vodafone

Vodafone MachineLink

OpenVPN Configuration Guide

Doc No CG01210

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

Note – This document is subject to change without notice.

Contents

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**

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.

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**

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. The Vodafone MachineLink router supports three different OpenVPN modes:

- **OpenVPN Server**
- **OpenVPN Client**
- **OpenVPN Peer-to-Peer VPN connection.**

This document describes how to configure the different OpenVPN types on the Vodafone MachineLink router.

Important notes about OpenVPN on the Vodafone MachineLink router

- When using two MachineLink routers in a Server-Client scenario, you should change the LAN IP Address of the devices so that they are on different subnets, otherwise you may find it impossible to access the web-interface of one of the routers when an OpenVPN connection is established.
- A MachineLink router acting as a Server must be connected to an APN that provides a publicly routable IP address.
- OpenVPN Certificates and Secret Keys are dependent on the time on each router being in synchronisation. If the time is not correct on the router due to NTP not working or for any other reason, the certificate or secret key timestamp may be expired and hence will not be useable.
- If both the OpenVPN Server and OpenVPN Client are in a private network, please ensure that the server is routable to the client and vice-versa before establishing the VPN connection.

OpenVPN Server Mode

In OpenVPN Server Mode, a MachineLink router acts as a host allowing M2M Routers in client mode or Windows/Linux software clients to establish a virtual private network connection. In order to establish a secure communications channel, a cryptographic key is exchanged between the server and the client using the Diffie-Hellman method of key exchange. Once a shared secret is established, certificates identifying each client node are issued which can be used as a means of authentication.

OpenVPN authentication is achieved through first establishing a public key infrastructure. The public key infrastructure includes:

- A public and private key for the server and each client
- A master Certificate Authority (CA) certificate and the key used to sign each of the server and client certificates.

This authentication method results in several benefits:

- The server only needs its own certificate and key. It does not need to have every certificate of every client that may connect to it.
- The server will only accept clients with certificates that were signed by the master certificate authority.
- If the security of a client certificate is compromised, that individual certificate can be revoked without requiring a new public key infrastructure to be generated.
- The server can enforce access rights for specific clients based on the certificate fields.

While certificate authentication is the more secure and desirable means of authentication, it is also possible to use a username and password for authentication. Username and password authentication is not used in conjunction with certificates.

An OpenVPN Server allows for one or many client routers to establish secure communication tunnels as illustrated below:

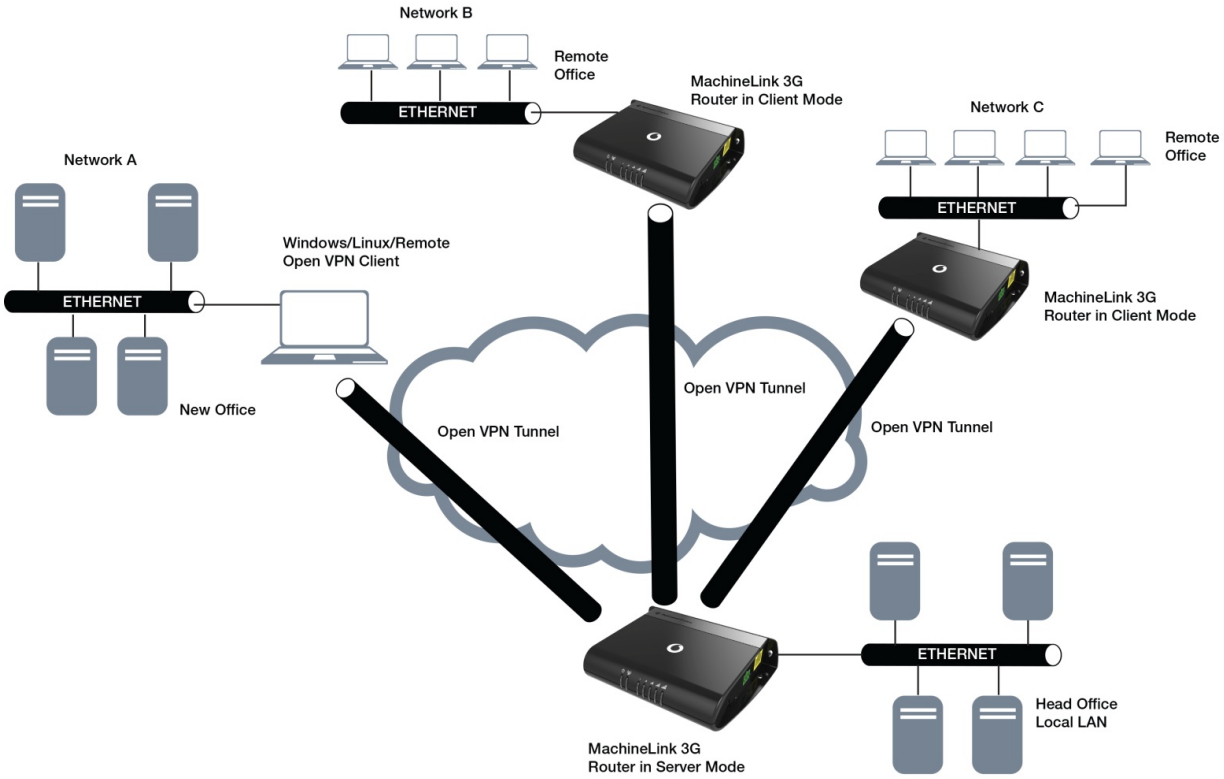


Figure 1 - OpenVPN Server Mode Diagram

Configuring an OpenVPN Server

1 Login to your MachineLink router using the “root” account.

2 Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **Open VPN** item.

3 The three types of OpenVPN lists are displayed.

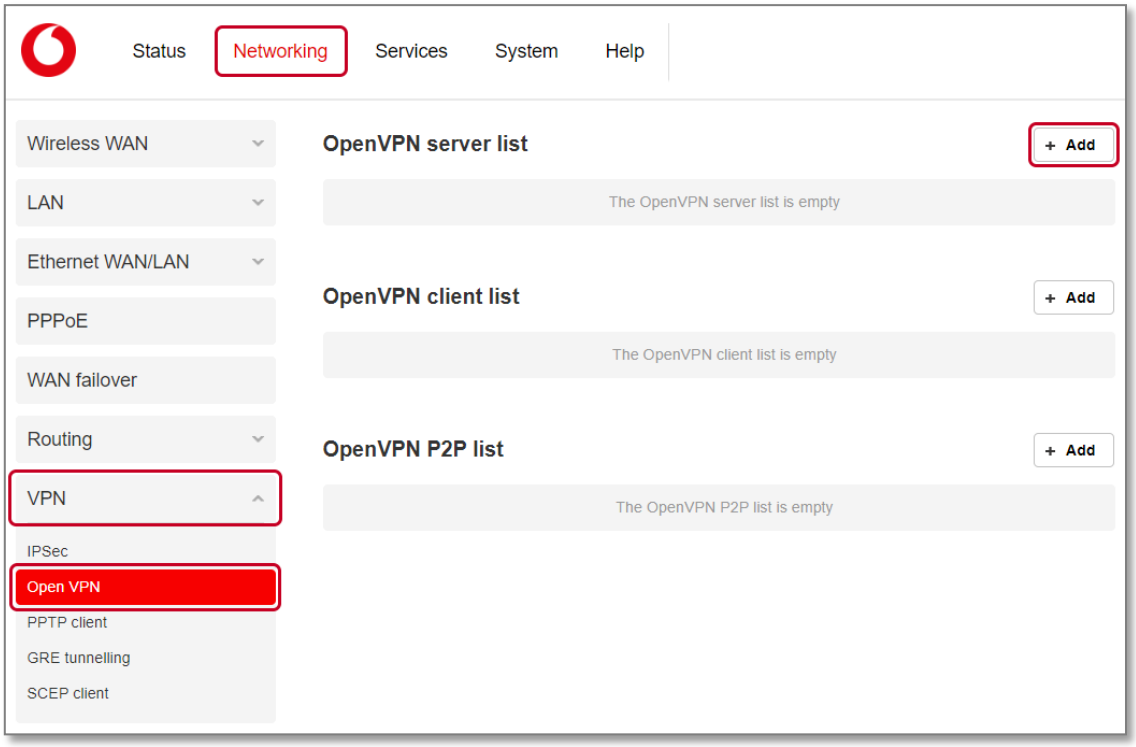


Figure 2 - OpenVPN profile list

4 Click the **+Add** button next to the **OpenVPN server list**. If you have not yet created a server certificate, a dialog box appears to prompt you to create one. Click the **OK** button.

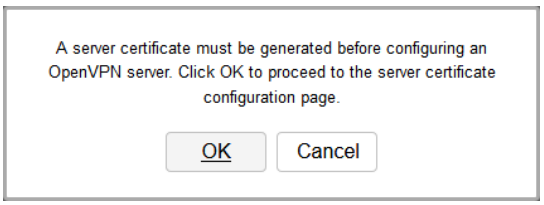


Figure 3 - Server certificate prompt

If you have already created a server certificate, skip to step 5.

Generating your own self-signed certificate

5 To generate your own self-signed certificate:

a Select a **Server key size**. A larger key size takes longer to generate but provides better security.

b Click the **Generate** button to begin generating Diffie-Hellman parameters.

c Enter the certificate details using the appropriate fields. All fields must be completed to generate a certificate.

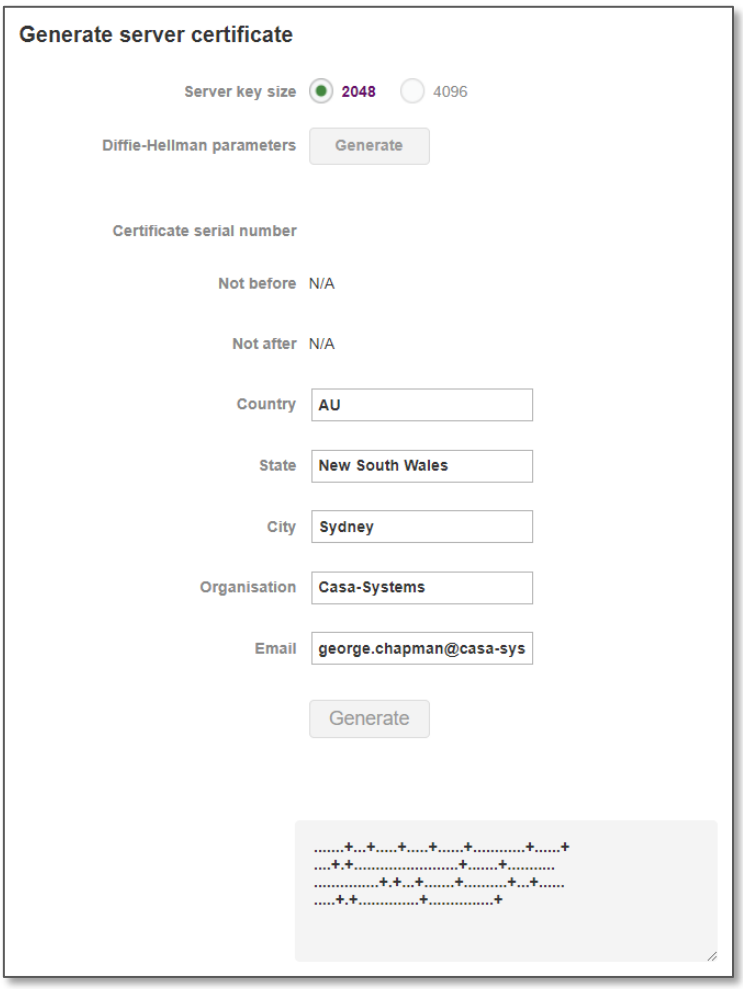


Figure 4 - Generate server certificate

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

d When you have entered all the required details, press the **Generate** button.

