

Configuration Guide



How to Configure OmniSSL on the DSR-Series

Overview

This guide describes how to configure and customize OmniSSL on the D-Link DSR Series Services Router for user authentication. All screenshots in this document are captured from firmware version 3.11 of DSR-250N.

The D-Link OmniSSL uses OpenVPN technology to create secure private connections for all types of enterprises. It provides a method for the user to securely connect from a remote site to the VPN server. Remote users are authenticated using certificates, which are automatically created by OmniSSL during the setup process of the OpenVPN server. It replaces complicated OpenVPN setups and digital certificate installations in just a few easy steps.

1. INTRODUCTION

1.1. Purpose

This document describes the configuration process of the OmniSSL Client portal for various operating systems. The procedure on how to connect to the server is also detailed in this document.

1.2. Scope

The setup required to work on OmniSSL, the procedure on how to install and uninstall the OmniSSL Client Portal on different operating systems.

1.3. Hardware Requirements

The OmniSSL requires a PC with Windows/MAC/LINUX operating system, or an Android mobile device.

1.4. Software Requirements

An installed web browser such as Internet Explorer, Firefox or Google Chrome.

2. OMNISSL CLIENT INSTALLATION

During the installation process, the client binaries create a TAP (on Windows) or TUN (on Linux or MAC) interface. This interface is labeled as TUN/TAP in the operating system's network interfaces. OmniSSL client installation can be run from the D-LINK router's portal page.

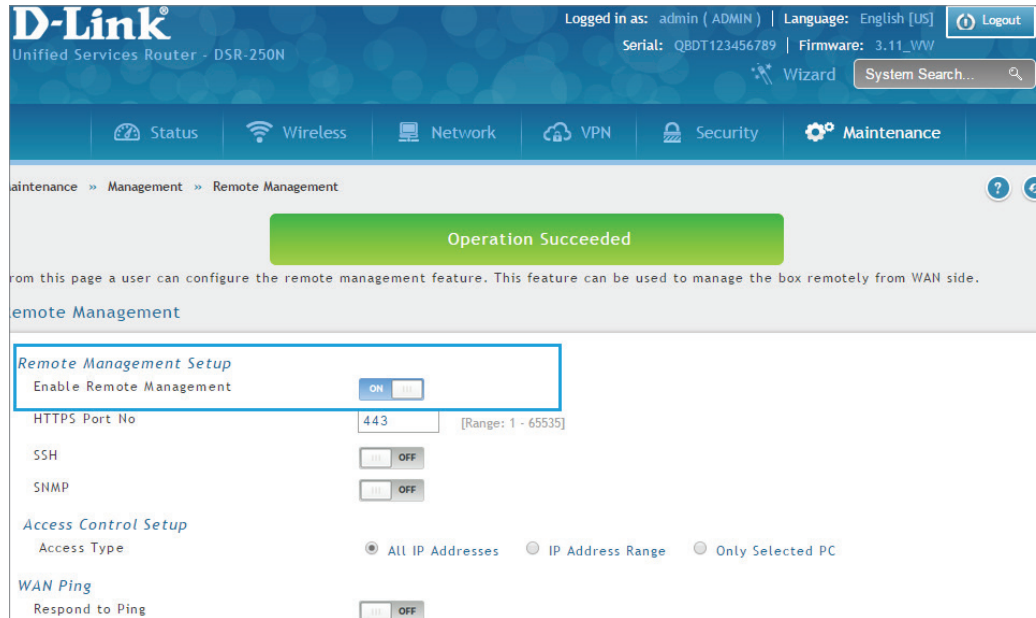
Depending on the operating system, the buttons for downloading the package and the client configuration will be on the OmniSSL portal page. The user can connect using the downloaded configuration, and the client opens an OpenVPN tunnel for secure communication between the host/mobile and the VPN router.

OmniSSL client installation is a straightforward procedure. The user must follow the installation steps for their specific operating system. The following sections explain these installation steps and recommendations in detail.

SERVER CONFIGURATION

On the server side, all of the operating systems have the same configuration and the procedure to configure it is as follows:

Step 1. Enable Remote Management ([Maintenance](#)>>[Management](#)>>[Remote Management](#)).



The screenshot shows the D-Link Unified Services Router (DSR-250N) web interface. The user is logged in as 'admin (ADMIN)' and the language is set to 'English [US]'. The interface includes a navigation menu with options like Status, Wireless, Network, VPN, Security, and Maintenance. The current page is 'Remote Management' under 'Management'.

A green banner at the top of the page indicates 'Operation Succeeded'. Below this, a text block states: 'From this page a user can configure the remote management feature. This feature can be used to manage the box remotely from WAN side.'

The 'Remote Management Setup' section is highlighted with a blue box and contains the following configuration options:

- Enable Remote Management:** A toggle switch set to 'ON'.
- HTTPS Port No:** A text input field containing '443' with a range of '[Range: 1 - 65535]'.
- SSH:** A toggle switch set to 'OFF'.
- SNMP:** A toggle switch set to 'OFF'.

The 'Access Control Setup' section includes an 'Access Type' radio button group with three options: 'All IP Addresses' (selected), 'IP Address Range', and 'Only Selected PC'.

The 'WAN Ping' section includes a 'Respond to Ping' toggle switch set to 'OFF'.

Step 2. Enable OpenVPN (VPN>>OpenVPN>>OpenVPN Settings).

OpenVPN Settings

OpenVPN ON

Mode Server Client Access Server Client

VPN Network

VPN Netmask

Duplicate CN OFF

Port [Default: 1194, Range: 1024 - 65535]

