SCENARIO/INTRODUCTION

Because remote access has become more and more popular for obvious reasons, and geographical boundaries do not necessarily need to impose restrictions on resource access, @Pel.Net has improved the existing SSL VPN system for unified access and SSO (Single Sign-On) optimization.

USER ACCOUNTS

Recently, the OpenVPN server has been re-configured to use LDAP for user authentication which means clients no longer require keys and certificates that may need to be regenerated if they are lost or if they forget the passphrase. All users can request VPN access by means of contacting the administrator, and once they are enabled, they can download the required files to connect at any time provided they know their LDAP credentials.

REQUIREMENTS

To be able to connect to the OpenVPN server, there are certain requirements which must be considered:

1. 32bit 150Mhz CPU or better
2. Win16/32/64, Linux, MacOS, Android or other compatible platform for OpenVPN
3. TCP/IPv4 support
4. Internet/network connection ~2Mbps or better (10Mbps recommended)
5. Keyboard (Mouse or compatible pointing device recommended for OpenVPN GUI)
6. Any revision of the OpenVPN client or compatible alternative
7. Administrative rights on the client machine

GETTING THE REQUIRED FILES TO CONNECT

Laptops installed by @Pel.Net may already have the OpenVPN client software installed. This document and these instructions apply to the Windows platform, although you can download different versions of the OpenVPN client for various platforms.

1. Navigate to http://datacenter.pelnet.eu/vpn and select “Download VPN Client Packages”. On the following page you will be presented with a list of files.

   Note: newer versions of the client software may be available from the developers. See the notes and the end of this document for more information.

2. Select the applicable version for your OS/platform and save the file to your harddrive (this document assumes you are using the OpenVPN GUI (**openvpn-2.0.9-gui-1.0.3-install.exe**) with Microsoft Windows 7).

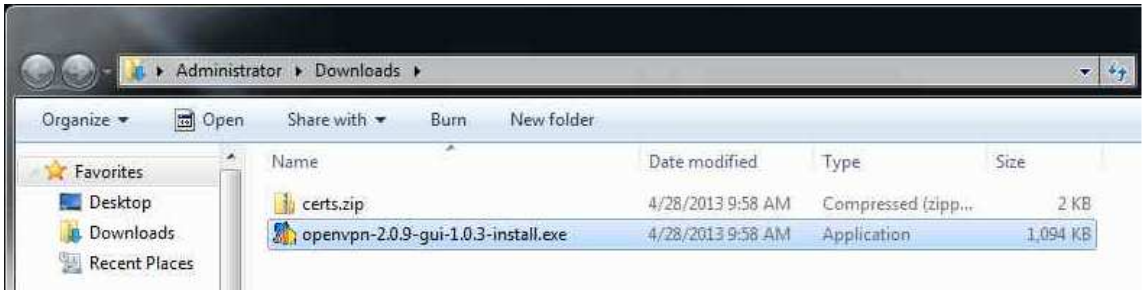
   You will need log on with your LDAP credentials to access these files. The format to use here is

   (example): `[domain.name]\[username]` or `[username]@[domain.name]`

   Note that you do not have to specify the domain explicitly when using most web browsers.

3. Next, download the required certificates for the connection by selecting the **certs.zip** file and save this to your harddrive as well.

