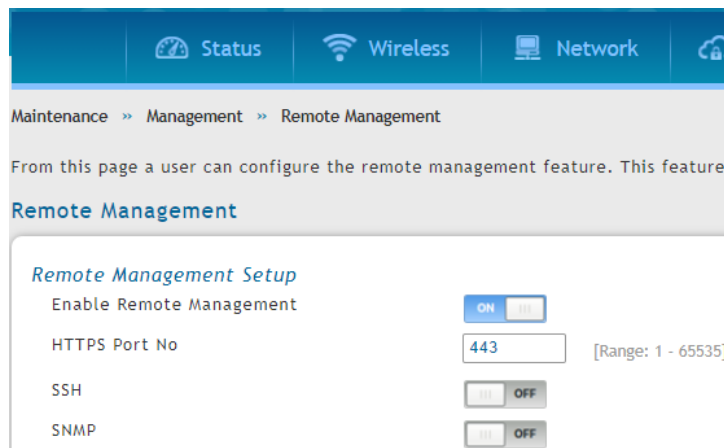


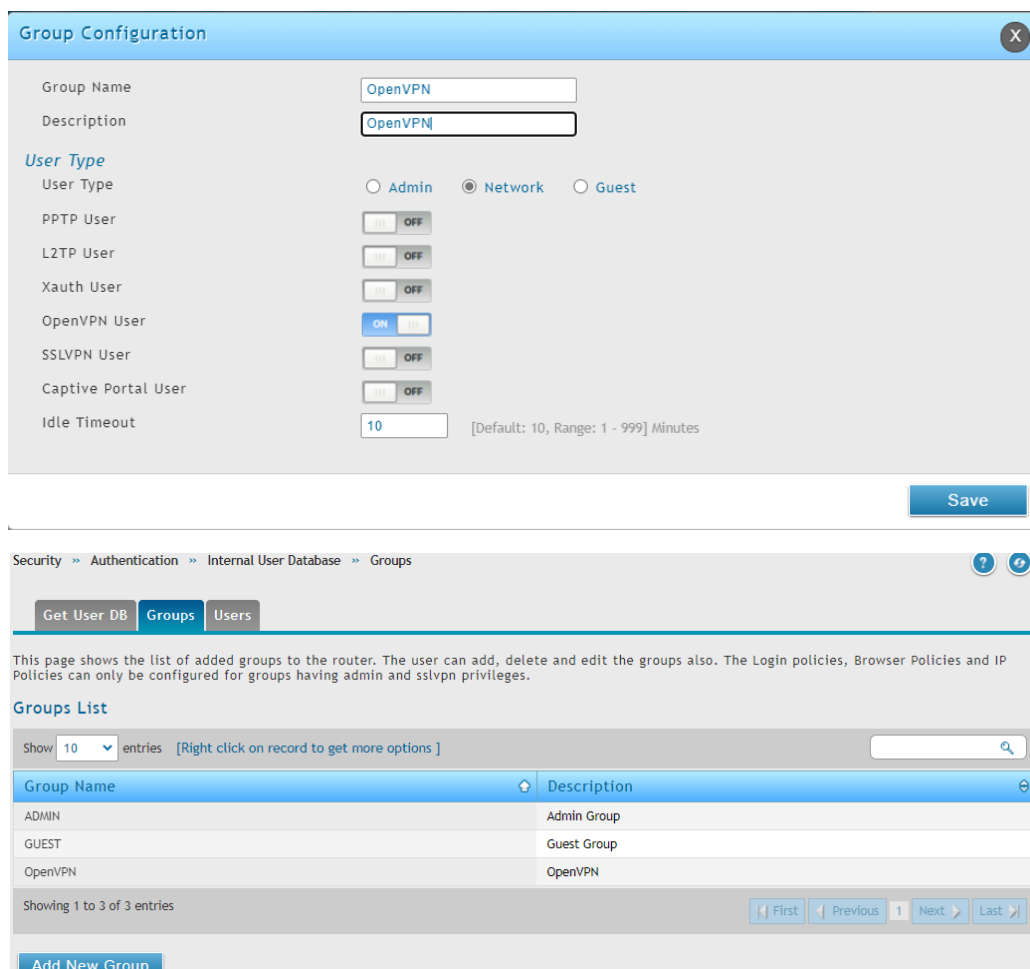
How to setup DSR-series Unified Services Router with OmniSSL Open VPN client

DSR-series router with firmware ver. 3.14

1. Enable remote Management under Maintenance -> Management -> Remote Management. Make sure to change the default admin password to a strong password for better security.