Tunnel Protocol TCP UDP

Encryption Algorithm

Hash Algorithm

Tunnel Type Full Tunnel Split Tunnel

Certificates

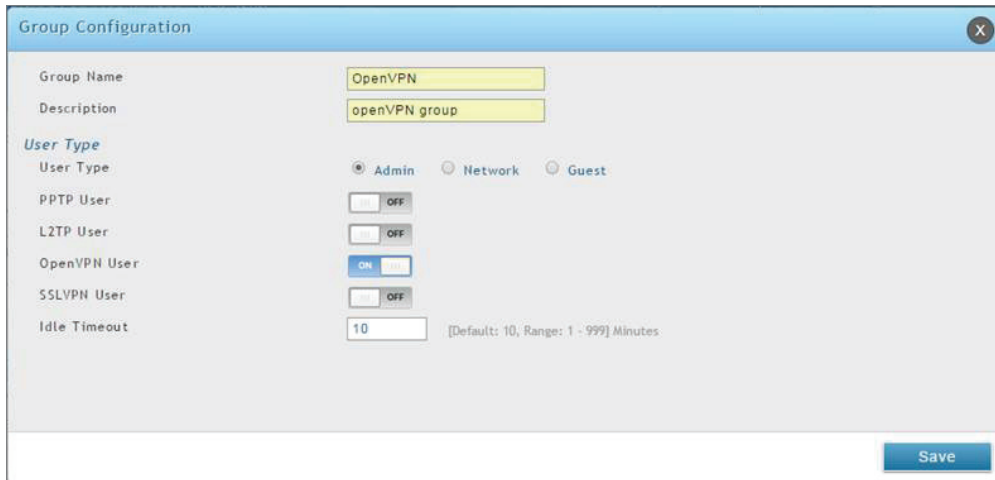
	CA Subject Name	Server / Client Cert Subject Name	Server / Client Key Uploaded	Dh Key Uploaded
<input checked="" type="checkbox"/>	C=TW, ST=Taiwan, L=Taipei, O=D-Link Corporation, OU=Certificate for DSR (Self-Signed), CN=D-Link Corporation	C=TW, ST=Taiwan, L=Taipei, O=D-Link Corporation, OU=Certificate for DSR (Self-Signed), CN=server ...	yes	yes

Enable Tls Authentication Key
 Enable Tls Authentication Key Disabled

Block Invalid Client Certificates
 Block Invalid Client Certificates Disabled

NOTE: If the OpenVPN authentication has any certificates uploaded, go to VPN>> OpenVPN settings page to enable the respective certificates first, then generate the OmniSSL client configuration for OmniSSL client feature.

Step 3. Create an **OpenVPN group** (Security>>Internal user database>>Groups) and enable OpenVPN User.



The Group Configuration dialog box is shown with the following fields and settings:

Group Name	OpenVPN
Description	openVPN group
User Type	
User Type	<input checked="" type="radio"/> Admin <input type="radio"/> Network <input type="radio"/> Guest
PPTP User	<input type="checkbox"/> OFF
L2TP User	<input type="checkbox"/> OFF
OpenVPN User	<input checked="" type="checkbox"/> ON
SSLVPN User	<input type="checkbox"/> OFF
Idle Timeout	10 [Default: 10, Range: 1 - 999] Minutes

Save

Step 4. Create an **OpenVPN User** (Include group>>Security>>Internal user database>>Users). Be sure to select the group you created in step 3.



The User Configuration dialog box is shown with the following fields and settings:

User Name	OmniSSL
First Name	test1
Last Name	test2
Select Group	OpenVPN
Password	***
Confirm Password	***

OpenVPN User is created successfully.

Security >> Authentication >> Internal User Database >> Users

Operation Succeeded

Get User DB Groups Users

Users List

Show 10 entries [Right click on record to get more options]

User Name	Group Name	Login Status
admin	ADMIN	Enabled (LAN) Enabled (WAN)
guest	GUEST	Disabled (LAN) Disabled (WAN)
o1	OpenVPN	Enabled (LAN) Enabled (WAN)

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Add New User

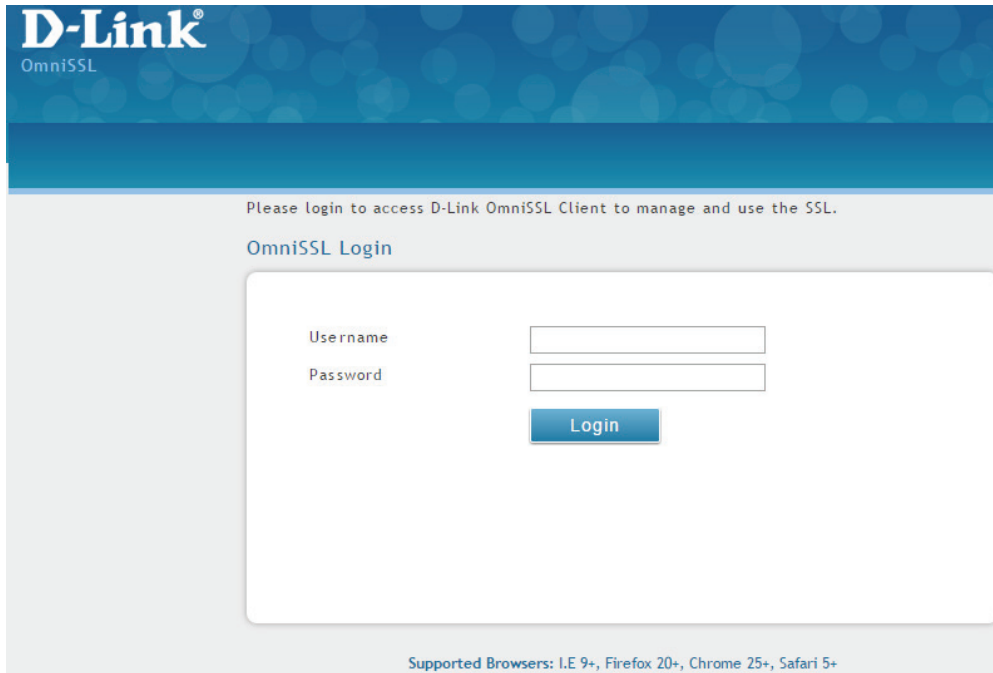
CLIENT CONFIGURATION

For each respective operating system, the procedure for client configuration is provided in the sections below.

2.1. Installation on a WINDOWS Operating System

Step 1. Enter the OmniSSL portal URL (<https://<WAN-IP>/OmniSSLPortal/>).

Step 2. Access the portal URL, and log in using the configured Open VPN username and password.



D-Link
OmniSSL

Please login to access D-Link OmniSSL Client to manage and use the SSL.

