

OpenVPN Client/Router with REX200/250

White paper

Version 1 / 1/29/2020

Notes

All rights reserved, including those related to the translation, reprinting, and reproduction of this white paper or of parts thereof.

No part of this manual may be reproduced, processed, duplicated, or distributed in any form (photocopy, microfilm, or any other methods), even for training purposes or with the use of electronic systems, without written approval from Helmholtz GmbH & Co. KG.

All rights reserved in the event of the granting of a patent or the registration of a utility model.

To download the latest version of this manual, please visit our website at www.helmholz.de.

We welcome all ideas and suggestions.

Copyright © 2017 by

Helmholtz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach

Contents

- 1 General Information 4**
 - 1.1 OpenVPN with REX 200/250..... 4
 - 1.2 Client/router connection 5
- 2 Installing the OpenVPN software..... 6**
- 3 Settings in the REX 200/250 7**
- 4 Preparation for OpenVPN connection 12**
 - 4.1 Complete connection parameters..... 12
 - 4.2 Establish and end tunnel connection 13
- 5 Appendix 15**

1 General Information

Here you will find a description of how you can set up an OpenVPN connection between a client PC and a REX 200/250. All REX200 and REX 250 derivatives that have been configured as classic routers can be used for this type of remote maintenance. A Windows¹ 7 PC (or higher) with an installed OpenVPN software is required as a dial-up medium.

Check the firmware status of the REX products prior to commissioning. Always use the latest version, which is always available under www.helmholz.de for download. All other basic knowledge necessary for dealing with the REX routers is presumed.

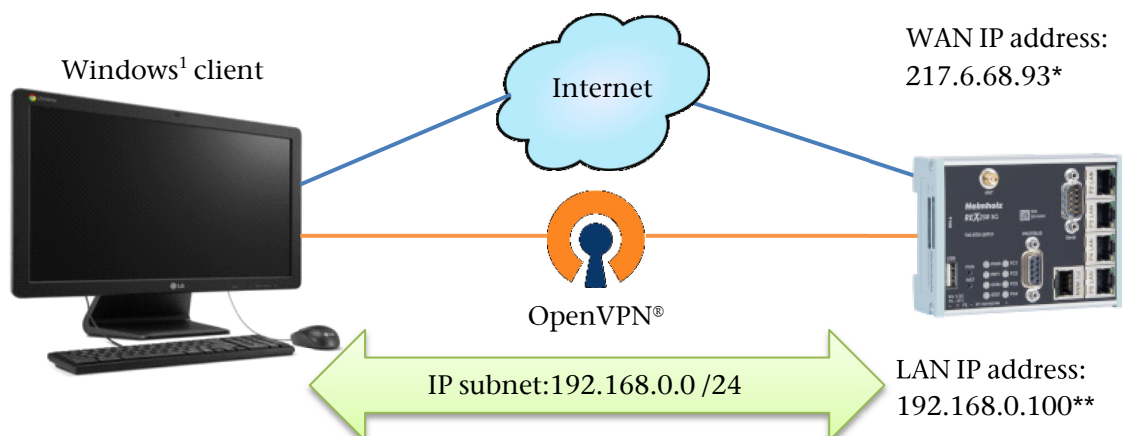
The contents of this white paper have been checked to ensure that they match the hardware and software described. However, Helmholz GmbH & Co. KG can assume no liability for any existing differences, as these cannot be fully ruled out. When using your purchased products, please make sure to use the latest version of the manual, which can be viewed and downloaded in the Internet under www.helmholz.de.



Configuration, execution, and operating errors can interfere with the proper operation of the REX devices and result in personal injury, as well as property or environmental damage. Only adequately qualified personnel may operate the REX devices!

1.1 OpenVPN with REX 200/250

VPN connections from a client PC to a REX 200/250, which represents the VPN server, can only be established via the Internet when the firewall router on the system side is permitted to forward incoming data to the REX 200/250. These prerequisites must be clarified in advance with the system operator or configured accordingly in the customer DMZ. No VPN connection with a REX 200/250 can be realized when the incoming data traffic has been completely blocked for the Internet connection.



