



# **Vodafone MachineLink**

PPTP Configuration Guide

## Document History

This guide covers the following products:

- Vodafone MachineLink 4G Lite NWL-221
- Vodafone MachineLink 4G Lite NWL-222
- Vodafone MachineLink 4G Lite NWL-224

| Ver.   | Document Description      | Date          |
|--------|---------------------------|---------------|
| v. 1.0 | Initial document release. | November 2019 |

*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 <http://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.

## Copyright

Copyright© 2019 NetComm Wireless Limited. All rights reserved.

Copyright© 2019 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.

# Contents

|   |    |
|---|----|
| Introduction .....                        | 4  |
| Site-to-site VPN.....                     | 4  |
| Remote Access VPN.....                    | 4  |
| PPTP Overview .....                       | 5  |
| Configuring the PPTP Client .....         | 6  |
| Verifying the PPTP Connection Status..... | 10 |
| PPTP Configuration Example.....           | 11 |

## Notations

The following symbols may be used in this document.



**Note** – The following note provides useful information.



**Important** – The following note includes important information that may require attention.



**Warning** – The following note provides a warning.

# Introduction

A VPN (Virtual private network) is a secure connection between two or more endpoints. It can also be seen as an extension to a private network.

There are two key types of VPN scenarios:

- **Site-to-site VPN**
- **Remote Access VPN**

## Site-to-site VPN

In a site to site VPN, data is encrypted from one VPN gateway to the other, providing a secure link between two sites over a third party insecure network like the Internet.

## Remote Access VPN

In a remote access VPN scenario, a secure connection would be made from an individual computer to a VPN gateway. This would enable a user to access their e-mail, files and other resources at work from wherever they may be, providing they have an Internet connection.

The Vodafone MachineLink router supports three types of Virtual Private Network (VPN) technologies:

- **Point-to-Point Tunnelling Protocol (PPTP) VPN**
- **Internet Protocol Security (IPsec) VPN**
- **OpenVPN**

PPTP is a popular choice when selecting a VPN type, mainly due to the large number of clients supporting it. Windows® Servers may be configured to function as PPTP VPN Servers. Owing to its popularity, the Vodafone MachineLink router has a PPTP client built-in enabling you to utilise this method of securing your data connection.

This document describes how to configure the PPTP client on the Vodafone MachineLink M2M IP Router.

# PPTP Overview

The following diagram illustrates a typical PPTP usage scenario:

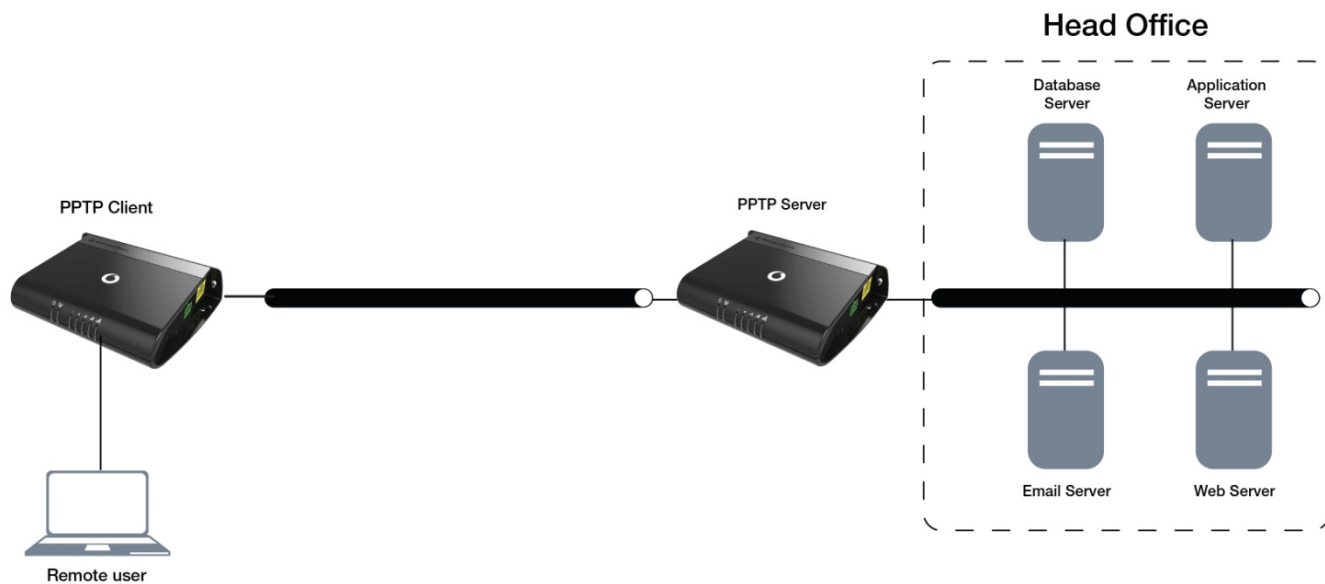


Figure 1 - PPTP Diagram

# Configuring the PPTP Client

- 1 Log in to your MachineLink router using the “root” account.
- 2 Click on **Networking**, then click on the **VPN** menu on the left, then the **PPTP client** item.
- 3 The **PPTP client list** is displayed.

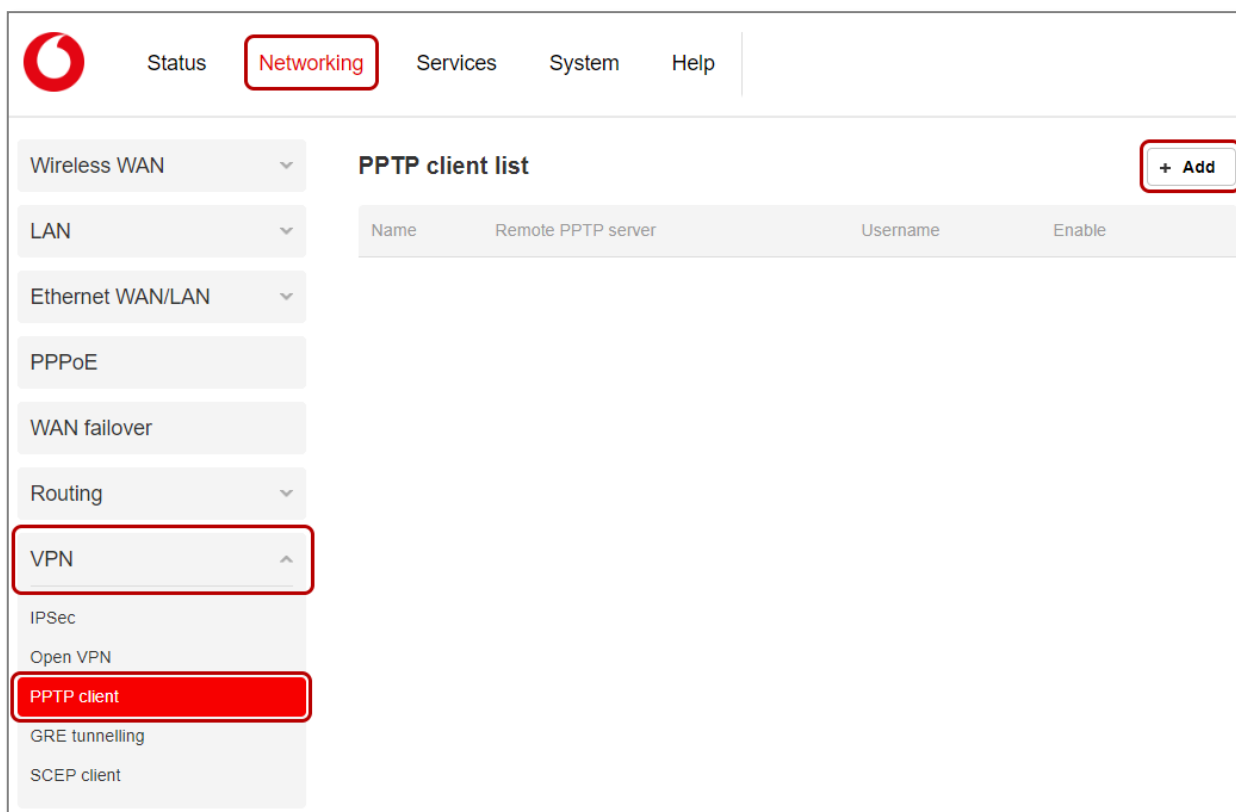


Figure 2 - PPTP Client List

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

### VPN PPTP client edit

Enable PPTP client

Name

Username

Password

PPTP server

Authentication type Any

Metric  (0-65535)

MTU  (68-65535)

Use peer DNS  0

NAT masquerading  0

Set PPTP server as default gateway  0

MPPE

Extra PPP option

Verbose logging  0

Reconnect delay  (30-65535) seconds

Reconnect retries  (0-65535, 0=Unlimited)

