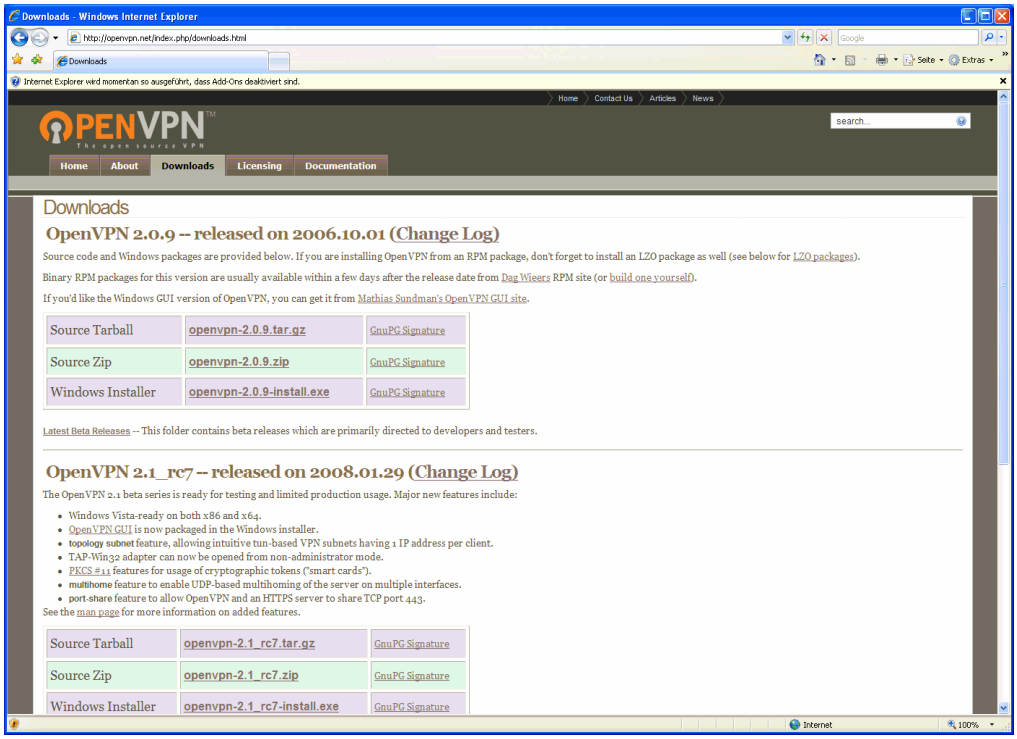
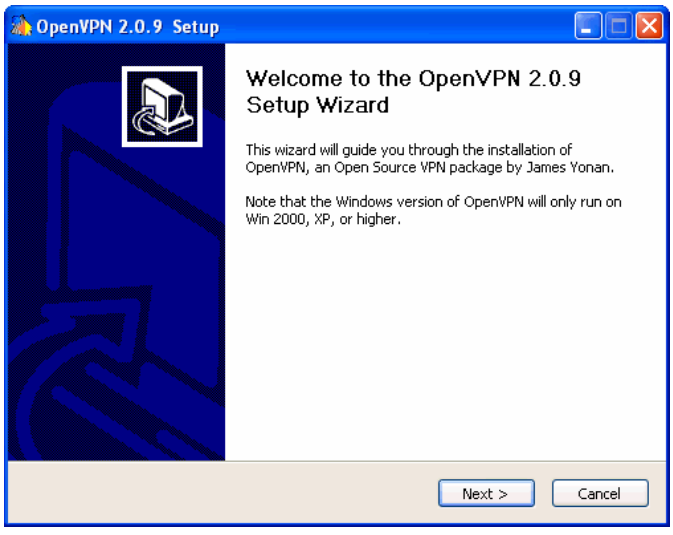
How to install and run an OpenVPN client on your Windows-based PC

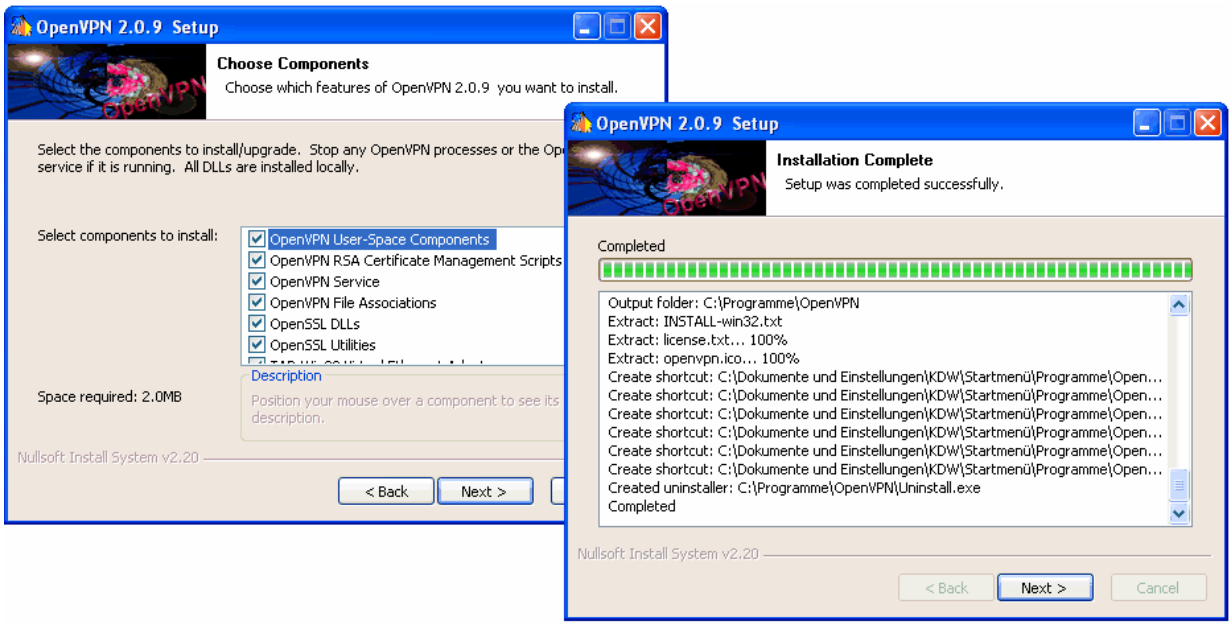
The DIL/NetPC ADNP/9200 is also available with a preinstalled OpenVPN server. This allows secure VPN connections between a PC as an OpenVPN client and the ADNP/9200. Before accessing the ADNP/9200 through a VPN tunnel please install and setup an OpenVPN client on your PC.