The certificate takes several minutes to generate.

e When the certificate has been generated, you are informed that it has been successfully generated and installed:

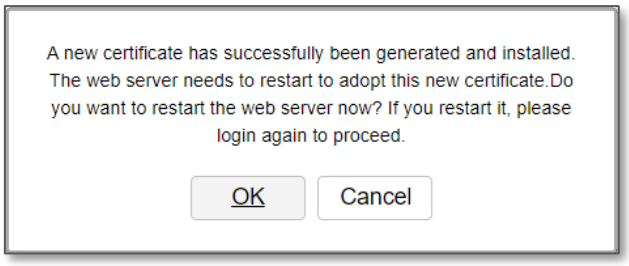


Figure 5 - New certificate successfully generated message

f Click **OK** to be taken back to the login screen.

g The web server on the router restarts and you are logged out of the router.

1 Login to your MachineLink router using the “root” account.

2 Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **Open VPN** item.

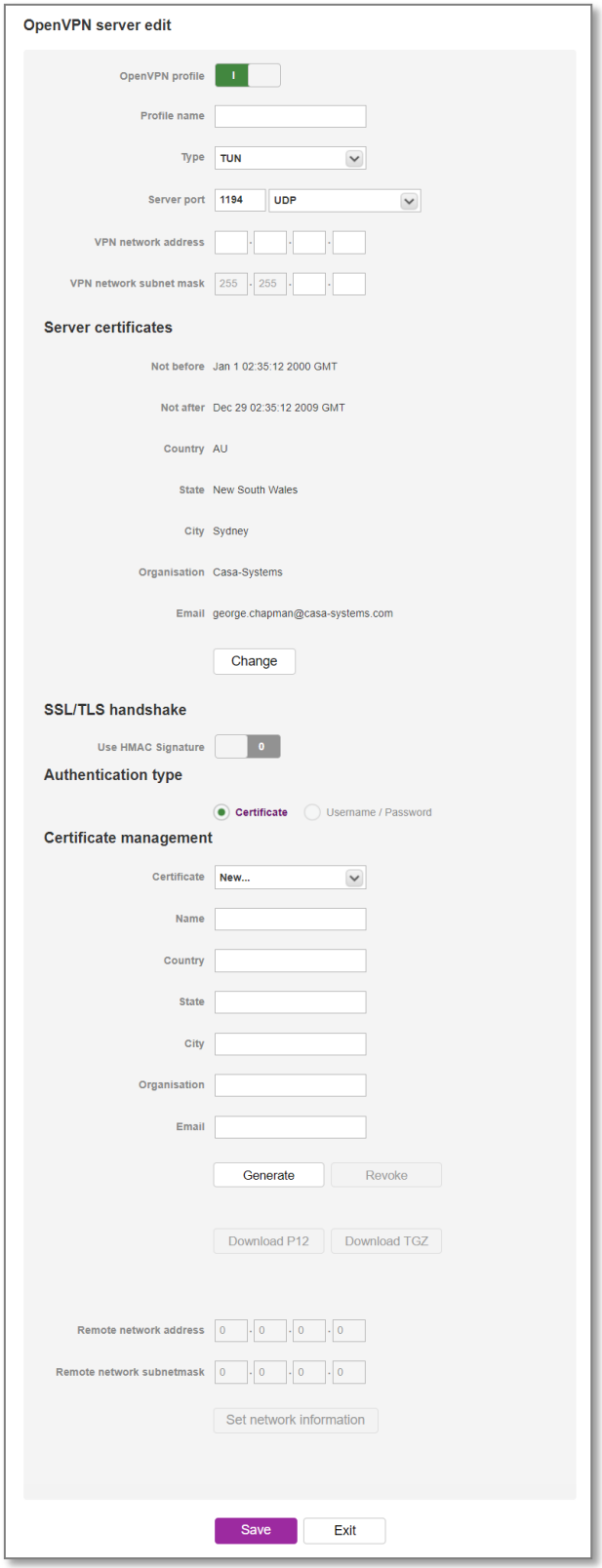


Figure 6 - OpenVPN Server configuration page

3 Set the OpenVPN profile option to **ON.**

4 In the **Profile name** field, type a name for the OpenVPN Server profile you are creating. This is used to identify the OpenVPN connection on the router.

5 Use the **Type** field to select TUN or TAP.

6 Use the **Server port** fields to enter a port number and select a packet type to use for your OpenVPN Server. The default OpenVPN port is 1194 and default packet type is UDP.

7 In the **VPN Network Address** and **VPN Network Mask** fields, enter the IP address and network mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme. The default settings may be used if you wish.

8 HMAC or Hash-based Message Authentication Code is a means of calculating a message authentication code through the use of a cryptographic hash function and a cryptographic key. If you wish to use the HMAC signature as an additional key and level of security, under the SSL/TLS handshake section, click the **Use HMAC Signature** toggle key so that it is in the **ON** position, then click the **Generate** button so that the router can randomly generate the key. The Server key timestamp field is updated with the time that the key was generated. Click the **Download** button to download the key file so that it can be uploaded on the client.

9 Under **Certificate Management**, enter the required details. All fields must be completed. The **Country** field must consist of one of the country codes listed in the Appendix. When the details have been entered, click the **Generate CA certificate** button to generate the Certificate Authority (CA) certificate based on this information.

10 Select the **Authentication Type** that you would like to use for the OpenVPN Server: ⦿ **Certificate** or ⦿ **Username/Password**

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.

Certificate Authentication

a In the **Certificate Management** section, enter the required details to create a client certificate. All fields are required.

b When you have finished entering the details, click the **Generate** button. The certificate should only take a moment to generate.

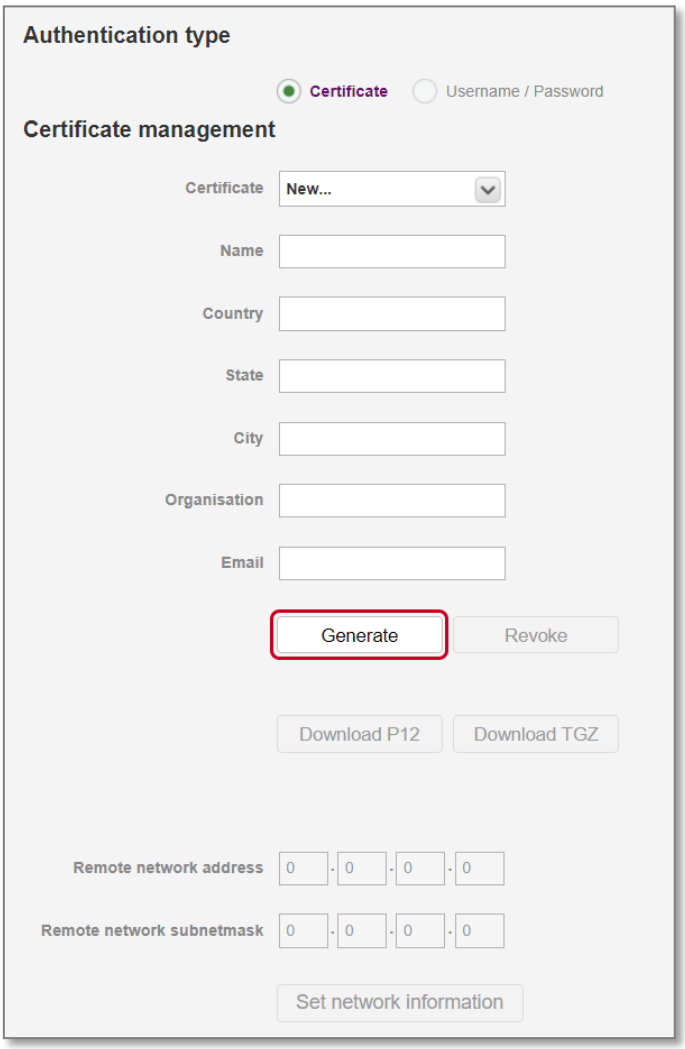


Figure 7 - OpenVPN Server - Certificate Management section

c When it is done, you can click the **Download** button to save the certificate file. 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.

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

Username / Password Authentication

e 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 certificate** button to save the **ca.crt** file. This file will need to be provided to the client.

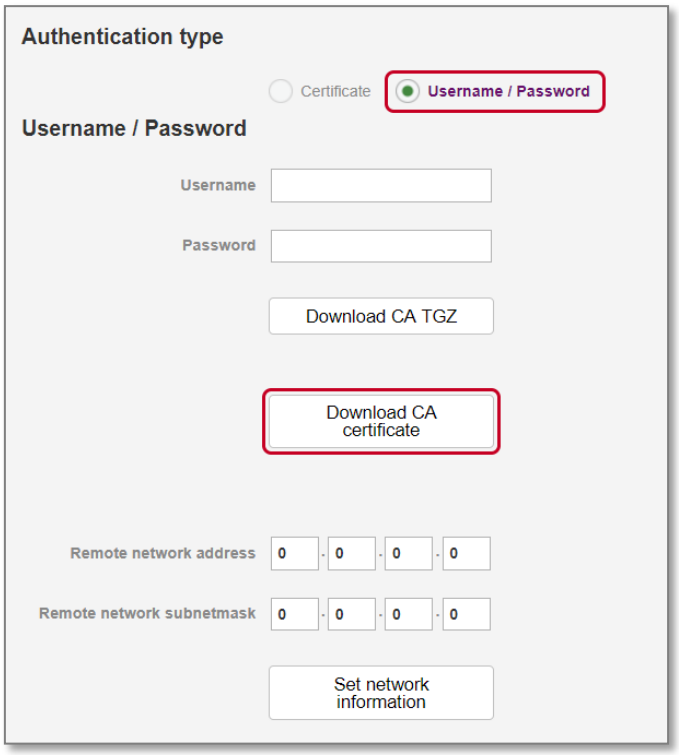


Figure 8 - OpenVPN Server - Username/Password section

f **Optional –** To inform the OpenVPN Server of the network address scheme of the currently selected certificate, enter the **Remote network address** and **Remote network subnetmask** in the respective fields. 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.

g When done, click the **Set network information** button.

