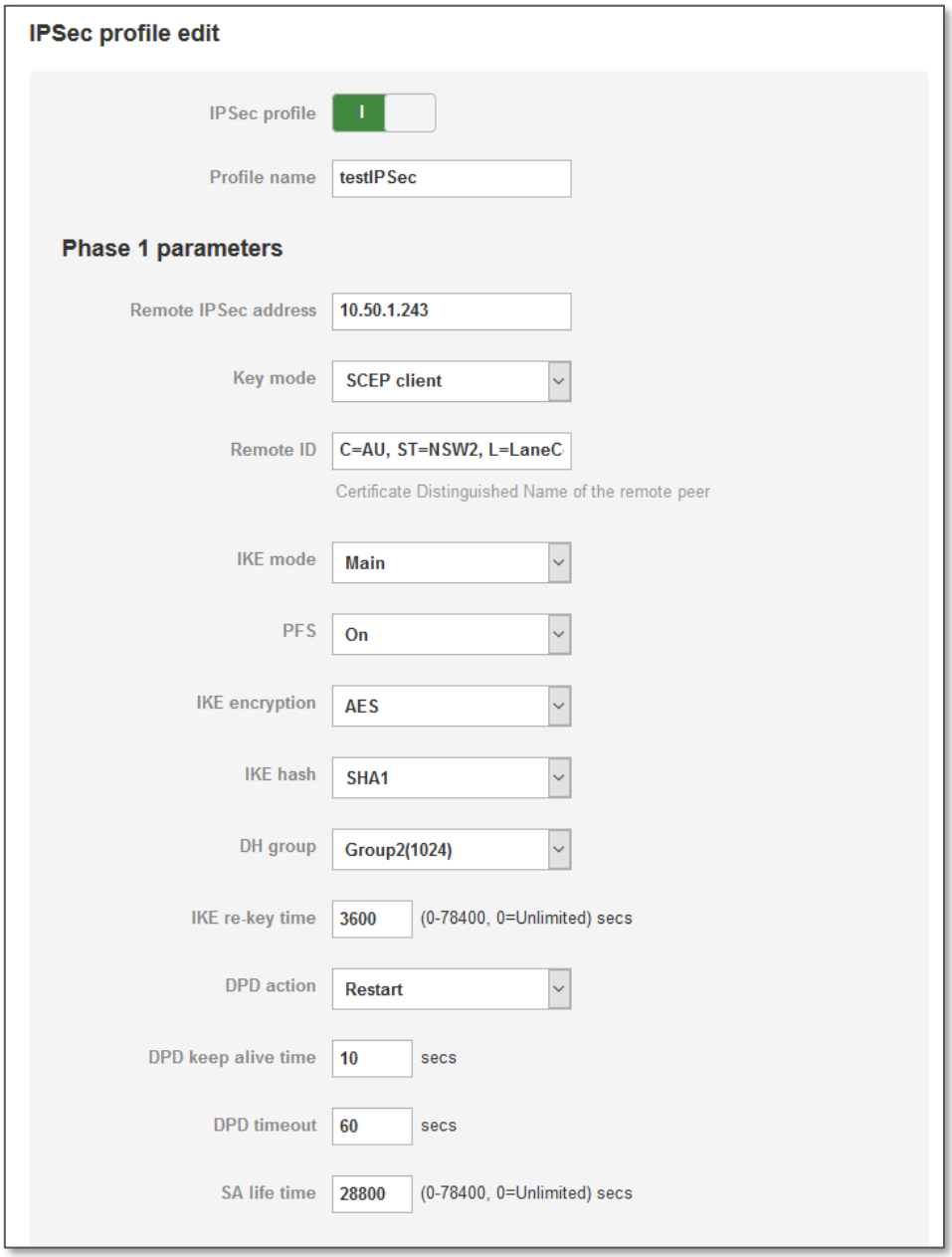


Figure 76 - Configuring IPSec using an SCEP certificate

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, Mac OS, Solaris, OpenBSD, FreeBSD, NetBSD and QNX.

Configuring an Open VPN server

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

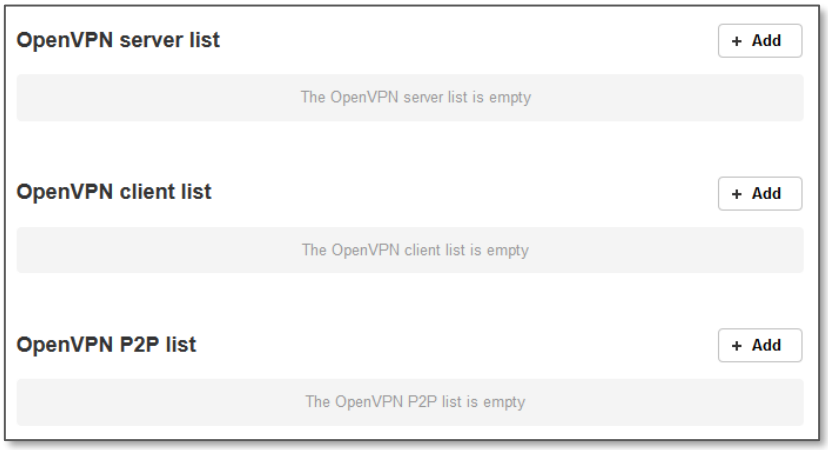


Figure 77 - OpenVPN VPN List

Click the **+Add** button for the type of OpenVPN server/client you would like to configure.

OpenVPN Server

To configure an OpenVPN Server:

1. Click the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. Type a name for the OpenVPN server profile you are creating.
3. Select OpenVPN connection type (TUN/TAP). Default is **TUN**.
4. Use the **Server port** field to select a port number and then use the drop down list to select a protocol to use for your OpenVPN Server. The default OpenVPN port is 1194 and default protocol is UDP.
5. In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
6. Select the server key size. The available options are 1024, 2048 and 4096. The default value is 1024 bit.
7. Next to Diffie-Hellman parameters, select appropriate encryption key size then click the **Generate DH** button. This will create an encryption key to secure your OpenVPN connection. Default key size is (1024) bit.

8 Under **Server certificates**, enter the required details. All fields must be completed. The **Country** field must consist of two characters only. When the details have been entered, click the **Generate CA certificate** button to generate the Certificate Authority (CA) certificate based on this information.

9 Under the **Server certificates** section, select the **Authentication type** that you would like to use for the OpenVPN Server.

Note: Because the Diffie-Hellman parameters are generated randomly and largely affected by the chosen key size, the time it takes to generate the parameters may differ. It may take a few minutes or a few hours where larger key sizes are selected. Please be patient

Certificate Authentication

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

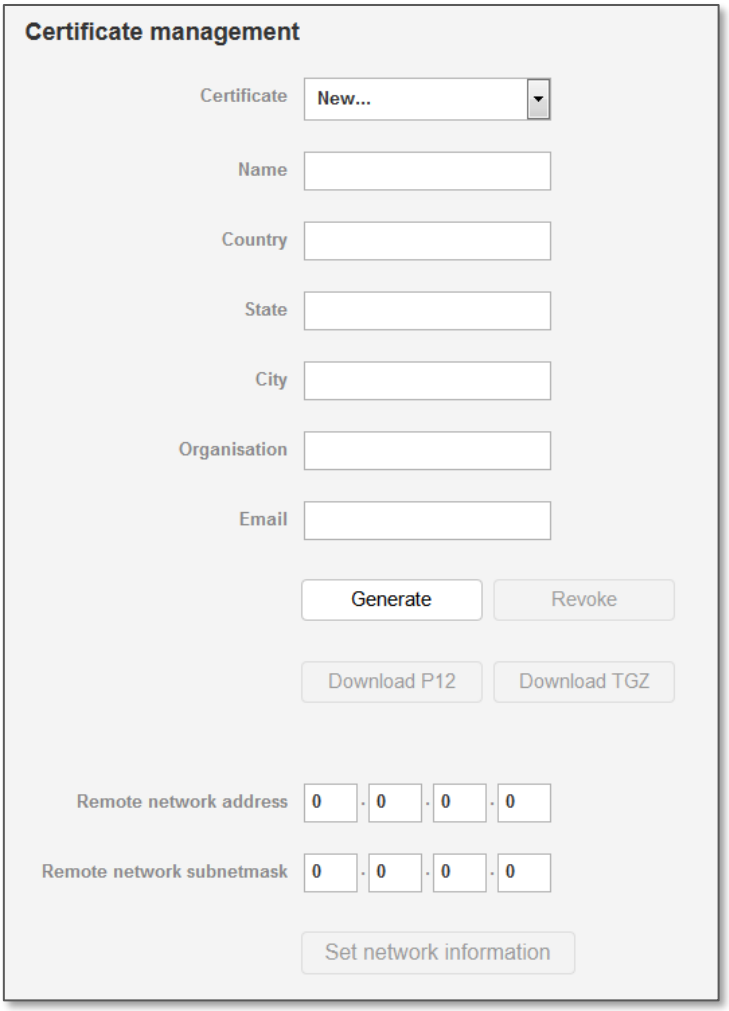


Figure 78 - OpenVPN server configuration – Certificate management

When it is done, you can click the **Download P12** button or the **Download TGZ** button to save the certificate file depending on which format you would like. If for some reason the integrity of your network has been compromised, you can return to this screen and use the Certificate drop down list to select the certificate and then press the Revoke button to disable it.

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

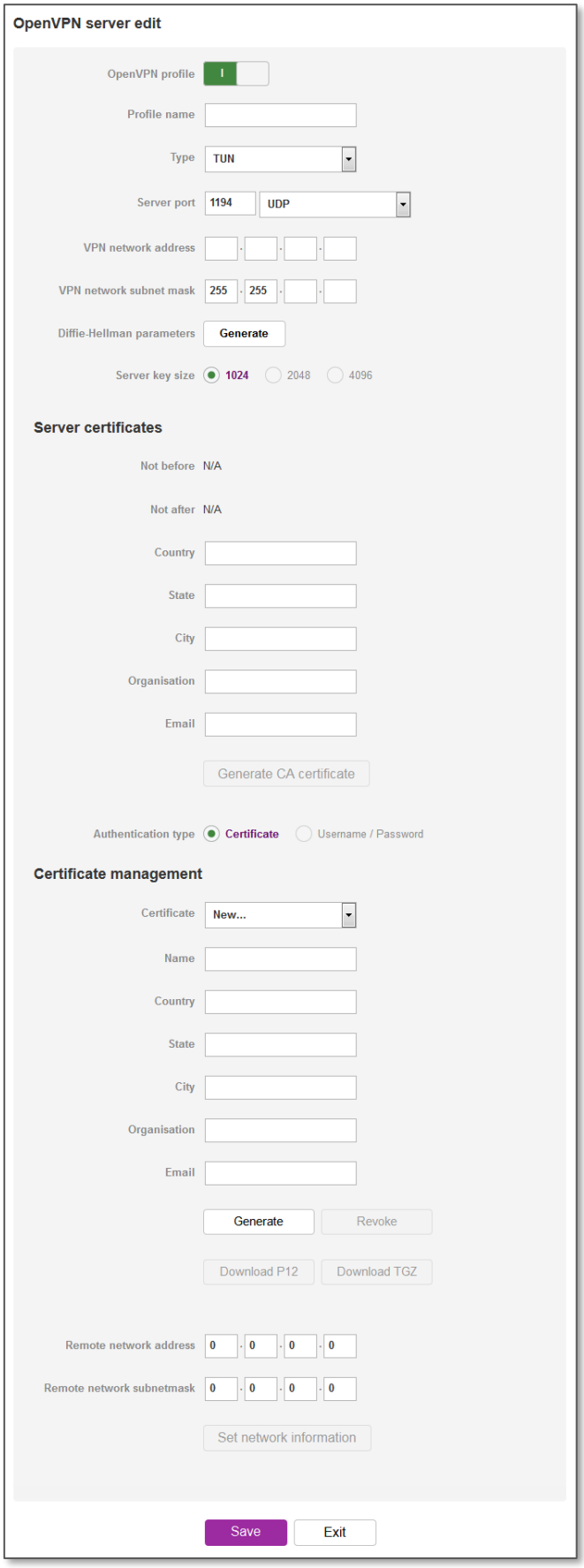


Figure 79 – OpenVPN server profile settings

Username / Password Authentication

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

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

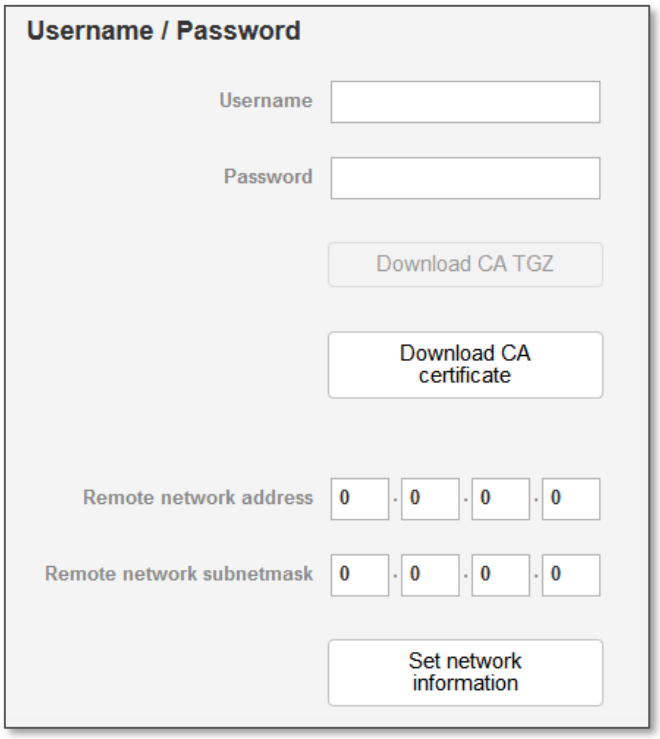


Figure 80 - OpenVPN Server – Username / Password section

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

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

Configuring an OpenVPN Client

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

6 If the **Default gateway** option is applied on the OpenVPN client page, the OpenVPN server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between this router and the remote OpenVPN server only.

7 Use the **Authentication type** options to select the Authentication type that you would like to use for the OpenVPN client.

Certificate Authentication

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

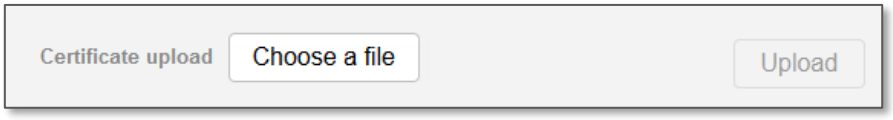


Figure 81 - OpenVPN client - Certificate upload

Username / Password Authentication

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

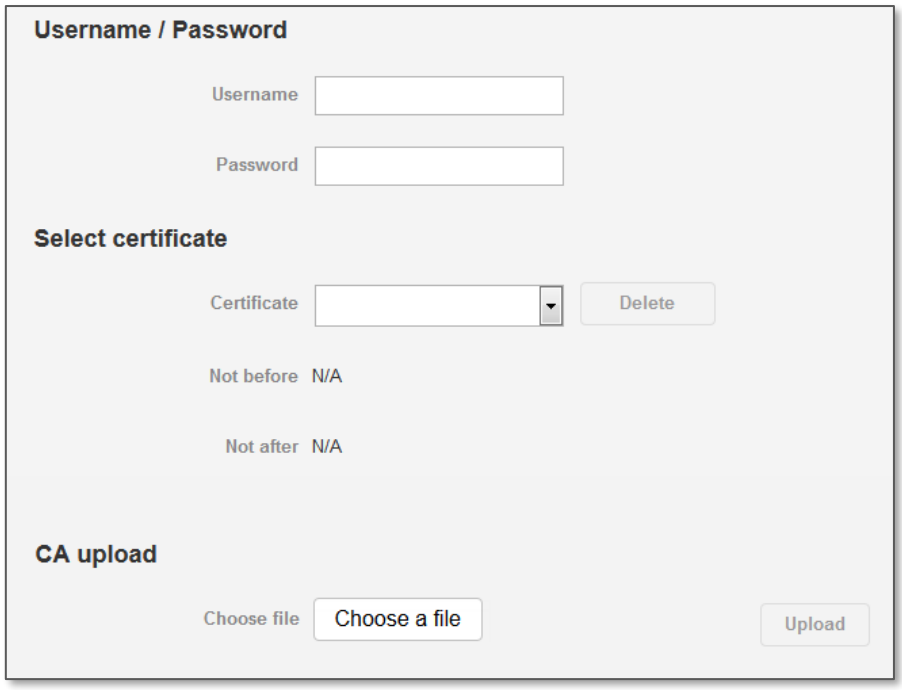


Figure 82 - OpenVPN Client - Username/Password section

2 Use the **Choose a file** button to locate the CA certificate file you saved from the OpenVPN Server and then press the **Upload** button to send it to the router.

3 Click the **Save** button to complete the OpenVPN Client configuration.

Certificate and Username / Password Authentication

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

Configuring an OpenVPN P2P Connection

To configure an OpenVPN peer-to-peer connection:

1. Set the **OpenVPN profile** toggle key to switch it to the ON position.
2. In the **Profile name** field, type a name for the OpenVPN P2P profile you are creating.
3. On the router designated as the server, leave the **Server IP address** field empty. On the router designated as the client, enter the WAN IP address/host domain name of the server.

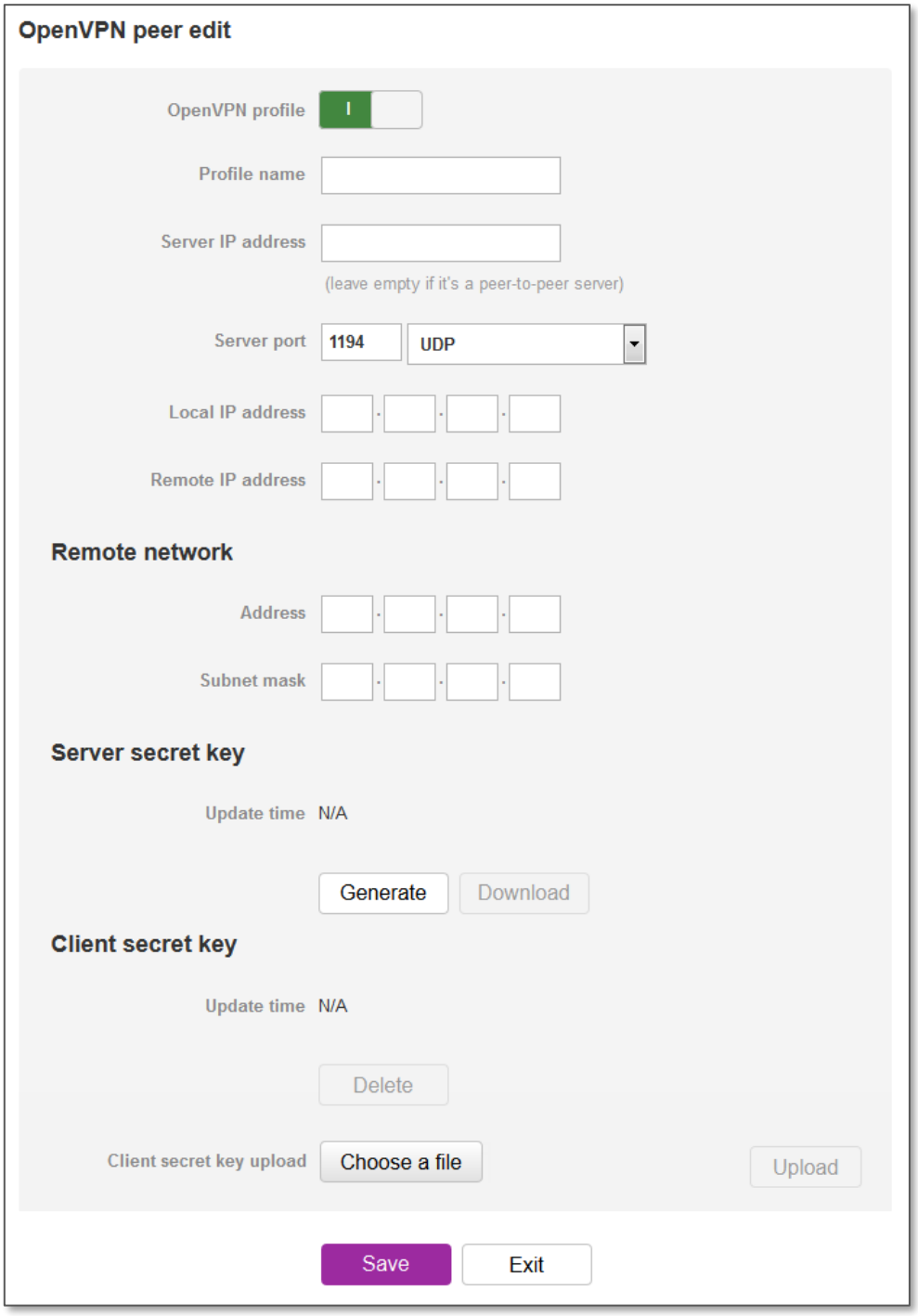


Figure 83 - OpenVPN P2P mode settings

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

5 In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The client should have the reverse settings of the server.

6 Under the **Remote network** section, enter the network **Address** and network **Subnet mask**. The Network Address and Network Mask fields inform the server node of the LAN address scheme of the client.

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

8 When you have saved the secret key file on each router, use the **Choose a file** button to locate the secret key file for the master and then press the **Upload** button. Perform the same for the other router, uploading the client's secret key file to the server.