- **1. Step**: Visit http://openvpn.net and download the latest stable version of the OpenVPN Windows install file (in this case **openvpn-2.0.9-install.exe**).

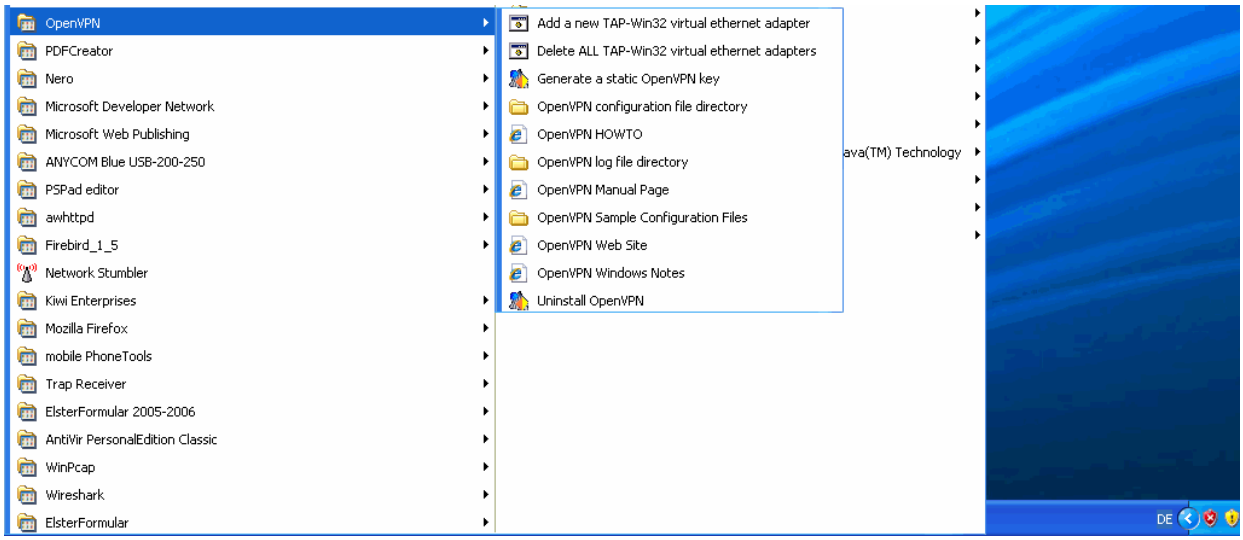


- **2. Step**: Then run the install file **openvpn-2.0.9-install.exe** on your PC and install all OpenVPN components.