11 When you have finished entering all the required information, click the **Save** button to finish configuring the OpenVPN Server.

OpenVPN Server Examples

OpenVPN Server Mode – Certificate Authentication

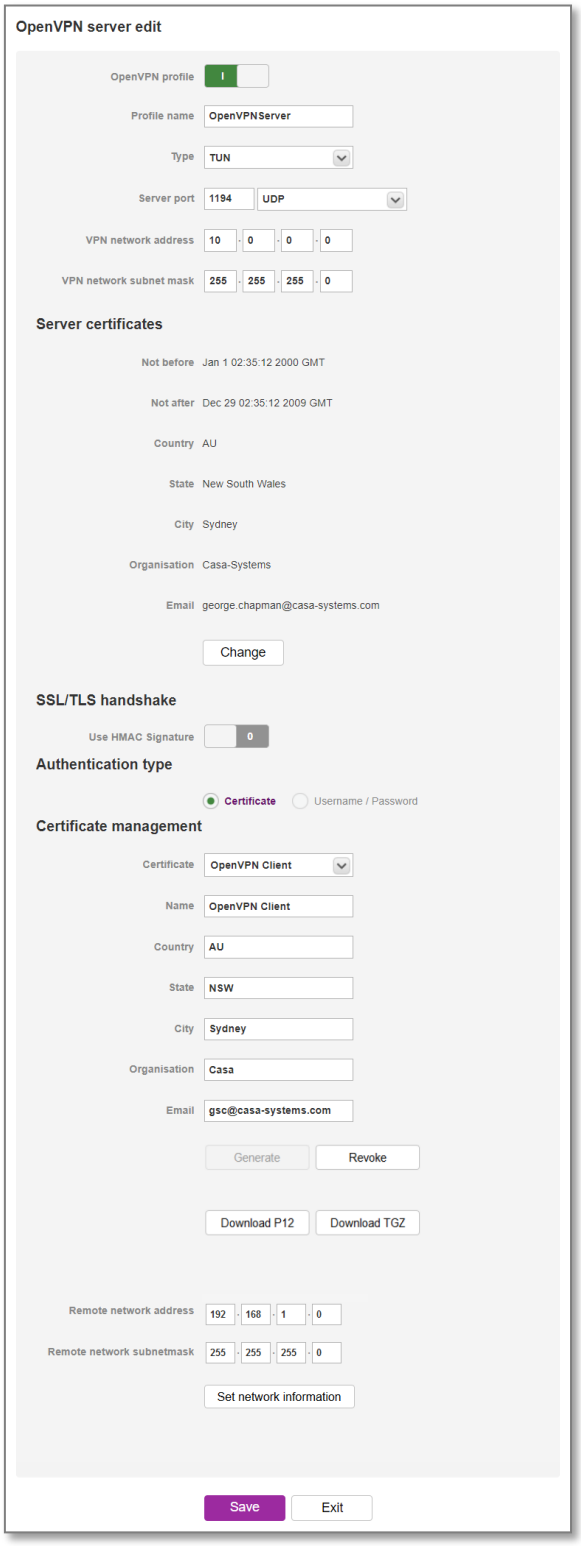


Figure 9 - OpenVPN Server - Certificate Authentication Example page

OpenVPN Server Mode – Username / Password Authentication

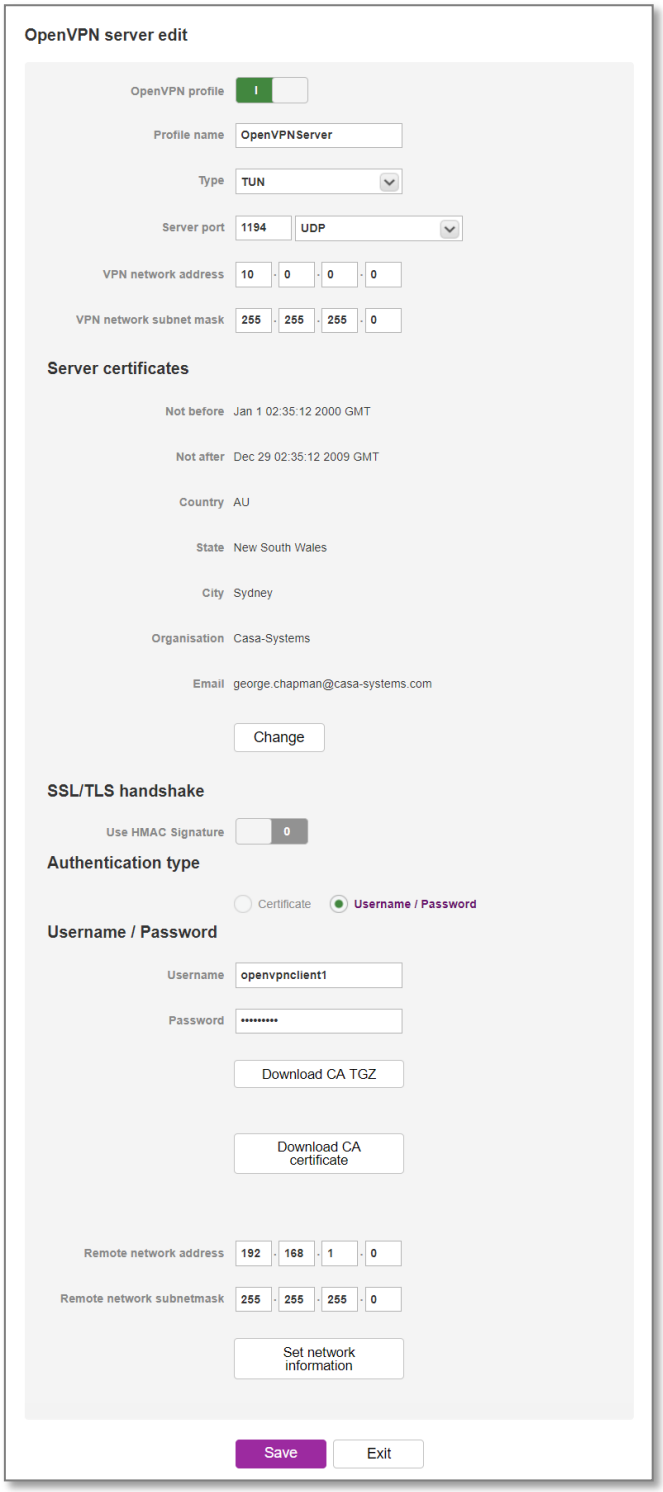


Figure 10 - OpenVPN Server - Username / Password Authentication Example page

Verifying the OpenVPN Connection Status

Open a command prompt and ping a client in the remote subnet and the OpenVPN Gateway address assigned to the remote router. See the screenshot below for an example.

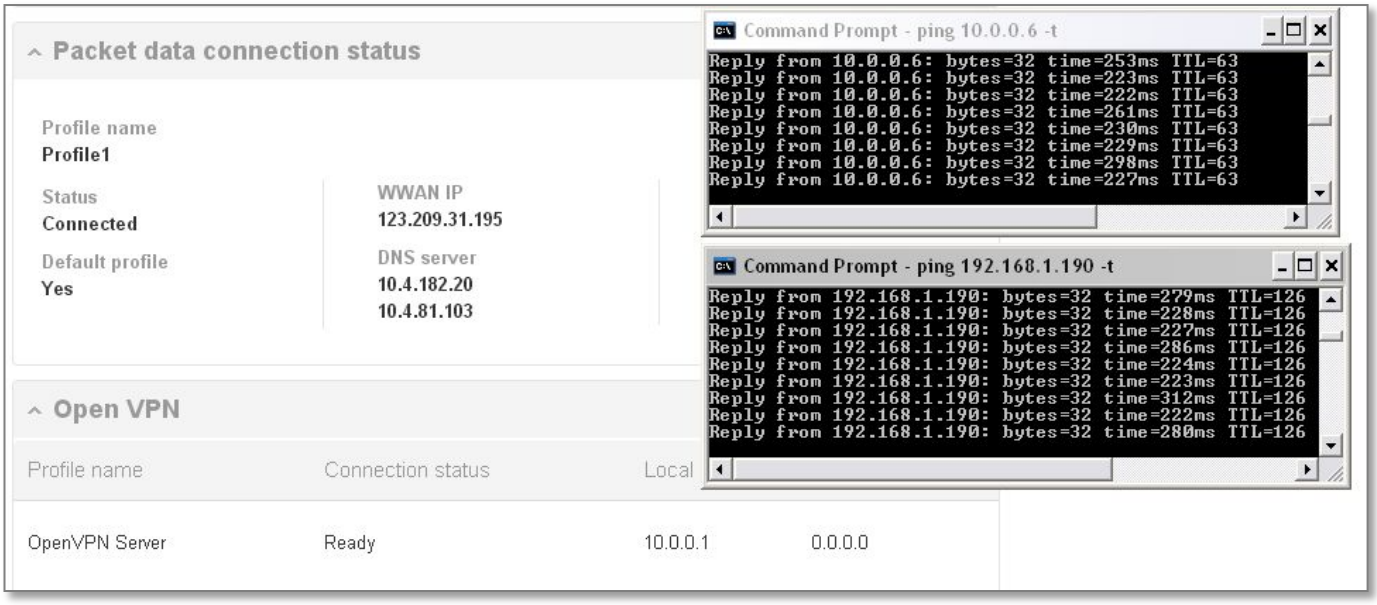


Figure 11 - OpenVPN Server connection verification

OpenVPN Client Mode

The Vodafone MachineLink router may be configured to operate as an OpenVPN Client and connect to an OpenVPN Server running on another MachineLink router or a software OpenVPN Server on a computer.