9 When they are uploaded click the **Save** button to complete the peer-to-peer OpenVPN configuration.

PPTP client

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

Configuring the PPTP Client

To configure the PPTP client:

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

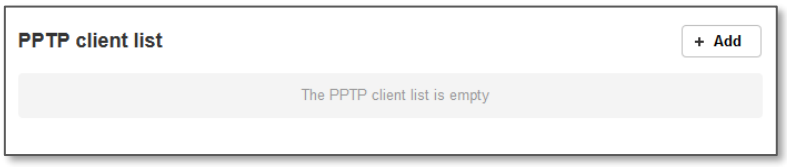


Figure 84 - PPTP client list

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

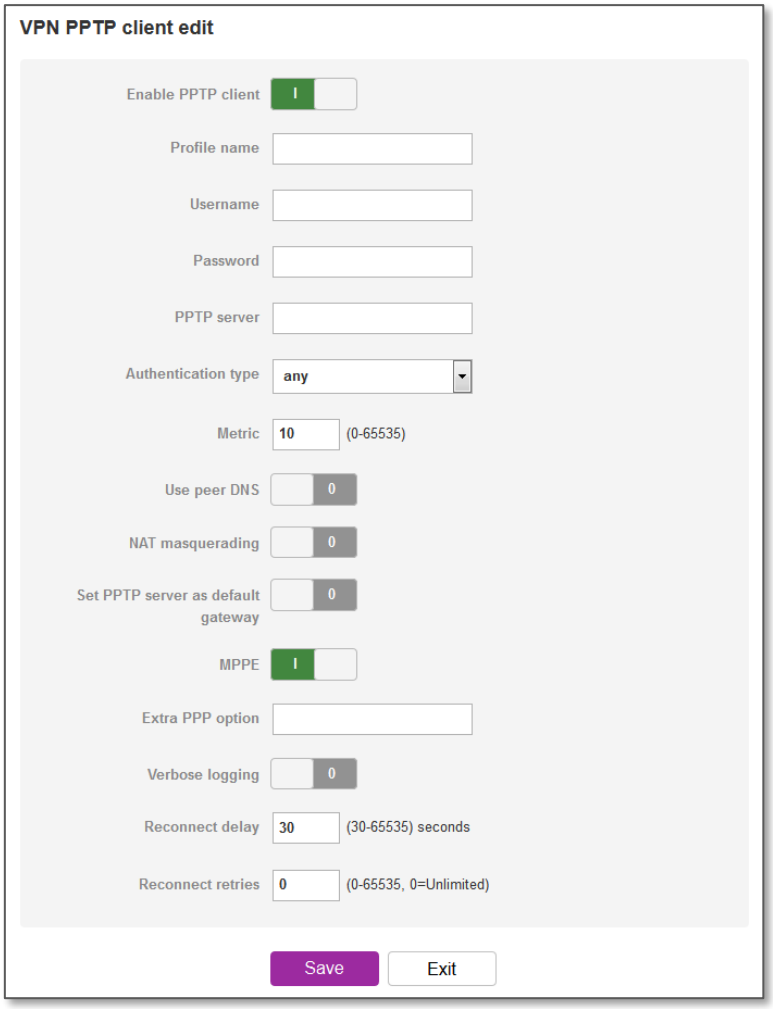


Figure 85 - VPN PPTP client edit

3 Click the **Enable PPTP client** toggle key to switch it to the **ON** position.

4 In the **Profile name** field**,** enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.

5 Use the **Username** and **Password** fields to enter the username and password for the PPTP account.

6 In the **PPTP server** field, enter the IP address/host domain name of the PPTP server.

7 From the **Authentication type** drop down list, select the Authentication type used on the server. If you do not know the authentication method used, select **any** and the router will attempt to determine the correct authentication type for you. There are 5 authentication types you can choose from:

- CHAP – uses a three way handshake to authenticate the identity of a client.
- MS-CHAP v1 – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista.
- MS-CHAP v2 - This is the Microsoft implementation of the Challenge Handshake Authentication Protocol which was introduced in Windows® NT 4.0 and is still supported today.

- PAP – The Password Authentication Protocol uses a password as a means of authentication and as such, is commonly supported. PAP is not recommended because it transmits passwords unencrypted and is not secure.
- EAP – Extensible Authentication Protocol. An Authentication protocol commonly used in wireless networks.

8 The **metric** value helps the router to prioritise routes and must be a number between 0 and 65535. The default value is 10 and should not be modified unless you are aware of the effect your changes will have.

9 The **Use peer DNS** option allows you to select whether the remote clients will use the Domain Name Server of the PPTP server. Click the toggle key to set this to ON or OFF as required.

10 **NAT masquerading** allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. Click the toggle key to switch this to the ON position if you want to use this feature.

11 Set **PPTP server as default gateway** sets all outbound data packets to go out through the PPTP tunnel. Click the toggle key to switch this to the ON position if you want to use this feature.

12 The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the **System Log** section of the router interface.

13 The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the PPTP server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the PPTP server with connection requests, while the maximum time to wait is 65335 seconds.

14 The **Reconnect retries** is the number of connection attempts that the router will make in the event that the PPTP connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.

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

GRE tunneling

The Generic Route Encapsulation (GRE) protocol is used in addition to Point-to-Point Tunneling Protocol (PPTP) to create VPNs (virtual private networks) between clients and servers or between clients only. Once a PPTP control session establishes the VPN tunnel GRE is used to securely encapsulate the data or payload.

Configuring GRE tunneling

To configure GRE tunneling:

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

Figure 86 - GRE client list

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

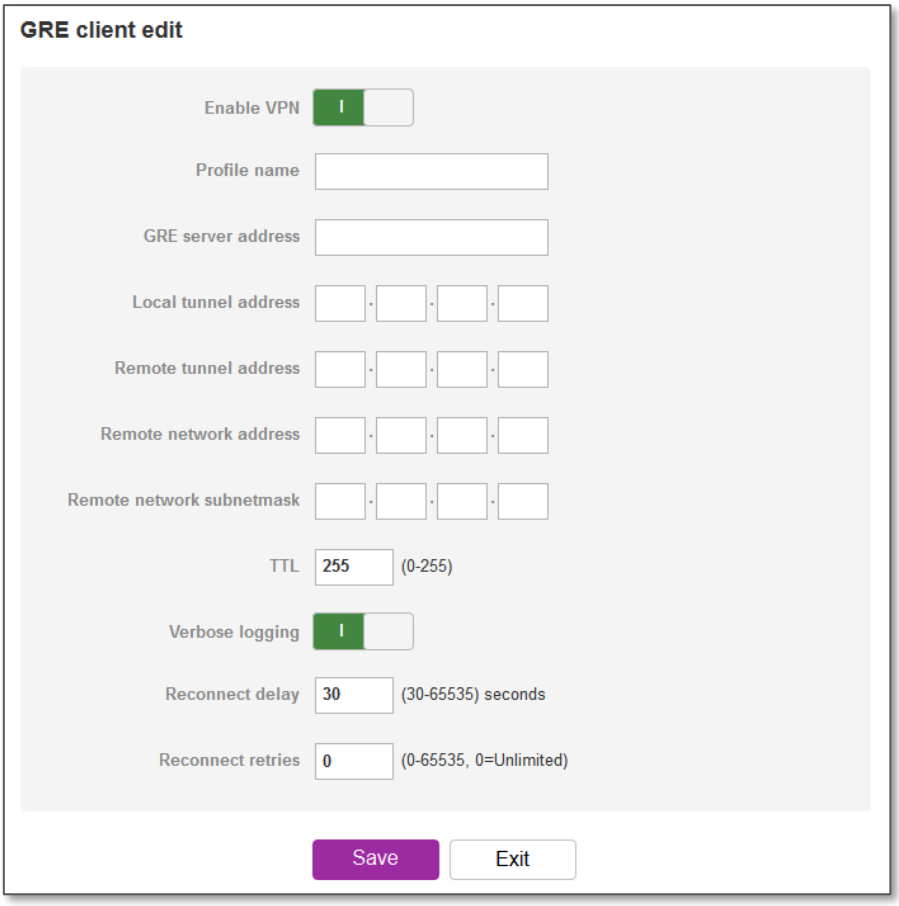


Figure 87 – GRE client edit

3 Click the **Enable GRE Tunnel** toggle key to switch it to the **ON** position.

4 In the **Profile name**, enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.

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

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

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

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

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

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

11 The **Verbose logging** option sets the router to output detailed logs regarding the GRE tunnel in the **System Log** section of the router interface.

12 The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the GRE server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the GRE server with connection requests, while the maximum time to wait is 65335 seconds.

13 The **Reconnect retries** is the number of connection attempts that the router will make in the event that the GRE connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.

14 Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save.

SCEP client

The Simple Certificate Enrolment Protocol (SCEP) is a popular protocol used to make the issuing of digital certificates as scalable as possible. It allows for a network user to request a digital certificate electronically and simply, removing the necessity for network administrators to provide input thereby freeing them up to perform more important tasks. The MachineLink 3G router includes an SCEP client allowing you to connect to an SCEP server.

To configure the SCEP client:

1 Click on the **SCEP client** toggle key so that it is in the **ON** position. Additional configuration options are displayed.

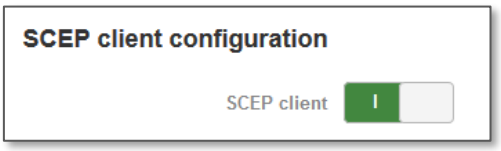


Figure 88 - SCEP client toggle key

2 In the **Server URL** field, enter the address of the SCEP server. Your network administrator will be able to provide this information.

Figure 89 - Server URL

3 If no CA certificates are displayed, select the **Query server** button.

4 When the certificates have loaded, use the **CA signature certificate** and **CA encryption certificate** drop down lists to select the appropriate certificates. You must select a certificate for both the signature and encryption certificate fields.

Figure 90 - CA signature and CA encryption certificates

5 In the **Challenge password** field, enter the password required to issue the certificate. This password may change at regular intervals. Your network administrator will be able to provide the password.

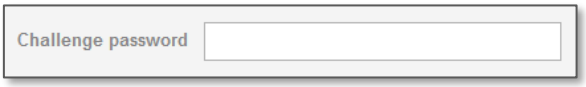


Figure 91 - Challenge password

6 In the **Renew before expiry (days)** field, enter the number of days before the certificate expires that the certificate should be renewed. If you do not wish to renew the certificate before expiry, set this to 0.

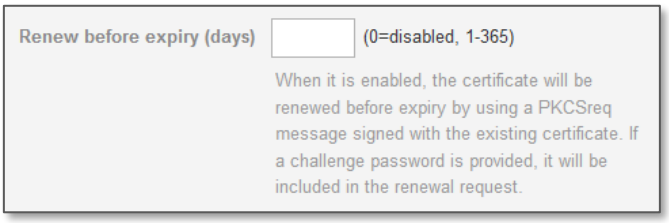


Figure 92 - Renew before expiry (days)

7 In the **Retry timer** field, enter the number of seconds that the SCEP client should wait before it attempts to query the server and download the issued certificate.

Figure 93 - Retry timer

8 The **Country (C)**, **State (S), Locality (L), Organisation (O), Organisational Unit (OU)** and **Common Name (CN)** fields comprise the Distinguished Name of the certificate being issued. Complete all fields to create the Distinguished Name.

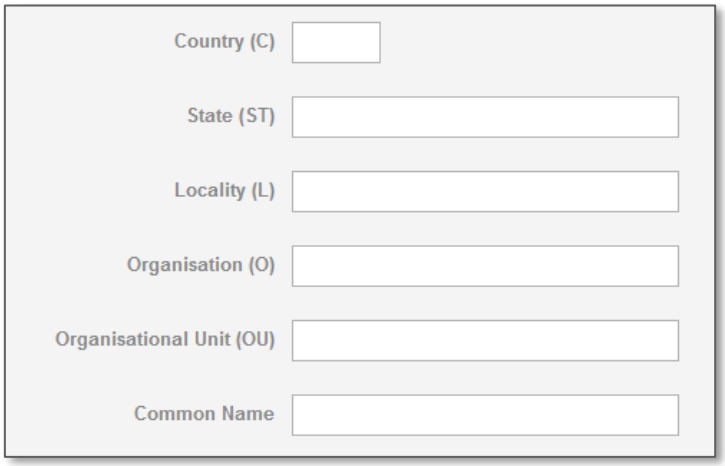


Figure 94 - Distinguished Name fields

Field name	Description
Country	The country code for the certificate. See the Server certificate section for a list of country codes.
State	The state for the certificate.
Locality	The locality for the certificate.
Organisation	The name of the organisation using the certificate.
Organisational Unit	Used to identify the organisational unit.
Common Name	Used to identify the connection to the server.

Table 18 - Distinguished Name field descriptions

9 Use the **Digest algorithm** field to select the cryptographic hash type to use for the certificate. This will depend on the SCEP server. If unsure, contact your IT administrator.

Figure 95 - Digest algorithm

10 Use the **Permitted string types** drop down list to select the strings allowed in the Distinguished Name fields.

Figure 96 - Permitted string types

11 When all the details have been entered, click the **Save** button. Wait for the period defined in the Retry timer field and then reload the page (e.g. by pressing F5 or clicking on the **SCEP client** menu item). If the SCEP server issues a certificate, it appears in the SCEP client certificate section. See below for an example screenshot.

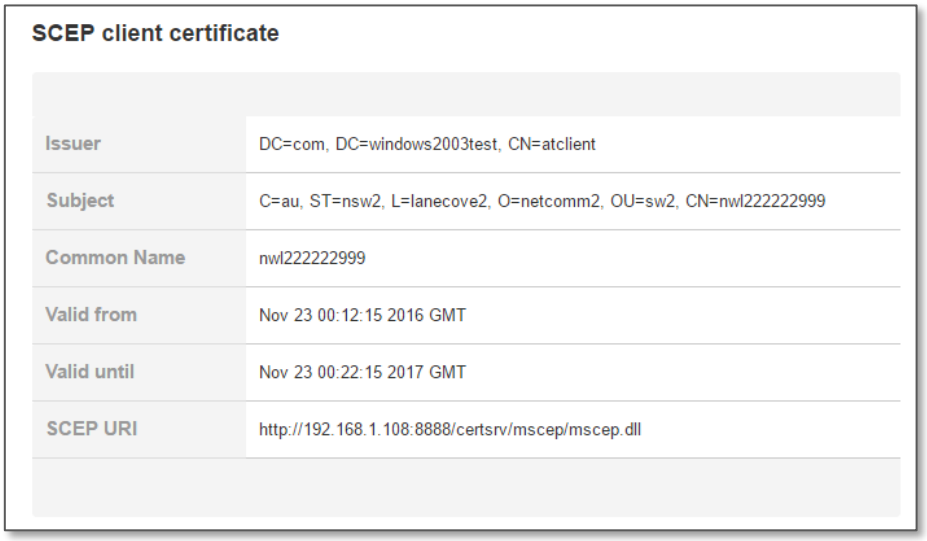


Figure 97 - SCEP client certificate

Services

Dynamic DNS

The DDNS page is used to configure the Dynamic DNS feature of the router. A number of Dynamic DNS hosts are available from which to select.

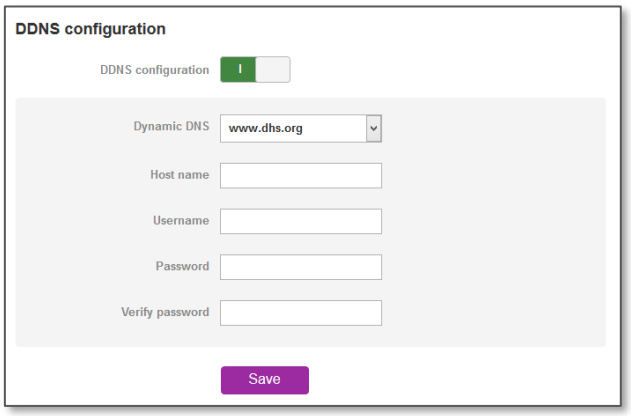


Figure 98 – Dynamic DNS settings

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

1. Click the **DDNS configuration** toggle key to switch it to the ON position.
2. From the **Dynamic DNS** drop down list, select the Dynamic DNS service that you wish to use. The available DDNS services available are:
   - www.dhs.org
   - www.dyndns.org
   - www.dyns.cx
   - www.easydns.com
   - www.justlinux.com
   - www.no-ip.com
   - www.ods.org
   - www.tzo.com
   - www.zoneedit.com
3. Enter a hostname in **Host name** field.

4 In the **Username** and **Password** fields, enter the logon credentials for your DDNS account. Enter the password for the account again in the **Verify password** field.

5 Click the **Save** button to save the DDNS configuration settings.

Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the Vodafone MachineLink 3G to synchronise its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded.

Any NTP server available publicly on the internet may be used. The default NTP server is 0.netcomm.pool.ntp.org.

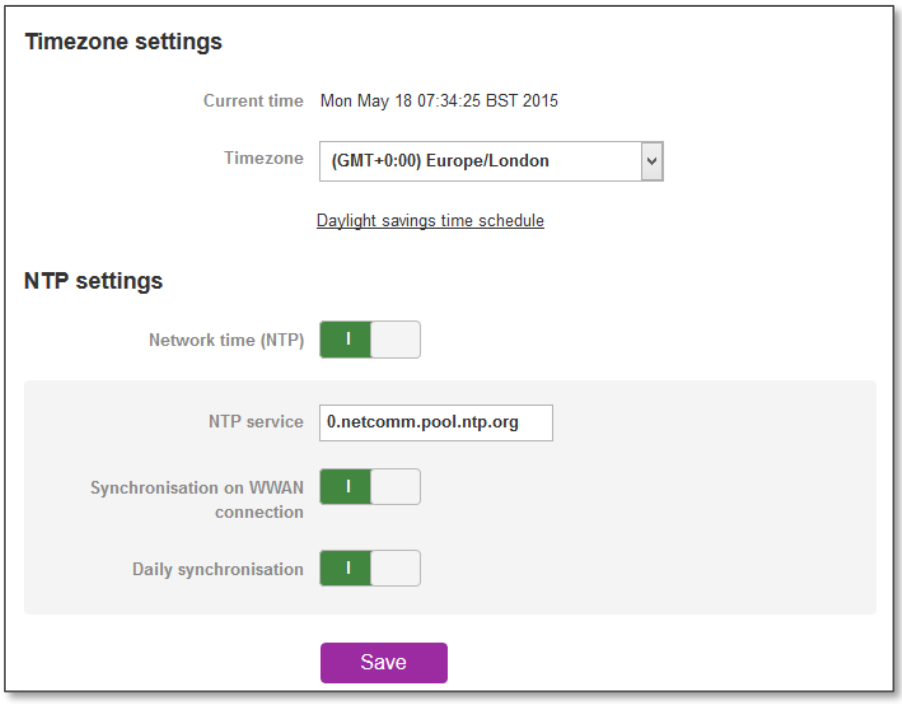


Figure 99 - NTP settings

Configuring Timezone settings

To configure time zone settings:

1. The **Current time** field shows the time and date configured on the router. If this is not accurate, use the **Timezone** drop down list to select the correct time zone for the router. If the selected zone observes daylight savings time, a **Daylight savings time schedule** link appears below the drop down list. Click the link to see the start and end times for daylight savings.
2. When you have selected the correct time zone, click the **Save** button to save the settings.

Configuring NTP settings

To configure NTP settings:

1. Click the **Network time (NTP)** toggle key to switch it to the **ON** position.
2. In the **NTP service** field, enter the address of the NTP server you wish to use.

3 The **Synchronisation on WWAN connection** toggle key enables or disables the router from performing a synchronisation of the time each time a mobile broadband connection is established.

4 The **Daily synchronisation** toggle key enables or disables the router from performing a synchronisation of the time each day.

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

SNMP

SNMP configuration

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

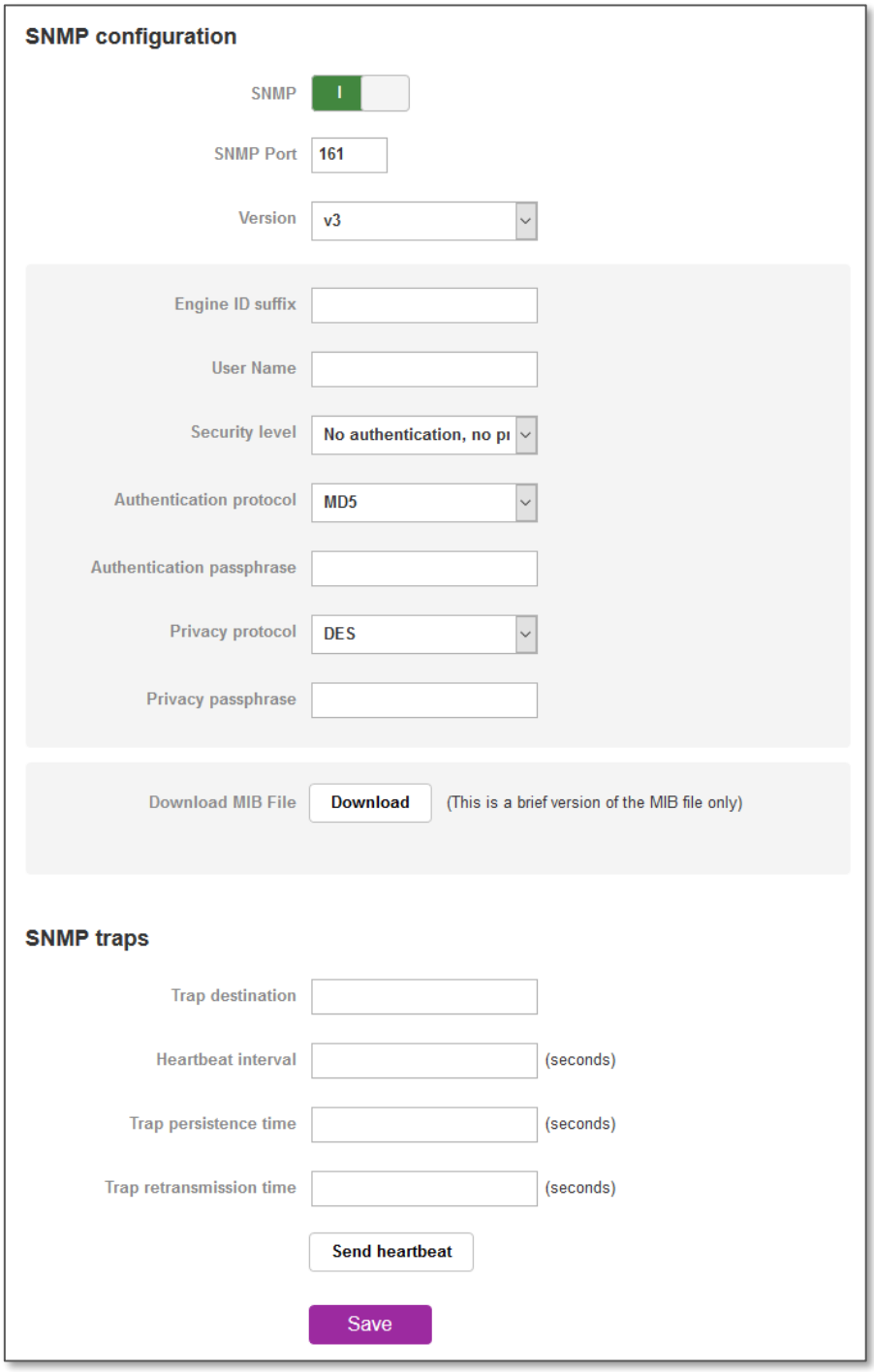


Figure 100 - SNMP configuration

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

Configuring SNMP

To configure SNMP:

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

v3 Configuration

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

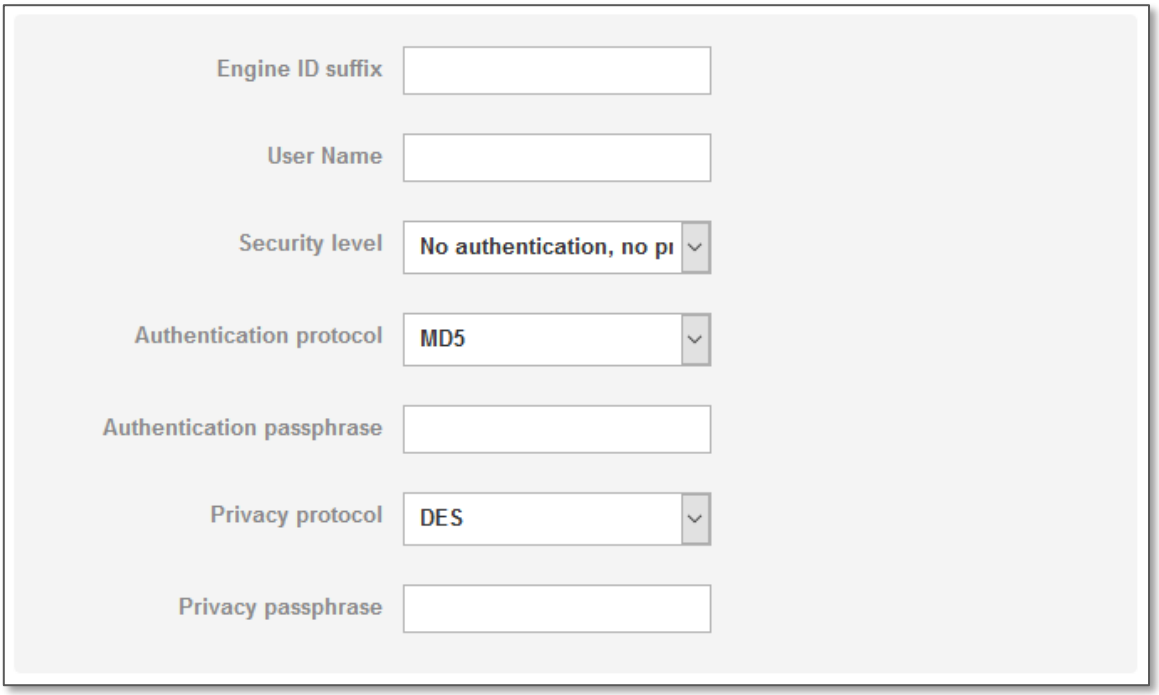


Figure 101 - SNMP v3 Configuration

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

Item	Description
Privacy passphrase	Select the privacy passphrase. This is only required if Security level is set to enforce privacy.