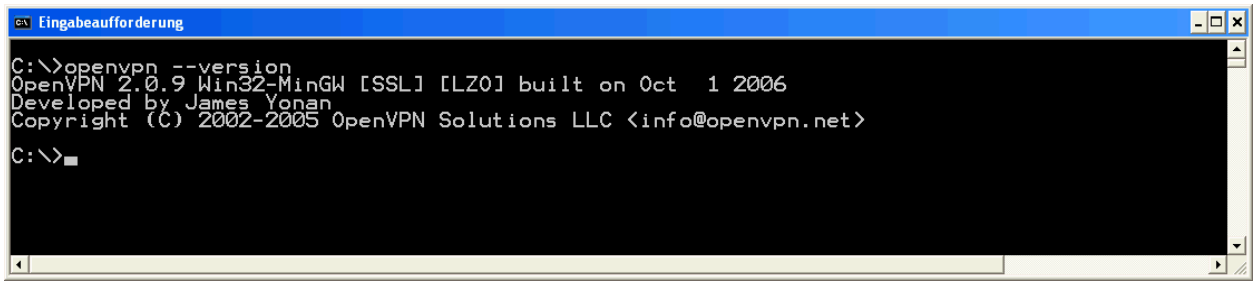




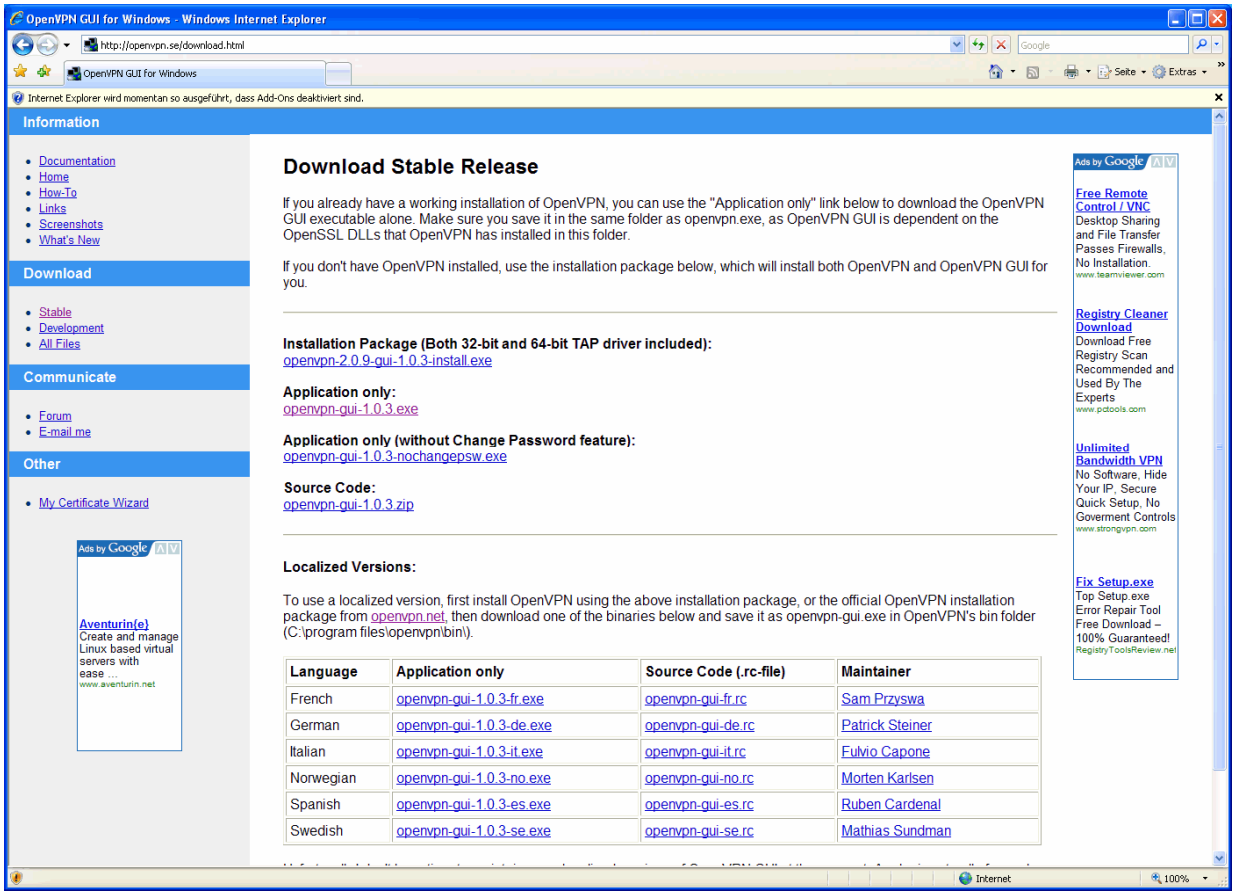
- **3. Step**: Wait until the OpenVPN installation is finished. After that you will find an OpenVPN item within your Windows program menu. OpenVPN is also available over the Windows command line.



We assume for the following steps that the OpenVPN installation directory on your Windows PC is **c:\Program Files\OpenVPN**.

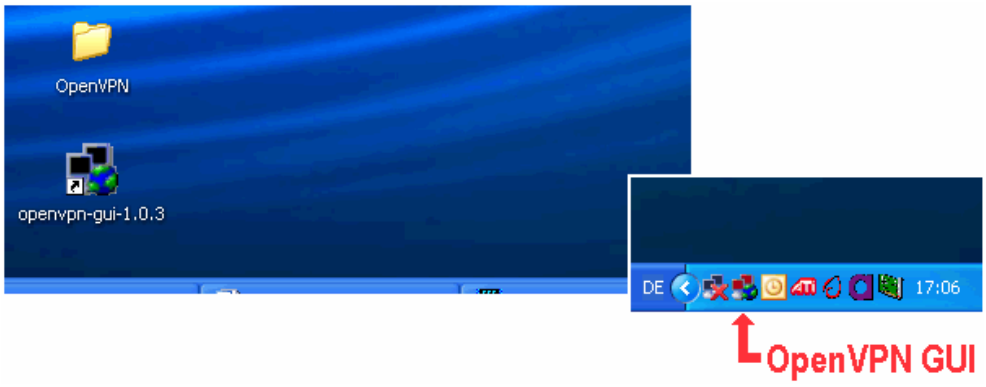


- **4. Step**: Download the OpenVPN GUI for Windows from http://openvpn.se. Please note: The next Windows versions of OpenVPN (2.1 or later) will include this tool. Version 2.0.9 needs the separate download and installs steps.