2. Create OpenVPN group under Security -> Authentication -> Internal User Database -> Groups.



3. Create OpenVPN user under Security -> Authentication -> Internal User Database -> Users.

User Configuration

User Name	<input type="text" value="vpnuser1"/>
First Name	<input type="text" value="vpnuser1"/>
Last Name	<input type="text" value="vpnuser1"/>
Select Group	<input type="text" value="OpenVPN"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

Security » Authentication » Internal User Database » Users

Operation Succeeded

Get User DB Groups Users

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can 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)
vpnuser1	OpenVPN	Enabled (LAN) Enabled (WAN)

Showing 1 to 3 of 3 entries

Add New User

4. Enable OpenVPN Server under VPN -> OpenVPN -> OpenVPN Settings. Leave everything with default values and enable User Based Auth. Click on Save.

Unified Services Router - DSR-1000AC | Serial: S37R1F6000020 | Firmware: 3.14_WW

Wizard | System Search...

Status | Wireless | Network | VPN | Security | Maintenance

VPN » OpenVPN » OpenVPN Settings

OpenVPN configuration page allows the user to configure OpenVPN as a server or client.

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

User Based Auth ENABLE

Certificate Verification ON

Certs Profile

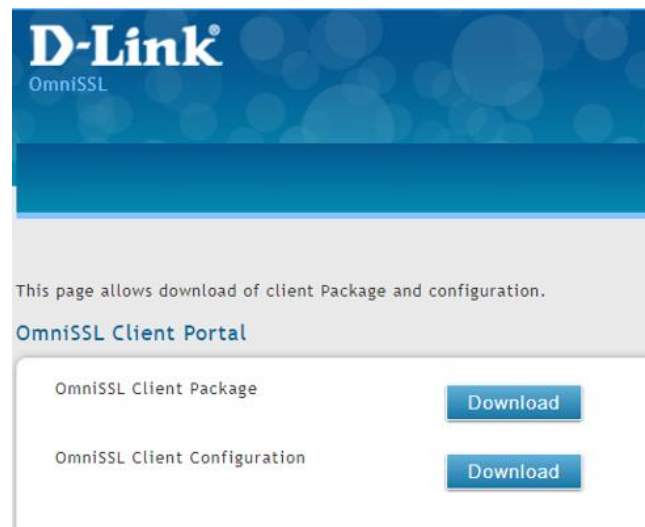
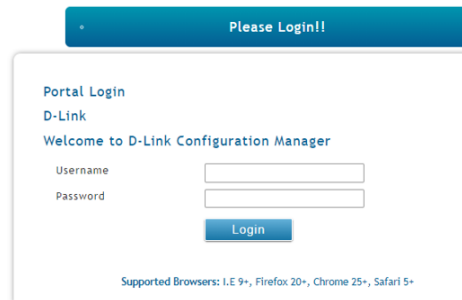
Name	CA Subject Name	Server Cert Subject Name	Client Cert Subject Name	Type	CA key Status
default	C=TW, ST=Taiwan, L=Taipei, O=D-Link Corporation, OU=Certificate for DSR (Self-Signed), CN=D-Link Corporation CA	C=TW, ST=Taiwan, L=Taipei, O=D-Link Corporation, OU=Certificate for DSR (Self-Signed), CN=server	C=TW, ST=Taiwan, L=Taipei, O=D-Link Corporation, OU=Certificate for DSR (Self-Signed), CN=client	Default: Server & Client	Available

TLS Authentication Key No TLS Keys Uploaded

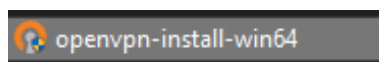
Invalid Client Certificate No CRL Certs Uploaded

5. On the client PC / remote PC, open the OmniSSL portal using <https://<DSR'sWANIP>/omnissl> e.g. <https://111.240.253.52/omnissl>

Enter the OpenVPN client username and password created in Step 3 and download the OmniSSL Client Package and OmniSSL Client Configuration.



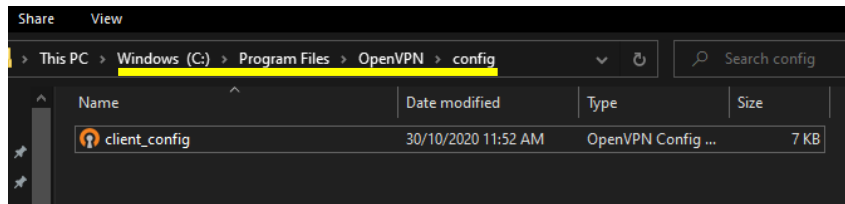
6. Install the OmniSSL Client package that you downloaded "openvpn-install-win64.exe".