Table 19 - SNMP v3 Configuration

v1/v2 Configuration

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

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

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

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

SNMP traps

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

Configuring SNMP traps

To configure SNMP traps:

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

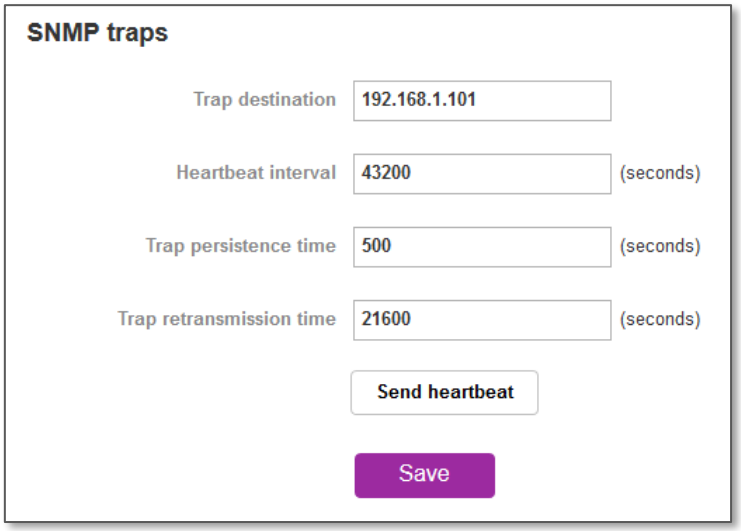


Figure 102 - SNMP traps

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

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

TR-069

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

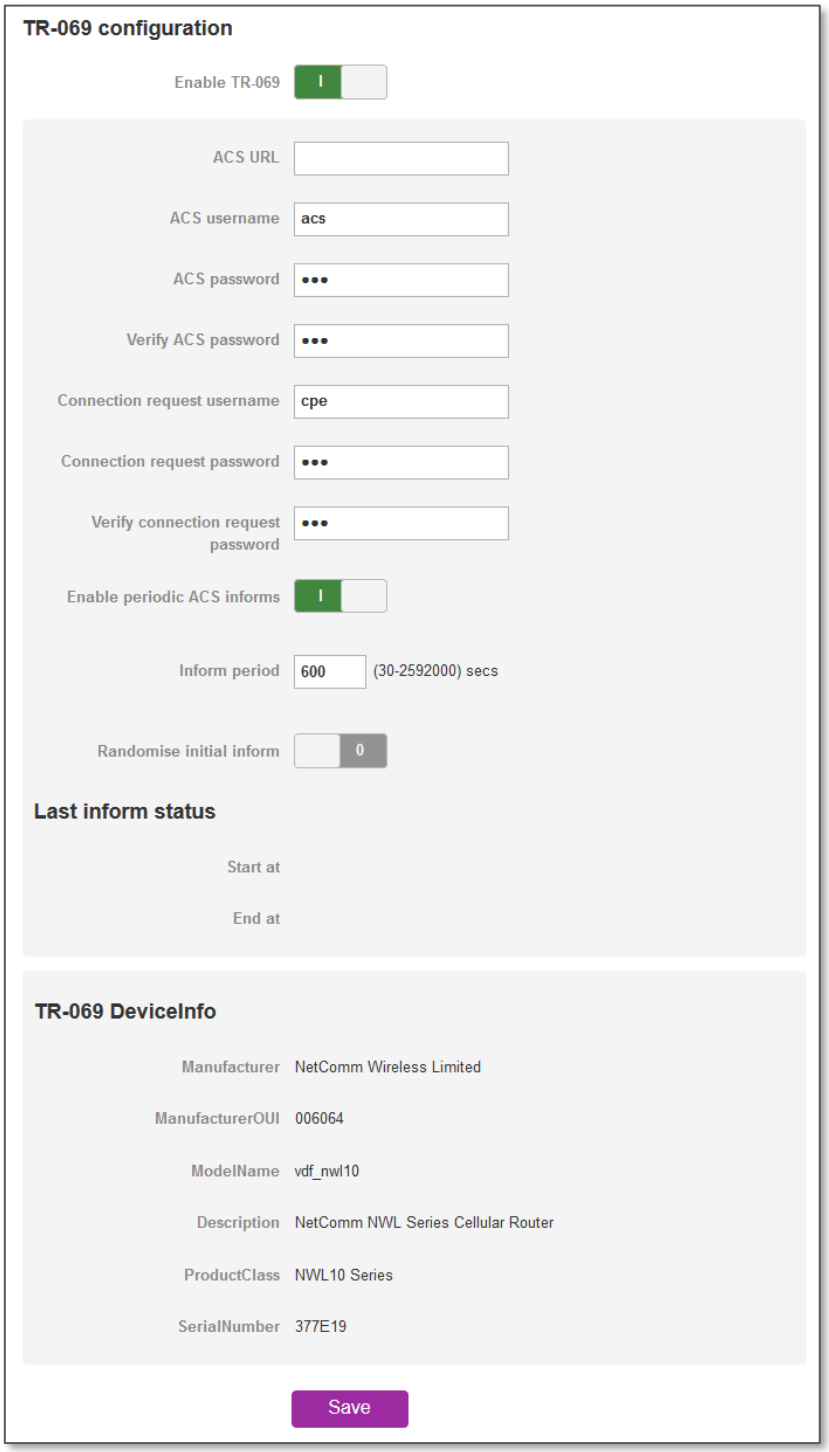


Figure 103 - TR-069 configuration

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

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

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

Note:

You must have your own compatible ACS infrastructure to use TR-069.

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

TR-069 configuration

To configure TR-069:

1. Click the **Enable TR-069** toggle key to switch it to the **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.
3. Use the **ACS username** field to specify the username for the Auto Configuration Server.
4. In the **ACS password** and **Verify ACS password** fields, enter the Auto Configuration Server password.
5. In the **Connection request username** field, enter the username to use for the connection requests.
6. In the **Connection request password** and Verify password fields, enter the connection request password.
7. The inform message acts as a beacon to inform the ACS of the existence of the router. Click the **Enable periodic ACS informs** toggle key to turn on the periodic ACS inform messages.
8. In the **Inform period** field, enter the number of seconds between the inform messages.
9. Enable **Randomize initial inform.**
10. Click the **Save** button to save the settings.

Event notification

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

Notification configuration

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

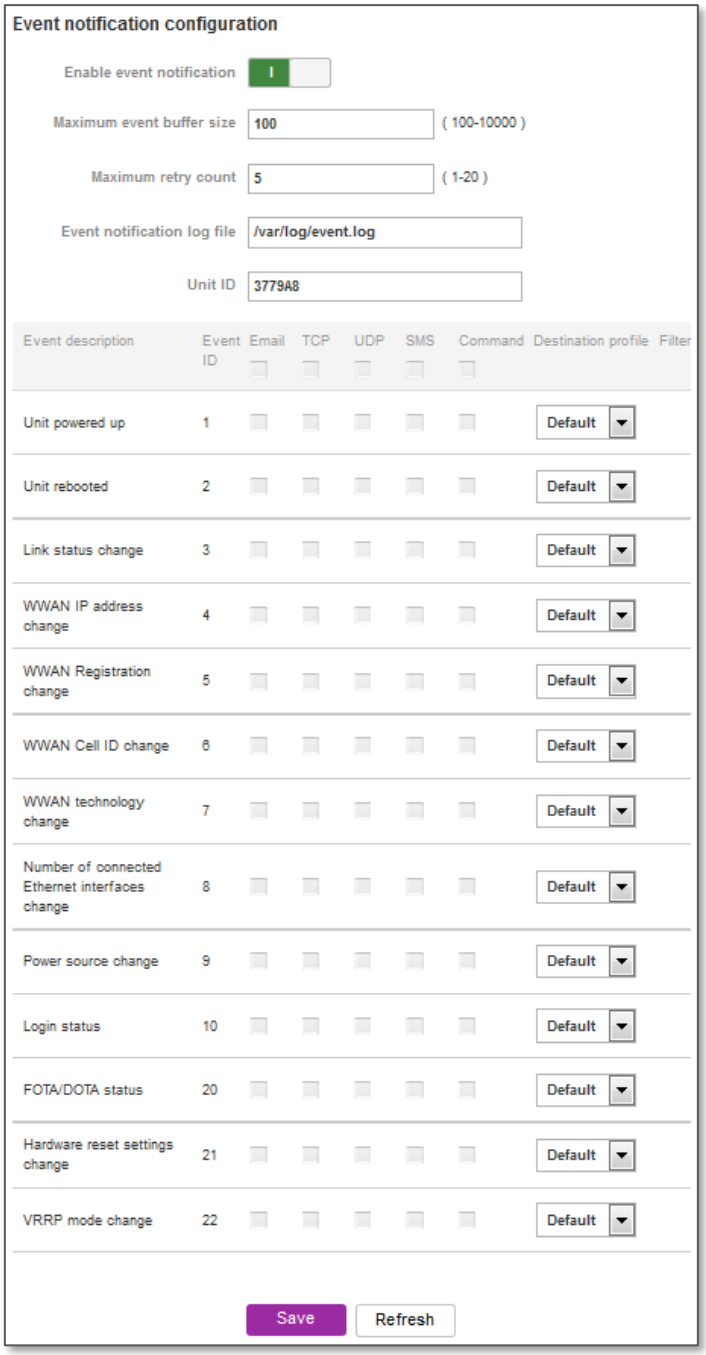


Figure 104 - Event notification configuration

Item	Description
Enable event notification	Toggles the event notification feature on and off.
Maximum event buffer size	Specifies the buffer size for event notifications which failed to be delivered or are yet to be sent. The minimum size is 100 and the maximum is 10000.
Maximum retry count	Specifies the maximum number of attempts that the router will make to deliver an event notification. The range is between 1 and 20.
Event notification log file	Specifies to the location and name of the file used to log the event notification activity.
Unit ID	The Unit ID field is used to specify an identifier for the router which is sent in the event notifications so that you know which router has an event. By default, the Unit ID field is configured with the last 6 characters of the MAC address of the router.

Table 20 - Event notification configuration options

Event types

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

Event	Event ID	Description	Example message
Unit powered up	1	Notification is sent when the unit is powered up through connection of a power source or after a soft-reset.	Power is up
Unit rebooted	2	Notification is sent when the unit is rebooted via Web UI, SMS diagnostics or via command line/telnet session.	Rebooting triggerred by internal application
Link status change	3	Notification is sent if the status of the data connection profile or any IPSec/OpenVPN/PPTP/GRE tunnel endpoint changes i.e. the link goes up or down.	Profile 1 WWAN status changed : down --> up
WWAN IP address change	4	Notification is sent if an active data connection profile's WWAN IP address changes.	WWAN IP address changed : N/A --> 10.103.4.149
WWAN Registration change	5	Notification is sent if the network registration status changed between "registered", "unregistered" or "roaming".	WWAN registration status changed : Not registered --> Registered to home network
WWAN Cell ID change	6	Notification is sent if the router connects to a different cell, marked by a changed in the Cell ID.	Cell ID changed : --> 15224145 Cell ID changed : 15224148 --> 15224145
WWAN technology change	7	Notification is sent if the router connects to a different network technology, e.g. 3G/2G.	WWAN network changed : N/A() --> 3G(UMTS) WWAN network changed : 3G(UMTS) --> 2G(GSM)
Number of connected Ethernet interfaces change	8	Notification is sent if there is a change to the number of directly connected Ethernet interfaces.	Ethernet device number changed : 0 --> 1
Power source change	9	Notification is sent if either the DC or POE is connected or disconnected.	Power source changed
Login status	10	Notification is sent if there was a failure to log in to the router via the Web UI.	WEBUI login failed, username root, password
FOTA/DOTA status	20	Notification is sent with the result of the Firmware Over-The-Air via SMS or TR-069.	FOTA/DOTA: upgrading firmware successful

Event	Event ID	Description	Example message
Hardware reset settings change	21	Notification is sent when the reset button is enabled or disabled in the web user interface.	Reset button is enabled
VRRP mode change	22	Notification is sent if a device configured as a slave becomes a master router or returns to slave status.	VRRP is in backup mode

Table 21 - Event notification – event types

Destinations

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

Configuring Event notification

To configure the event notification feature:

1. Click the **Services** menu item at the top of the screen. From the **Event notification** menu on the left of the screen, select the **Destination configuration** menu item.
2. Click the **+Add** button at the top right corner of the window. The Event destination profile edit screen is displayed.
3. In the **Destination name** field enter a name for the destination profile then enter the contact details for the each type of destination i.e. Email address, TCP address and port, UDP address and port and/or SMS number.

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

4. Click the **Save** button when you have entered the required details.
5. From the **Event notification** menu on the left of the screen, select the **Notification configuration** menu item.
6. Select the **Enable event notification** toggle key to turn it to the **ON** position.
7. If desired, set the **Maximum event buffer size**, **Maximum retry count**, **Event notification log file** and **Unit ID** fields. See table 22 for descriptions of these options.
8. From the **Destination profile** column, use the drop down menus to select the desired destination profiles to use for the corresponding events, then select the checkboxes for the types of notifications to send to the chosen destination profile. If the Destination profile does not contain the required contact details, you are notified when you click the Save button.
9. Click the **Save** button.

Destination configuration

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

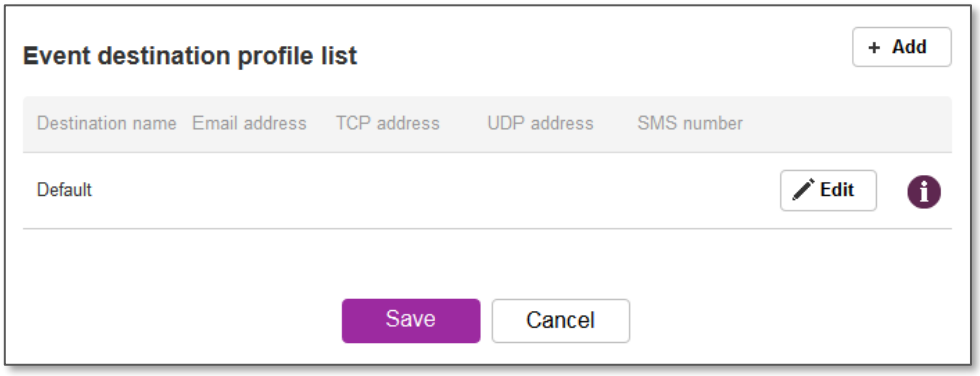


Figure 105 - Event destination profile list

To add a new destination profile:

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

To edit a destination profile:

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

To delete a destination profile:

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

Clicking the button next to any destination profile displays a list of event notifications which are linked to that profile.

Email settings

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

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

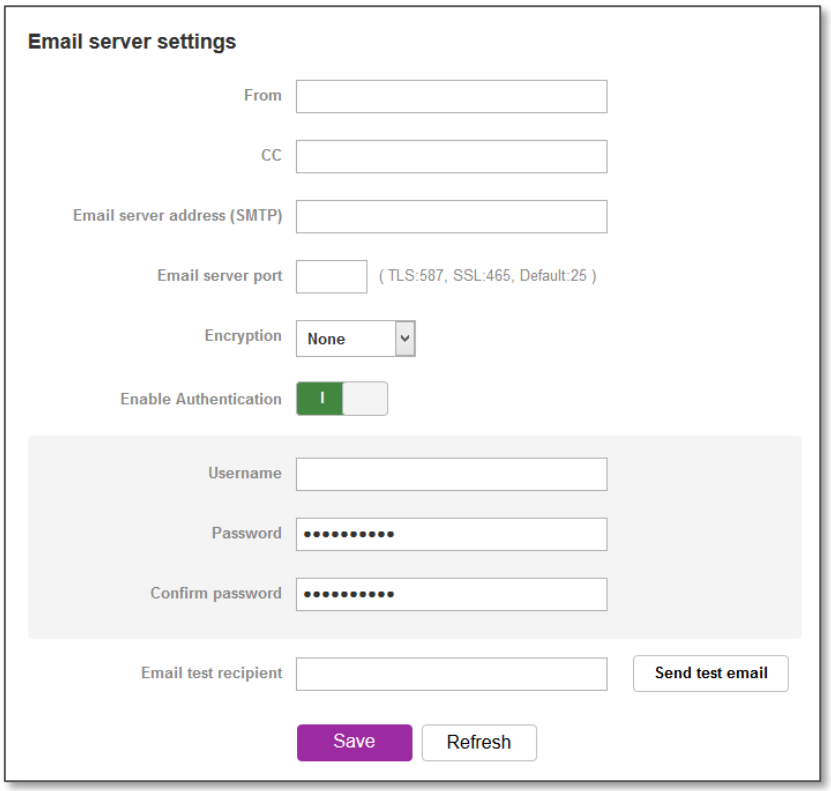


Figure 106 - Email client settings

Item	Description
From	Enter the email address of the account you will be using to send emails.
CC	(Optional) Enter an email address which will be copied on all messages sent.
Email server address (SMTP)	Enter the SMTP server address of the email server. This may be an IP address or a hostname.
Email server port	Enter the Email server's SMTP port.
Encryption	Choose from SSL or STARTTLS encryption methods or select None to use no encryption. The main point of difference between SSL and STARTTLS is that SSL opens a secure connection first, and then begins the SMTP transaction. STARTTLS starts the SMTP transaction and then looks for support for TLS in the response message.
Username	Enter the username of the account to be used for sending emails.
Password	Enter the password of the account to be used for sending emails.
Confirm password	Enter the password of the account to be used for sending emails once more for confirmation.

Item	Description
Email test recipient	Enter an email address to send a test message to, then click the **Send test email** button.

Table 22 - Email client settings

SMS messaging

The Vodafone MachineLink 3G offers an advanced SMS feature set, including sending messages, receiving messages, redirecting incoming messages to another destination, as well as supporting remote commands and diagnostics messages.

Some of the functions supported include:

- Ability to send a text message via a 2G/3G network and store it in permanent storage
- Ability to receive a text message via a 2G/3G network and store it in permanent storage
- Ability to forward incoming text messages via a 3G network to another remote destination which may be a TCP/UDP server or other mobile devices
- Ability to receive run-time variables from the device (e.g. uptime) on request via SMS
- Ability to change live configuration on the device (e.g. connection APN) via SMS
- Ability to execute supported commands (e.g. reboot) via SMS
- Ability to trigger the Vodafone MachineLink 3G to download and install a firmware upgrade
- Ability to trigger the Vodafone MachineLink 3G to download and apply a configuration file

To access the SMS messaging functions of the Vodafone MachineLink 3G, click on the **Services** menu item from the top menu bar, and then select one of the options under the **SMS messaging** section on the left hand menu.

Setup

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

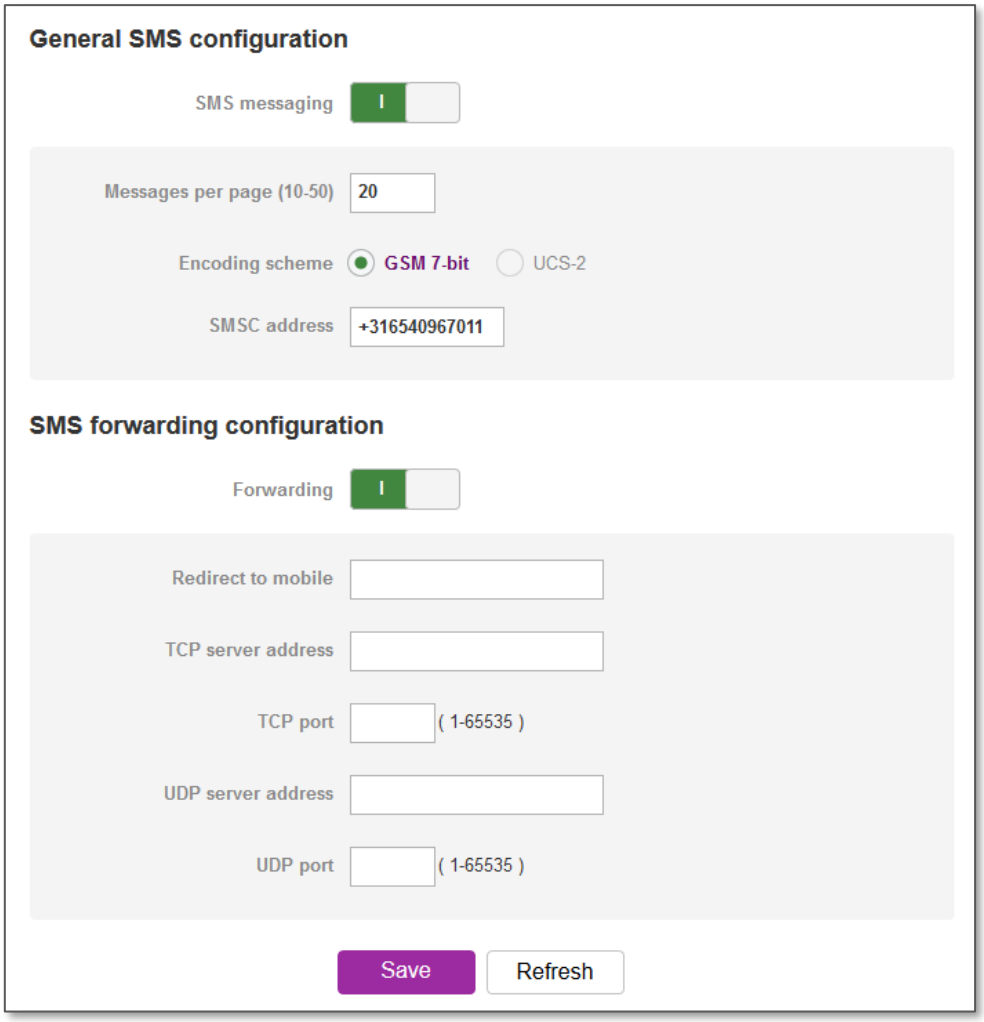


Figure 107 - General SMS Configuration

Option	Definition
General SMS configuration	
SMS messaging	Toggles the SMS functionality of the router on and off.
Messages per page (10-50)	The number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding scheme	The encoding method used for outbound SMS messages. GSM 7-bit mode permits up to 160 characters per message but drops to 50 characters if the message includes special characters. UCS-2 mode allows the sending of Unicode characters and permits a message to be up to 50 characters in length.
SMSC address	The short message service centre (SMSC) address is the number of your mobile broadband SMS provider. The SMSC address is used when sending text messages and is stored on the SIM card. If the SMSC address field is blank, the router will not be able to send any SMS messages.