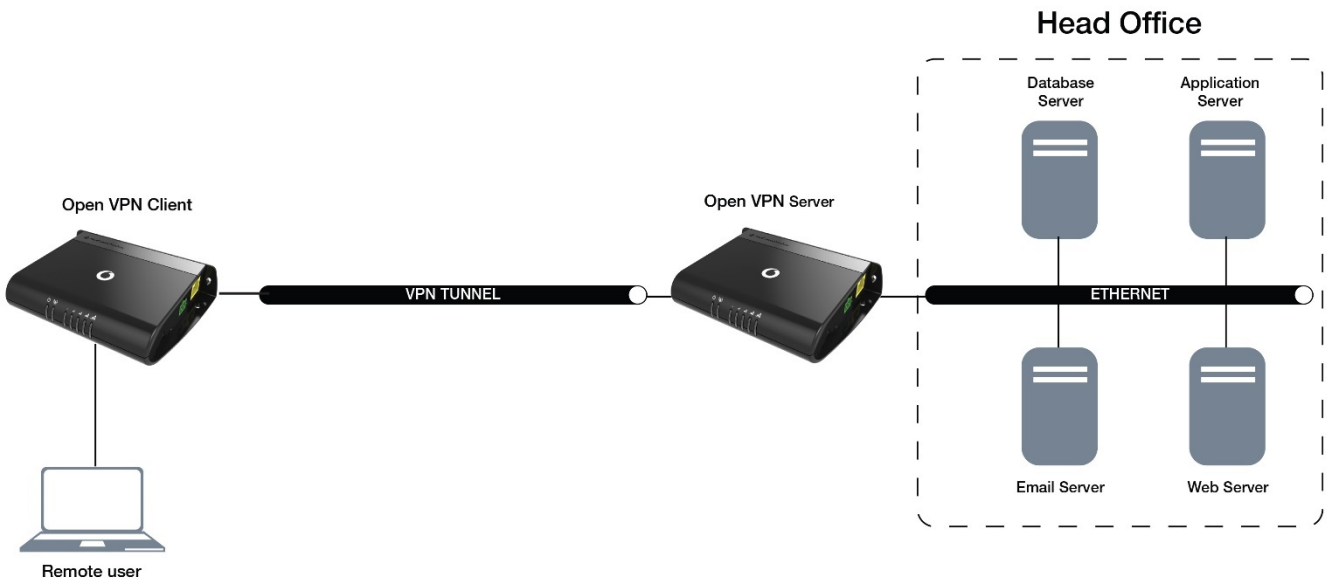


Figure 12 - OpenVPN Client mode diagram

Certificate Files

When using two MachineLink routers to establish an OpenVPN connection, the certificate generated by the server will be recognised by the client and will not require modification.

In situations where you are using another third-party OpenVPN Server to generate certificates, the MachineLink router will expect a tar archive compressed using GZip. There are three files that the OpenVPN client in the MachineLink router will expect to see within a .tgz file:

- The master Certificate Authority (CA) certificate file named **ca.crt**
- Client certificate file (e.g., **OpenVPN Test Client.crt**)
- Client key file (e.g., **OpenVPN Test Client.key**)

If you have used a third-party OpenVPN Server to generate certificates and keys, you will need to archive these three files in a **.tgz** file to provide the OpenVPN Client on your MachineLink router.

You can perform this in Linux by using the command:

```
tar -zcvf netcommclient.tgz netcommclient.crt netcommclient.key ca.crt
```

For more information on creating .tgz files, please refer to http://www.cs.duke.edu/~ola/courses/programming/tar.html

Configuring an OpenVPN Client

12 Login to your Vodafone MachineLink router using the "root" account.

13 Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **OpenVPN** item.

14 The OpenVPN lists are displayed.

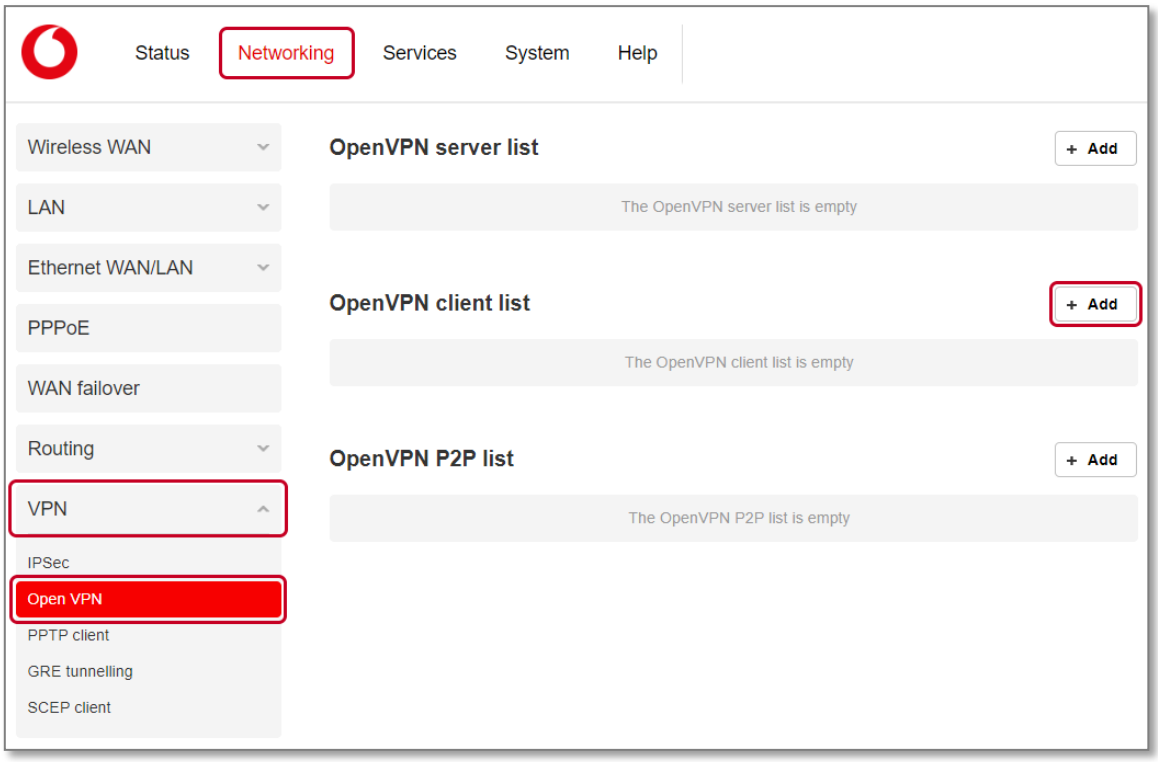


Figure 13 - OpenVPN profile list

15 Click the **+Add** button next to the **OpenVPN client list**.

16 The **Open VPN client edit** window is displayed.

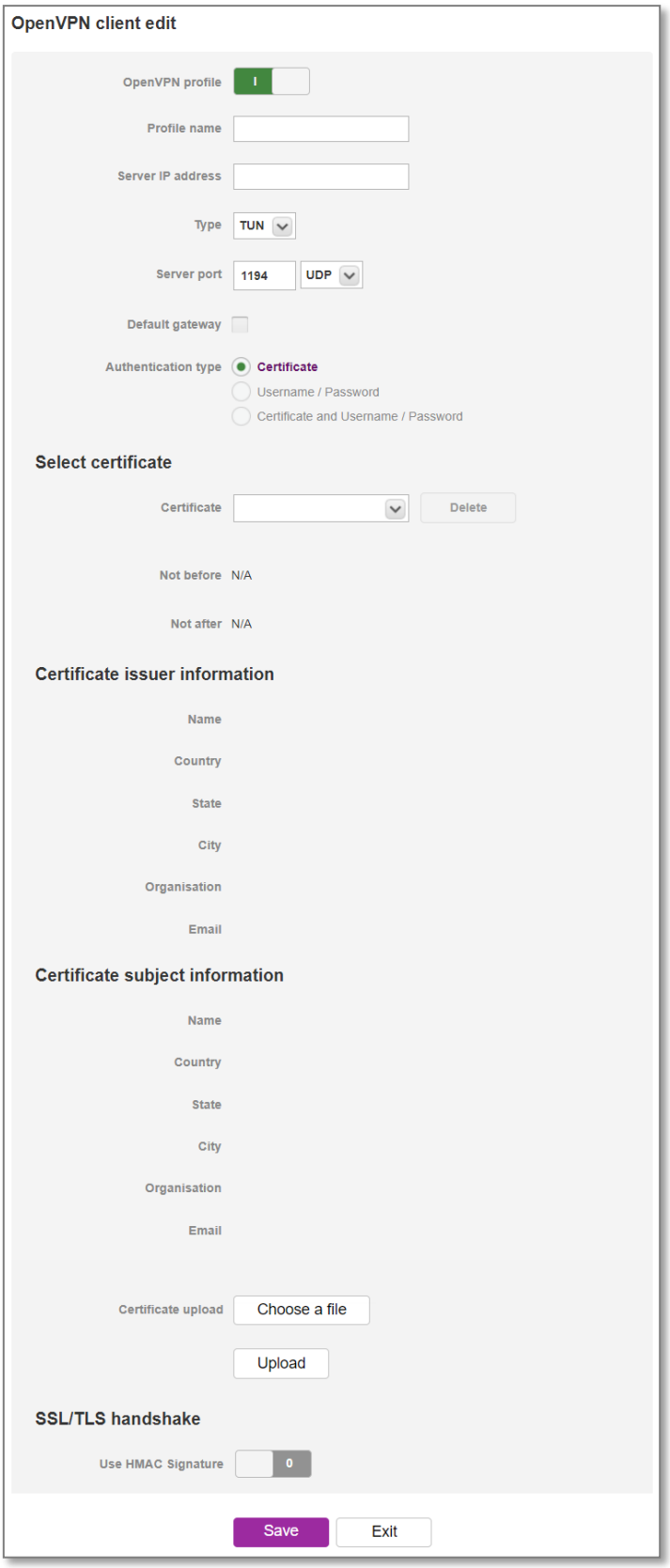


Figure 9 - OpenVPN Client - Configuration page

17 Set the **OpenVPN profile** option to **ON.**

18 In the **Profile name** field type a name for the OpenVPN Client profile you are creating.

19 In the **Server IP address** field type the WAN IP address of the OpenVPN Server.

20 In the **Server port** fields enter the Server Port and packet type (UDP or TCP) to use for the connection.

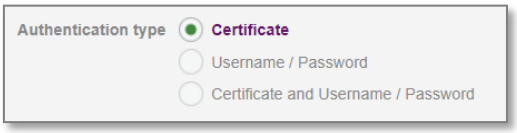
21 If the **Default gateway** option is applied on the OpenVPN Client page, the OpenVPN Server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between the remote office and the head office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

22 For the **Authentication type** option, select the authentication type that you would like to use for the OpenVPN Client:

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

Certificate Authentication

If you want to exclusively use a Certificate as your method of authentication select the ⦿ **Certificate** option.