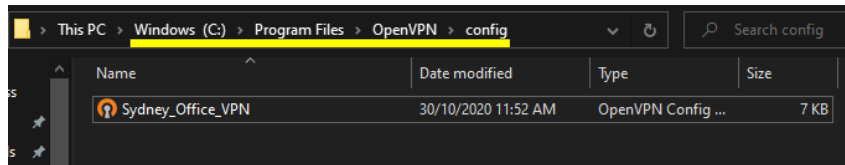
7. Run the OmniSSL Client configuration that you downloaded which is "client_script" and it will create a "client_config" OpenVPN icon as shown below.



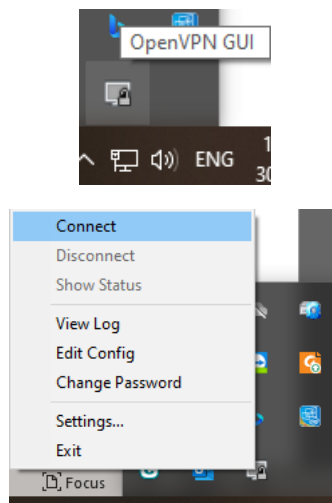
8. Copy and paste the “client_config” file to C:\Program Files\OpenVPN\config folder.



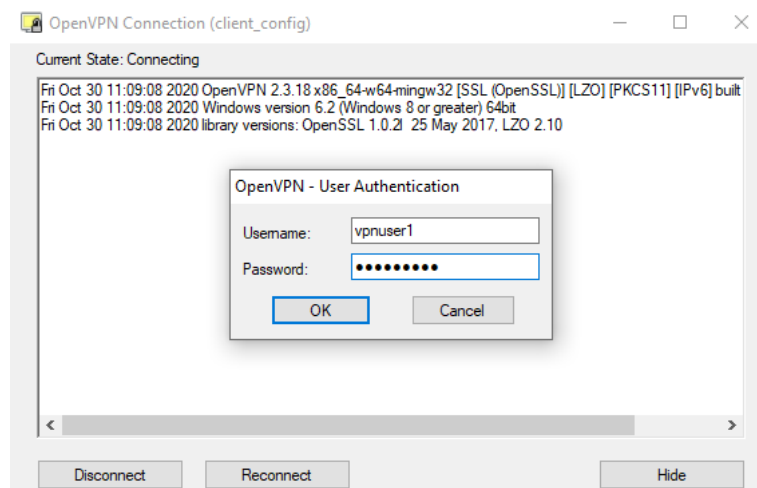
You can rename the file to something you can easily identify:



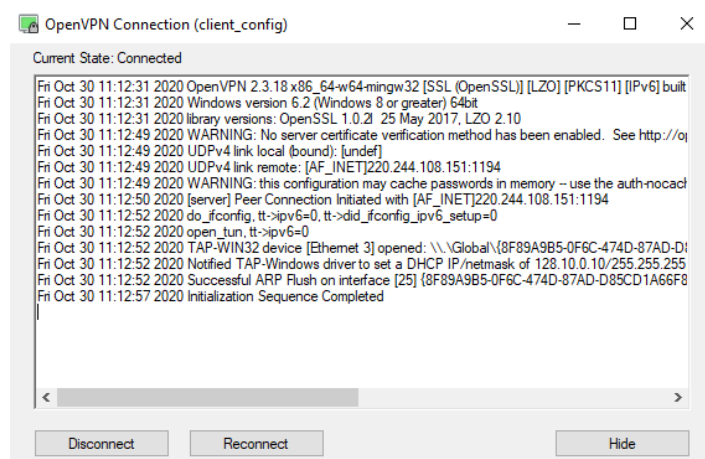
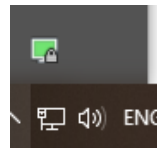
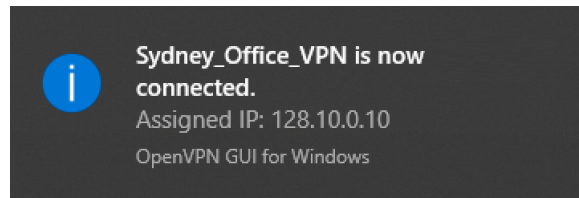
9. Locate the OpenVPN icon in the lower-right corner of the windows taskbar then click Connect.



10. Enter the OpenVPN username and password you set in Step 3.



11. Once authenticated, you will see a notification below and a green OpenVPN icon and status.



You can verify connectivity by pinging an IP address on the remote end.