Option	Definition
Routing Option	Allows you to configure the method used to route SMS messages. **Packet-switched:** Uses the switched IP packet network to deliver messages. Messages are broken up into packets and transmitted through the network independently, then re-assembled when they reach the destination. In packet switched networks, network links are shared by packets from multiple competing communication sessions. Packet switching generally results in a lower quality of service compared with circuit switched networks because the packets may take different routes to the destination and cause delay in their re-assembly. **Circuit-switched:** Creates a route with reserved bandwidth from the source to the destination, emulating a physical connection with an electrical circuit. Data transmitted in a circuit switched network is delivered in order and has a constant bit delay meaning the service is predictable and reliable. **Packet-switched preferred:** Attempts to use the packet-switched network for SMS delivery but fails over to the circuit-switched network if messages are undeliverable. **Circuit-switched preferred:** Attempts to use the circuit-switched network for SMS delivery but fails over to the packet-switched network if messages are undeliverable.
SMS forwarding configuration	
Forwarding	Toggles the SMS forwarding function of the router on and off.
Redirect to mobile	Enter a mobile number as the destination for forwarded SMS messages.
TCP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP.
TCP port	The TCP port on which to connect to the remote destination.
UDP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP.
UDP port	The UDP port on which to connect to the remote destination.

Table 23 - SMS Setup Settings

SMS forwarding configuration

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

Redirect to mobile

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

For Example:

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

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

Redirect to TCP / UDP server address

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

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

For Example:

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

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

New message

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

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

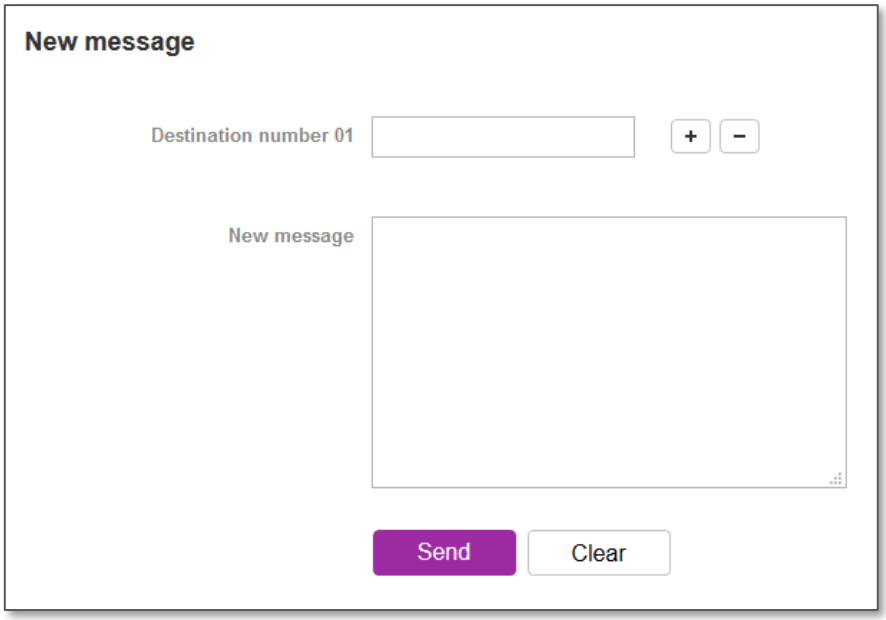


Figure 108 - SMS - New Message

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

For example:

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

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

Inbox / Sent Items

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

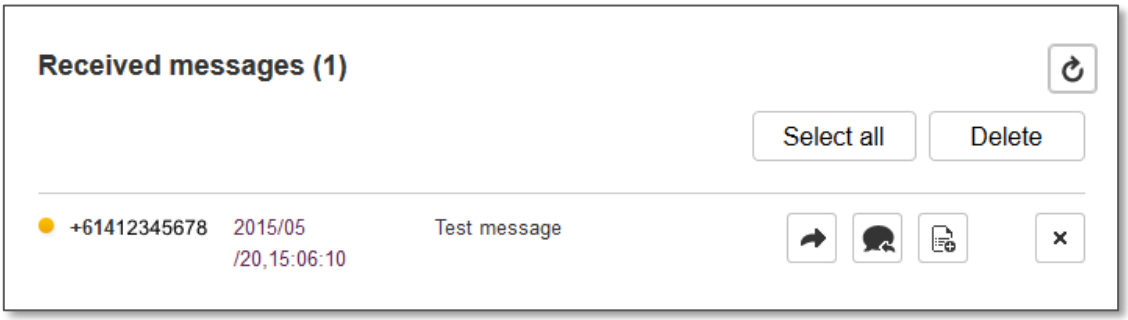


Figure 109 - SMS Inbox

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

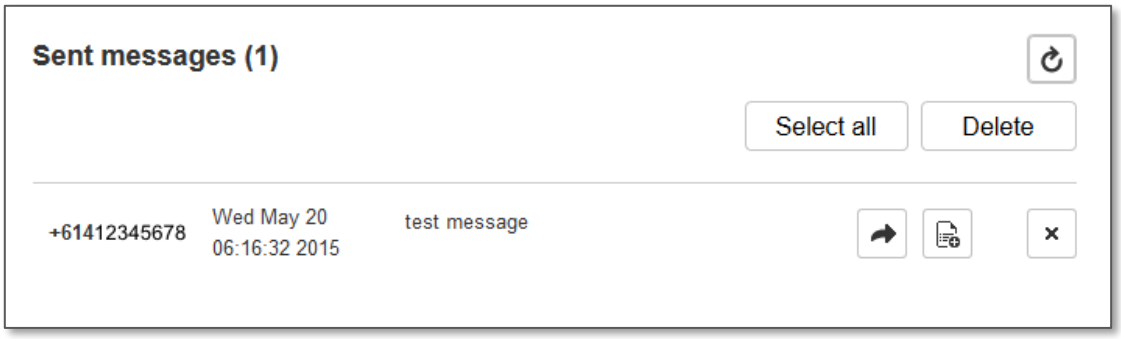


Figure 110 - SMS Outbox

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

Table 24 - Inbox/Outbox icons

Diagnostics

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

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

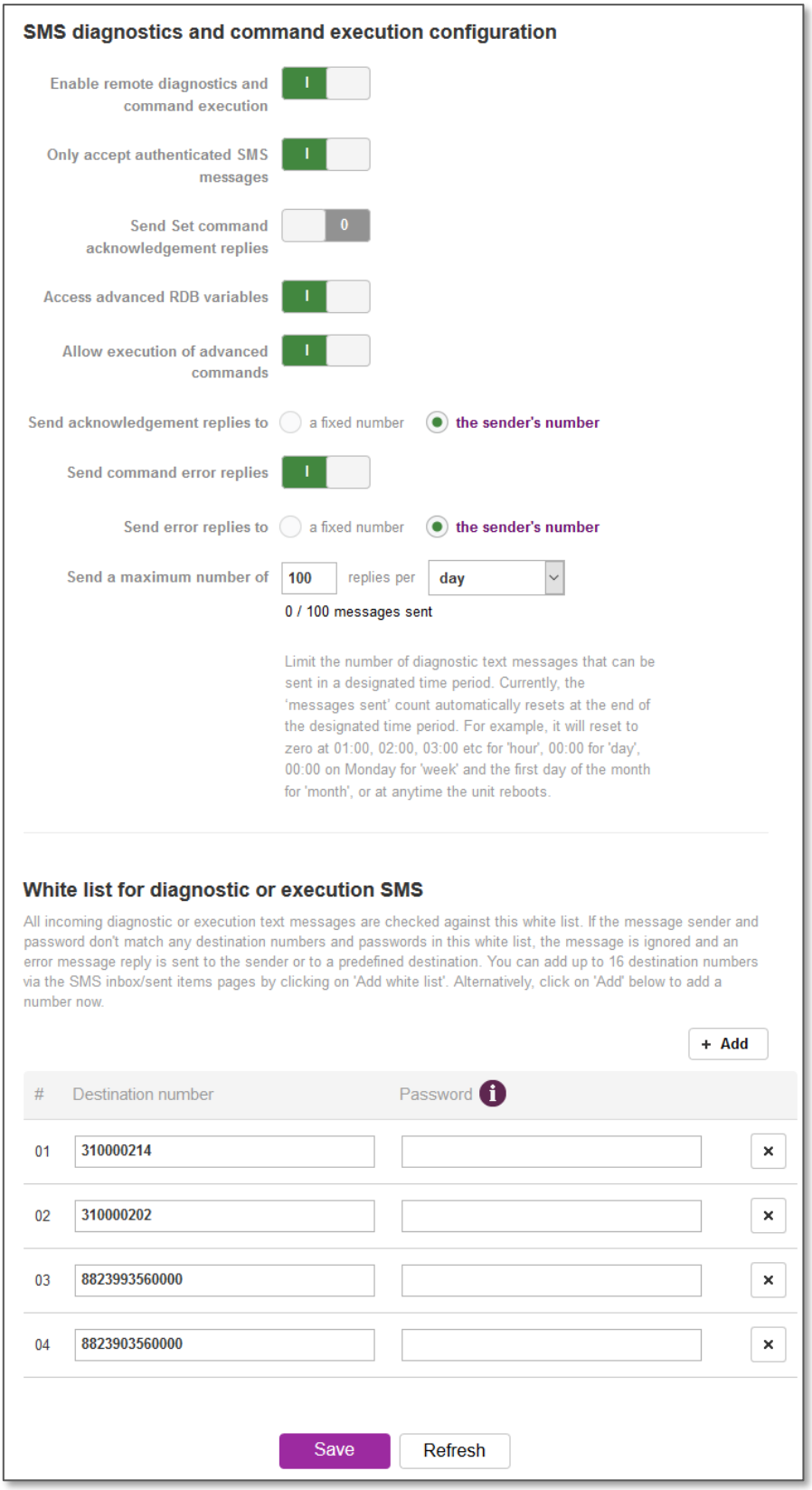


Figure 111 - SMS diagnostics and command execution configuration

SMS diagnostics and command execution configuration

The options on this page are described below.

Enable remote diagnostics and command execution

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

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

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

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

Only accept authenticated SMS messages

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

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

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

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

Send Set command acknowledgement replies

The Vodafone MachineLink 3G router will automatically reply to certain types of commands received, such as *get* commands, or *execute* commands. However acknowledgement replies from the Vodafone MachineLink 3G router are optional with *set* commands and the *Wakeup* command. This option Enables or disables sending an acknowledgment message after execution of a *set* command or SMS Wakeup command. If disabled, the router does not send any acknowledgement after execution of a *set* command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.

Access advanced RDB variables

By default, this option is turned on and allows access to the full list of RDB variables via SMS. When it is turned off, you are only allowed access to the basic RDB variables listed later in this guide.

Allow execution of advanced commands

By default, this option is turned on and allows execution of advanced commands such as those which are common to the Linux command line. For example: “execute ls /usr/bin/sms*” to list the contents of the /etc folder on the router.

When it is turned off you are only allowed to execute the basic commands listed later in this guide.

Send acknowledgement replies to

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

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

Fixed number to send replies to

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

Send command error replies

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

Send error replies to

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

Send a maximum number of

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

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

White list for diagnostic or execution SMS

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

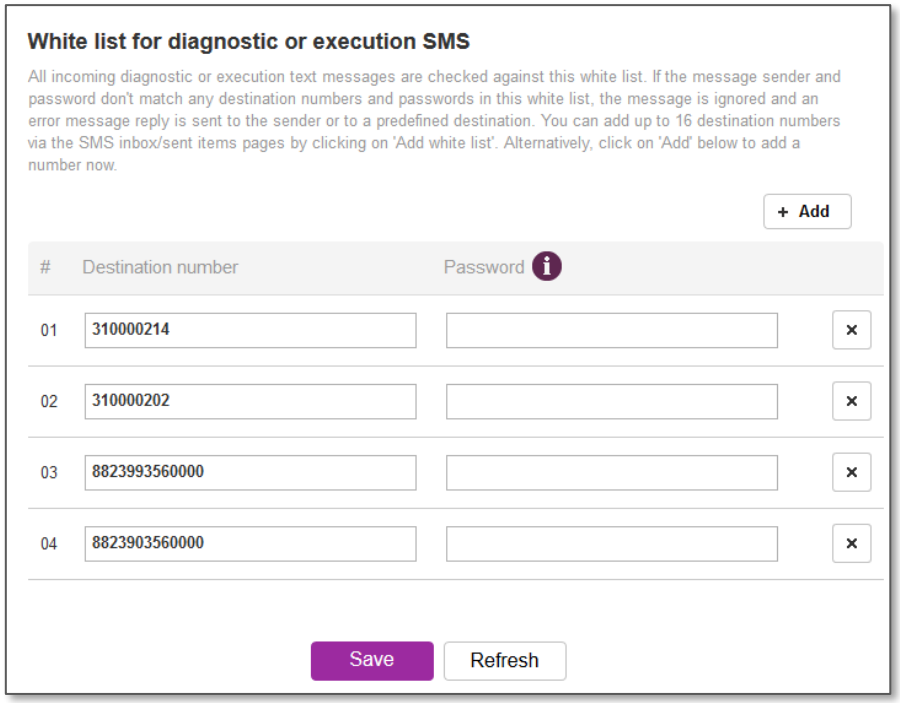


Figure 112 - White list for diagnostic or execution SMS

Up to 20 numbers may be stored in the white list, however, when using a Vodafone GDSP SIM, 4 entries are reserved for system numbers and may not be removed. To add a number to the white list, click the "**+Add**" button.

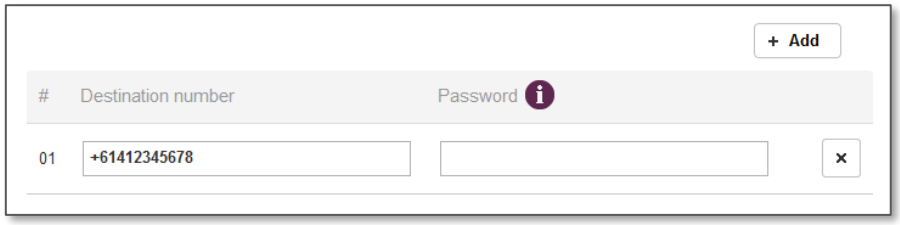


Figure 113 – Adding a number to the SMS white list

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

- Be a minimum of 8 characters and no more than 128 characters in length.
- Contain at least one upper case, one lower case character and one number.
- Contain at least one of the following special characters: !*()?/

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

Sending an SMS Diagnostic Command

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

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

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

5. Click the **Save** button.

Types of SMS diagnostic commands

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

- execute COMMAND
- get VARIABLE
- set VARIABLE=VALUE

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

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

The following are some examples of SMS diagnostic commands:

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

SMS acknowledgment replies

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

SMS command format

Generic Format for reading variables:

```
get VARIABLE
PASSWORD get VARIABLE
```

Generic Format for writing to variables:

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

Generic Format for executing a command:

```
Execute COMMAND
PASSWORD execute COMMAND
```

Replies

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

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

Table 25 - SMS Diagnostic Command Syntax

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

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

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

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

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

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

For Example:

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

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

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

For Example:

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

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

“PASSWORD get Variable1”; “get VARIABLE2”

“PASSWORD set VARIABLE1=VALUE1”; “set VARIABLE2=VALUE2”

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

For Example:

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

Note – Commands, variables and values are case sensitive.

List of basic commands

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

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

Item		Definition
1	reboot	Immediately performs a soft reboot.
2	pdpcycle	Disconnects (if connected) and reconnects the data connection. If a profile number is selected in the command, try to disconnect/reconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect/reconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
3	pdpdown	Disconnects the PDP. If a profile number is selected in the command, the router tries to disconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
4	pdpup	Reconnects the PDP. If a profile number is selected in the command, the router tries to connect with the specified profile. If no profile number is selected, the router tries to connect to the last active profile. The gateway will check the currently activated profile and disconnect this profile before executing the command. The router reports an error if no profile number is selected and there is no stored last active profile number.
5	factorydefaults	Performs a factory reset on the router. Be aware that this command also clears the SMS white list on the router.

Item		Definition
6	download	Performs a download and install of a Firmware Upgrade (.cdi), Config File (.tar.gz) or a help document (.pdf) file. If the file is a firmware image as in the case of a .cdi file, the router will apply the recovery image first and then the main firmware image. The download location is specified immediately after the command and may be from an HTTP or FTP source URL. If the file is a .cdi file, the router will apply the file as a configuration file update for the device and reboot afterwards. If the file is a .pdf, the router will assume this is a user guide document and save it to the router and make the file available for viewing via the help menu on the Web-UI. Note: If your download URL includes any space characters, please encode these prior to transmission according to RFC1738, for example: ftp://username:password@serveraddress/directory%20with%20spaces/filename.cdi Note: Authenticated FTP addresses may be used following the format as defined in RFC1738, for example: ftp://username:password@serveraddress/directory/filename.cdi
7	codconnect	Causes the router to activate the PDP context when the Connect on demand feature is enabled.
8	coddisconnect	Causes the router to de-activate the PDP context when the Connect on demand feature is enabled.
10	ssh.genkeys	Instructs the router to generate new public SSH keys.
11	ssh.clearkeys	Instructs the router to clear the client public SSH key files.

Table 26 - List of basic SMS diagnostic commands

List of get/set commands

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

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

Command name	Example	Description
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.

Command name	Example	Description
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 and “3” is the Mobile Network Code for Vodafone. 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, telstra.internet, test	Sets the PPPoE status on, APN to telstra.internet, and service name to test.

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

Table 27 - List of get/set commands

List of basic RDB variables

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

#	RDB variable name	SMS variable name	Read/Write	Description	Example VALUE
0	link.profile.1.enable link.profile.1.apn link.profile.1.user link.profile.1.pass link.profile.1.auth_type link.profile.1.iplocal link.profile.1.status	profile	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,apn,username,password, chap,202.44.185.111,up Write: (apn, user, pass,auth) apn,username,password
2	link.profile.1.user	username	RW	Cellular broadband username	Guest, could also return “null”
3	link.profile.1.pass	password	RW	Cellular broadband password	Guest, could also return “null”
4	link.profile.1.auth_type	authtype	RW	Cellular broadband Authentication type	”pap” or”chap”
5	link.profile.1.iplocal	wanip	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rssi	R	Cellular signal strength	-65 dBm
7	wwan.0.imei	imei	R	IMEI number	357347050000177
8	statistics.usage_current	usage	R	Cellular broadband data usage of current session	“Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes” or “Rx 0 byte, Tx 0 byte, Total 0 byte” when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current cellular broadband session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current band	WCDMA850

Table 28 - List of basic SMS diagnostics RDB variables

Network scan and manual network selection by SMS

Performing a network scan

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

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

- MCC

- MNC
- Network Type (LTE, 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
```

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

Table 29 - Network types 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.

Table 30 - Operator status codes returned by get plmnscan SMS command

Notes about the network connection status when using the **get plmnscan** command:

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=505,3
```

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

```
set forceplmn=505,3,7
```

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

Notes about the **set forceplmn** command:

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:

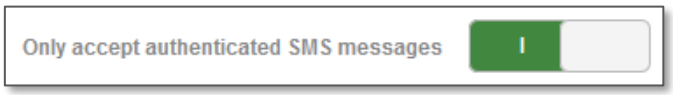
```
Automatic,505,3
```

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

SMS diagnostics examples

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

If the default setting of **Only accept authenticated SMS messages** is enabled:



Password authentication is required. Add your password followed by a space as a prefix to the command, for example

If authentication required:

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

If authentication not required:

```
set username=’NetComm’
```

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

Description	Input Command (without *PASSWORD* prefix)
Send SMS to change the data connection username	set username=’NetComm’
Send SMS to change the data connection password	set password= `NetComm`
Send SMS to change the data connection authentication	set authtype= ‘pap’
Send SMS to reboot	execute reboot
Send SMS to check the WAN IP address	get wanip
Send SMS to check the mobile signal strength	get rssi
Send SMS to check the IMEI number	get imei
Send SMS to check the current band	get band
Send SMS to Disconnect (if connected) and reconnect the data connection	execute pdpcycle
Send SMS to disconnect the data connection	execute pdpdown
Send SMS to connect the data connection	execute pdpup
Send multiple get command	get wanip; get rssi
Send multiple set command	set ssh.genkeys=1; set username=test; set auth=pap
Send SMS to reset to factory default settings	execute factorydefaults
Send SMS to retrieve status of router	get status
Send SMS to retrieve the history of the session, including start time, end time and total data usage	get sessionhistory
Send SMS to configure the router to send syslog to a remote syslog server	set syslogserver=123.209.56.78
Send SMS to 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 https://download.com:8080/firmware_image.cdi execute download https://download.com:8080/firmware_image_r.cdi

Description	Input Command (without *PASSWORD* prefix)
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 https://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

Table 31 - SMS diagnostics example commands

Network quality

The Network quality page provides some basic diagnostic information regarding the speed and quality of your cellular network connection. To perform a network quality test, click the **Refresh** button. The network quality test can take a few minutes to complete.

This test can be initiated remotely by an SMS command. See SMS Diagnostics examples.