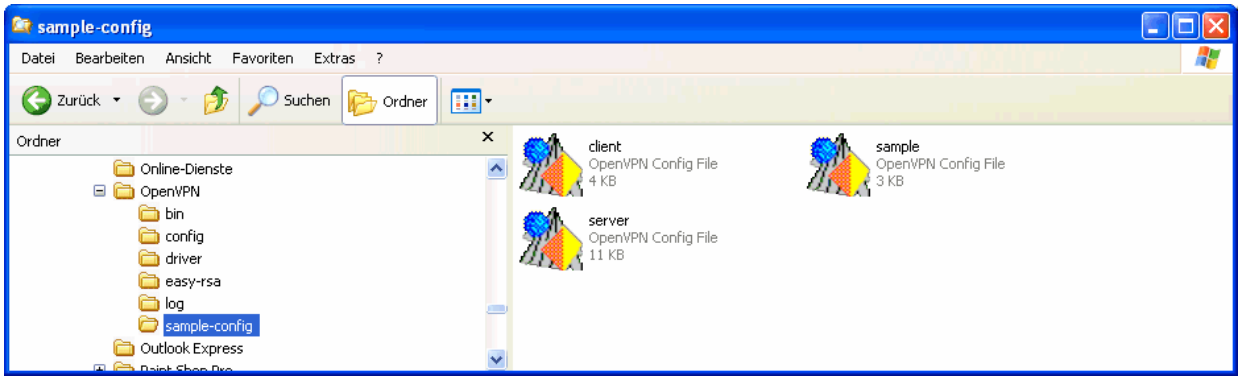


- **5. Step**: Store the *.exe (e.g. **openvpn-gui-1.0.3.exe**) file with the OpenVPN GUI for Windows on your PC. The Windows program directory **c:\Program Files\OpenVPN\bin** is a good place.

- **6. Step**: Create a desktop icon for the OpenVPN GUI for Windows and then run the OpenVPN GUI. This creates a new small icon within the Windows system tray.



- **7. Step**: Copy the file **client.ovpn** from the directory **c:\Program Files\OpenVPN\sample-config** to the directory **c:\Program Files\OpenVPN\config**.



- **8. Step**: Please rename the file **c:\Program Files\OpenVPN\config\client.ovpn** to the new name **client-adnp9200.ovpn**.

- **9. Step**: Please edit the configuration file **client-adnp9200.ovpn** and change the following five lines within this text file (see the red coloured and underlined text lines in the next sample configuration file).

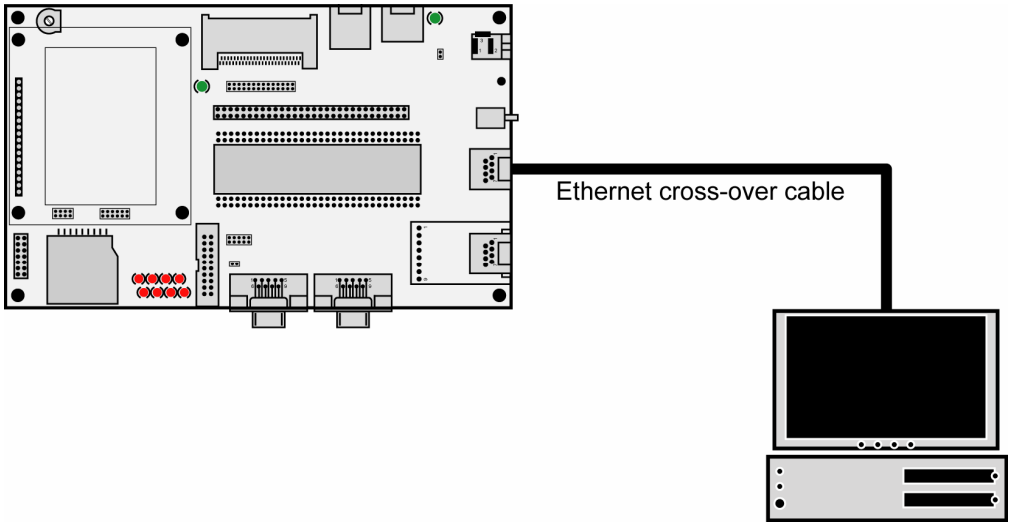
```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap
;dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
```

```
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.126 1701
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
```

