



Secure Online Shares for Windows

What are Secure Online Shares ?

KERRY LINUX offers **Secure Online Shares** as an alternative to other online files storage solutions like rsync.net, which store their customer's files unencrypted. But if you like to combine ease of use and maximum security of your data, Kerry Linux Secure Online Shares, are ideal for you, as you can mount your data conveniently as a drive letter under Windows while your data is exclusively available to you once you have established an encrypted tunnel (a VPN connection) between your computer and our server.

Your files will be safe inside an encrypted filesystem on our server most of the time you don't use it, because your secure filesystem will be automatically decrypted and ready for use only when you initiate the secure tunnel. The filesystem will then be disabled on the full hour after you started the VPN connection automatically, so that your data will be unavailable and safely encrypted unless you restart the VPN connection again. Of course, if you wish to share your filesystem with co-workers, your trusted companion is able to establish a second VPN connection himself, providing access to the same data until the files become unavailable within the next hour.

To be able to establish a secure VPN tunnel to our server you need to use a piece of software for Windows, called OpenVPN. You can download a GUI version of OpenVPN for Windows here: <http://openvpn.se/download.html>

Making OpenVPN Ready For Use

Step 1

After downloading the file **openvpn-2.0.9-gui-1.0.3-install.exe** double-click on the icon to start the installation process. After a while the setup wizard starts greeting you, click "Next" to continue the installation and click "I Agree" if you accept OpenVPN's license agreement which is in fact GPL, version 2 with a few additional conditions.

It is safe to accept the default values, so click "Next" to install the software in c:\Programs\OpenVPN. Following the usual scaremongering about software that does not pass the Windows-Logo-Test, you can install the driver software for the TAP-Win32 network tunnel interface, that is necessary for the encrypted VPN connection, if you continue and finish the installation.

Step 2

Before you can start the VPN connection to Kerry Linux's server it is necessary to prepare another network interface for the encrypted tunnel. Select "Add a new TAP-Win32 virtual ethernet adapter" from the new OpenVPN program menu and click "Continue Installation" several times until you are requested to press a button in the dosbox that had come up.

Now you have created another network interface that shows up alongside the other LAN adapters. The new TAP-Win32 network adapter is not yet active, because you have not set up the secure VPN connection, which will be our last task.

Step 3

For the initial setup to work, four files have to be copied into the directory c:\Programs\OpenVPN\config:

CA.cert, **client.kerry-linux.ie.cert**, **client.kerry-linux.ie.key** and the config file **safelinux.ovpn**

You will get all of these files after you have signed up for the service from Kerry Linux by email. So place these files in the configuration directory and you can connect to our server by right-clicking on on the tiny OpenVPN-GUI icon that shows up in the bottom right application tab. Give your user name and the current password to establish the encrypted tunnel to our server.

Step 4

As a last step we can now mount the secure filesystem as a drive letter under Windows. As we have just successfully connected to Kerry Linux's server we are on the same subnet and can access the server with its **IP address 10.66.66.1**. Click on "Connect Network drive" in the "Extras" menu and enter **\\10.66.66.1\yoursharename** in the textfield. You are requested to enter a user name and password to connect. Please bear in mind that your username on the server is your eight digit number, not your email address and that the password used is the one you can get from your Customer Portal, that changes every day. Fortunately these network drives stay visible on the working place, so that you do not have to repeat this last step anymore. Just connect and your files should be visible on the network drive, until the hour has passed away.