A group of fields specifically related to this mode of authentication will populate the window:

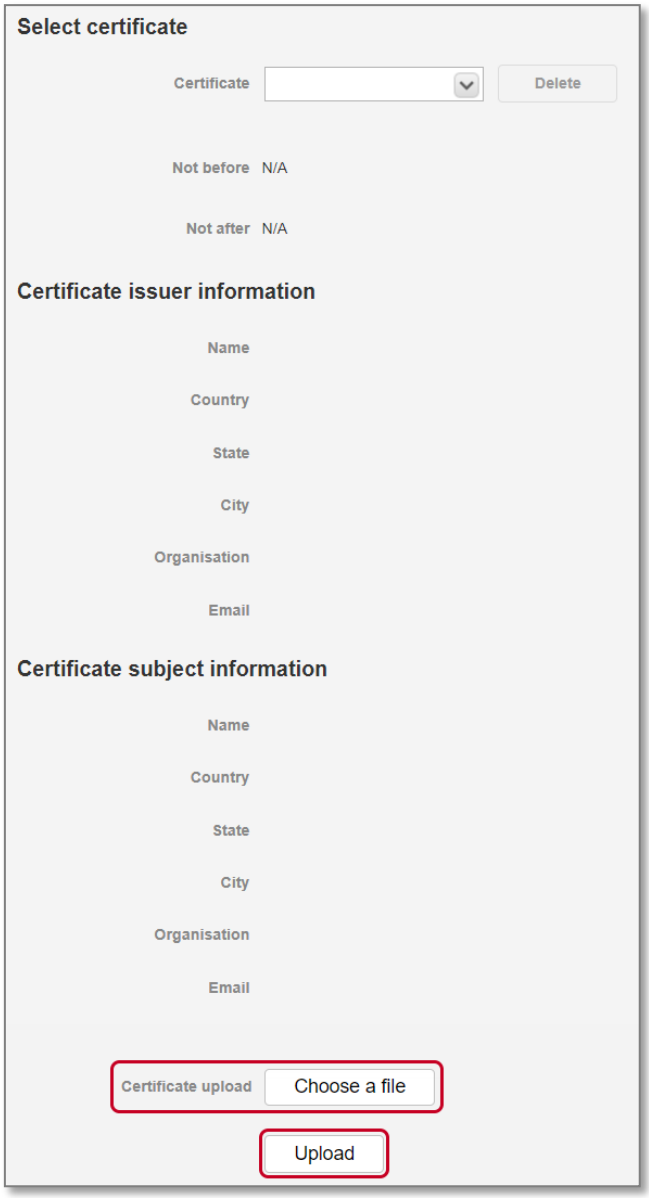


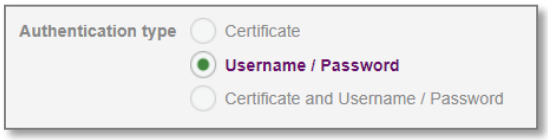
Figure 14 - OpenVPN Client - Certificate Authentication section

1 Click the **Choose file** button and locate the certificate file you downloaded when you configured the OpenVPN Server.

2 When it has been selected, click the **Upload** button to send it to the router.

Username / Password Authentication

If you want to exclusively use Username and Password as your method of authentication select the ⦿ **Certificate** option.



A group of fields specifically related to this mode of authentication will populate the window:

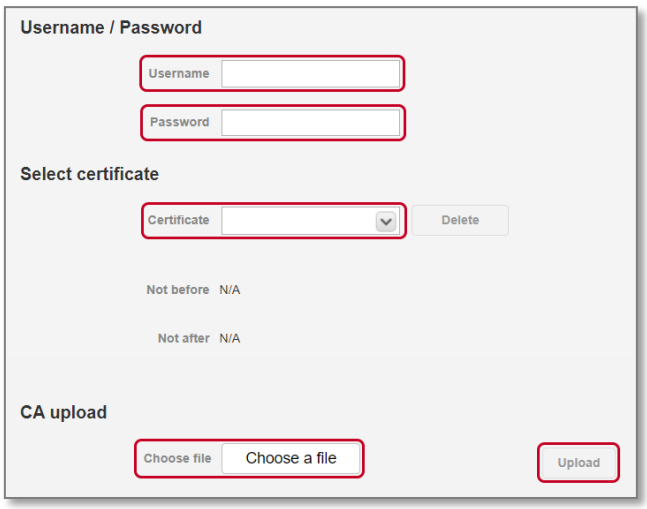


Figure 15 - OpenVPN Client - Username/Password section

a Enter the **Username** and **Password** to authenticate with the OpenVPN Server.

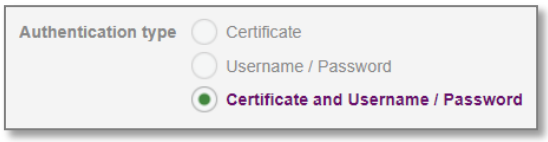
b Use the **Browse** button to locate the CA certificate file you saved from the OpenVPN Server.

c Click the **Upload** button to send it to the router.

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

Use both Modes

Alternatively, you can use both modes of authentication. Select **Certificate and Username / Password**.



All the fields described in the previous two sections will populate the window.

OpenVPN Client Example

OpenVPN Client – Certificate Authentication

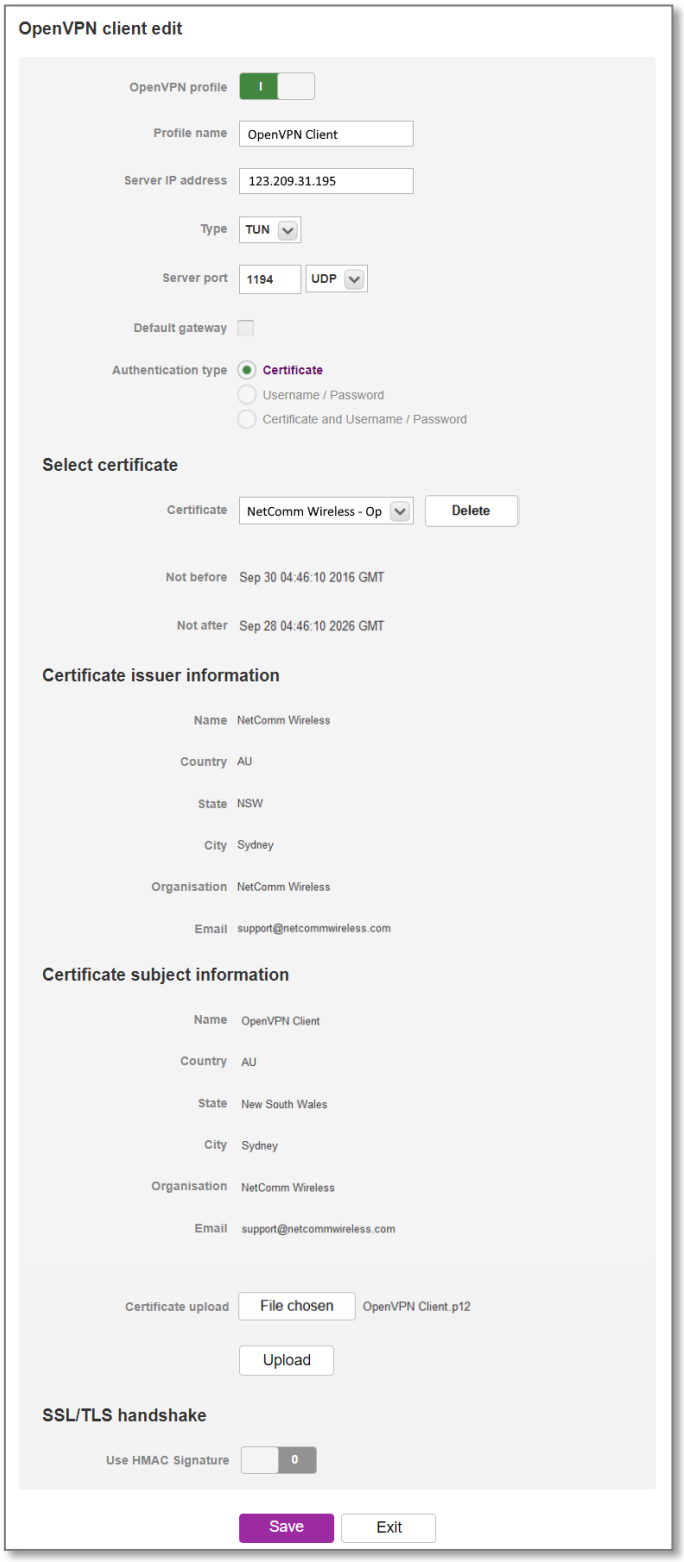


Figure 16 - OpenVPN Client Mode - Certificate Authentication Example

OpenVPN Client – Username / Password Authentication

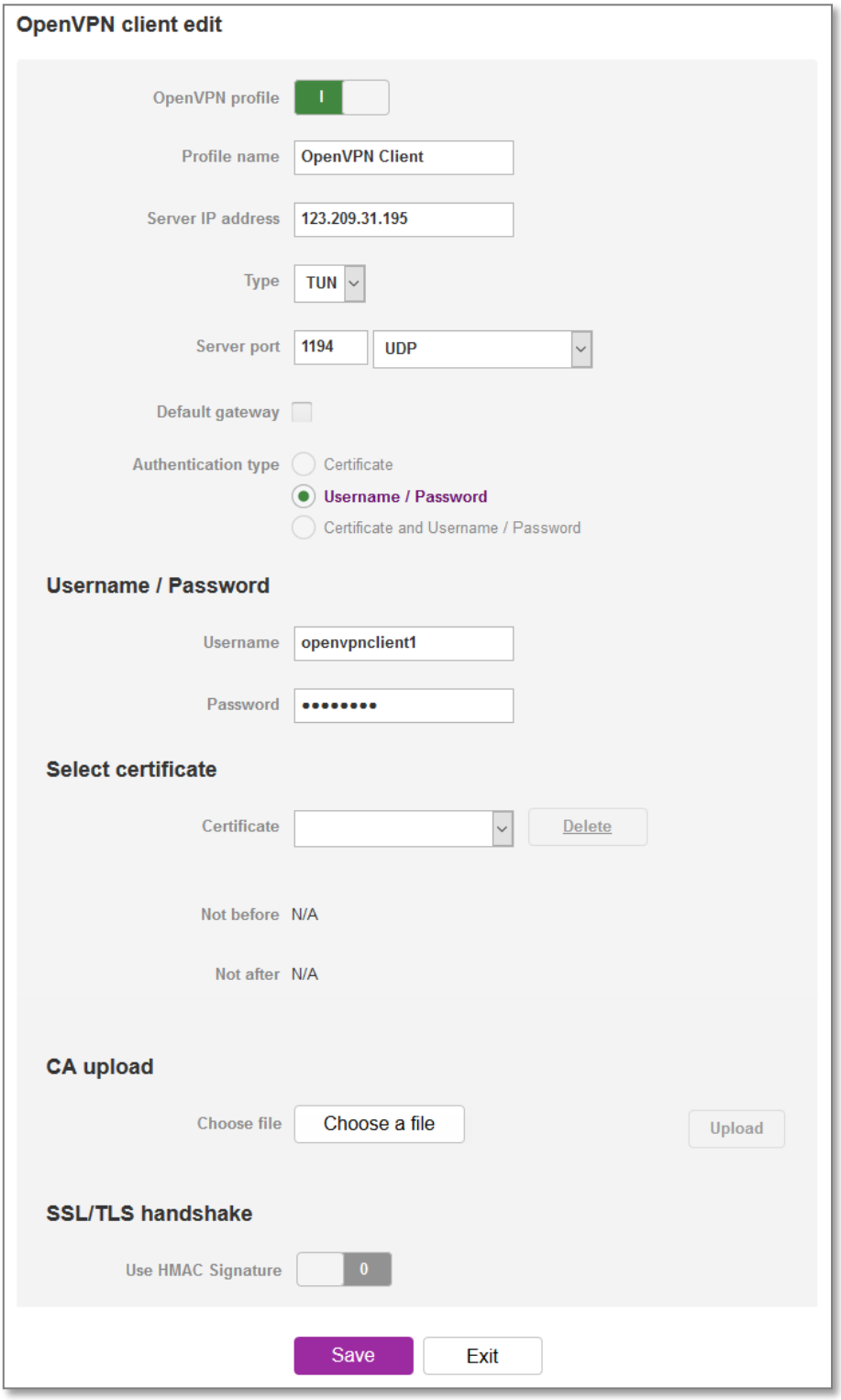


Figure 17 - OpenVPN Client Mode - Username / Password Authentication Example

Verifying the OpenVPN Connection Status

Open a command prompt and ping the OpenVPN Gateway address assigned to the remote router. See the screenshot below for an example.