OmniSSL Login

Use rname

Password

Login

Supported Browsers: I.E 9+, Firefox 20+, Chrome 25+, Safari 5+

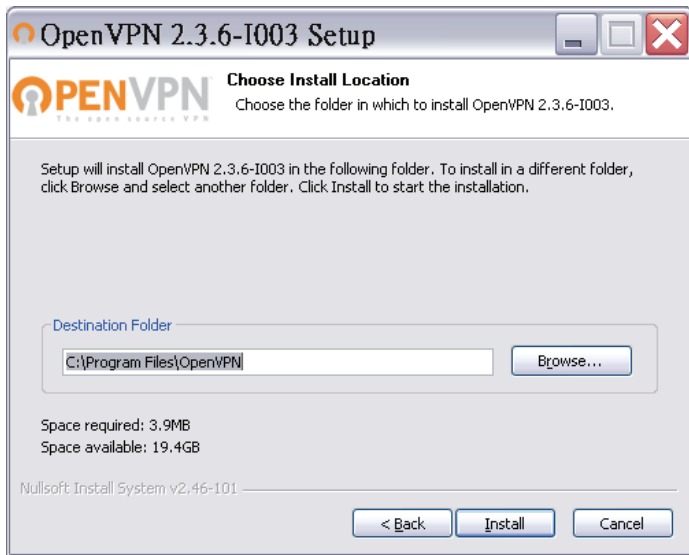
NOTE: You can check your <WAN-IP> in the Web GUI: Status>>System Information>>Device>>Dedicated WAN.

Step 3. Download the OmniSSL Client Package software and Client Configuration.

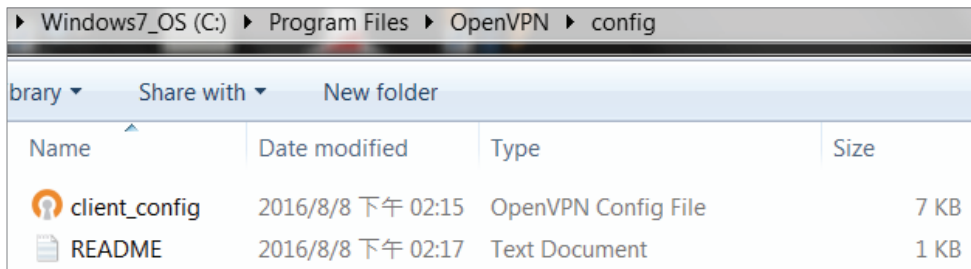


Step 4. Open the client software and the pop-up wizard will walk you through the installation step-by-step.

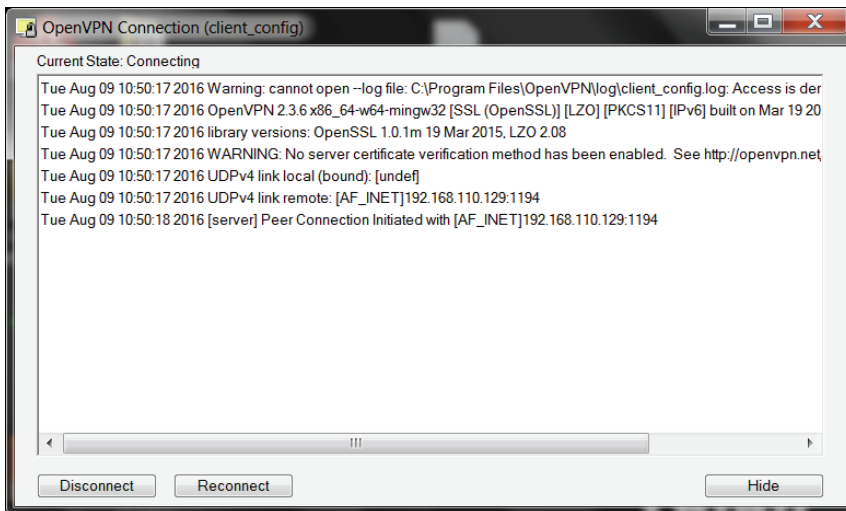
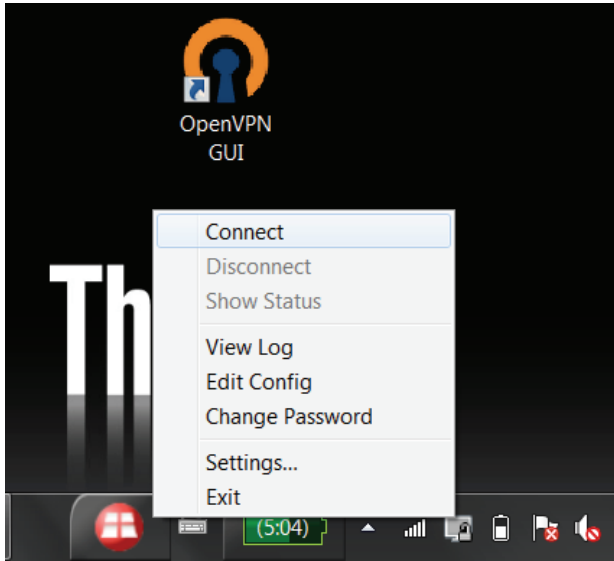




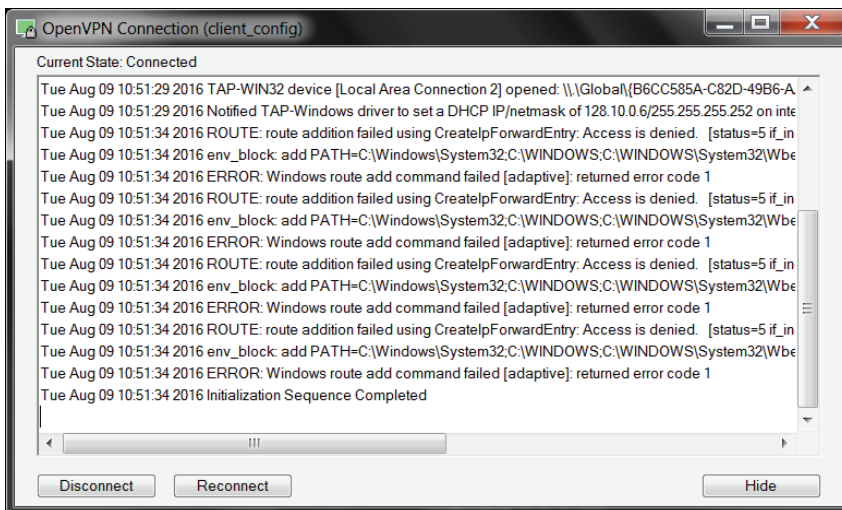
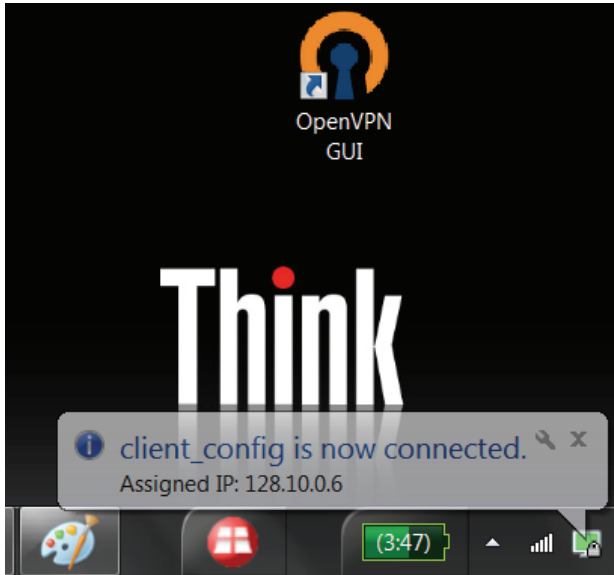
Step 5. Right click the OmniSSL Client Configuration (.bat) file, then click *Run as Administrator*.