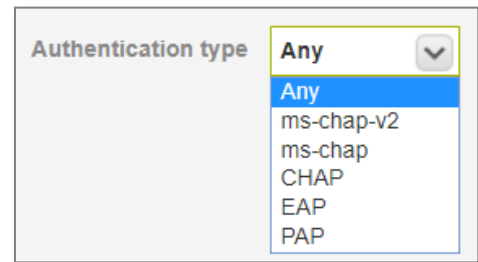
Figure 3 - VPN PPTP client edit

- 5 Click the **Enable PPTP client** toggle key to switch it to the **ON** position.
- 6 In the **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.
- 7 Use the **Username** and **Password** fields to enter the username and password for the PPTP account.
- 8 In the **PPTP server** field, enter the IP address of the PPTP server.
- 9 From the **Authentication type** drop down list, select the Authentication type used on the server.

There are 5 authentication types you can choose from:

- a **Any** – Select if you do not know the authentication method to use and the router will attempt to determine the correct authentication type for you.
- b **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.

- c **MS-CHAP** – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows@ Vista.
- d **CHAP** – uses a three-way handshake to authenticate the identity of a client.
- e **EAP** – The Extensible Authentication Protocol is an authentication protocol commonly used in wireless networks.
- f **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.



- 10 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.
- 11 The **MTU** (Maximum Transmission Unit) determines the maximum size of each packet in any transmission.  
Use the default value of 1300
- 12 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.
- 13 **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.
- 14 **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.
- 15 The **MPPE** toggle key turns the Microsoft Point-to-Point Encryption feature on or off. This is used to secure transmissions.
- 16 In the **Extra PPP option** field, specify any extra commands or parameters that you wish to use when the PPP connection is established.
- 17 The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the **System Log** section of the router interface.
- 18 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.
- 19 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 retries cannot be greater than 65335.
- 20 Click the **Save** button to save the changes.  
The VPN will attempt to connect after your click **Save**.

## PPTP client list

The newly defined **VPN PPTP client** will be added to the **PPTP client list**.



✓ **Success!**  
 Your PPTP client configuration changes were successfully saved and applied

### PPTP client list + Add

| Name            | Remote PPTP server | Username | Enable  |        |   |
|-----------------|--------------------|----------|---------|--------|---|
| PPTP-tunnel-No1 | 114.30.122.119     | root     | enabled | ✎ Edit | ✕ |

*Figure 4 - PPTP Client List*

Check the details and if they are incorrect, click the Edit button to return to the **VPN PPTP client edit** screen to make the necessary changes.

If the PPTP client is no longer required, click the **X** button to permanently remove it.