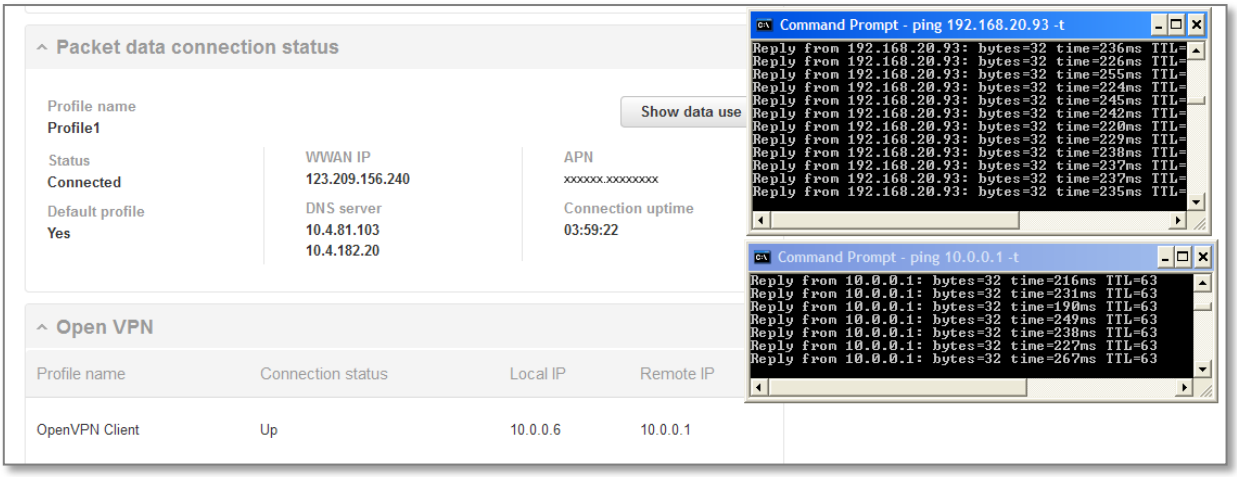


Figure 18 - OpenVPN Client verification of connection

OpenVPN Peer-To-Peer Mode

OpenVPN Peer-To-Peer Mode is the quickest and easiest way to establish a secure connection between two points. In Peer-To-Peer Mode one node acts as a master and accepts a single connection from a slave.

In OpenVPN Peer-To-Peer mode, both the master and the slave generate a secret key which is then passed on to the other for authentication. This is the only form of authentication available in Peer-To-Peer mode.

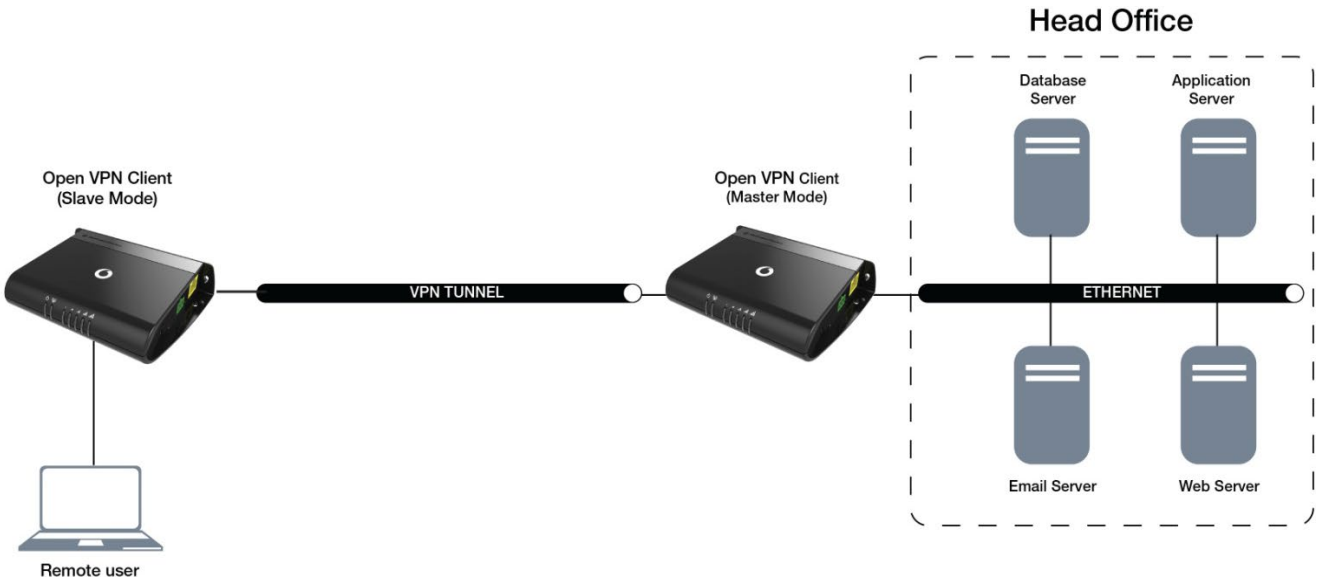


Figure 19 - OpenVPN Peer-To-Peer mode diagram

Configuring an OpenVPN Peer-To-Peer Connection

Perform the following steps on two Vodafone MachineLink routers:

1. Login to your MachineLink routers using the “root” account.
2. Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **OpenVPN** item**.** The OpenVPN lists are displayed.

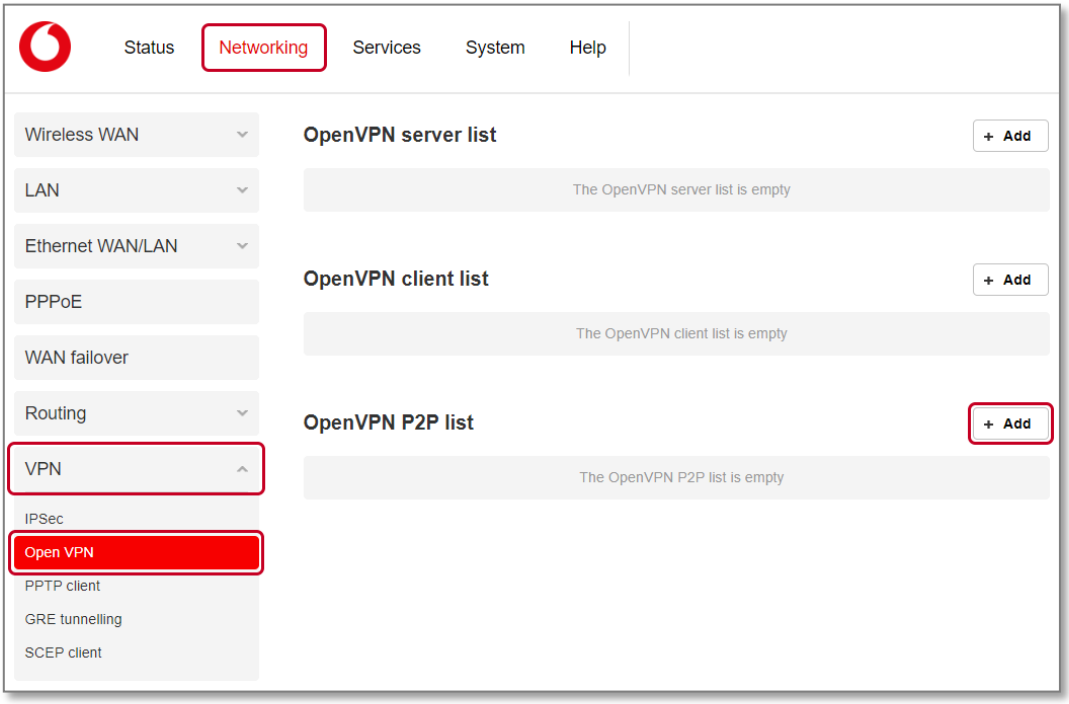


Figure 20 - OpenVPN profile list

3 Click the **+Add** button next to the **OpenVPN P2P list**. The configuration window is displayed.

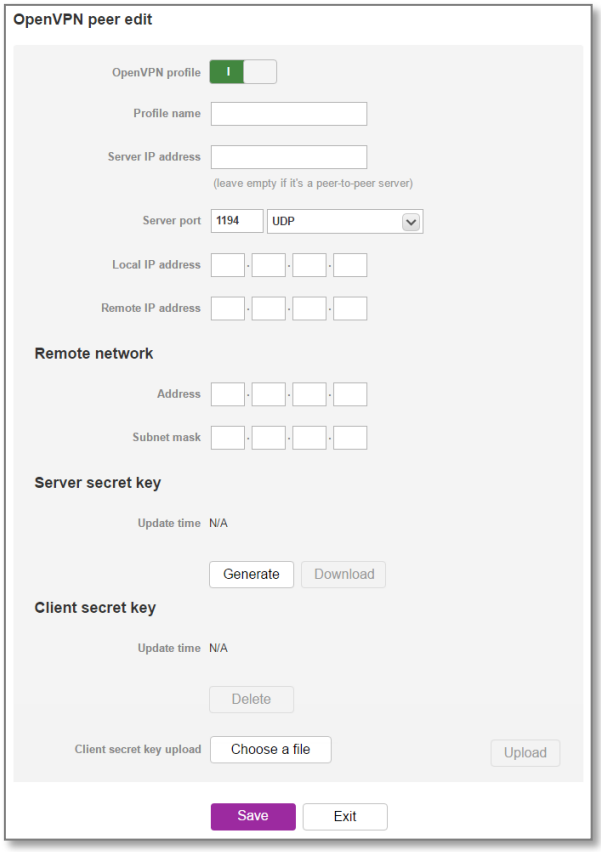


Figure 9 - OpenVPN Peer-To-Peer Mode

4 Set the **OpenVPN profile** option to **ON.**

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

6 In the **Server IP address** field, type the WAN IP address of the OpenVPN Server.

7 In the **Server port** field, enter the Server Port and packet type to use for the connection.

8 In the **Local IP address** and **Remote IP address** fields, enter the local and remote IP addresses to use for the OpenVPN tunnel. The slave should have the reverse settings of the master.