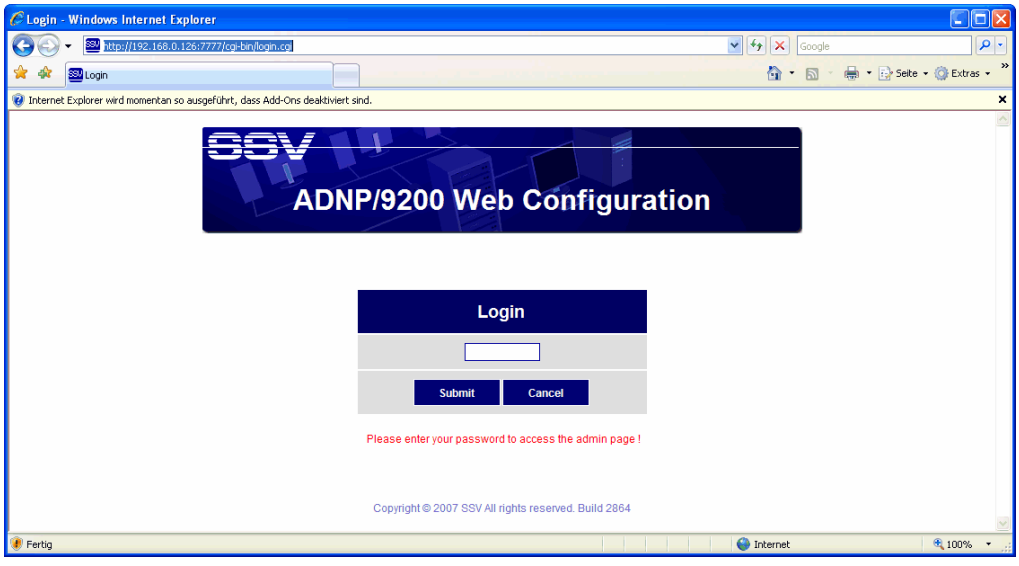
```
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client1.crt
key client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
```

```
# enabled in the server config file.
;comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

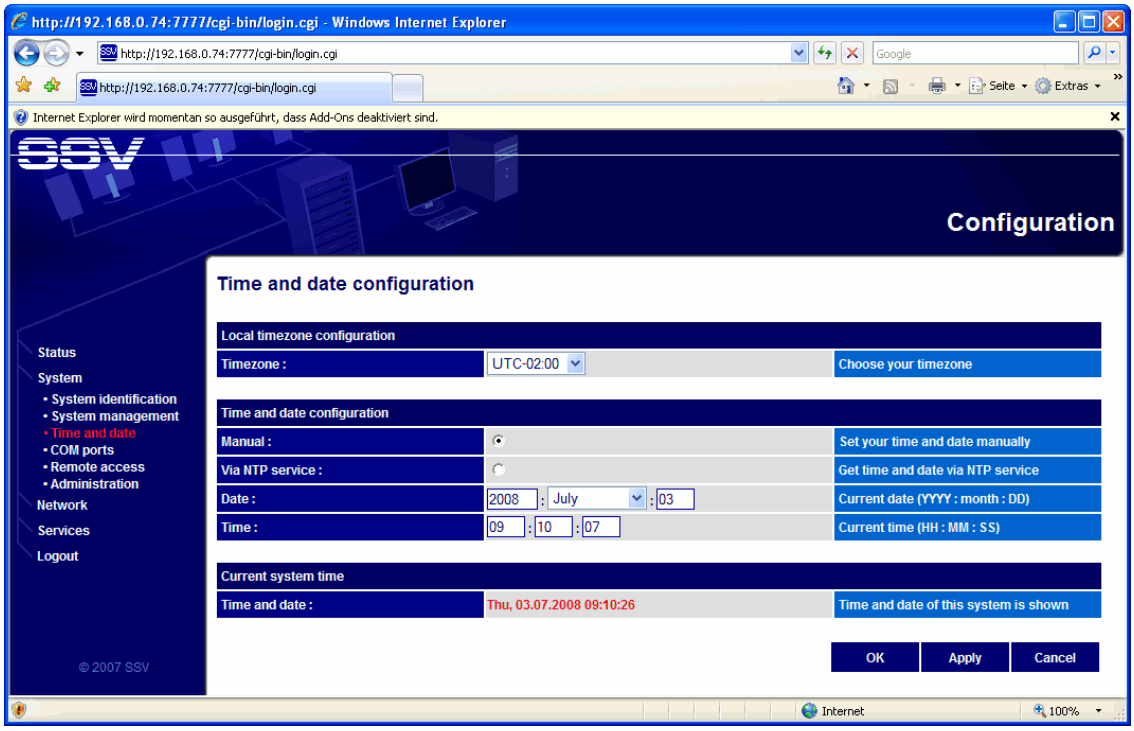
- **10. Step**: Setup the Ethernet LAN link between the LAN1 connector of the DNP/SK27 starter kit and your PC. Use an Ethernet cross-over cable or a switch-based infrastructure for this LAN connection. We assume for the following steps that the ADNP/9200 is using the IP address 192.168.0.126.



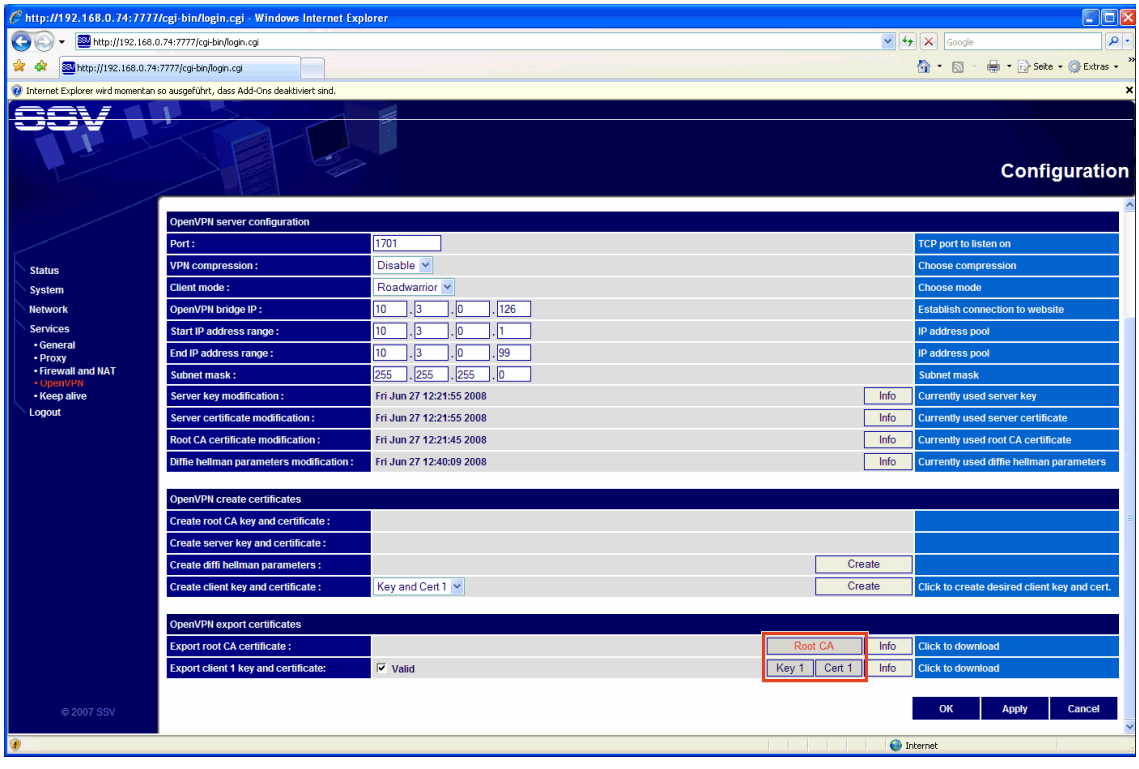
- **11. Step**: Run a web browser on your PC and access the ADNP/9200 web interface with the URI http://192.168.0.126:7777 or http://192.168.0.126:7777/cgi-bin/login.cgi. Please use the logon password **adnp** for your login.