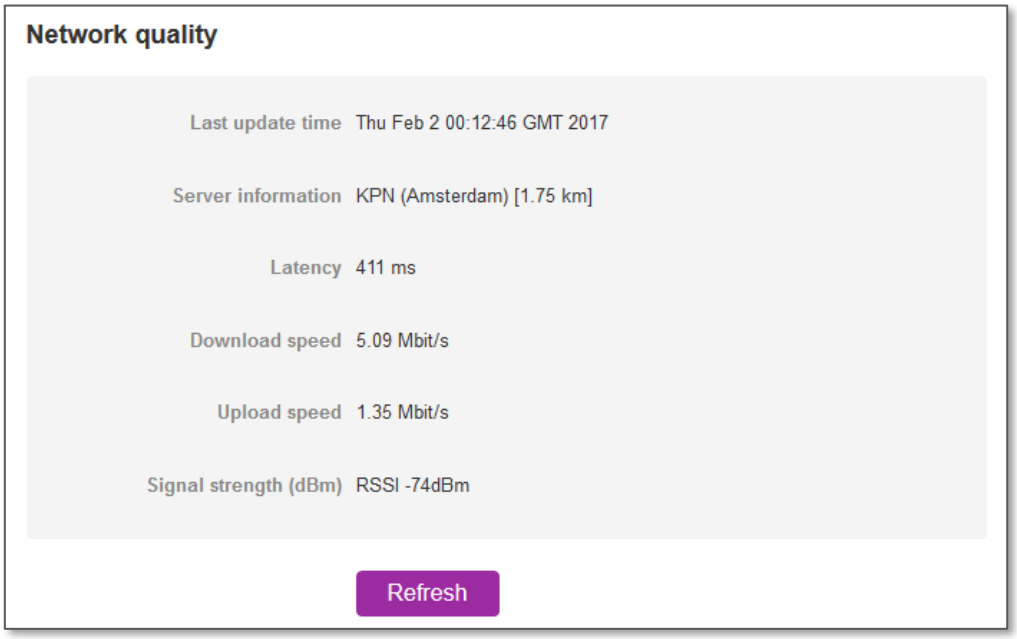


Figure 114 – Network quality test result page

Item	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.
Latency	Latency limits the maximum rate, expressed 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 speed achieved between the server and the router, measured in megabits per second (Mbit/s).
Upload speed	Average 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: ▪ **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).

Item	Description
Refresh	When the **Refresh** button is clicked, the router performs 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.

Table 32 – Network quality test result details

System

Log

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

System log

The System Log enables you to troubleshoot any issues you may be experiencing with your MachineLink 3G router. To access the System Log page, click on the **System** menu. The System Log is displayed.

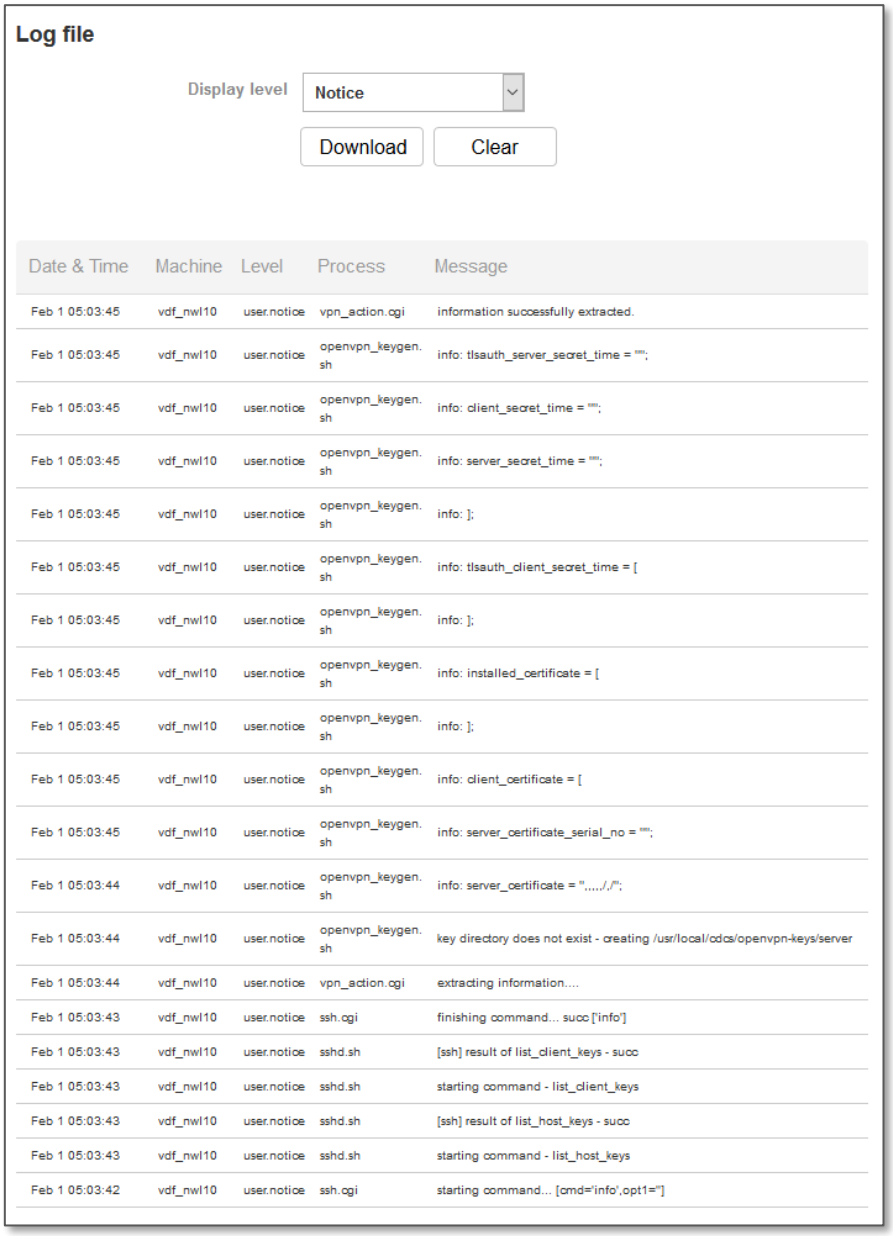


Figure 115 - System log page

Log file

The **Log capture level** drop down list lets you select the level of logs that are written to the log file. Set the level that you would like to capture first, then set the **Display level** since the Display level chosen filters only the messages that are captured.

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

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

1 Enable the Log to non-volatile memory option

2 Use a remote syslog server

Enable log to non-volatile memory

When the router is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the router. Up to 512kb of log data will be stored before it is overwritten by new log data. Flash memory has a finite number of program-erase operations that it may perform to the blocks of memory. While this number of program-erase operations is quite large, we recommend that you do not enable this option for anything other than debugging to avoid excessive wear on the memory.

Use a remote syslog server

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

To configure the MachineLink 3G to output log data to a remote syslog server:

1. Click on the **System** menu from the top menu bar. The System log item is displayed.
2. Under the **Remote syslog server** section, enter the IP address or hostname of the syslog server in the **IP / Hostname [:PORT]** field. You can also specify the port number after the IP or hostname by entering a colon and then the port number e.g. 192.168.1.102:514. If you do not specify a port number, the router will use the default UDP port 514.
3. Click the **Save** button to save the configuration.

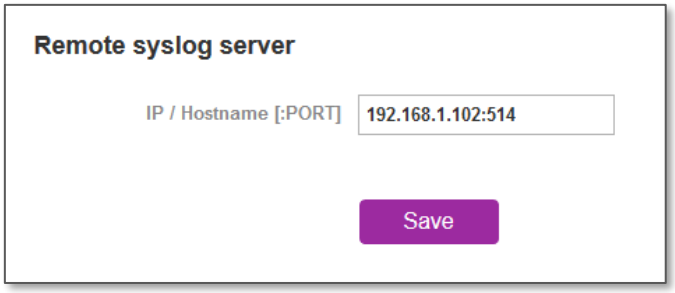


Figure 116 – Remote syslog server configuration

Log capture level

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

Log levels

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

Table 33 - System log detail levels

IPSec log

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

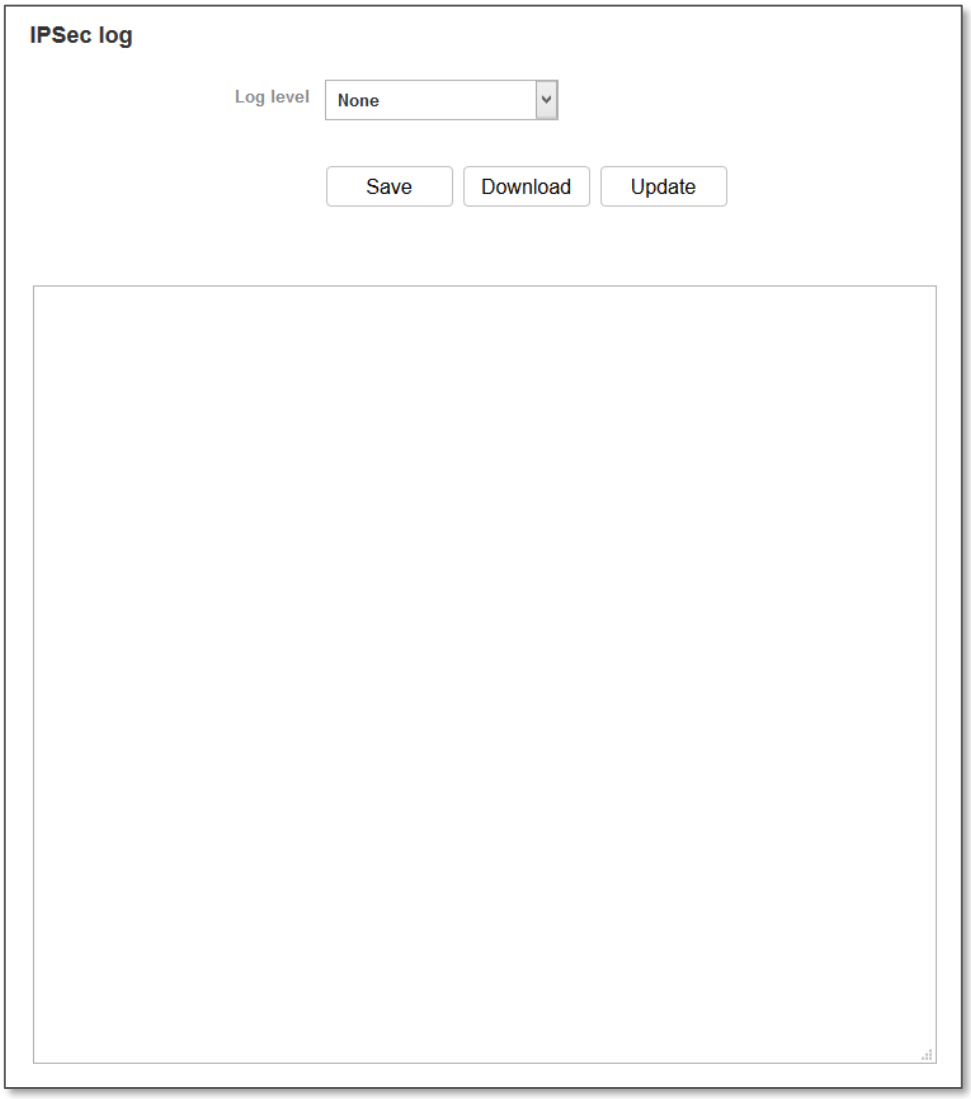


Figure 117 - IPSec log

Use the **Log level** drop down list to specify the type of detail you want to capture in the log and then click the **Save** button. When you change the logging level, any active IPSec VPN tunnels will be disconnected as a change in logging level requires the IPSec service to be restarted. The **Update** button forces a refresh of the display to show any entries since the display was last loaded. To download the IPSec log, click the **Download** button and you will be prompted to save the file.

Event notification log

The Event notification log displays a history of the notifications that have been triggered. You can download the log file or manually force the log to be updated using the provided buttons. The Clear button clears the Event notification history window and also clears the number of events displayed on the **Status** page. The Event notification section of the Status page shows the number of events that have been triggered and provides a link to this Event notification history window.

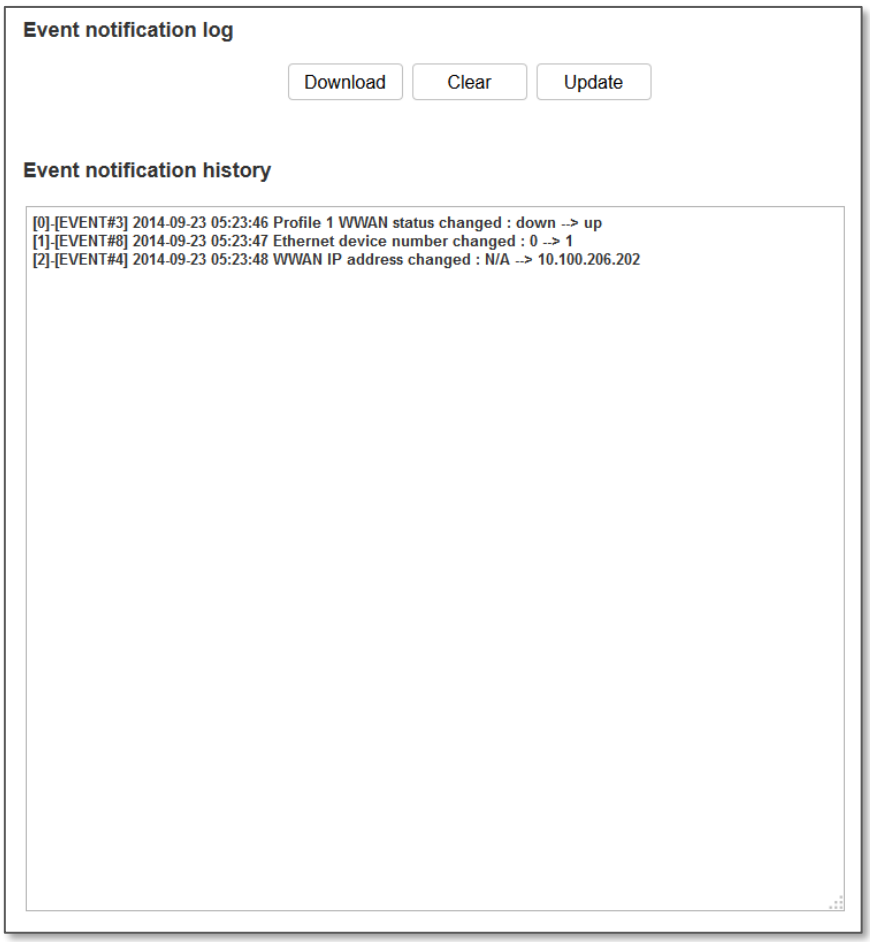


Figure 118 – Event notification log

System log settings

To access the System log settings page, click on the **System** menu item then select the **Log** menu on the left and finally select **System log settings** beneath it.

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

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

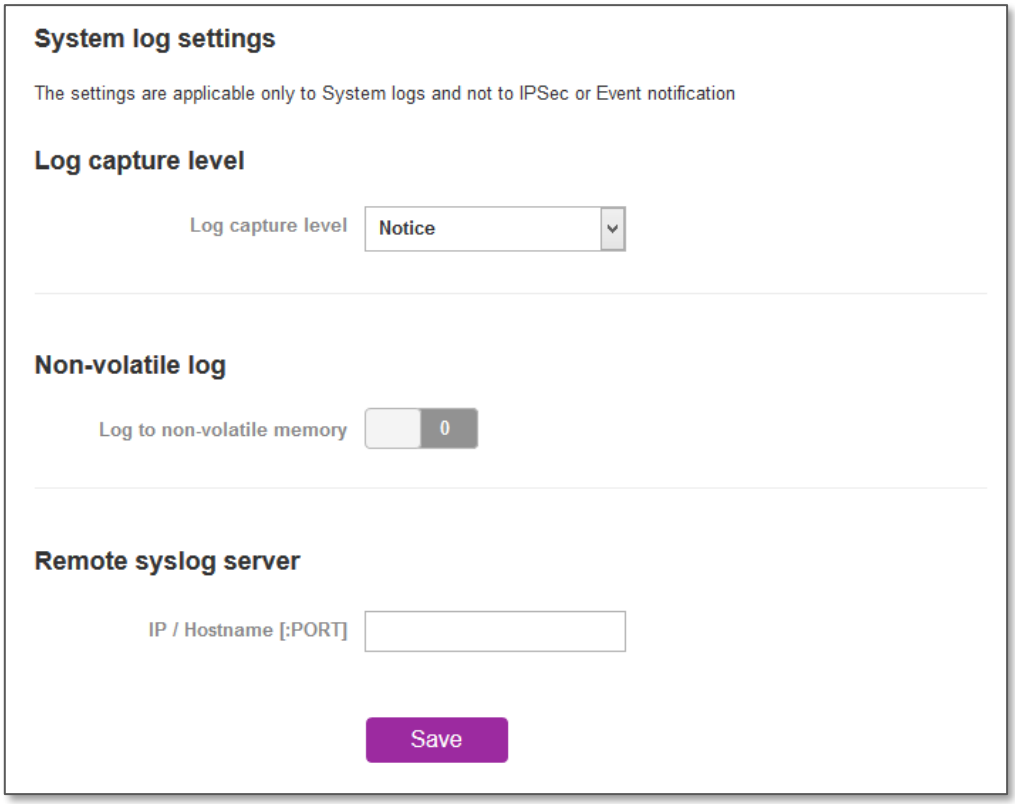


Figure 119 - System log settings

Ping watchdog

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

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

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

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

The feature operates as follows:

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

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

d The router then sends 3 consecutive pings to the “Destination address” and 3 consecutive pings to the “Second address” every “Periodic Ping accelerated timer” configured interval.

e If all accelerated pings in step C above fail then number of time configured in “Fail count”, the router reboots.

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

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

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

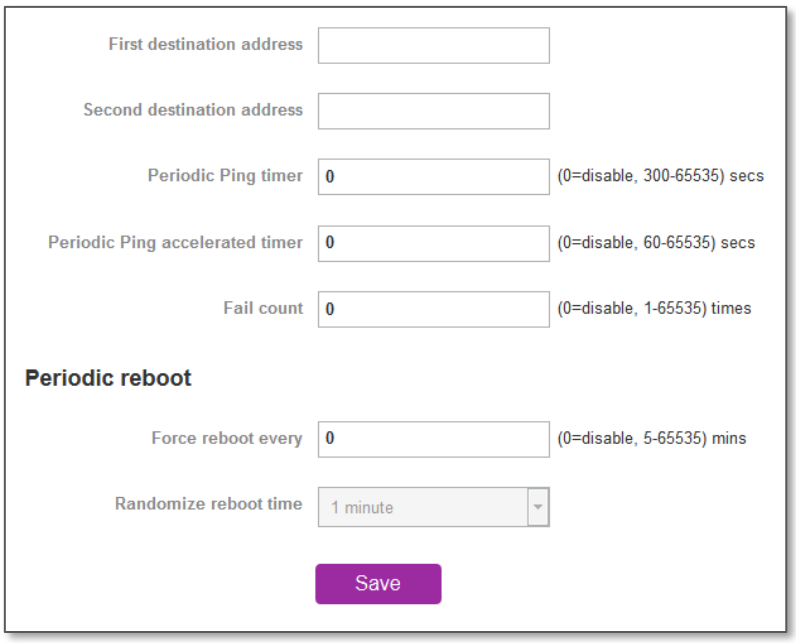


Figure 120 – Ping watchdog settings

Configuring Periodic Ping settings

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

To configure the ping watchdog:

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

Disabling the Ping watchdog function

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

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

Configuring a Periodic reboot

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

1. In the **Force reboot every** field, enter the time in minutes between forced reboots. The default value is 0 which disables the Periodic reboot function. The minimum period between reboots is 5 minutes while the maximum value is 65535 minutes.
2. If you have configured a forced reboot time, you can use the **Randomise reboot time** drop down list to select a random reboot timer. Randomising the reboot time is useful for preventing a large number of devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured **Force reboot every** time and then randomly selects a time that is less than or equal to the **Randomise reboot time** setting**.** After that randomly selected time has elapsed, the router reboots.
3. Click the **Save** button to save the settings.

Note: 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**.

System configuration

Settings backup and restore

The settings backup and restore page is used to backup or restore the router's configuration or to reset it to factory defaults. In order to view the settings page you must be logged into the web user interface as **root** using the password **admin**. The backup and restore functions can be used to easily configure a large number of MachineLink 3G Routers by configuring one router with your desired settings, backing them up to a file and then restoring that file to multiple MachineLink 3G Routers.

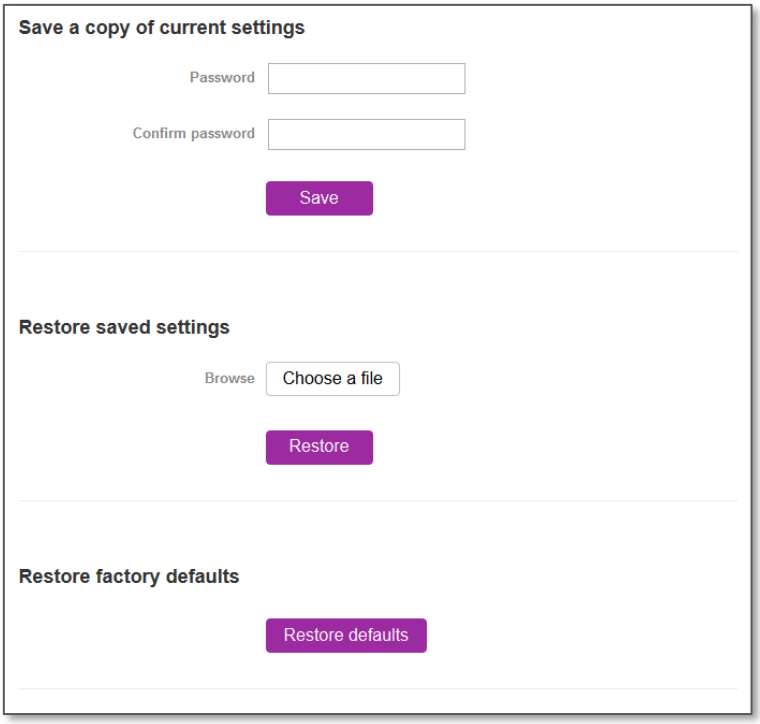


Figure 121 – Settings backup and restore

Back up your router's configuration

1 Log in to the web configuration interface, click on the **System** menu and select **Settings backup and restore**.

2 If you want to password protect your backup configuration files, enter your password in the fields under **Save a copy of current settings** and click on **Save**. If you don't want to password protect your files, just click on **Save**. The router will then prompt you to select a location to save the settings file.

Note: The following conditions apply:-

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

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

Do not enter a password for the backup configuration file if you are planning to use it for remote restore

Restore your backup configuration

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

Restoring the router's factory default configuration

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

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

Upload

The Upload page allows you to upload firmware files, HTTPS certificates or user created application packages to the Vodafone MachineLink 3G. When firmware files have been uploaded, they can also be installed from this page. PDF files, such as this user guide may also be uploaded for access on the router's help page.