Step 6. Double click the desktop shortcut, right click the icon on the bottom right side and click *Connect*. The connection will be made in a few seconds.



Step 7. The client is connected.



2.2. Installation on LINUX(Ubuntu) Operating System

Step 1. Step 1. Open Chrome web browser and log into the OmniSSL portal via URL ([https://DSR_WAN_IP address/OmniSSLPortal/](https://DSR_WAN_IP/omniSSLPortal/)). Log in using the configured Open VPN username and password.

Step 2. Download the OpenVPN Client Configuration.

NOTE: The default web browser in Linux is Ubuntu, which is a lightweight browser, is unable to download the OpenVPN client configuration. Therefore, it is suggested to use the Chrome browser instead.

Step 3. Execute OmniSSL Client Configuration by following either of the two procedures given below:

Procedure 1

Change the directory to the location where the downloaded files are present, and execute the command below with root privilege.

2.1.1 Open the Terminal.

2.1.2 Type in pwd to show current working directory.

2.1.3 Type ls to list the Download directory that the configuration file is saved to.

2.1.4 Type in cd Downloads to go to the Downloads directory.

2.1.5 Type in ls to list the configuration file that has been properly saved in the directory.

2.1.6 Type in sh client_config.sh to execute the configuration file.

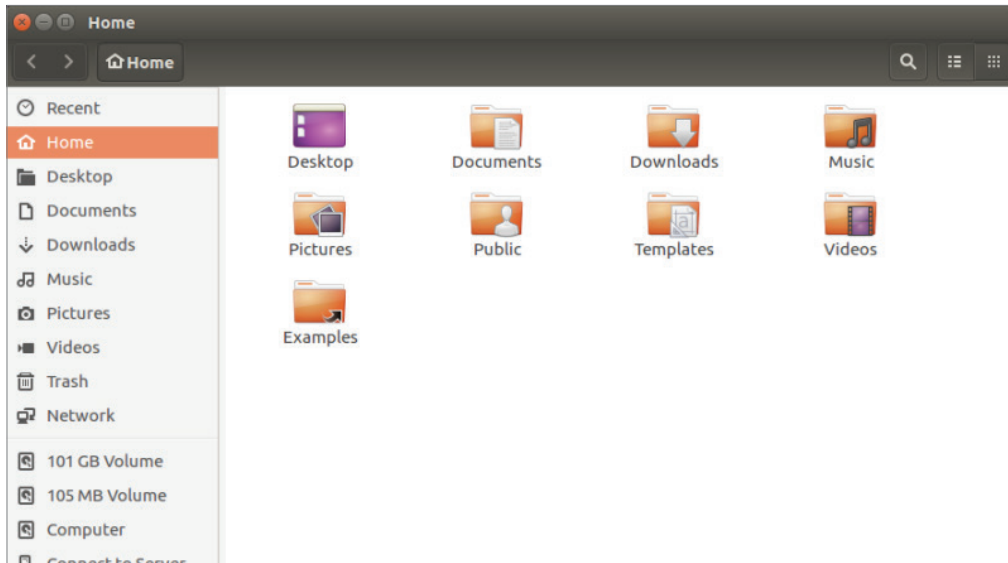
```
srd2@srd2-ThinkPad-X200s: ~/Downloads
srd2@srd2-ThinkPad-X200s:~/Downloads$ sh client_config.sh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 linux-headers-4.4.0-31 linux-headers-4.4.0-31-generic linux-headers-4.4.0-45
 linux-headers-4.4.0-45-generic linux-image-4.4.0-31-generic
 linux-image-4.4.0-45-generic linux-image-extra-4.4.0-31-generic
 linux-image-extra-4.4.0-45-generic ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 libpkcs11-helper1
Suggested packages:
 easy-rsa
The following NEW packages will be installed:
 libpkcs11-helper1 openvpn
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 462 kB of archives.
After this operation, 1163 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://tw.archive.ubuntu.com/ubuntu xenial/main amd64 libpkcs11-helper1 am
d64 1.11-5 [44.0 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu xenial/main amd64 openvpn amd64 2.3.10
-1ubuntu2 [418 kB]
Fetched 462 kB in 0s (4018 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libpkcs11-helper1:amd64.
(Reading database ... 271795 files and directories currently installed.)
Preparing to unpack ../libpkcs11-helper1_1.11-5_amd64.deb ...
Unpacking libpkcs11-helper1:amd64 (1.11-5) ...
Selecting previously unselected package openvpn.
Preparing to unpack ../openvpn_2.3.10-1ubuntu2_amd64.deb ...
Unpacking openvpn (2.3.10-1ubuntu2) ...
Processing triggers for libc-bin (2.23-0ubuntu7) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu16) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
Setting up libpkcs11-helper1:amd64 (1.11-5) ...
Setting up openvpn (2.3.10-1ubuntu2) ...
```