- **12. Step**: Select the menu item **System** and the sub-menu item **Time and date**. Then select **Manual** (Set your time and date manually) and press the **Apply** button. This sets the ADNP/9200-internal real time clock to the current time and date. The valid time is necessary to use OpenVPN. Without a time setting the pre-build OpenVPN certificates are invalid.

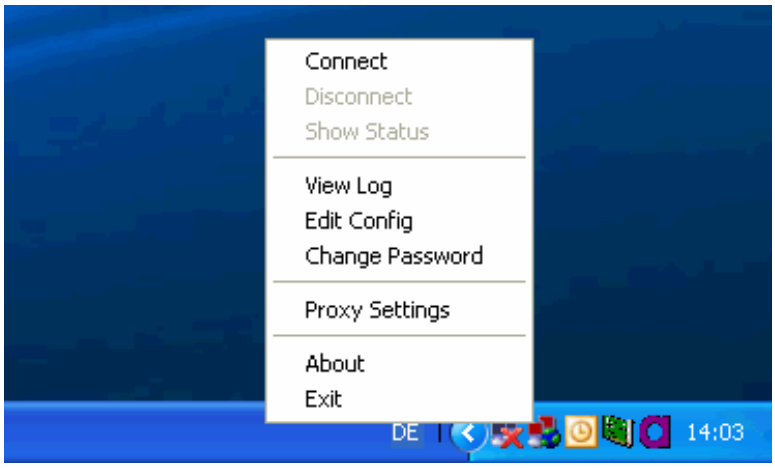


- **13. Step**: Click with the right mouse button to the buttons **Root CA**, **Key1** and **Cert1**. Download and save all three files to the PC directory **c:\Program Files\OpenVPN\config**.

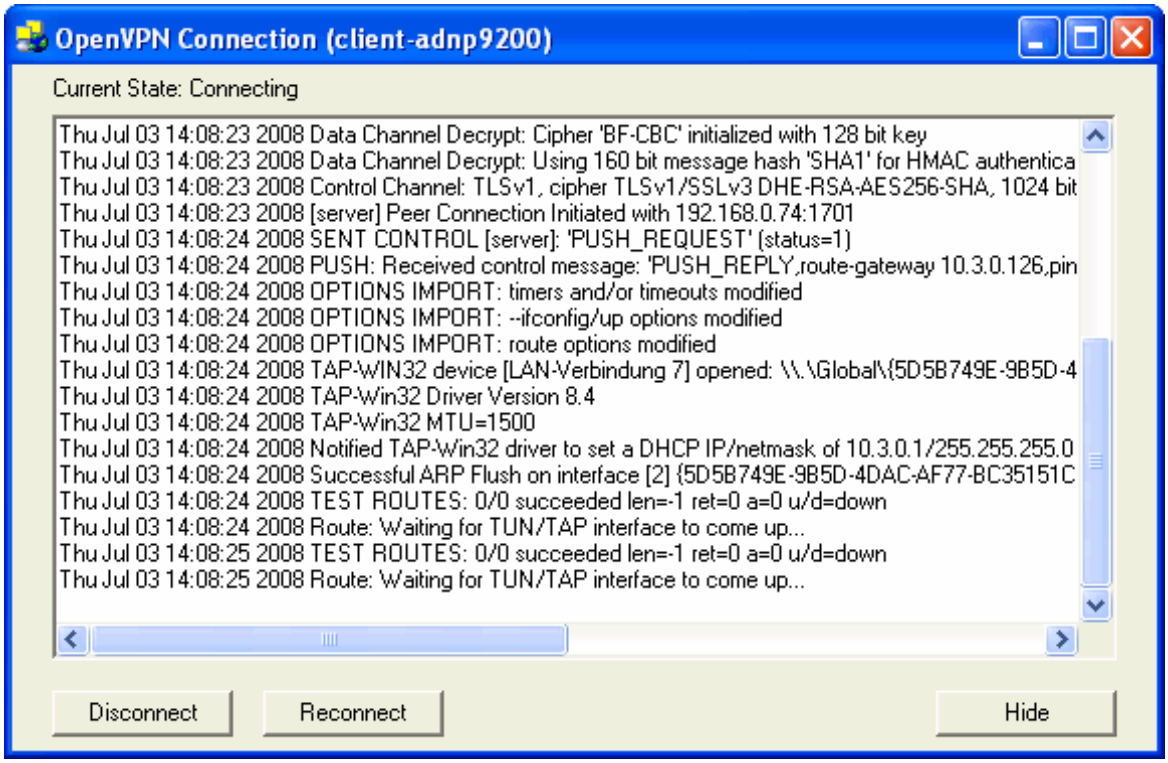


- **14. Step**: We have now the three pre-build certificate files from the ADNP/9200 OpenVPN installation within the PC directory **c:\Program Files\OpenVPN\config**. Please logout from the ADNP/9200 web interface.

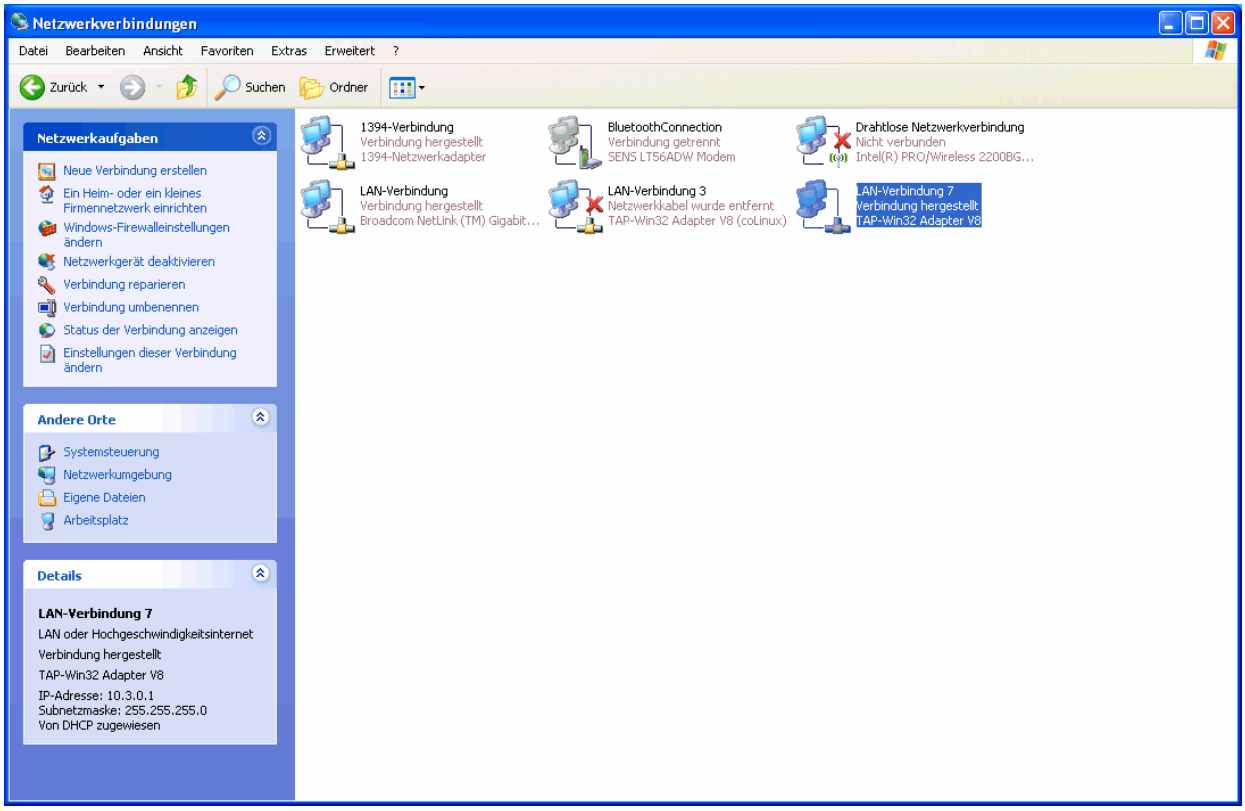