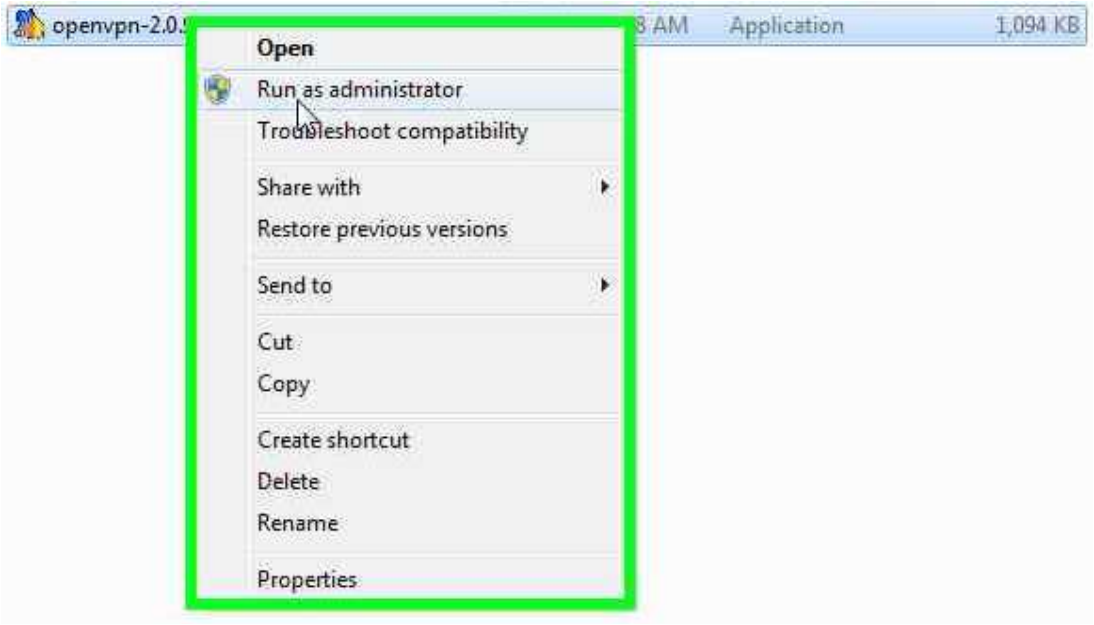
4. Navigate to the directory where you saved the files from the last step.



INSTALLING THE OPENVPN CLIENT

Depending on your client platform and operating system, the procedure to install the client may be quite different to the method outlined in this document. In almost all cases you will nee administrative rights on the machine and approximately 5 – 10MB storage space.

If you are running Windows Vista or Windows 7 with UAC enabled, always select "Allow" for any actions described in this guide.



1. To install the OpenVPN GUI client, right click on the installer and select "Run as Administrator".

2. Select "Next" in the installer dialog and "I agree" when presented with the EULA.

3. You can enable and disable various components of OpenVPN, but it is recommended that you only change the default setup if you are familiar with the functionality of the client. For example, the "AutoStart OpenVPN GUI" and "OpenVPN Service" items are not required to connect but can provide a smoother experience when connecting regularly. You can also safely disable the "OpenVPN RSA Certificate Management Scripts" and "OpenSSL Utilities" – these are not required by the client.

4. Select "Next" and "Install".

5. Depending on your Windows configuration, you may be presented with a dialog requesting confirmation to install the driver software for the virtual TAP interface. Select "Install this driver software anyway" and let the installation continue.

CREATING A CLIENT CONFIGURATION FILE

Before you can connect, you will need to create a configuration file. On most platforms the extension of the file does not matter, however the OpenVPN GUI exclusively handles **.ovpn** files. An example configuration file is provided below to guide you through the process.

1. Navigate to the directory where you installed OpenVPN (this document assumes you used the default path).

2. Open the "**config**" directory and create a new text file. Make sure to provide the ".ovpn" extension to the file. The icon of the file should change to the OpenVPN logo after a couple of seconds (assuming you did not disable the association of the OVPN file type during the installation). If the icon does not change from the default "Notepad" logo, enable the "Show extensions for known file types" setting in Folder Options (see http://support.microsoft.com/kb/865219 for more infomation).