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

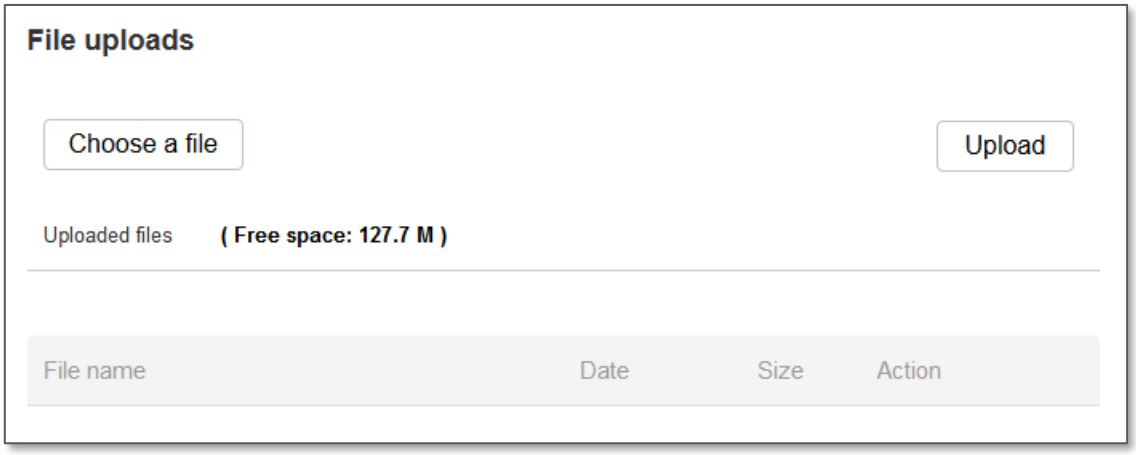


Figure 122 - Upload page

Updating the Firmware

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

Note: To perform an update, you must be logged into the router with the root manager account (see the Logging on to the MachineLink 3G router section for more details).

To update the MachineLink 3G firmware:

1. Power on the router as described in the Installing the router section.
2. Log in to the router with the root user account (See the Advanced configuration section for details)
3. Select the **System** item from the top menu bar, select the **System configuration** item from the menu on the left and then select the **Upload** menu item.
4. Under the **File uploads** section, click the **Choose a file** button. Locate the recovery firmware image file on your computer and click **Open**. The recovery image is named **vdf_nwl10_x.xx.xx.x_r.cdi** while the main system firmware image is named **vdf_nwl10_x.xx.xx.x.cdi**.
5. Click the **Upload** button. The firmware image is uploaded to the storage on the router.

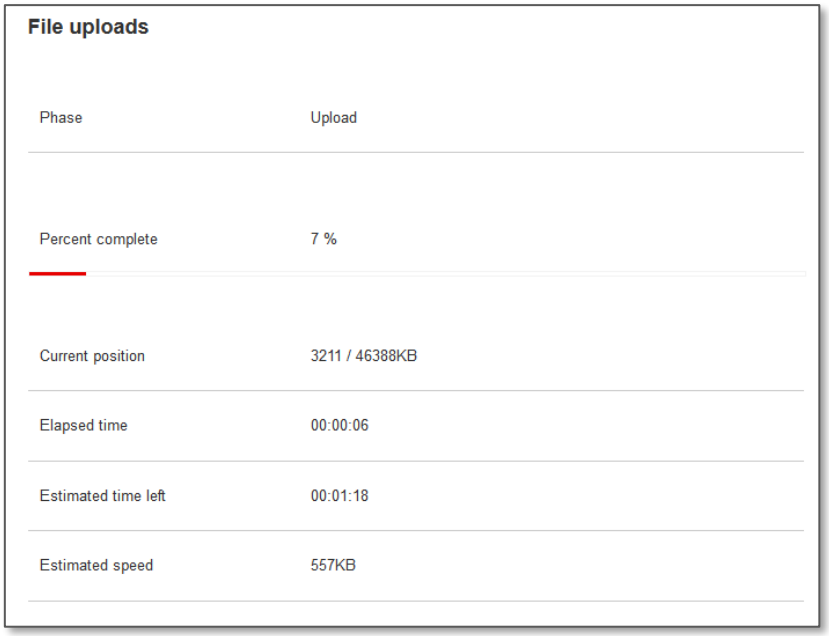


Figure 123 - File upload

6 Repeat steps 4 and 5 for the main system firmware image.

7 The uploaded firmware images are listed in the **Uploaded files** section. Click the **Install** link next to the recovery image to begin installing the recovery firmware image and then click **OK** on the confirmation window that appears.

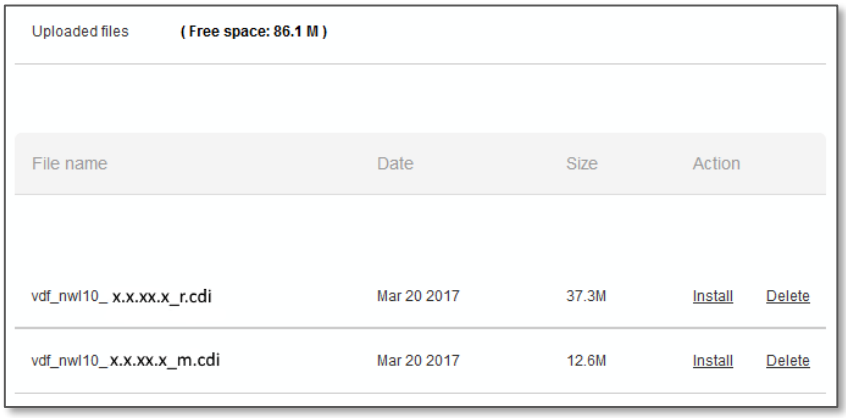


Figure 124 - Uploaded files

8 The recovery firmware image is flashed and when it is complete, the router displays “The firmware update was successful” and returns to the main Upload screen.

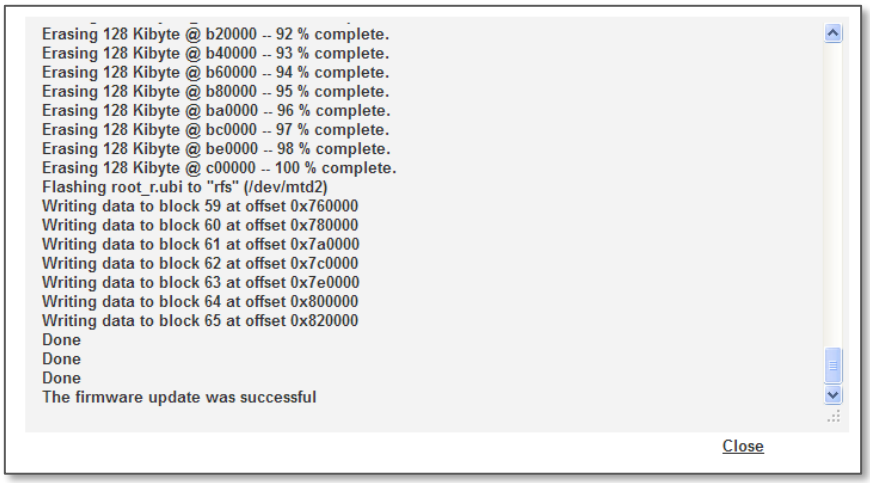


Figure 125 - Recovery firmware flash process

9 Click the **Install** link to the right of the main firmware image you uploaded and then click **OK** to confirm that you want to continue with the installation.

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 and the router prompts you to perform a reboot.

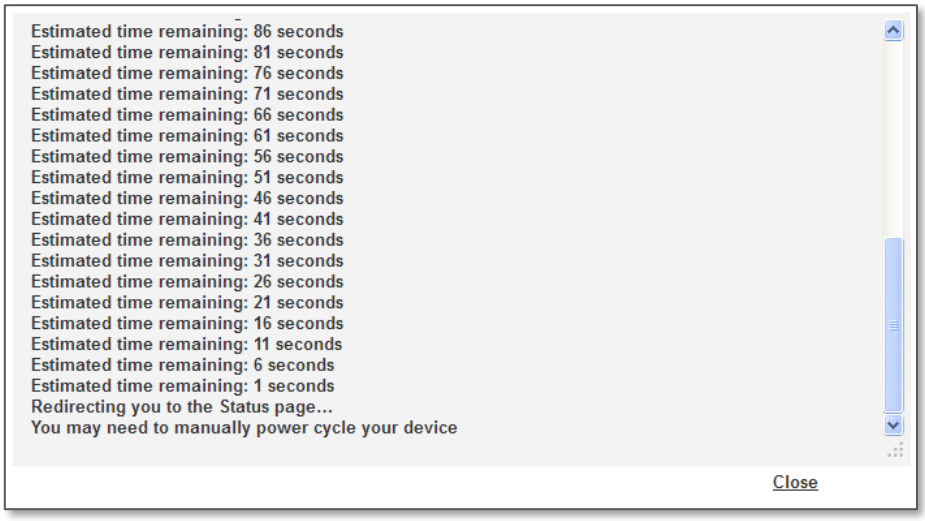


Figure 126 -– Installing main firmware image

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

Software applications manager

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

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

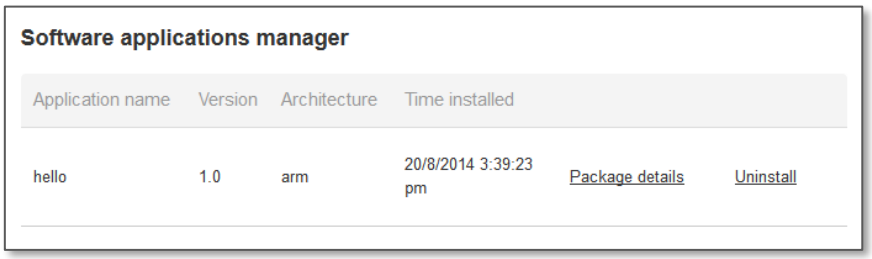


Figure 127 – Software applications manager

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

To uninstall any software applications, click the **Uninstall** link.

Administration

Administration settings

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

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

The page is divided into four sections:

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

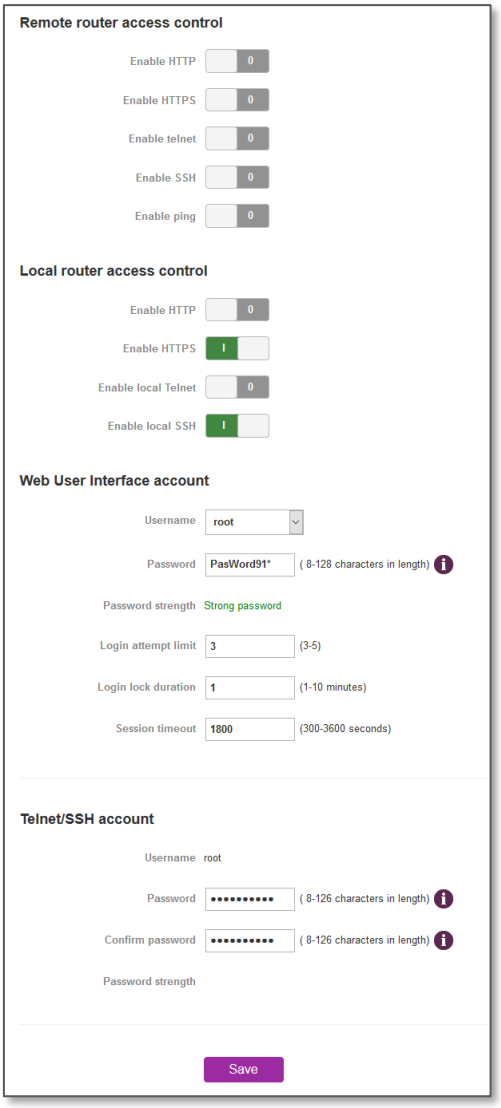
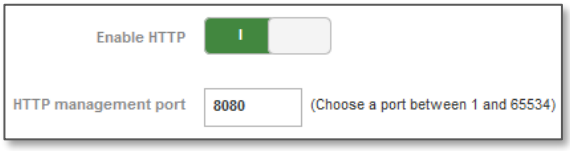
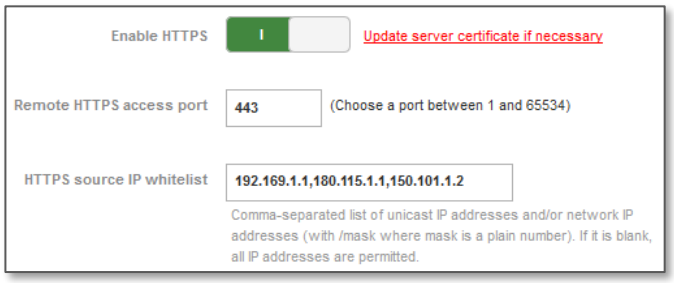


Figure 128 - Administration page

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

Option	Definition
Enable local Telnet	Enable or disable local telnet (command line) access to the router. The default setting is disabled.
Enable local SSH	Enable or disable local Secure Shell on the router. The default setting is enabled.
Web User Interface account	
Username	Use the drop down list to select the root or user account to change its web user interface password.
Password	Enter the desired web user interface password. When logged in with the root account the password will display in clear text, otherwise the password is masked. Only the root account can view and change passwords.
Password strength	From firmware version 2.0.57.0, the Vodafone MachineLink 3G router includes algorithms to ensure that the password you enter is strong. Any password configured on the router must now meet the following criteria: • Be a minimum of 8 characters and no more than 128 characters in length. • Contain at least one upper case, one lower case character and one number. • Contain at least one special character, such as: ` ~ ! @ # $ % ^ & * ( ) - _ = + [{] } \ | ; : ' " , < > / ? Additionally, the password must also satisfy an algorithm which analyses the characters as you type them, searching for commonly used patterns, passwords, names and surnames according to US census data, popular English words from Wikipedia and US television and movies and other common patterns such as dates, repeated characters (aaa), sequences (abcd), keyboard patterns (qwertyuiop) and substitution of numbers for letters.
Login attempt limit	Set the number of unsuccessful login attempts that are allowed before the login lock applies (see next item). You can choose 3, 4 or 5 login attempts. The default is 3.
Login lock duration	Set the time users must wait before they can attempt to login after reaching the login attempt limit, see previous item above. The duration can be set from one minute to ten minutes. The default is one minute.
Session timeout	Set the time in seconds that the system must remain idle before it automatically logs out. 1800 seconds (30 minutes) is the default. You can choose a time between 300 seconds (5 minutes) and 3600 seconds (one hour).
Telnet/SSH account	
Username	Displays the Telnet/SSH.username. This may not be changed.
Password	Enter the desired Telnet/SSH password.
Confirm password	Re-enter the desired Telnet/SSH password.

Table 34 - Administration configuration options

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.

WARNING – We highly recommend that you change the default web user interface password for both the root and user accounts as soon as possible. We also highly recommend that you change the Telnet/SSH account password from the default setting.

Server certificate

What is HTTP Secure?

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

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

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

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

Each Vodafone MachineLink 3G router contains a self-signed digital certificate which is identical on all Vodafone MachineLink 3G routers. For a greater level of security, the router also supports generating your own unique key. Additionally, you may use third party software to generate your own self-signed digital certificate or purchase a signed certificate from a trusted certificate authority and then upload those certificates to the router.

Generating your own self-signed certificate

To generate your own self-signed certificate:

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

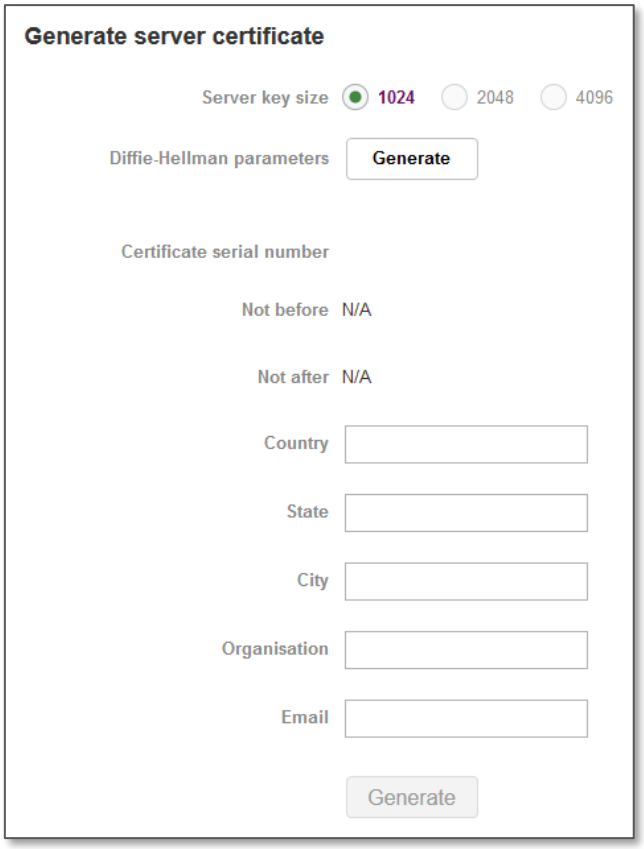


Figure 129 - Generate server certificate

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

Code	Country	Code	Country	Code	Country	Code	Country
AX	Åland Islands	**ER**	Eritrea	**LS**	Lesotho	**SA**	Saudi Arabia
AD	Andorra	**ES**	Spain	**LT**	Lithuania	**SB**	Solomon Islands
AE	United Arab Emirates	**ET**	Ethiopia	**LU**	Luxembourg	**SC**	Seychelles
AF	Afghanistan	**FI**	Finland	**LV**	Latvia	**SE**	Sweden
AG	Antigua and Barbuda	**FJ**	Fiji	**LY**	Libya	**SG**	Singapore
AI	Anguilla	**FK**	Falkland Islands (Malvinas)	**MA**	Morocco	**SH**	St. Helena
AL	Albania	**FM**	Micronesia	**MC**	Monaco	**SI**	Slovenia
AM	Armenia	**FO**	Faroe Islands	**MD**	Moldova	**SJ**	Svalbard and Jan Mayen Islands
AN	Netherlands Antilles	**FR**	France	**ME**	Montenegro	**SK**	Slovak Republic
AO	Angola	**FX**	France, Metropolitan	**MG**	Madagascar	**SL**	Sierra Leone
AQ	Antarctica	**GA**	Gabon	**MH**	Marshall Islands	**SM**	San Marino
AR	Argentina	**GB**	Great Britain (UK)	**MK**	Macedonia	**SN**	Senegal
AS	American Samoa	**GD**	Grenada	**ML**	Mali	**SR**	Suriname

Code	Country	Code	Country	Code	Country	Code	Country
AT	Austria	**GE**	Georgia	**MM**	Myanmar	**ST**	Sao Tome and Principe
AU	Australia	**GF**	French Guiana	**MN**	Mongolia	**SU**	USSR (former)
AW	Aruba	**GG**	Guernsey	**MO**	Macau	**SV**	El Salvador
AZ	Azerbaijan	**GH**	Ghana	**MP**	Northern Mariana Islands	**SZ**	Swaziland
BA	Bosnia and Herzegovina	**GI**	Gibraltar	**MQ**	Martinique	**TC**	Turks and Caicos Islands
BB	Barbados	**GL**	Greenland	**MR**	Mauritania	**TD**	Chad
BD	Bangladesh	**GM**	Gambia	**MS**	Montserrat	**TF**	French Southern Territories
BE	Belgium	**GN**	Guinea	**MT**	Malta	**TG**	Togo
BF	Burkina Faso	**GP**	Guadeloupe	**MU**	Mauritius	**TH**	Thailand
BG	Bulgaria	**GQ**	Equatorial Guinea	**MV**	Maldives	**TJ**	Tajikistan
BH	Bahrain	**GR**	Greece	**MW**	Malawi	**TK**	Tokelau
BI	Burundi	**GS**	S. Georgia and S. Sandwich Isls.	**MX**	Mexico	**TM**	Turkmenistan
BJ	Benin	**GT**	Guatemala	**MY**	Malaysia	**TN**	Tunisia
BM	Bermuda	**GU**	Guam	**MZ**	Mozambique	**TO**	Tonga
BN	Brunei Darussalam	**GW**	Guinea-Bissau	**NA**	Namibia	**TP**	East Timor
BO	Bolivia	**GY**	Guyana	**NC**	New Caledonia	**TR**	Turkey
BR	Brazil	**HK**	Hong Kong	**NE**	Niger	**TT**	Trinidad and Tobago
BS	Bahamas	**HM**	Heard and McDonald Islands	**NF**	Norfolk Island	**TV**	Tuvalu
BT	Bhutan	**HN**	Honduras	**NG**	Nigeria	**TW**	Taiwan
BV	Bouvet Island	**HR**	Croatia (Hrvatska)	**NI**	Nicaragua	**TZ**	Tanzania
BW	Botswana	**HT**	Haiti	**NL**	Netherlands	**UA**	Ukraine
BZ	Belize	**HU**	Hungary	**NO**	Norway	**UG**	Uganda
CA	Canada	**ID**	Indonesia	**NP**	Nepal	**UM**	US Minor Outlying Islands
CC	Cocos (Keeling) Islands	**IE**	Ireland	**NR**	Nauru	**US**	United States
CF	Central African Republic	**IL**	Israel	**NT**	Neutral Zone	**UY**	Uruguay
CH	Switzerland	**IM**	Isle of Man	**NU**	Niue	**UZ**	Uzbekistan
CI	Cote D'Ivoire (Ivory Coast)	**IN**	India	**NZ**	New Zealand (Aotearoa)	**VA**	Vatican City State (Holy See)
CK	Cook Islands	**IO**	British Indian Ocean Territory	**OM**	Oman	**VC**	Saint Vincent and the Grenadines
CL	Chile	**IS**	Iceland	**PA**	Panama	**VE**	Venezuela
CM	Cameroon	**IT**	Italy	**PE**	Peru	**VG**	Virgin Islands (British)
CN	China	**JE**	Jersey	**PF**	French Polynesia	**VI**	Virgin Islands (U.S.)
CO	Colombia	**JM**	Jamaica	**PG**	Papua New Guinea	**VN**	Viet Nam
CR	Costa Rica	**JO**	Jordan	**PH**	Philippines	**VU**	Vanuatu
CS	Czechoslovakia (former)	**JP**	Japan	**PK**	Pakistan	**WF**	Wallis and Futuna Islands
CV	Cape Verde	**KE**	Kenya	**PL**	Poland	**WS**	Samoa
CX	Christmas Island	**KG**	Kyrgyzstan	**PM**	St. Pierre and Miquelon	**YE**	Yemen
CY	Cyprus	**KH**	Cambodia	**PN**	Pitcairn	**YT**	Mayotte