2.1.7 The client is connected.

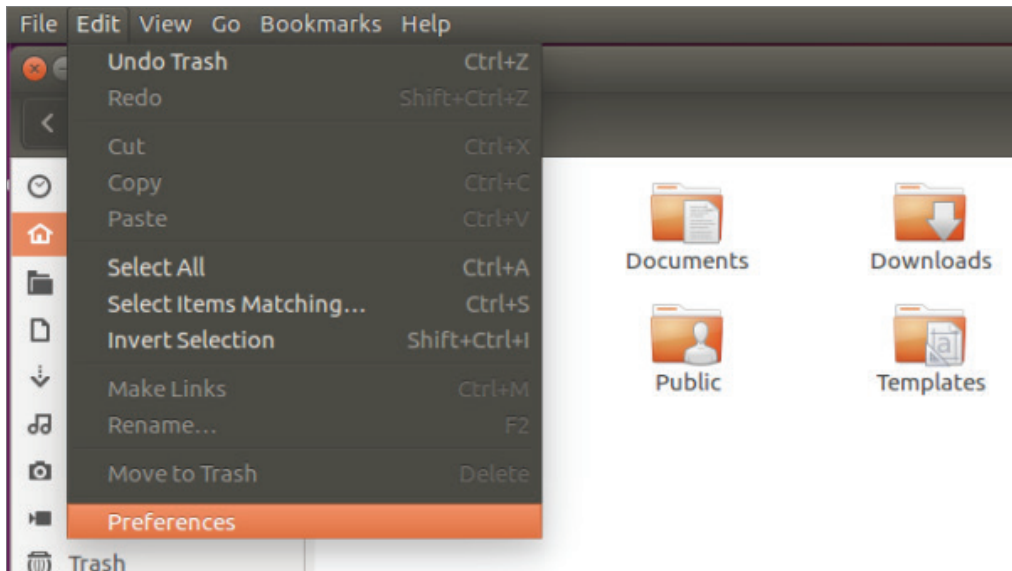
```
* Restarting virtual private network daemon(s)...
* No VPN is running.
Processing triggers for libc-bin (2.23-0ubuntu7) ...
Processing triggers for systemd (229-4ubuntu16) ...
Processing triggers for ureadahead (0.100.0-19) ...
Wed Jun 14 14:18:11 2017 OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO
] [EPOLL] [PKCS11] [MH] [IPv6] built on Feb  2 2016
Wed Jun 14 14:18:11 2017 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Wed Jun 14 14:18:11 2017 WARNING: No server certificate verification method has
been enabled. See http://openvpn.net/howto.html#mitm for more info.
Wed Jun 14 14:18:11 2017 UDPv4 link local (bound): [undef]
Wed Jun 14 14:18:11 2017 UDPv4 link remote: [AF_INET]111.250.106.218:1194
Wed Jun 14 14:18:11 2017 [server] Peer Connection Initiated with [AF_INET]111.25
0.106.218:1194
Wed Jun 14 14:18:14 2017 TUN/TAP device tun1 opened
Wed Jun 14 14:18:14 2017 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Jun 14 14:18:14 2017 /sbin/ip link set dev tun1 up mtu 1500
Wed Jun 14 14:18:14 2017 /sbin/ip addr add dev tun1 local 128.10.0.6 peer 128.10
.0.5
Wed Jun 14 14:18:14 2017 Initialization Sequence Completed
```

Procedure 2

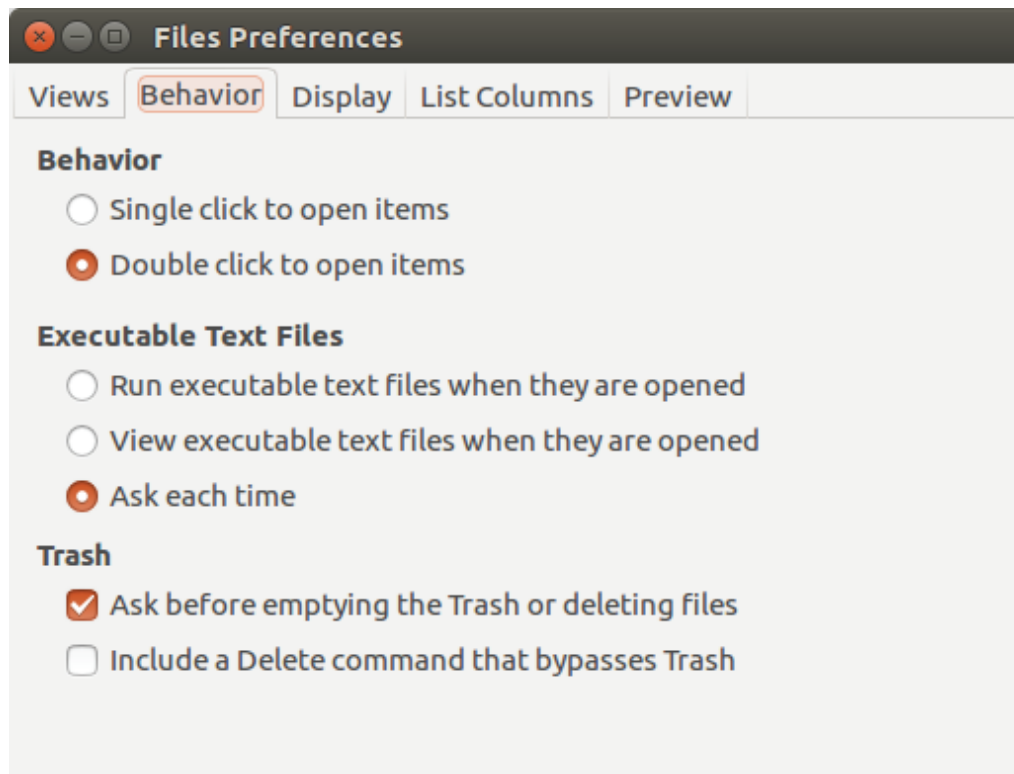
2.2.1 Open the file browser in the left pane.