9 Under the Remote Network section, enter the network address and network mask. The Network Address and Network Mask fields inform the Master node of the LAN address scheme of the Slave.

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

11 When you have saved the secret key file on each router, use the **Browse** button to locate the secret key file for the master and then press the **Upload** button to send it to the slave. Perform the same for the other router, uploading the slave's secret key file to master.

12 When they are uploaded click the **Save** button to complete the Peer-To-Peer OpenVPN configuration.

OpenVPN Peer-To-Peer Example

OpenVPN Peer-To-Peer Master

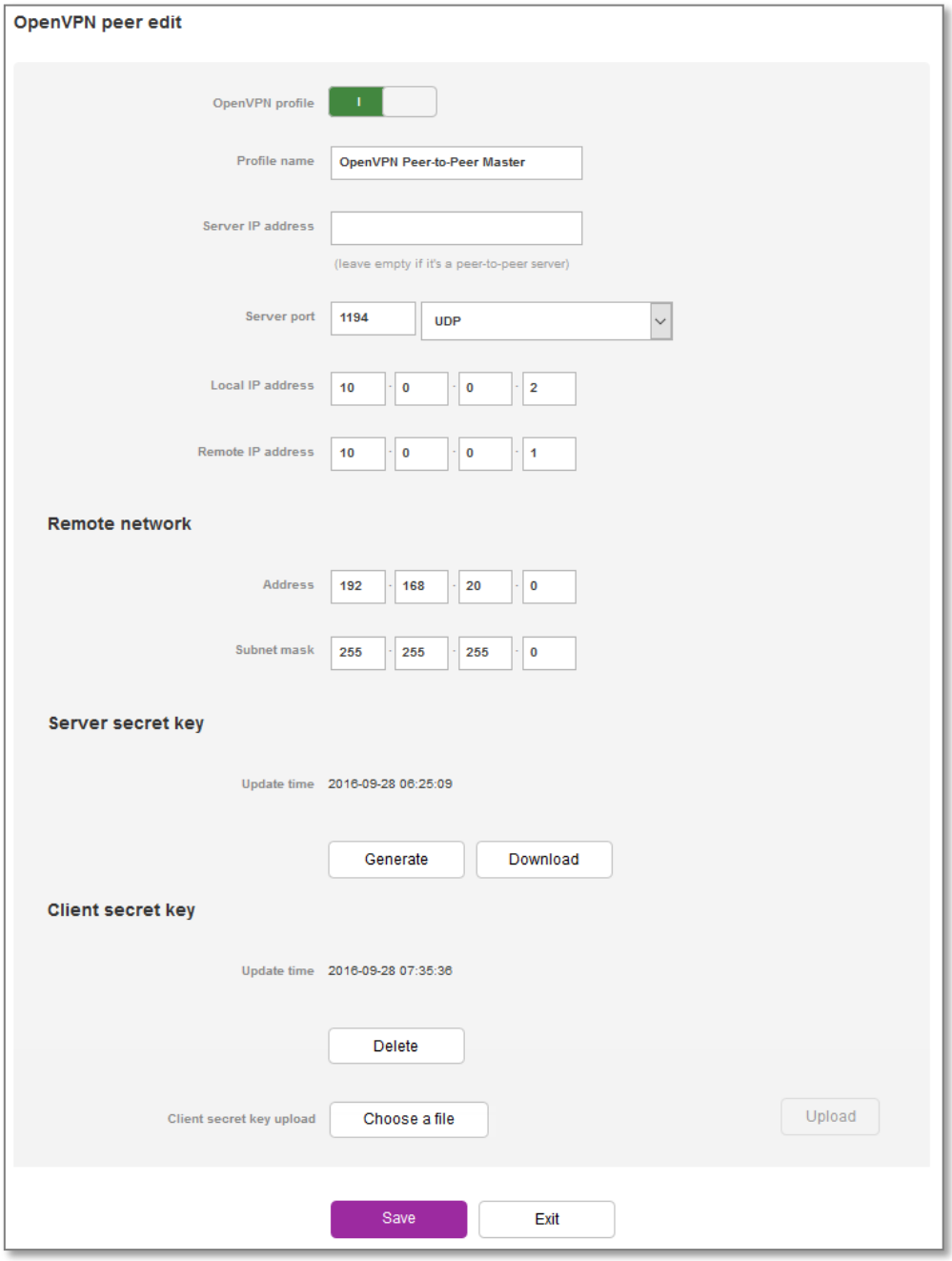


Figure 21 - OpenVPN Peer-To-Peer Master example

OpenVPN Peer-To-Peer Slave

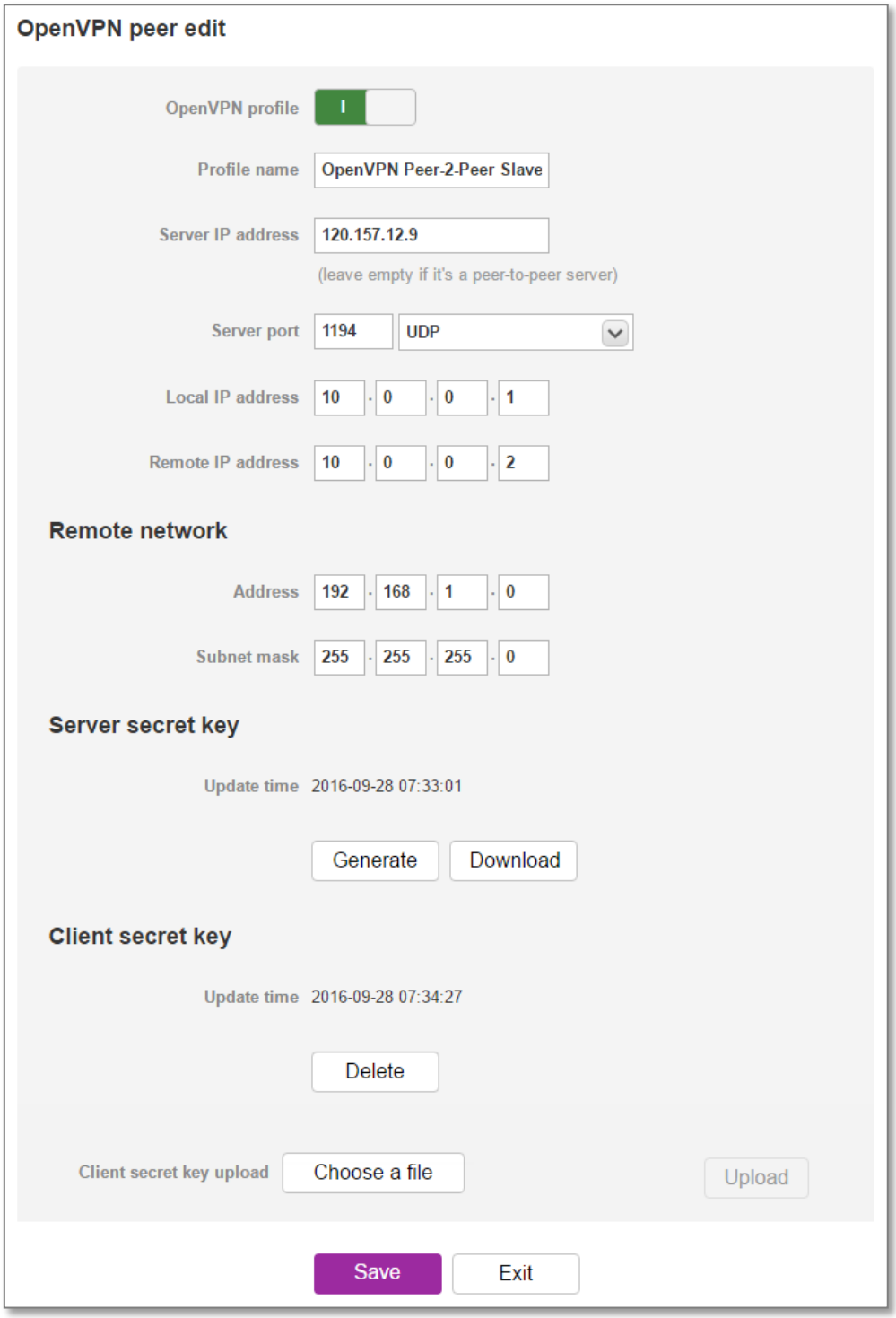


Figure 22 - OpenVPN Peer-To-Peer Slave example

Verifying the OpenVPN Peer-To-Peer Connection Status

Open a command prompt on either the master or the slave and ping the OpenVPN Gateway address assigned to the remote router. See the screenshots below for an example.