3. Launch OpenVPN GUI from the Start Menu or Desktop and right click on the icon in the System Tray.

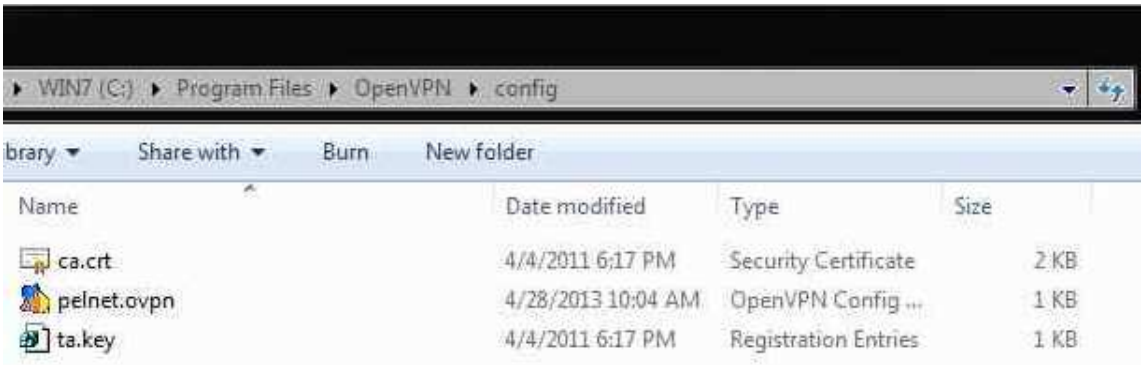
4. Select "Edit Config" and copy the following text into the editor window that pops up.

```
client
dev tun
proto udp
remote datacenter.pelnet.eu 1194
;remote-random
resolv-retry infinite
nobind
persist-key
persist-tun
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
ca "c:\\program files\\openvpn\\keys\\ca.crt"
ns-cert-type server
tls-auth "c:\\program files\\openvpn\\keys\\ta.key" 1
;cipher x
comp-lzo
verb 3
;mute 20
auth-user-pass
```

The lines starting with a semi-colon are not strictly required, however they may be required depending on the network from which you are connecting to the VPN service. Make sure to change the "**ca**" and "**tls-auth**" parameters to include the correct path to the relevant files on your machine. It is recommended to keep these in the "**config**" directory together with the **.ovpn** file.

LOADING THE CA CERTIFICATE AND TLS KEY

If you have not already done so, extract the "**ca.crt**" and "**ta.key**" files from the "**certs.zip**" archive which you downloaded earlier and place them at the location specified in your **.ovpn** config file (generally this would be "**C:\Program Files\OpenVPN\config**").

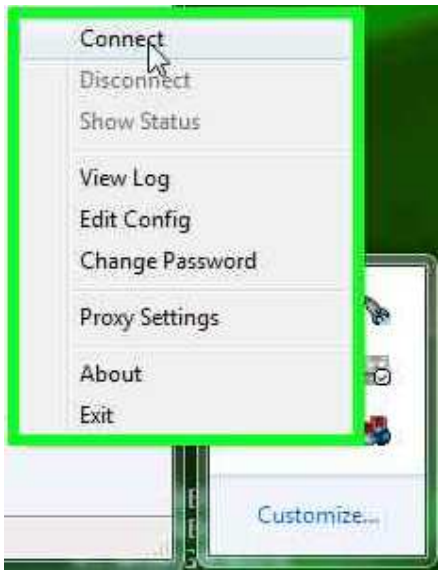


To provide improved security in a multi-user configuration, you may want to place these files somewhere within your user profile, although this is not strictly required.

CONNECTING TO THE OPENVPN SERVICE

The following steps outline the procedure to connect to the OpenVPN service. If the OpenVPN GUI is not already active and running in your System Tray, launch it from the Start Menu or the Desktop.
Note that you can configure OpenVPN to run as a service and permanently connect to OpenVPN server whenever there is Internet access. See the notes and the end of this document for more information.