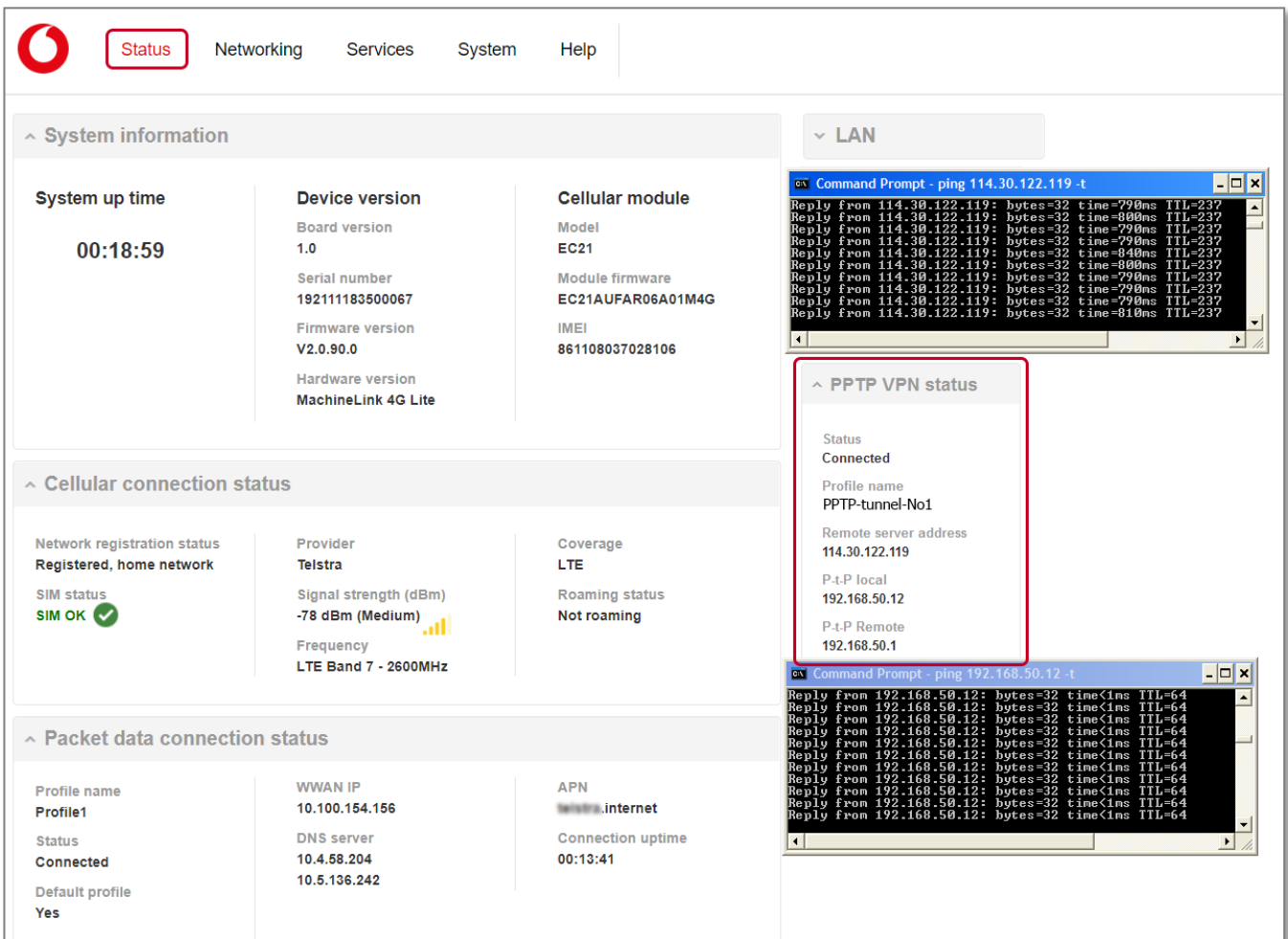
# Verifying the PPTP Connection Status

Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.

Perform a ping test in both directions.

On the server, open a command prompt and ping the client IP address (shown under **P-t-P Local**).

To test the tunnel in the other direction, telnet to the client router (username: root password: your strong password) and ping the **P-t-P Remote** IP address. See the screenshots below for an example.



The screenshot displays the NetCommWireless management interface with the **Status** button highlighted. The interface is divided into several sections:

- System information:**
  - System up time: 00:18:59
  - Device version: Board version 1.0, Serial number 192111183500067, Firmware version V2.0.90.0, Hardware version MachineLink 4G Lite
  - Cellular module: Model EC21, Module firmware EC21AUFAR06A01M4G, IMEI 861108037028106
- Cellular connection status:**
  - Network registration status: Registered, home network
  - SIM status: SIM OK
  - Provider: Telstra
  - Signal strength (dBm): -78 dBm (Medium)
  - Frequency: LTE Band 7 - 2600MHz
  - Coverage: LTE
  - Roaming status: Not roaming
- Packet data connection status:**
  - Profile name: Profile1
  - Status: Connected
  - Default profile: Yes
  - WWAN IP: 10.100.154.156
  - DNS server: 10.4.58.204
  - APN: internet
  - Connection uptime: 00:13:41
- LAN:** A command prompt window showing a successful ping test to 114.30.122.119. The output shows 10 successful replies with varying times and TTL values.
- PPTP VPN status:** A red box highlights the PPTP VPN status section, which shows:
  - Status: Connected
  - Profile name: PPTP-tunnel-No1
  - Remote server address: 114.30.122.119
  - P-t-P local: 192.168.50.12
  - P-t-P Remote: 192.168.50.1
- Command Prompt:** A second command prompt window shows a successful ping test to 192.168.50.12. The output shows 10 successful replies with times <1ms and TTL=64.

Figure 5 – PPTP connection verification

# PPTP Configuration Example

The following details were entered for the **PPTP-tunnel-No1** PPTP client.

### VPN PPTP client edit

Enable PPTP client

Name

Username

Password

PPTP server

Authentication type

Metric  (0-65535)

MTU  (68-65535)

Use peer DNS

NAT masquerading

Set PPTP server as default gateway

MPPE

Extra PPP option

Verbose logging

Reconnect delay  (30-65535) seconds

Reconnect retries  (0-65535, 0=Unlimited)

Figure 6 – PPTP Client configuration example