OpenVPN Peer-To-Peer Master

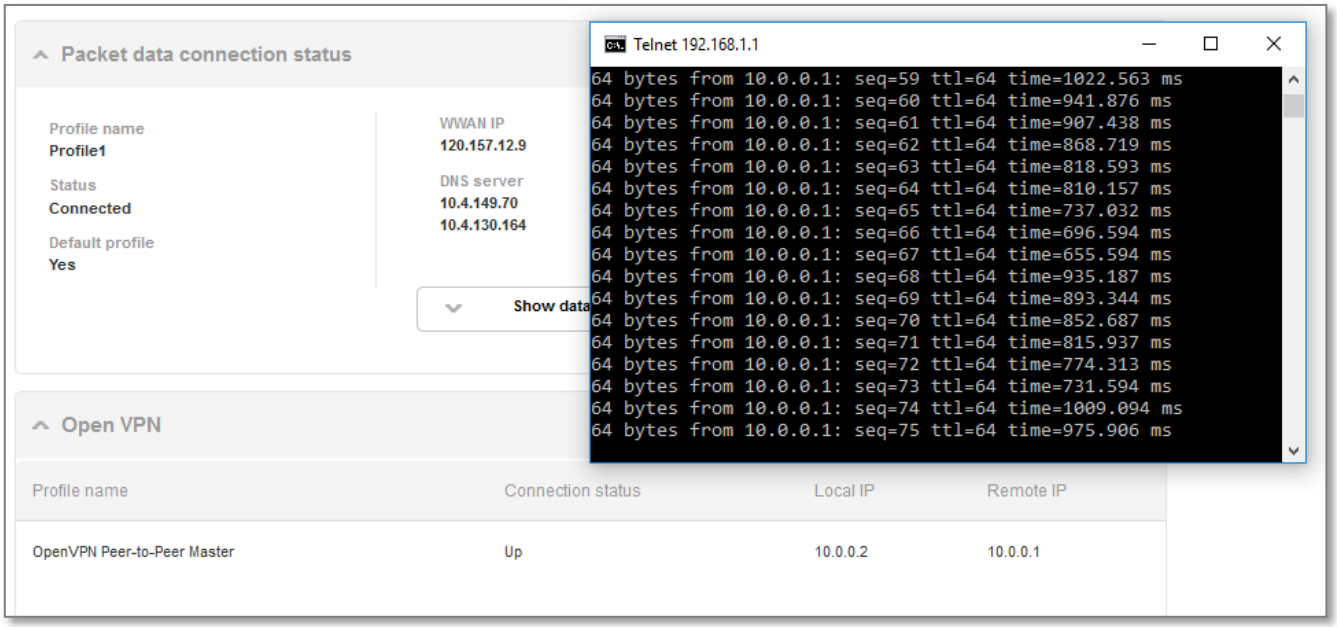


Figure 23 - OpenVPN Peer-To-Peer Master verification

OpenVPN Peer-To-Peer Slave

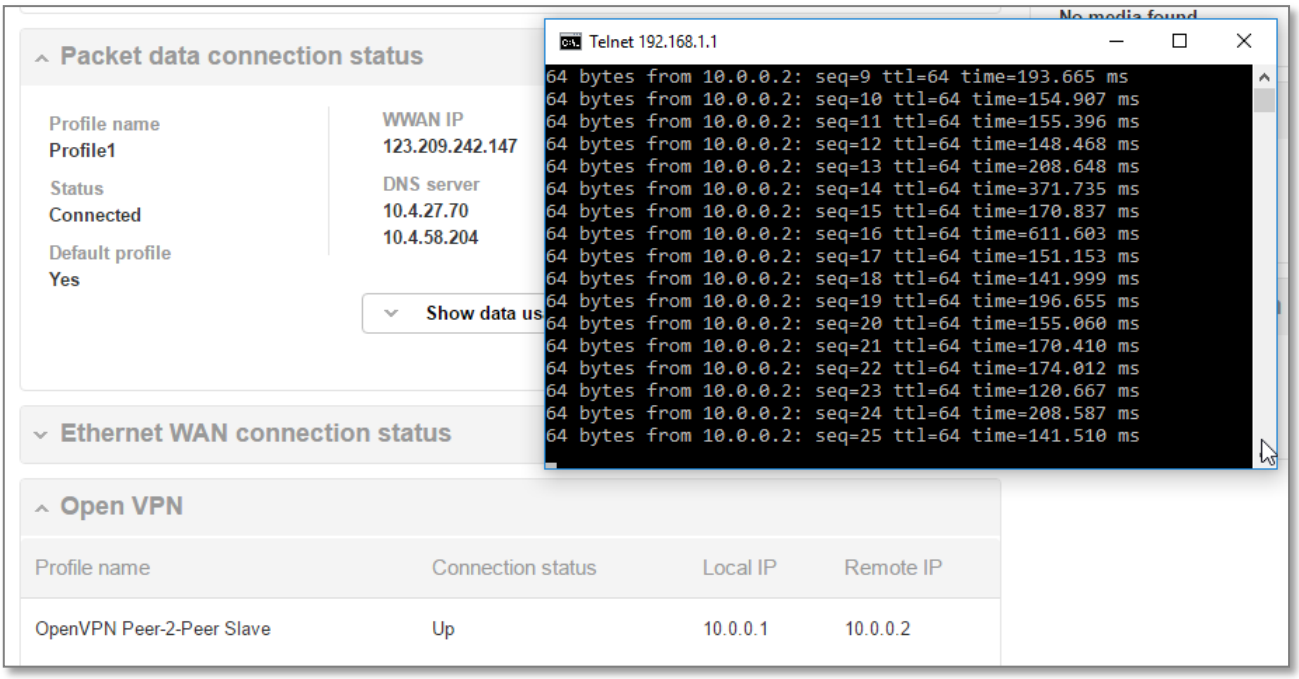


Figure 24 - OpenVPN Peer-To-Peer Slave verification

Appendix: Country codes

Code	Country	Code	Country	Code	Country	Code	Country
AX	Åland Islands	**ES**	Spain	**LU**	Luxembourg	**SE**	Sweden
AD	Andorra	**ET**	Ethiopia	**LV**	Latvia	**SG**	Singapore
AE	United Arab Emirates	**FI**	Finland	**LY**	Libya	**SH**	St. Helena
AF	Afghanistan	**FJ**	Fiji	**MA**	Morocco	**SI**	Slovenia
AG	Antigua and Barbuda	**FK**	Falkland Islands (Malvinas)	**MC**	Monaco	**SJ**	Svalbard and Jan Mayen Islands
AI	Anguilla	**FM**	Micronesia	**MD**	Moldova	**SK**	Slovak Republic
AL	Albania	**FO**	Faroe Islands	**ME**	Montenegro	**SL**	Sierra Leone
AM	Armenia	**FR**	France	**MG**	Madagascar	**SM**	San Marino
AN	Netherlands Antilles	**FX**	France, Metropolitan	**MH**	Marshall Islands	**SN**	Senegal
AO	Angola	**GA**	Gabon	**MK**	Macedonia	**SR**	Suriname
AQ	Antarctica	**GB**	Great Britain (UK)	**ML**	Mali	**ST**	Sao Tome and Principe
AR	Argentina	**GD**	Grenada	**MM**	Myanmar	**SU**	USSR (former)
AS	American Samoa	**GE**	Georgia	**MN**	Mongolia	**SV**	El Salvador
AT	Austria	**GF**	French Guiana	**MO**	Macau	**SZ**	Swaziland
AU	Australia	**GG**	Guernsey	**MP**	Northern Mariana Islands	**TC**	Turks and Caicos Islands
AW	Aruba	**GH**	Ghana	**MQ**	Martinique	**TD**	Chad
AZ	Azerbaijan	**GI**	Gibraltar	**MR**	Mauritania	**TF**	French Southern Territories
BA	Bosnia and Herzegovina	**GL**	Greenland	**MS**	Montserrat	**TG**	Togo
BB	Barbados	**GM**	Gambia	**MT**	Malta	**TH**	Thailand
BD	Bangladesh	**GN**	Guinea	**MU**	Mauritius	**TJ**	Tajikistan
BE	Belgium	**GP**	Guadeloupe	**MV**	Maldives	**TK**	Tokelau
BF	Burkina Faso	**GQ**	Equatorial Guinea	**MW**	Malawi	**TM**	Turkmenistan
BG	Bulgaria	**GR**	Greece	**MX**	Mexico	**TN**	Tunisia
BH	Bahrain	**GS**	S. Georgia and S. Sandwich Isls.	**MY**	Malaysia	**TO**	Tonga
BI	Burundi	**GT**	Guatemala	**MZ**	Mozambique	**TP**	East Timor
BJ	Benin	**GU**	Guam	**NA**	Namibia	**TR**	Turkey
BM	Bermuda	**GW**	Guinea-Bissau	**NC**	New Caledonia	**TT**	Trinidad and Tobago
BN	Brunei Darussalam	**GY**	Guyana	**NE**	Niger	**TV**	Tuvalu
BO	Bolivia	**HK**	Hong Kong	**NF**	Norfolk Island	**TW**	Taiwan
BR	Brazil	**HM**	Heard and McDonald Islands	**NG**	Nigeria	**TZ**	Tanzania
BS	Bahamas	**HN**	Honduras	**NI**	Nicaragua	**UA**	Ukraine
BT	Bhutan	**HR**	Croatia (Hrvatska)	**NL**	Netherlands	**UG**	Uganda
BV	Bouvet Island	**HT**	Haiti	**NO**	Norway	**UM**	US Minor Outlying Islands
BW	Botswana	**HU**	Hungary	**NP**	Nepal	**US**	United States
BZ	Belize	**ID**	Indonesia	**NR**	Nauru	**UY**	Uruguay

Code	Country	Code	Country	Code	Country	Code	Country
CA	Canada	**IE**	Ireland	**NT**	Neutral Zone	**UZ**	Uzbekistan
CC	Cocos (Keeling) Islands	**IL**	Israel	**NU**	Niue	**VA**	Vatican City State (Holy See)
CF	Central African Republic	**IM**	Isle of Man	**NZ**	New Zealand (Aotearoa)	**VC**	Saint Vincent and the Grenadines
CH	Switzerland	**IN**	India	**OM**	Oman	**VE**	Venezuela
CI	Cote D'Ivoire (Ivory Coast)	**IO**	British Indian Ocean Territory	**PA**	Panama	**VG**	Virgin Islands (British)
CK	Cook Islands	**IS**	Iceland	**PE**	Peru	**VI**	Virgin Islands (U.S.)
CL	Chile	**IT**	Italy	**PF**	French Polynesia	**VN**	Viet Nam
CM	Cameroon	**JE**	Jersey	**PG**	Papua New Guinea	**VU**	Vanuatu
CN	China	**JM**	Jamaica	**PH**	Philippines	**WF**	Wallis and Futuna Islands
CO	Colombia	**JO**	Jordan	**PK**	Pakistan	**WS**	Samoa
CR	Costa Rica	**JP**	Japan	**PL**	Poland	**YE**	Yemen
CS	Czechoslovakia (former)	**KE**	Kenya	**PM**	St. Pierre and Miquelon	**YT**	Mayotte
CV	Cape Verde	**KG**	Kyrgyzstan	**PN**	Pitcairn	**ZA**	South Africa
CX	Christmas Island	**KH**	Cambodia	**PR**	Puerto Rico	**ZM**	Zambia
CY	Cyprus	**KI**	Kiribati	**PS**	Palestinian Territory	**COM**	US Commercial
CZ	Czech Republic	**KM**	Comoros	**PT**	Portugal	**EDU**	US Educational
DE	Germany	**KN**	Saint Kitts and Nevis	**PW**	Palau	**GOV**	US Government
DJ	Djibouti	**KR**	Korea (South)	**PY**	Paraguay	**INT**	International
DK	Denmark	**KW**	Kuwait	**QA**	Qatar	**MIL**	US Military
DM	Dominica	**KY**	Cayman Islands	**RE**	Reunion	**NET**	Network
DO	Dominican Republic	**KZ**	Kazakhstan	**RO**	Romania	**ORG**	Non-Profit Organization
DZ	Algeria	**LA**	Laos	**RS**	Serbia	**ARPA**	Old style Arpanet
EC	Ecuador	**LC**	Saint Lucia	**RU**	Russian Federation		
EE	Estonia	**LI**	Liechtenstein	**RW**	Rwanda		
EG	Egypt	**LK**	Sri Lanka	**SA**	Saudi Arabia		
EH	Western Sahara	**LS**	Lesotho	**SB**	Solomon Islands		
ER	Eritrea	**LT**	Lithuania	**SC**	Seychelles		

Table 1 - Country codes