- **15. Step**: Click with right mouse button to the OpenVPN GUI item within the Windows system tray. Then select the **Connect** menu item.



- **16. Step**: Your PC creates an OpenVPN link to the ADNP/9200. A window shows the creation steps and the status/error messages.



- **17. Step**: The OpenVPN link between your PC and the ADNP/9200 creates a new (virtual) IP network interface on your PC. The name is "**TAP-Win32 …**" (in this sample **TAP-Win32 Adapter V8**). The ADNP/9200 supplies this interface with an IP address (in this case **10.3.0.1**).



- **18. Step**: Check the VPN connection between the PC and the DIL/NetPC ADNP/9200 with a simple **ping**. The IP address of the ADNP/9200 within this VPN is **10.3.0.126**.

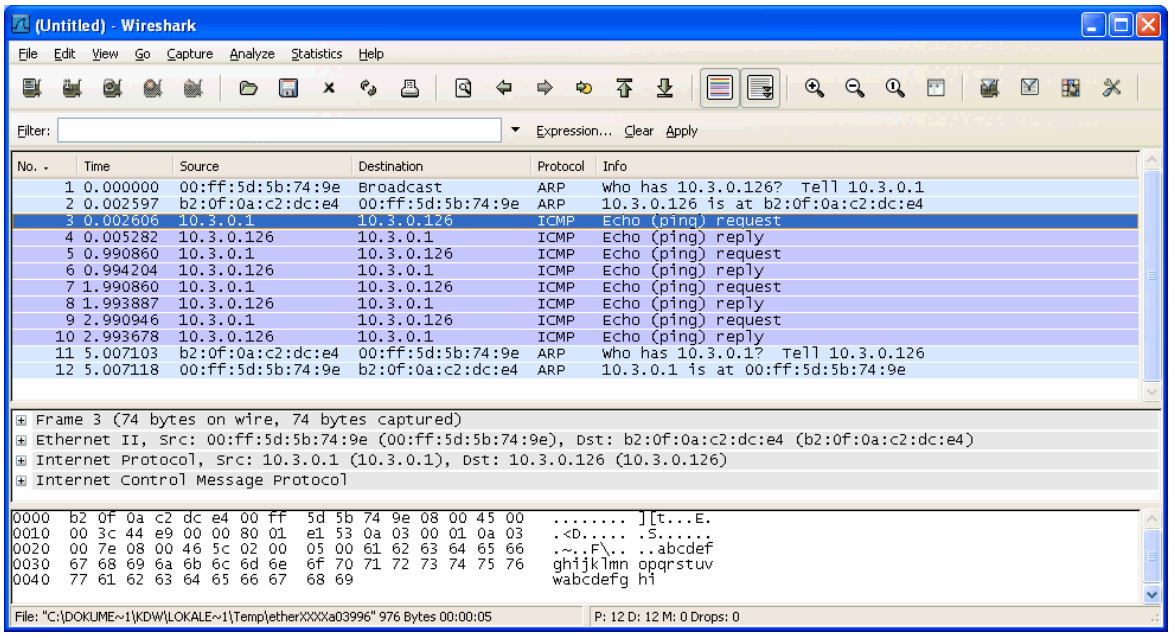
```
ping 10.3.0.126
```

- **19. Step**: Please try to trace the Ethernet-based link between the PC and the ADNP/9200. Use a simple LAN sniffer (e.g. **Wireshark**) for this task.