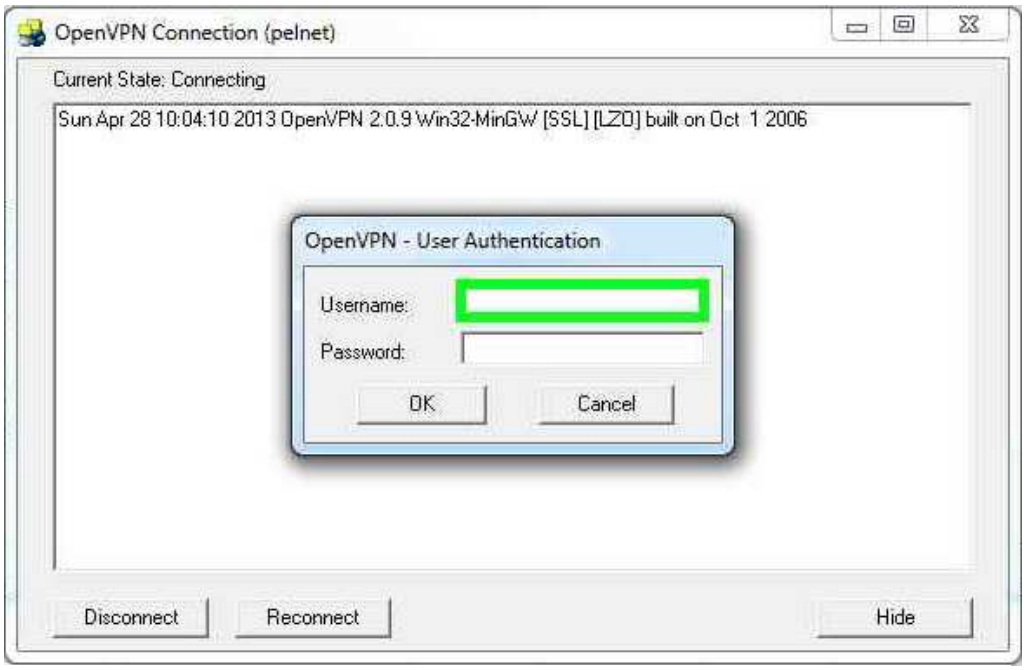
1. Right click on the OpenVPN GUI icon in the System Tray.
2. Select "Connect" from the context menu.



If you do not see the option "Connect" listed, make sure the .ovpn file exists in the right location (CREATING A CLIENT CONFIGURATION FILE, Step 2).

3. You should now see an authentication dialog where you must enter your LDAP credentials to authenticate. These must be entered in the following format:

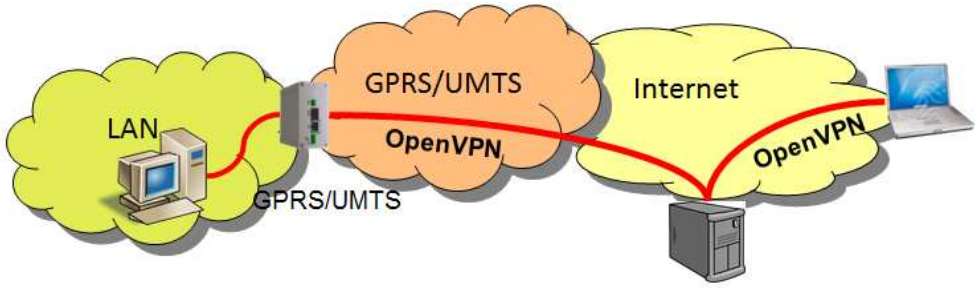
   (example): `[username]@[domain.name]`



4. Enter your password in the Password input box and click OK or press Enter.

5. The OpenVPN GUI dialog should disappear after briefly displaying the connection progress. A balloon notice should pop up in your System Tray, informing you that the connection has been established and listing the client IP address for the VPN connection.

You should now be connected to the OpenVPN @Pel.Net service which provides access to various internal resources such as the file servers, internal web services, Citrix Program Neighborhood and a lot more.



See the following section for troubleshooting information in case the connection was not established or if you cannot access internal resources via the VPN tunnel. You can also contact support for assistance in resolving your problem. Contact details are listed at the end of this document.

TROUBLESHOOTING IN CASE OF PROBLEMS

Use the following table to identify your problem and try the suggested solutions. If you are unable to resolve the problem, contact support and provide information regarding the troubleshooting steps that you have attempted.