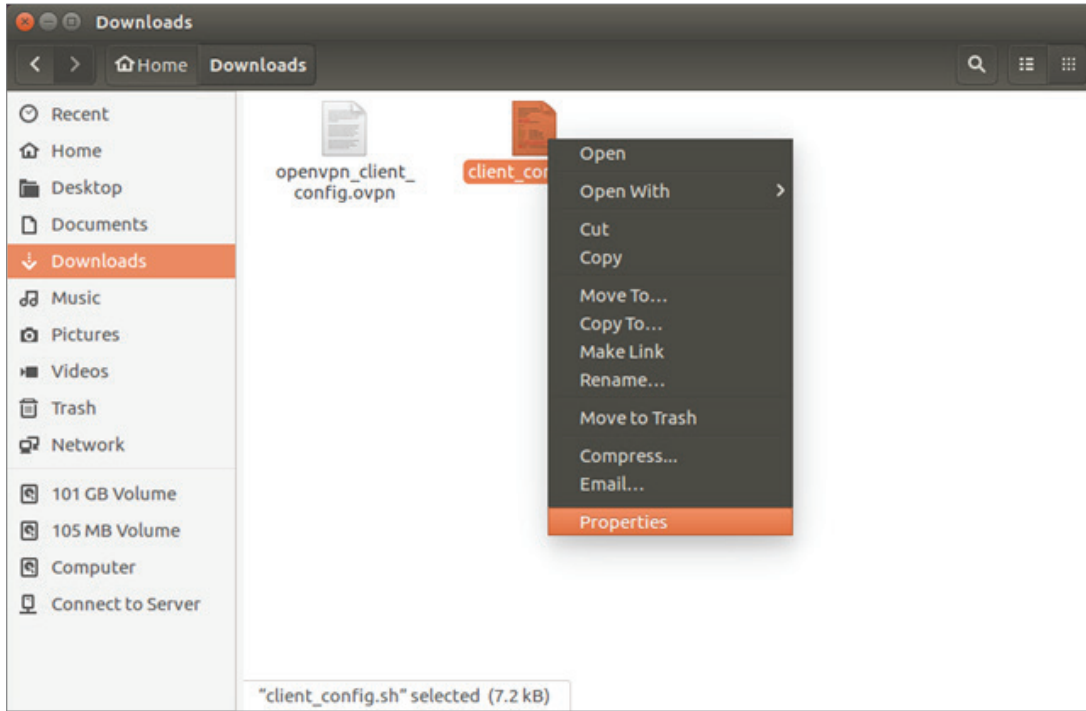
2.2.2 Go to [Edit > Preferences](#).



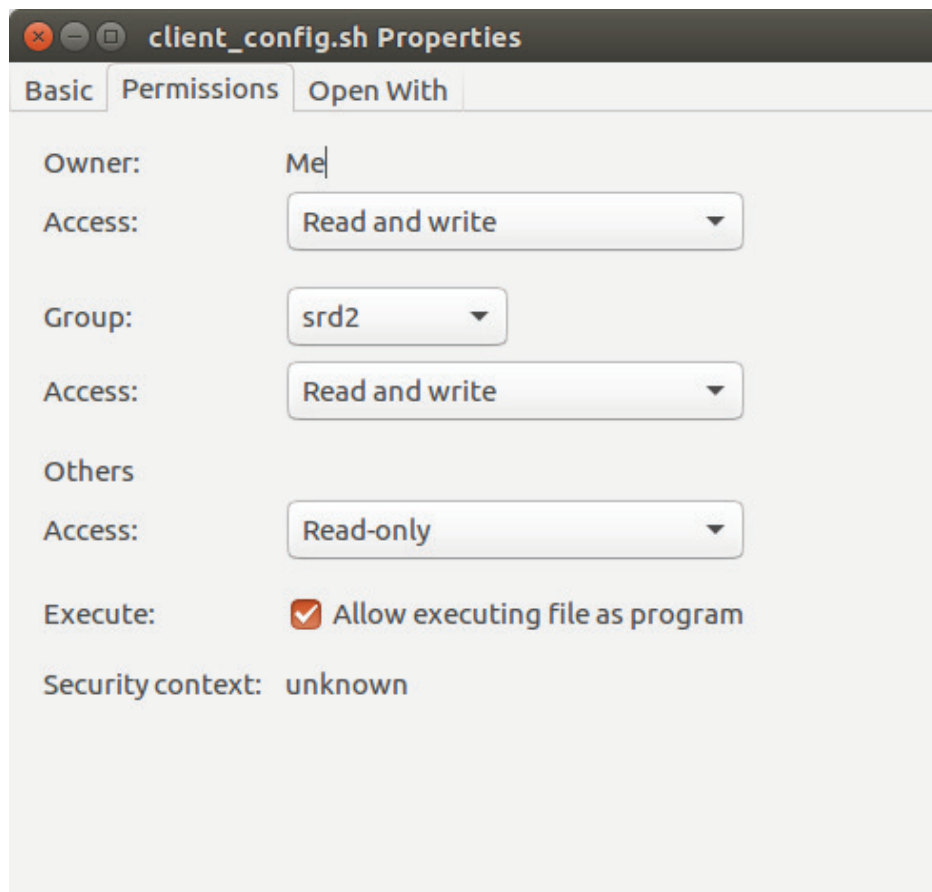
2.2.3 In Preferences, go to Behavior tab>>select Ask each time under Executable Text Files:



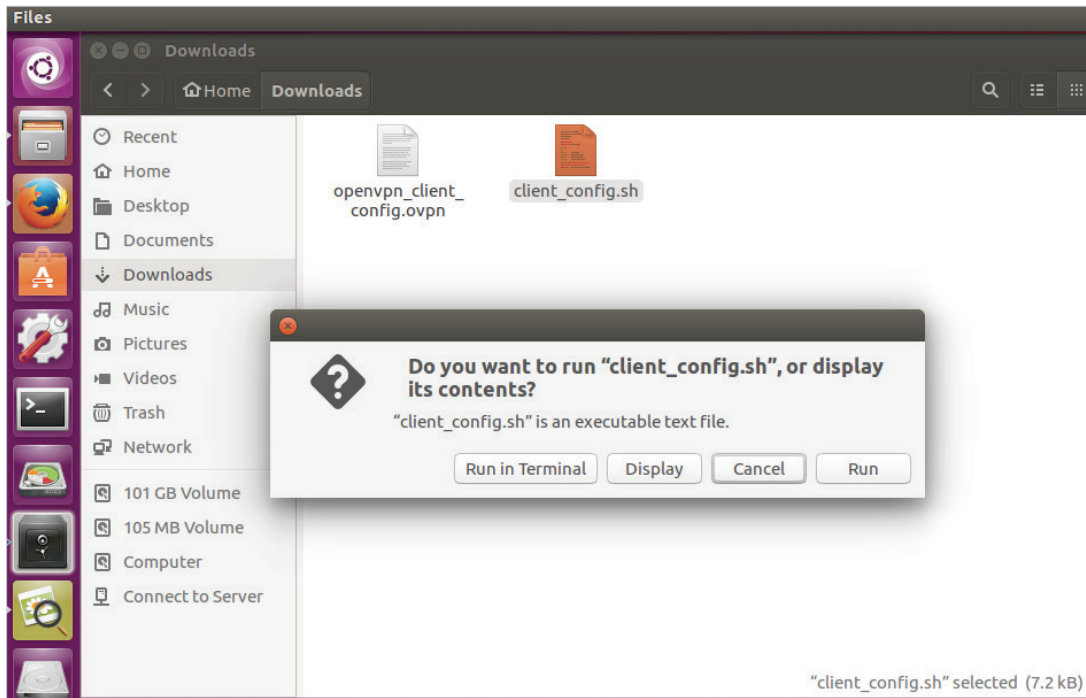
2.2.4 Right click on the client configuration file, and go to Properties.