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

Table 35 - Country codes

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

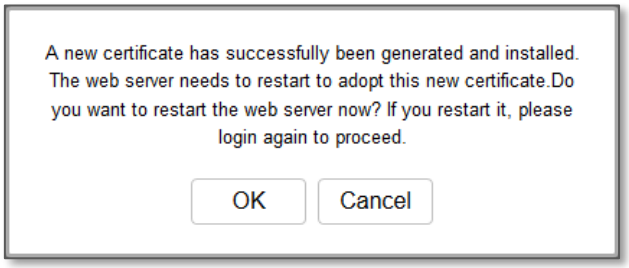


Figure 130 - New certificate successfully generated message

SSH key management

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

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

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

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

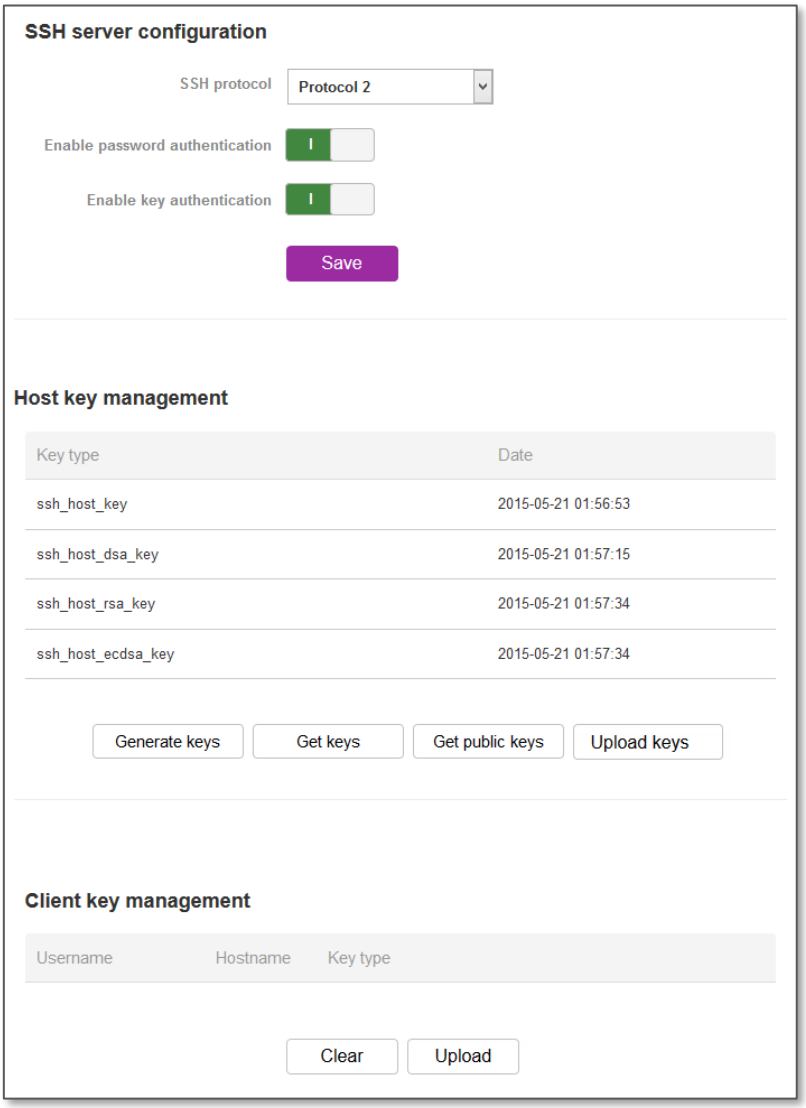


Figure 131 - SSH Server Configuration

SSH Server Configuration

To configure the SSH server settings:

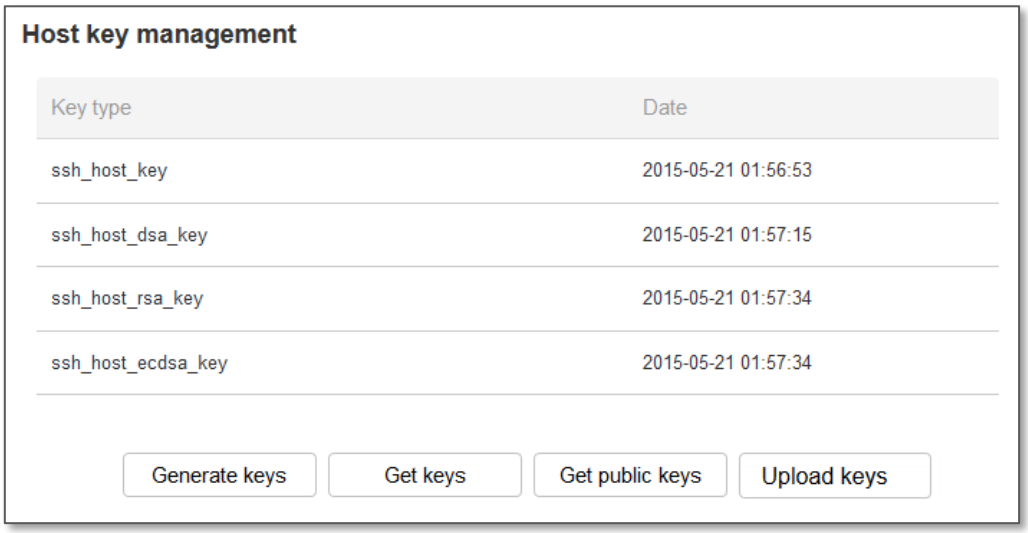
1. Use the SSH Protocol drop down list to select the protocol that you want to use. Protocol 2 is more recent and is considered more secure.
2. Select the types of authentication you want to use by clicking the **Enable password authentication** and **Enable key authentication** toggle keys on or off.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

Host key management

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

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

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



Generating new keys

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

Downloading keys

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

Uploading your own key files

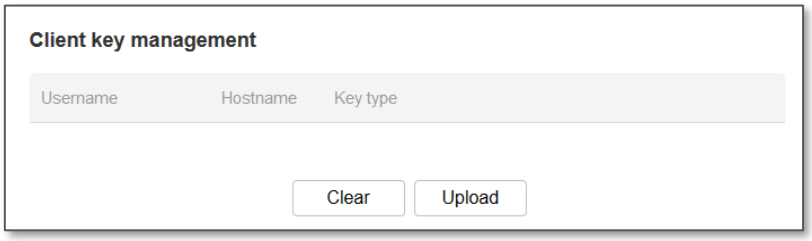
You can generate your own SSH keys and upload them to the router. To generate keys on a Linux-based machine, use the following commands:

```
mkdir keys
cd keys
ssh-keygen -t rsa1 -f ssh_host_key -N ""
ssh-keygen -t dsa -f ssh_host_dsa_key -N ""
ssh-keygen -t rsa -f ssh_host_rsa_key -N ""
ssh-keygen -t ecdsa -f ssh_host_ecdsa_key -N ""
zip -e -P "PASSWORDHERE" -j keys.zip *
```

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

Client key management

The Client Key Management section is used for uploading the public key file of clients. To upload a client public key, click the Upload button, browse to the file and click Open.



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, click the **System** menu, then **Administration** on the left and finally select **LED Operation Mode**.

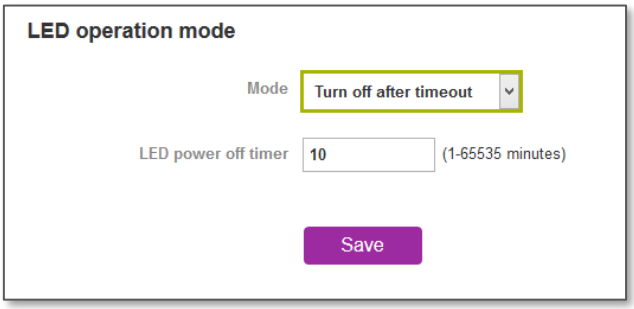


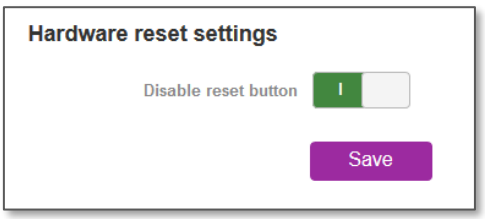
Figure 132 - LED Operation Mode

The **Mode** drop down list sets the operation mode of the LEDs on the front panel of the router. To set the lights to operate at all times, set this to Always on. To set the lights to turn off after a specified period, select **Turn off after timeout**. When configured to turn off after timeout, use the **LED power off timer** field to specify the time in minutes to wait before turning off the LED indicators. The LED Power Off Timer must be an integer between 1 and 65535.

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

Hardware reset settings

To prevent unauthorised reset via the physical reset button, go to **System -> Administration -> Hardware reset settings** and select **Disable reset button**:



WARNING – Before disabling the reset button, be sure that you remember your root account password. If you disable the reset button and you forget your root account password, you will effectively be locked out of your device. Disabling the reset button prevents you from rebooting the router, accessing the recovery partition and factory resetting the device, therefore preventing you from resetting the root account password.

A notification can be sent each time this button setting changes. To configure notification settings, go to **Services -> Event notification -> Notification configuration** and configure a notification type and destination for event 21.

Reboot

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

To reboot the router:

1 Click the **System** menu item from the top menu bar.

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

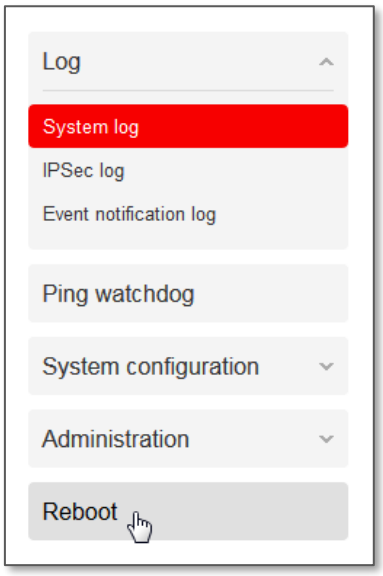


Figure 133 - Reboot menu option

3 The router displays a warning that you are about to perform a reboot. If you wish to proceed, click the **Reboot** button then click **OK** on the confirmation window which appears.

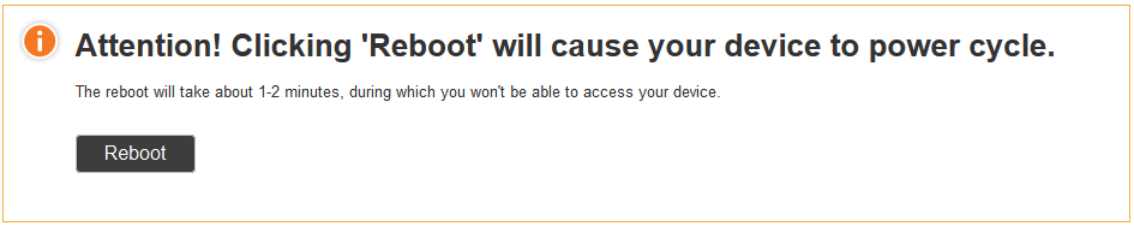


Figure 134 - Reboot confirmation

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

Logging out

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

Appendix A: Tables

Table 1 - Device Dimensions 10
Table 2 - LED Indicators 12
Table 3 - Signal strength LED descriptions 13
Table 4 - Ethernet port LED indicators description 14
Table 5 - Interfaces 16
Table 6 - PoE power classes 24
Table 7 - Locking power block pin outs 25
Table 8 - Average power consumption figures 26
Table 9 - Management account login details – Root manager account 28
Table 10 - Management account login details –User account 28
Table 11 - Status page item details 34
Table 12 - Data connection item details 36
Table 13 - Roaming settings options 51
Table 14 - Connect on demand - Connect and disconnect timers descriptions 61
Table 15 - Current MAC / IP / Port filtering rules in effect 81
Table 16 - Current MAC / IP / Port filtering rules in effect list 82
Table 17 - IPSec Configuration Items 86
Table 18 - Distinguished Name field descriptions 105
Table 19 - SNMP v3 Configuration 113
Table 20 - Event notification configuration options 119
Table 21 - Event notification – event types 120
Table 22 - Email client settings 124
Table 23 - SMS Setup Settings 127
Table 24 - Inbox/Outbox icons 130
Table 25 - SMS Diagnostic Command Syntax 136
Table 26 - List of basic SMS diagnostic commands 138
Table 27 - List of get/set commands 141
Table 28 - List of basic SMS diagnostics RDB variables 142
Table 29 - Network types returned by get plmnscan SMS command 143
Table 30 - Operator status codes returned by get plmnscan SMS command 143
Table 31 - SMS diagnostics example commands 146
Table 32 – Network quality test result details 148
Table 33 - System log detail levels 151
Table 34 - Administration configuration options 166
Table 35 - Country codes 171
Table 36 - LAN Management Default Settings 182
Table 37 - Web Interface Default Settings 182
Table 38 - Telnet Access 182
Table 39 - RJ-45 connector pin outs 192

Appendix B: Device Mounting Dimensions

The image below is at 100% scale and may be used as a template for mounting the device. All dimensions shown are in millimetres.

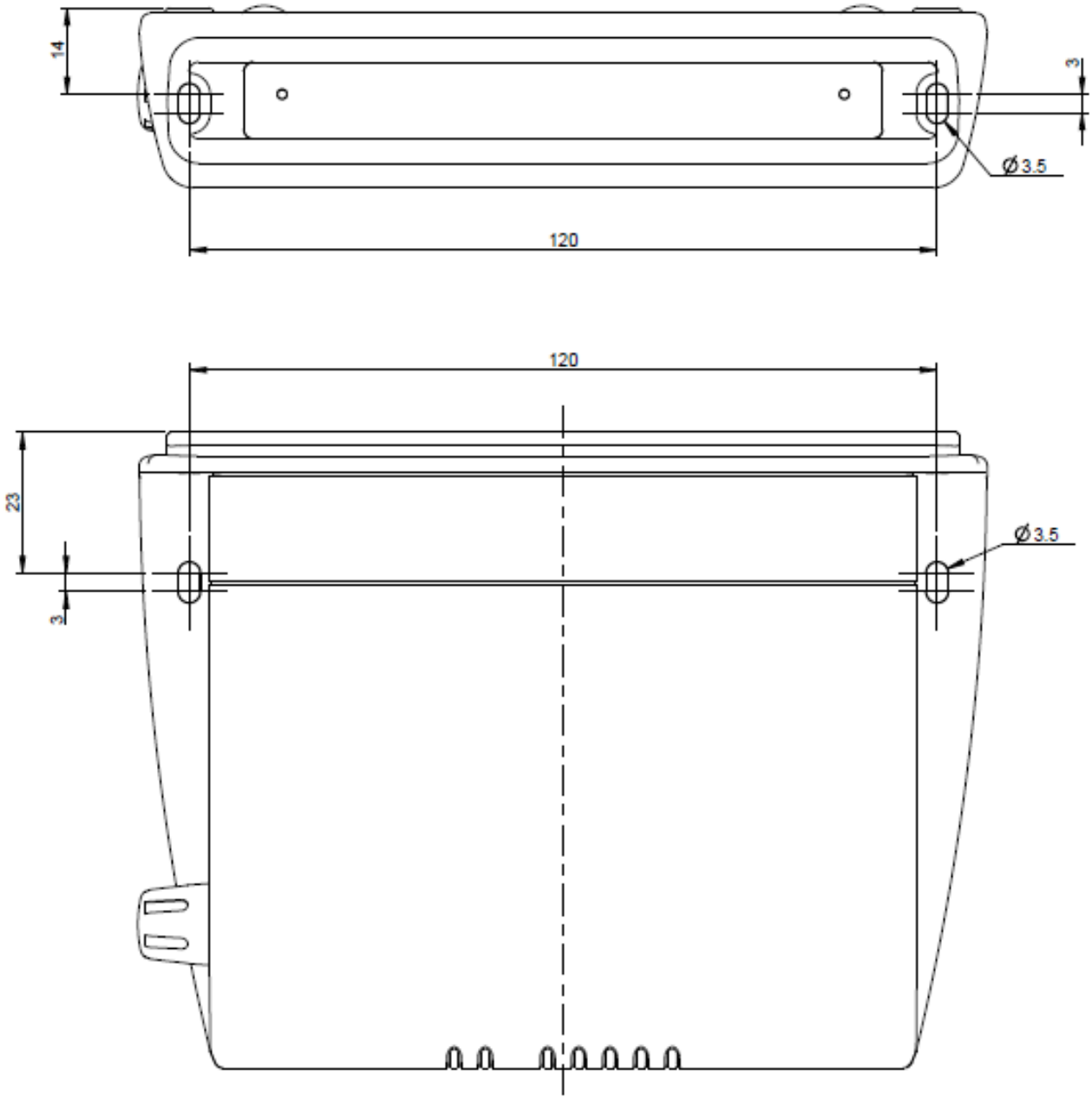


Figure 135 - Device mounting dimensions

Appendix C: Mounting Bracket

The image below is at 100% scale and may be used as a template for mounting the bracket. All dimensions shown are in millimetres.

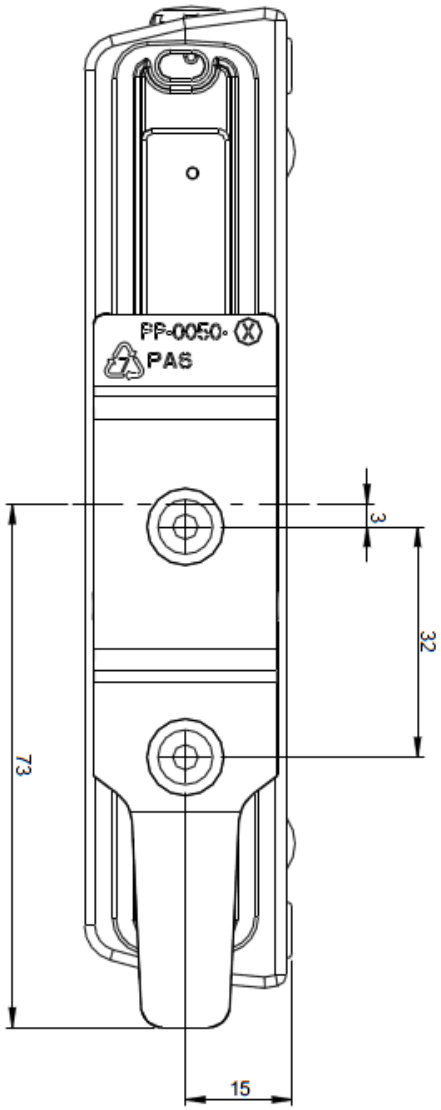


Figure 136 - Mounting bracket

Appendix D: Default Settings

The following tables list the default settings for the Vodafone MachineLink 3G.

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

Table 36 - LAN Management Default Settings

User account		Root manager account	
Username:	user	Username:	root
Password:	admin	Password:	admin

Table 37 - Web Interface Default Settings

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

Vodafone MachineLink 3G Telnet Access	
Username:	root
Password:	admin

Table 38 - Telnet Access

Restoring factory default settings

Restoring factory defaults will reset the Vodafone MachineLink 3G to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your Vodafone MachineLink 3G such as:

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

There are two methods you can use to restore factory default settings on your Vodafone MachineLink 3G:

- Using the web-based user interface
- Using the reset button on the interface panel of the router

Using the web-based user interface

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

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

Using the reset button on the interface panel of the router

Use a pen to depress the Reset button on the device for 15-20 seconds. The router will restore the factory default settings and reboot.

When you have reset your Vodafone MachineLink 3G Router to its default settings you will be able to access the device's configuration web interface using https://192.168.1.1 with username **`admin`** or **`root`** and password **`admin`**.

Appendix E: Recovery mode

The Vodafone MachineLink 3G router features two independent operating systems, each with its own file systems. These two systems are referred to as 'Main' and 'Recovery'. It is always possible to use one in order to restore the other in the event that one system becomes damaged or corrupted (such as during a firmware upgrade failure). The recovery console provides limited functionality and is typically used to restore the main firmware image in the case of a problem.

Accessing recovery mode

Both systems have web interfaces that can be used to manipulate the other inactive system. The Vodafone MachineLink 3G 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. When the LEDs on the front panel change to amber and countdown in a sequence, release the reset button. The router then boots into recovery mode.
2. In your browser, navigate to https://192.168.1.1. The router's recovery mode is hardcoded to use this address regardless of the IP address that was configured in the main system. The router's recovery console is displayed.