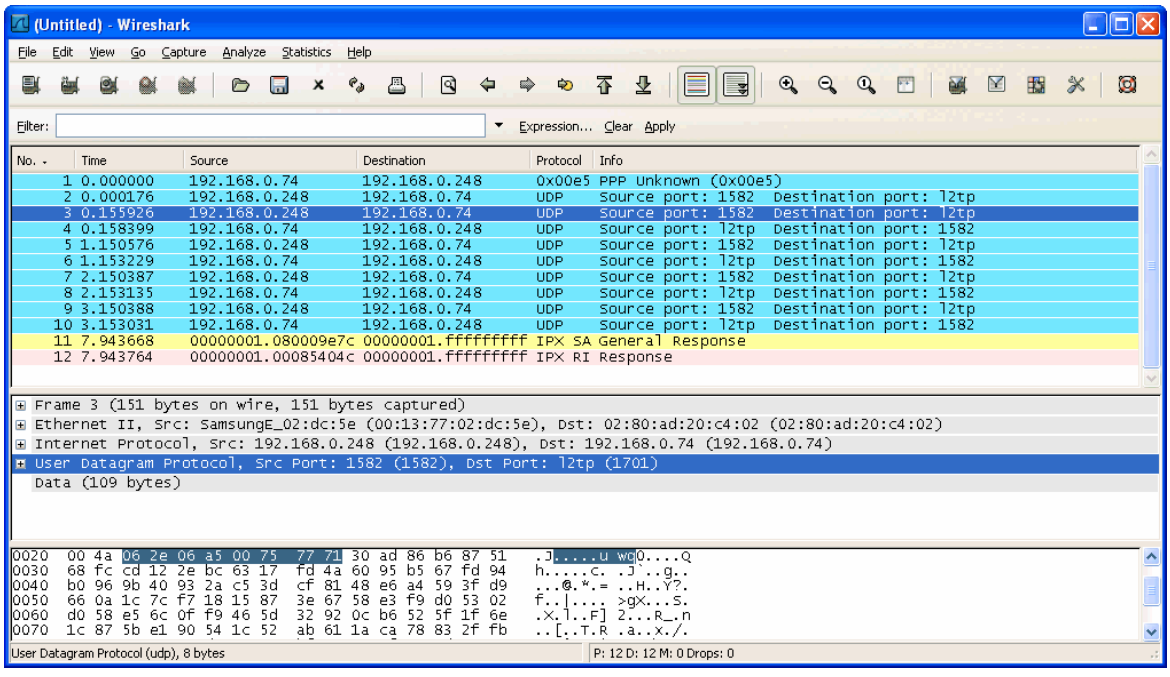
  First select the "**TAP-Win32 …**" interface for your LAN sniffer. This trace will show the ICMP traffic.

  Then select the Ethernet LAN interface of your PC. This trace will show only some UDP traffic

between your PC and the ADNP/9200 UDP port 1701. UDP is the tunnelling protocol for this VPN. The traffic within a UDP packet is encrypted by OpenVPN.



Please note: In next screen shot the IP address 192.168.0.74 is used by the ADNP/9200 as an OpenVPN server. IP address 192.168.0.248 is assigned to the PC as the OpenVPN client.



Please note: For a secure connection to the ADNP/9200 it is also necessary to close the ADNP/9200 Ethernet LAN with the IP address 192.168.0.126 with the help of **Iptables**. Without this step there are two connections between the PC and the ADNP/9200. One over the 192.168.0.0 IP network and the second over the 10.3.0.0 VPN-based network.

That is all.