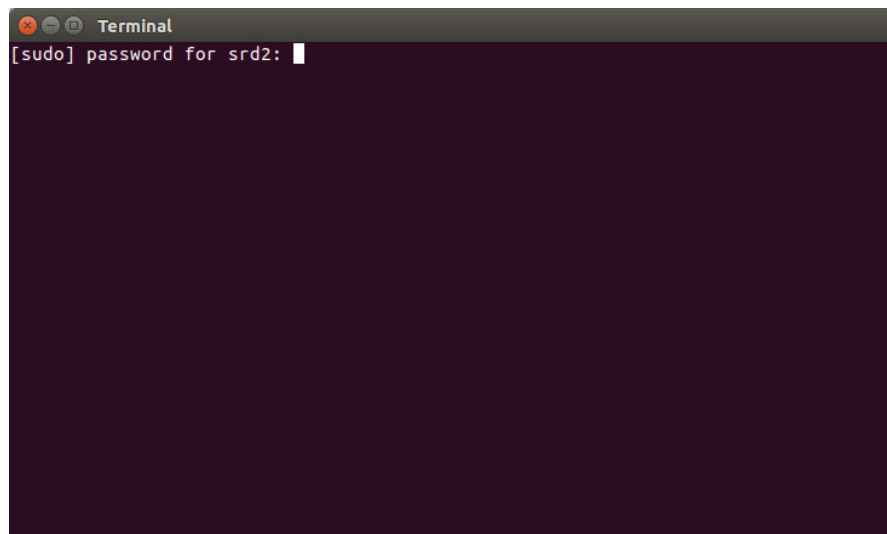
2.2.5 Click on Allow executing file as program in Permissions tab:



2.2.6 Double click on the client configuration file (client_config.sh), and select *Run in Terminal*.

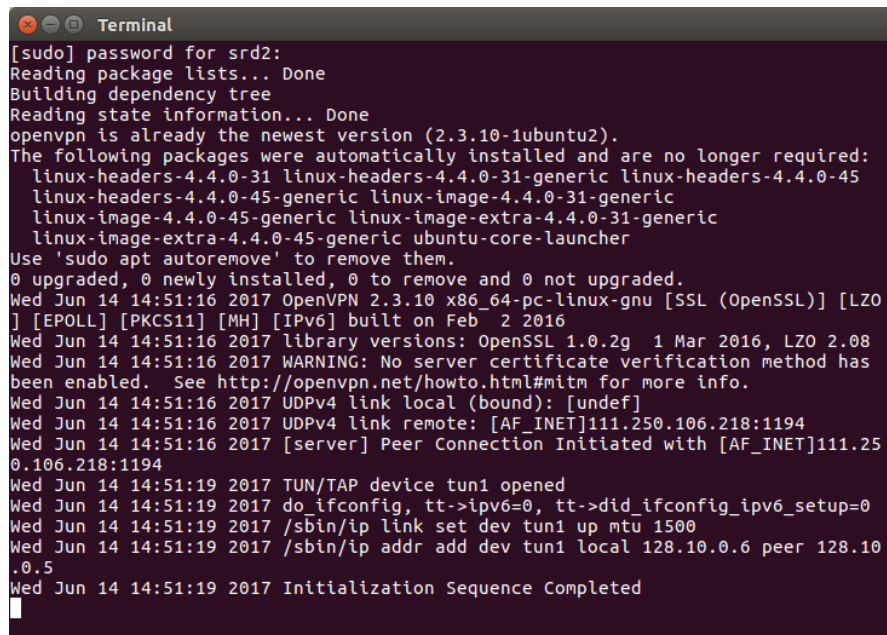


2.2.7 Enter the password for the currently shown Linux account.



```
Terminal
[sudo] password for sr2: █
```

2.2.8 Connected successfully.



```
Terminal
[sudo] password for sr2:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openvpn is already the newest version (2.3.10-1ubuntu2).
The following packages were automatically installed and are no longer required:
  linux-headers-4.4.0-31 linux-headers-4.4.0-31-generic linux-headers-4.4.0-45
  linux-headers-4.4.0-45-generic linux-image-4.4.0-31-generic
  linux-image-4.4.0-45-generic linux-image-extra-4.4.0-31-generic
  linux-image-extra-4.4.0-45-generic ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Wed Jun 14 14:51:16 2017 OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO
] [EPOLL] [PKCS11] [MH] [IPv6] built on Feb  2 2016
Wed Jun 14 14:51:16 2017 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Wed Jun 14 14:51:16 2017 WARNING: No server certificate verification method has
been enabled. See http://openvpn.net/howto.html#mitm for more info.
Wed Jun 14 14:51:16 2017 UDPv4 link local (bound): [undef]
Wed Jun 14 14:51:16 2017 UDPv4 link remote: [AF_INET]111.250.106.218:1194
Wed Jun 14 14:51:16 2017 [server] Peer Connection Initiated with [AF_INET]111.25
0.106.218:1194
Wed Jun 14 14:51:19 2017 TUN/TAP device tun1 opened
Wed Jun 14 14:51:19 2017 do ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Jun 14 14:51:19 2017 /sbin/ip link set dev tun1 up mtu 1500
Wed Jun 14 14:51:19 2017 /sbin/ip addr add dev tun1 local 128.10.0.6 peer 128.10
.0.5
Wed Jun 14 14:51:19 2017 Initialization Sequence Completed
█
```