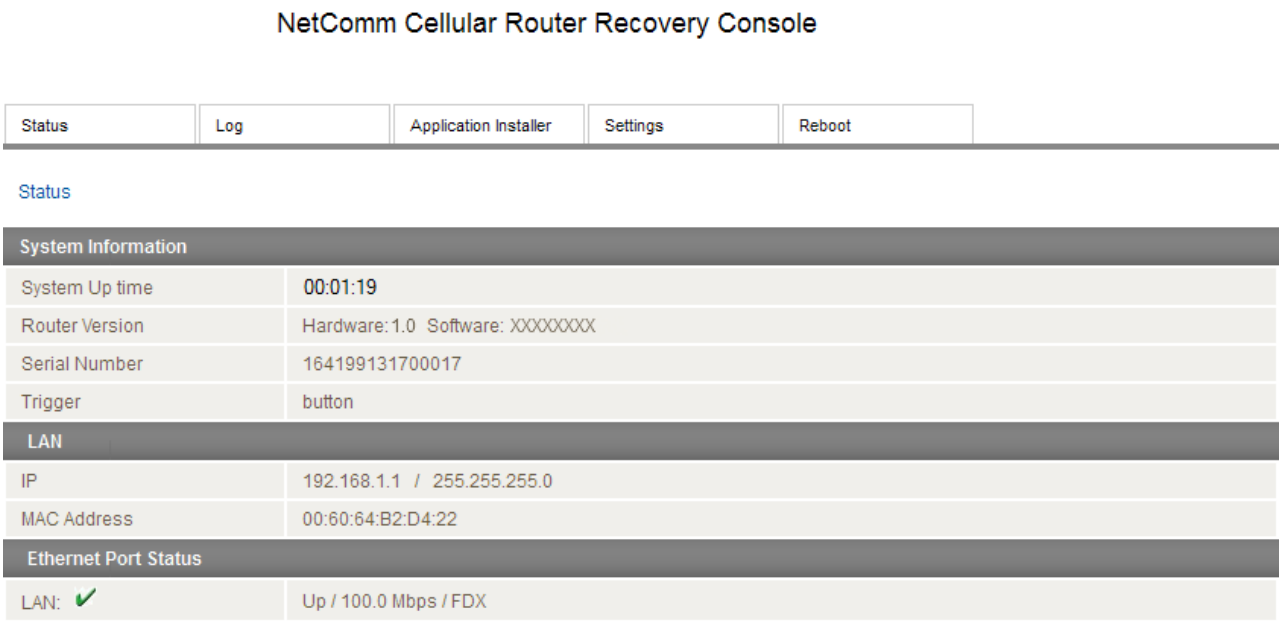


Figure 137 - Recovery console

Status

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

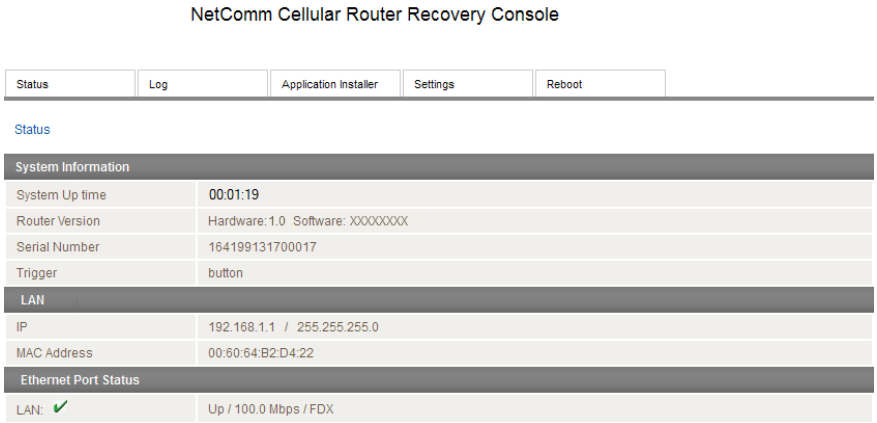


Figure 138 - Recovery mode - Status

Log

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

NetComm Cellular Router Recovery Console

Status | Log | Application Installer | Settings | Reboot

Log File Display Level Notice Page 1 of 4 Clear Log File

Date & Time	Machine	Level	Process	Message
Jan 1 00:01:12	vdf_nwl10	daemon.warn	dnsmasq[359]	overflow: 5 log entries lost
Jan 1 00:00:10	vdf_nwl10	user.err	dispd[416]	syslog LOG_ERR
Jan 1 00:00:10	vdf_nwl10	user.err	dispd[416]	=================
Jan 1 00:00:10	vdf_nwl10	user.err	dispd[416]	loglevel check
Jan 1 00:00:10	vdf_nwl10	user.err	dispd[416]	=================
Jan 1 00:00:09	vdf_nwl10	user.warn	kernel	[4.190000] Disabling lock debugging due to kernel taint
Jan 1 00:00:09	vdf_nwl10	user.warn	kernel	[4.190000] cdcs_DD: module license 'CDCS Proprietary' taints kernel.
Jan 1 00:00:09	vdf_nwl10	user.err	kernel	[4.110000] stmp3xxx_wdt: h/w watchdog timer changed to 15 sec(s)
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.340000] UBIFS: reserved for root: 0 bytes (0 KiB)
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.330000] UBIFS: default compressor: lzo
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.330000] UBIFS: media format: w4/r0 (latest is w4/r0)
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.320000] UBIFS: journal size: 9023488 bytes (8812 KiB, 8 MiB, 72 LEBs)
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.310000] UBIFS: file system size: 10031104 bytes (9796 KiB, 9 MiB, 79 LEBs)
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.310000] UBIFS: mounted UBI device 0, volume 0, name "rootfs"
Jan 1 00:00:09	vdf_nwl10	user.err	kernel	[2.090000] drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.090000] Key type encrypted registered
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.070000] Key type dns_resolver registered
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[2.050000] Bridge firewalling registered
Jan 1 00:00:09	vdf_nwl10	user.err	kernel	[1.920000] stmp3xxx_wdt: h/w watchdog disabled
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[1.550000] UBI: background thread "ubi_bgt0d" started, PID 38
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[1.540000] UBI: image sequence number: 366603322
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[1.540000] UBI: max/mean erase counter: 2/0
Jan 1 00:00:09	vdf_nwl10	user.notice	kernel	[1.530000] UBI: number of PEBs reserved for bad PEB handling: 2

Download Log File

Figure 139 - Recovery mode – Log

Application Installer

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

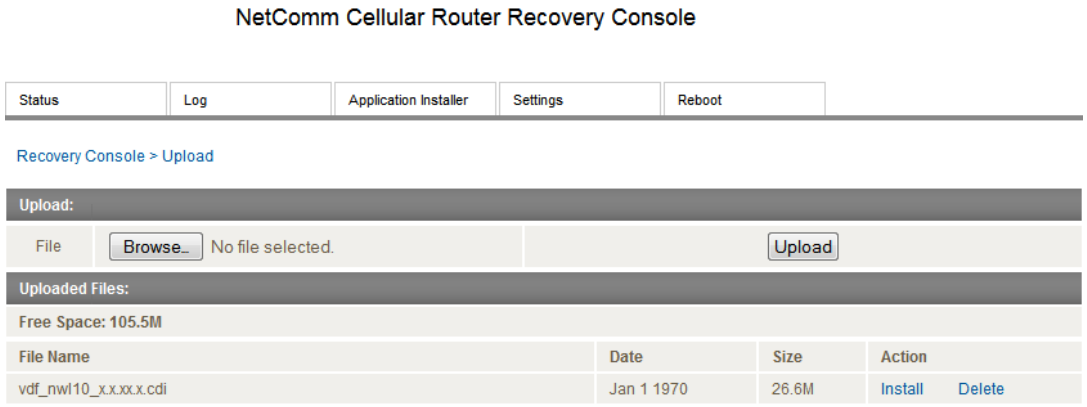


Figure 140 - Recovery mode - Application Installer

Settings

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

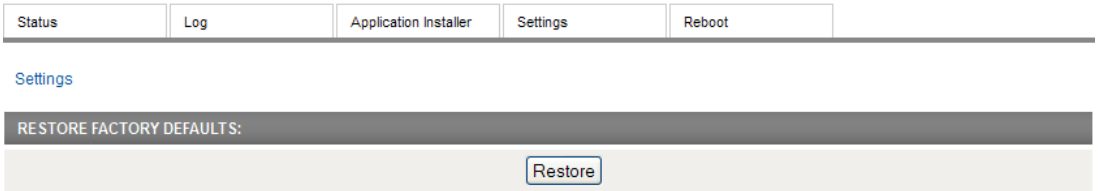


Figure 141 - Recovery mode – Settings

Reboot

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

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

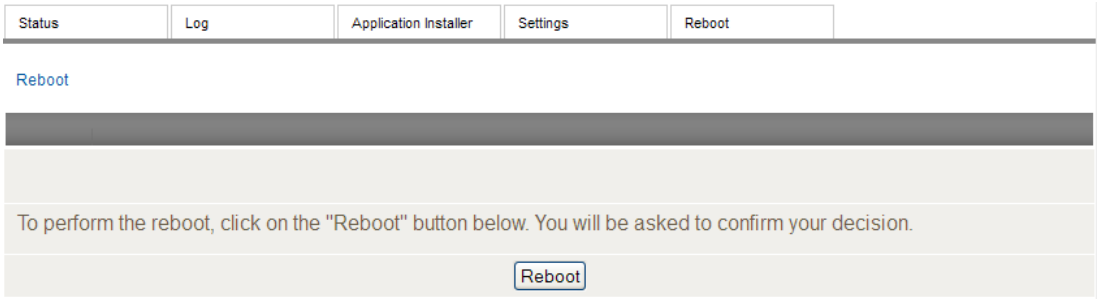


Figure 142 - Recovery mode - Reboot

Appendix F: HTTPS - Uploading a self-signed certificate

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

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

To upload your certificate:

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

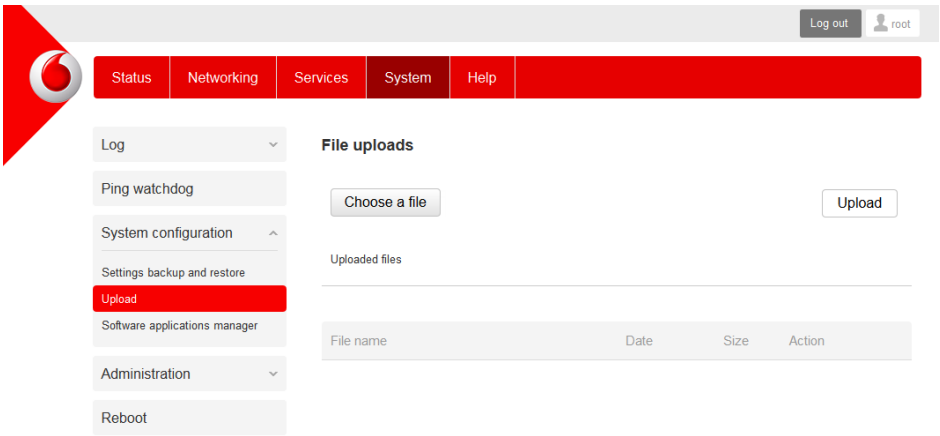


Figure 143 - Upload page

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

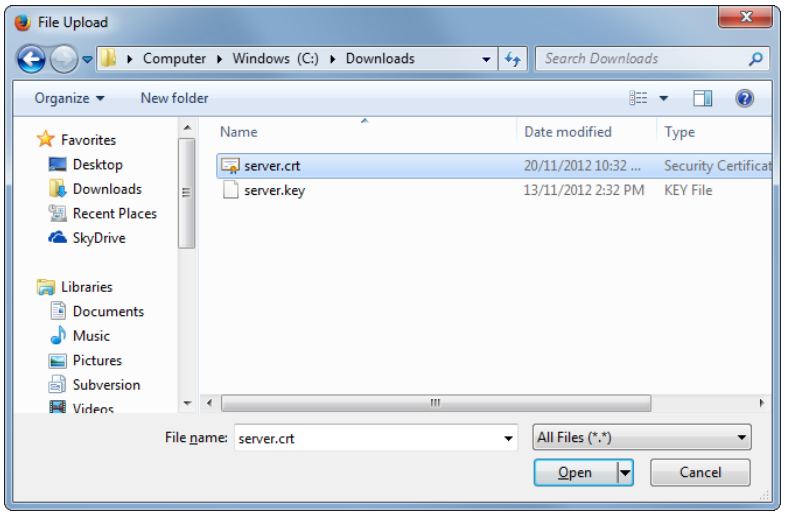


Figure 144 - Browse for server.crt

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

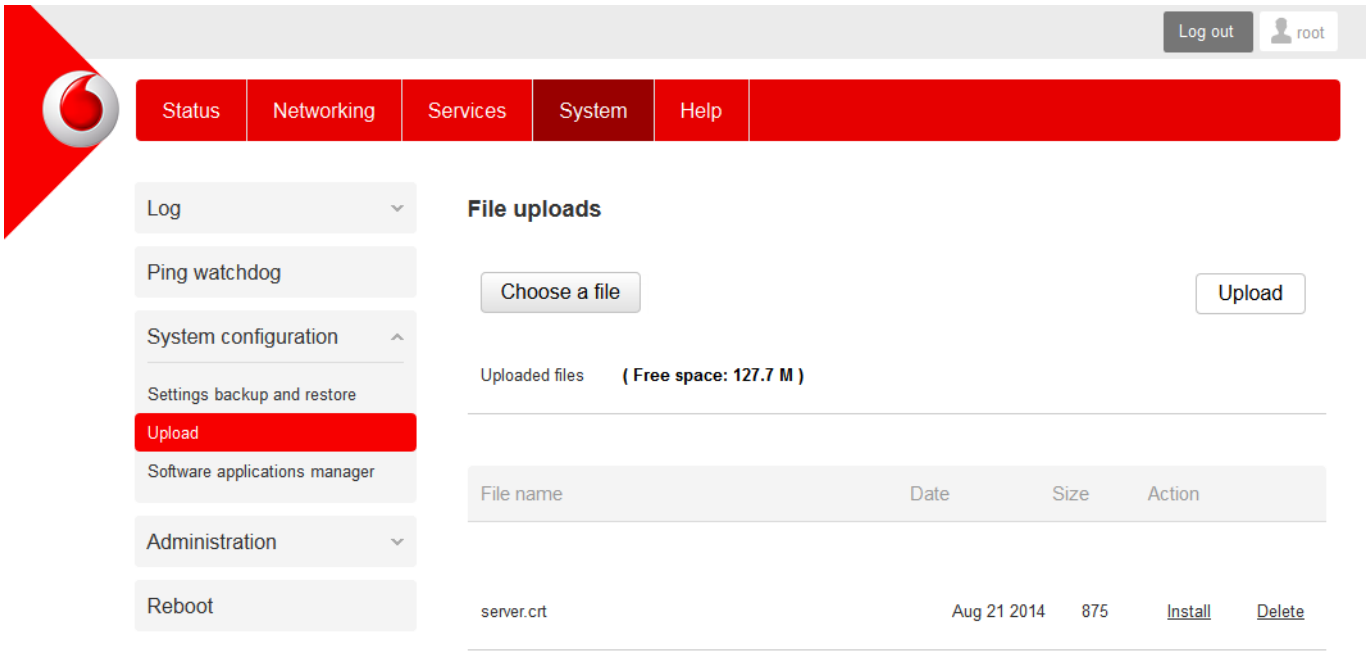


Figure 145 - Server certificate file uploaded

4 Repeat steps 2 and 3 for the server key file.

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

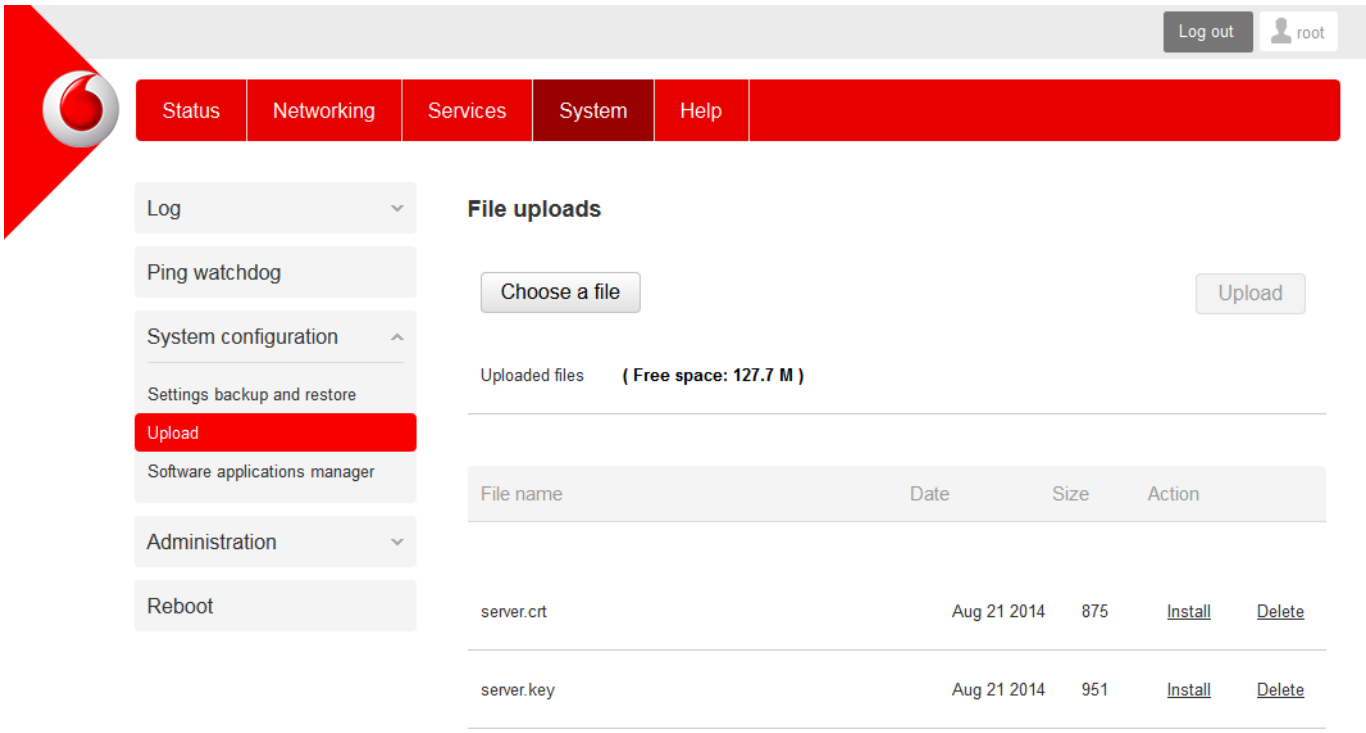


Figure 146 - Installing the server.crt file

Appendix G: RJ-45 connector

The RJ-45 connector provides an interface for a data connection and for device input power using the pin layout shown below.

Pin: 8 1

Figure 147 -The RJ-45 connector

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

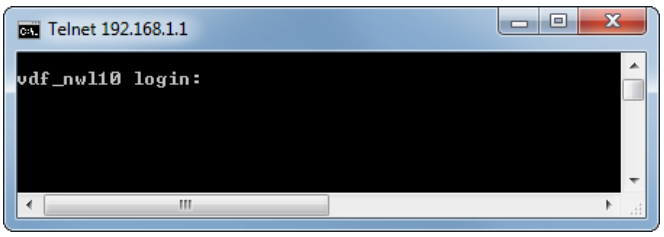
Table 39 - RJ-45 connector pin outs

Appendix H: Obtaining a list of RDB variables

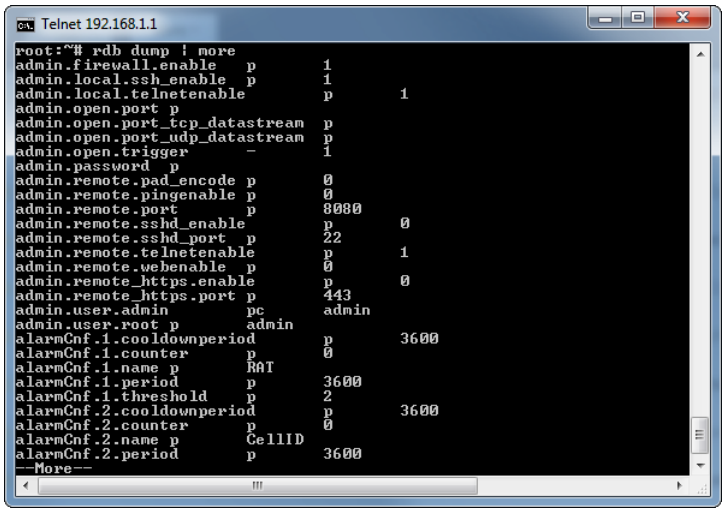
The RDB is a database of variables that contain settings on the router. You can retrieve (get) and set the values of these variables through the command-line or via SMS Diagnostics. To access a full list of the RDB variables, follow these steps:

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

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



7. At the login prompt, type `root` and press Enter. At the password prompt, enter the password that you configured in step 4.
8. At the root prompt, enter the command `rdb dump | more`. This will display a list of every rdb variable on the router one page at a time.



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

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 log in to the web configuration interface and click on the Help section.

Safety and product care

Electrical safety

Accessories

Only use approved accessories.

Do not connect with incompatible products or accessories.

Connection to a car

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

Distraction

Operating machinery

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

Driving

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

Product handling

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

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

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

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

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

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

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

Do not paint your device or its accessories.

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

Do not expose your device or its accessories to extreme temperatures. Ensure that the device is installed in an area where the temperature is within the supported operating temperature range (-40°C to 80°C).

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

Please check local regulations for disposal of electronic products.

Do not operate the device where ventilation is restricted

Installation and configuration should be performed by trained personnel only.

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

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

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

Small children

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

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

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

Demagnetisation

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

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

Electrostatic discharge (ESD)

Do not touch the SIM card's metal connectors.

Air Bags

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

Mount the device safely before driving your vehicle.

Emergency & other situations requiring continuous connectivity

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

Device heating

Your device may become warm during normal use.

Faulty and Damaged Products

Do not attempt to disassemble the device or its accessory.

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

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

Interference

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

Pacemakers

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

Hearing aids

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

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

Medical devices

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

Hospitals

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

Aircraft

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

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

Interference in cars

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

Explosive environments

Petrol stations and explosive atmospheres

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

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

Blasting caps and areas

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

Regulatory compliance

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 20cm 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. The maximum antenna gain for this device as reported to the FCC is: 3.92 dBi (850MHz) and 2.5 dBi (1900MHz).

FCC Statement

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.

IC regulations

This device complies with Industry Canada 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.

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."

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

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

IMPORTANT NOTE:
IC radiation exposure statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and users body.

Anatel Statement

"Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário".

Para maiores informações, consulte o site da ANATEL www.anatel.gov.br

NBTC Statement

เครื่องวิทยุคมนาคมนี้มีระดับการแผ่คลื่นแม่เหล็กไฟฟ้าสอดคล้อง
ตามมาตรฐานความปลอดภัยต่อสุขภาพของมนุษย์จากการใช้เครื่องวิทยุคมนาคม
ที่คณะกรรมการกิจการโทรคมนาคมแห่งชาติประกาศกำหนด

NCC Statement

NCC 電信終端設備警語:「減少電磁波影響，請妥適使用」

Vietnam RoHS (Circular 30/2011/TT-BCT) Statement

Vodafone products supplied by NetComm Wireless that are offered through authorized distributors in Vietnam on and after December 1, 2012 comply with the substance restrictions and permitted uses in Circular 30/2011/TT-BCT of the Vietnamese Ministry of Industry and Trade temporarily regulating the permissible content limitation of some hazardous chemicals in the electrical and electronic products, commonly referred to as Vietnam RoHS.

Pursuant to the requirements, we understand the permissible content limits of the restricted substances, which is listed in the below table*. Vodafone products are designed and manufactured in accordance with Vietnam RoHS.

No.	Chemicals	Permissible content limitation
1	Pb	0,1% volume
2	Hg	0,1% volume
3	Cd	0,01% volume
4	Cr6+	0,1% volume
5	PBB	0,1% volume
6	PBDE	0,1% volume

*Issuing together with the Circular No.30/2011/TT-BCT dated August 10, 2011 of the Ministry of Industry and Trade

CE Regulation

RF Exposure Information (MPE)

This device meets the EU requirements and the International Commission on Non-Ionizing Radiation Protection (ICNIRP) on the limitation of exposure of the general public to electromagnetic fields by way of health protection. To comply with the RF exposure requirements, this equipment must be operated in a minimum of 20 cm separation distance to the user.

Maximum RF Power

Functions	Max Average Output Power
GSM 900	33 dBm
DCS 1800	30 dBm
WCDMA I	24 dBm
WCDMA VIII	24 dBm

WEEE Regulation

Waste Electrical and Electronic Equipment (WEEE)

This symbol means that according to local laws and regulations your product and/or its battery shall be disposed of separately from household waste. When this product reaches its end of life, take it to a collection point designated by local authorities. Proper recycling of your product will protect human health and the environment.

Vodafone MachineLink 3G (ML3G) Simplified EU DoC

Hereby, Vodafone S.à r.l. declares that the radio equipment type NWL-10 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:
http://vodafone.netcommwireless.com/info/nwl-10/collateral/NWL-10_DoC.PDF

Hong Kong Certification

Certified for use in Hong Kong
經驗證可在香港使用

Certificate No. 證書號碼
HK0011501200

通訊事務管理局
COMMUNICATIONS
AUTHORITY

IMDA Standards

Complies with
IMDA Standards
DA103798

UAE TRA

TRA
REGISTERED No:
ER47342/16
DEALER No:
DA0051460/10