Connect option is not displayed in the OpenVPN GUI	- Check that your OpenVPN config file is in the "**config**" directory. If it isn't, create the file by following the steps outlined in CREATING A CLIENT CONFIGURATION FILE. - A sample OVPN file can be downloaded from http://datacenter.pelnet.eu/vpn/ which you can use as a template.
ca.crt and/or **ta.key** not found	- Check that the "**ca.crt**" and/or "**ta.key**" files are extracted to a location your machine. - Verify that the paths for these two files are set up correctly in the OVPN configuration file. Note that a backslash in the path is represented by two backslashes in the configuration file (e.g. "**C:\\VPN**" instead of "**C:\VPN**"). Paths containing spaces must be enclosed by quotation marks.
Authentication failure	- Verify your LDAP login credentials. You can do this by accessing any of the files listed at http://datacenter.pelnet.eu/vpn/downloads.html - Confirm that you are specifying the credentials as outlined in CONNECTING TO THE OPENVPN SERVICE, Step 3. - Contact the admin to verify your access.
Permission denied (OS)	- Some Windows versions require you to run the OpenVPN software with administrative privileges. If you do not have administrative privileges, contact @Pel.Net support for further assistance.
Unable to access internal resources	- Check that you have been assigned a valid IP address by clicking on the OpenVPN GUI icon and selecting View Status. Valid IP addresses for the OpenVPN connection start with **10.15.2x.x**. - Check that your routing table has been modified to provide access. To you're your routing table, enter "**route print**" in a CMD window. You should see references to the **10.15.x.x** subnets.

TAP interface not found	- Verify that your TAP adapter is installed and enabled in Windows. If the TAP adapter is not listed among your network interfaces, run the OpenVPN GUI installation again and make sure to select “Install TAP Driver”
Remote host/server not found	- Verify that you have Internet connectivity. - Confirm that the “**remote**” parameter in the OVPN configuration file contains the value “**datacenter.pelnet.eu**”. - Verify your DNS resolution is working correctly.
Unable to connect	- Confirm that the “**port**” parameter in the OVPN configuration file contains the value “**1194**” and that “**proto**” is set to “**udp**”. - Check whether a local hard- or software firewall may be restricting your Internet access. If required, configure the proxy details in the OVPN configuration file.

EXTERNAL INFORMATION RESOURCES

@Pel.Net has attempted to provide you with sufficient information to use and configure your OpenVPN connection, however specific problems or situations may arise that differ from this document and can in some cases be challenging for support to resolve without external assistance. Examples of this are specific possible conflicts with other installed software or obscure operating systems.
Below is a list of URLs where you may be able to find useful information and updated or enhanced versions of the software described in this document.

http://www.openvpn.net/	OpenVPN official website
http://www.openvpn.se/	OpenVPN GUI for Windows
http://support.microsoft.com/kb/865219	Microsoft KB article dealing with displaying file extensions

SUPPORT

Feedback and support

@Pel.Net is aware that despite vigorous testing and constant improvements, sessions can hang, crash or otherwise display incorrect behavior. Because of this, @Pel.Net has prepared a number of support channels which can be used not only for assistance but also for establishing errors in the environment and/or limitations in the service provided.

Should you encounter such a problem, @Pel.Net would like to urge you to contact us as soon as possible, to ensure that any problems are investigated. In the case that you are under the assumption that you may have discovered an inconsistency please make a note of any errors, including related events in the Windows Event Viewer and related client logs, if available.

To contact support concerning the Citrix application environment, select one of the following methods::

Email contact:

citrix@pel.net	Administrator @Pel.Net (internal)
administrator@pelnet.eu	Administrator @Pel.Net (external)

Phone contact:

9000	Administrator@Pel.Net (internal)
0031625234070	Administrator @Pel.Net (mobile)
0031534783348	Administrator @Pel.Net (office)
0031534783348	Administrator @Pel.Net (fax)

Support Request

Support request	Click on the **Support Request** icon on the desktop or press **F11** if you are using a Windows computer within the @Pel.Net headquarters.
Web Support Request	http://pelnet.no-ip.org/?cat=helpdesk
Mail Support Request	support@pel.net (internal only)

Information and Documentation

Information and updates	http://datacenter.pelnet.eu/support/