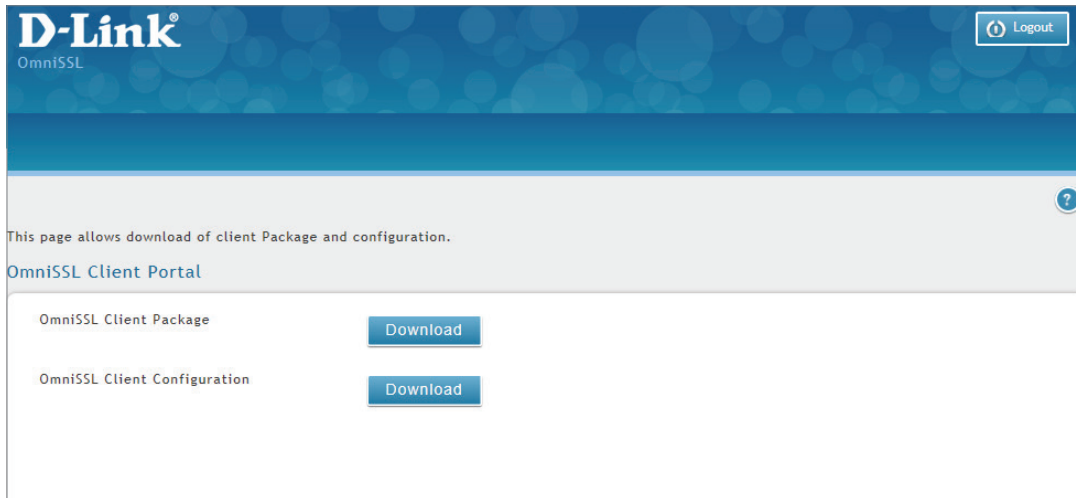
2.2.9 To end the session, press Ctrl + C to close the VPN connection.

2.3 Installation on MAC Operating System

Step 1. Enter the OmniSSL portal URL: <https://<WAN-IP>/OmniSSLPortal/> into the web browser.

Step 2. Access the portal URL and log in with the configured user.

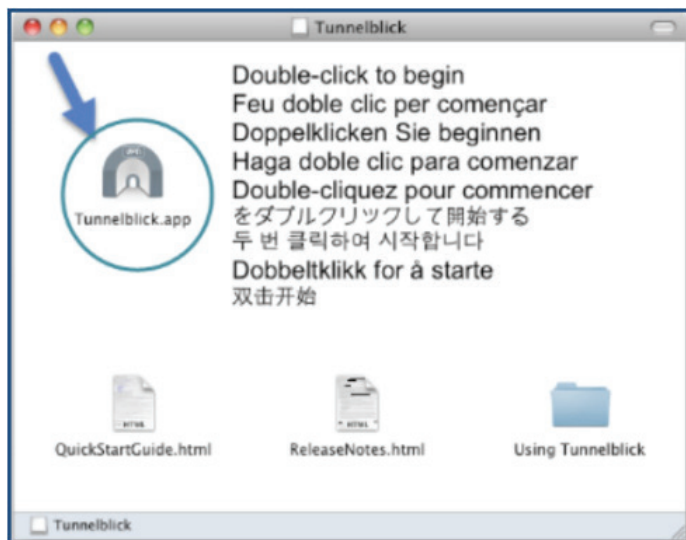
Step 3. After logging in, download the OmniSSL Client Package and OmniSSL Client Configuration.



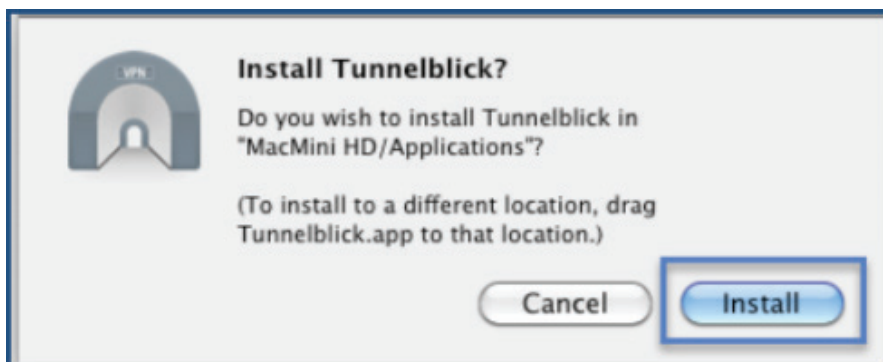
NOTE: If your MAC OS version is X.XX.X or later version, please visit Tunnelblick official website to download the latest OmniSSL Client (<https://tunnelblick.net/>).

Step 4. After download completes, a *.dmg file will appear in the Downloads folder.

Step 5. Double click the *.dmg file.



Step 6. Double click the Tunnelblick icon, and click *Install*.



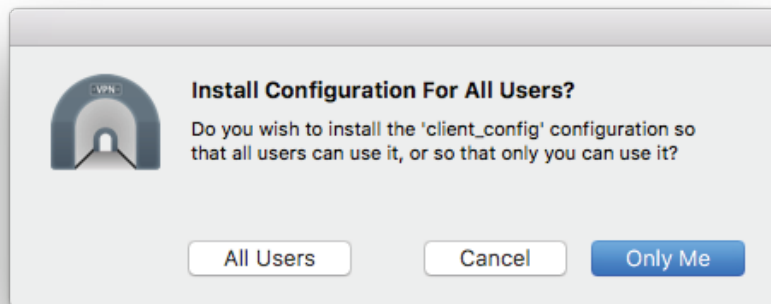
Step 7. Once the installation is successfully done, click *Launch*.



Step 8. An icon for Tunnelblick will appear in the system tray at the top-right.

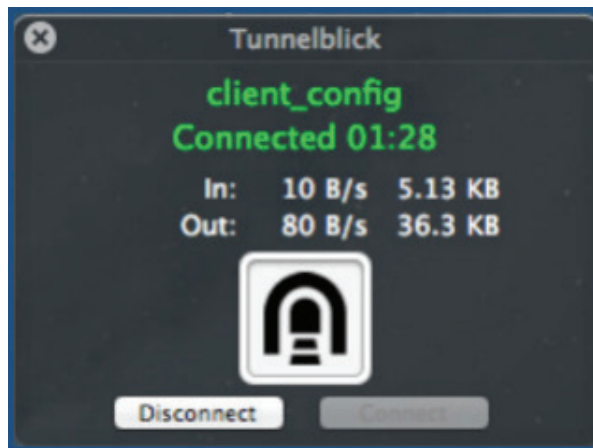


Step 9. Double click the configuration file to install it.



Step 10. Click *Connect* in client_config on the Tunnelblick application icon.

Step 11. "Connected" will be displayed to indicate the VPN is active.



D-Link[®]

Visit our website for more information
www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries.
All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2017 D-Link Corporation. All Rights Reserved.