*Static IP address that can be accessed from the Internet at the deployment location of the REX 200/250

**Default IP address in the delivery condition

VPN connections allow you access to the LAN interface of the REX 200/250. This means that a VPN tunnel must first always be established for the remote maintenance connection. The connected Ethernet participants from the IP address range of the LAN interface of the REX 200/250 are subsequently accessible.

Two types of encryptions can be chosen from. In the example described here, a randomly generated static key is used. It is not possible to establish several simultaneous OpenVPN connections with an OpenVPN server with this predefined key.

A description of the use of X.509 certificates is not a component of this documentation.

1.2 Client/router connection

A REX 200/250 with the LAN IP address 192.168.0.100 preset at the factory is reached via the Internet in this white paper. As soon as the VPN connection from your Windows¹ PC with the REX 200/250 has been established, you can, for example, access the web interface of the REX 200/250 by entering 192.168.0.100 in your browser URL. The VPN now arranges for the query to the IP 192.168.0.100 be sent to the REX 200/250 through the VPN tunnel via the Internet. This will send the data of the web interface back to you and first query the device-specific login data. You can then view the router configuration, adjust and save parameters.

When using the MPI/PROFIBUS interface in a REX 250, the LAN IP address of the REX is also required. In order to be able to access the MPI/PROFIBUS interface via VPV, this IP must be stored in the NETLink driver (SH S7-NET). You can also find more information on this in the Quick Start Guide of the product.

2 Installing the OpenVPN software

The freely available OpenVPN software can be downloaded under: “<https://openvpn.net/community-downloads/>”. Version 2.4.7 is used in this white paper. We recommend always using the latest version from the official download area.

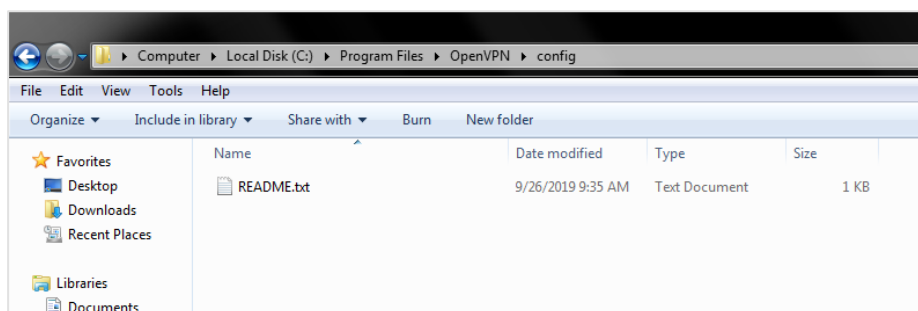


HINWEIS

Please always carry out the OpenVPN instances as the administrator (right mouse click - “Carry out as administrator”) and confirm the query of the user account control system with “Yes”.

In the menu-guided OpenVPN setup, please confirm all dialogs in order to go to the respective next installation step (no adjustment needs to be carried out in the suggested component selection). Following successful installation, all files will have been filed in the OpenVPN standard installation folder “C:\Program Files (x86)\OpenVPN” of your PC.

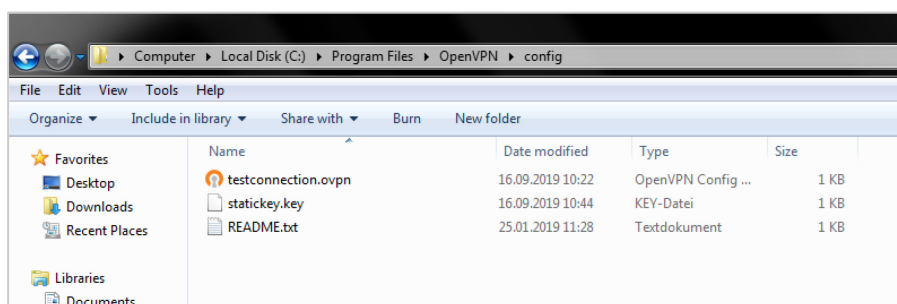
OpenVPN automatically creates the folder “\config” during installation.



The two OpenVPN configuration files

- testconnection.ovpn and
- statickey.key

must later be filed in this directory.



The preconfigured testconnection.ovpn file is also available to you in the www.helmholz.de download area. The adjustments to the .ovpn parameters you still need to carry out are described in the following chapters in detail.

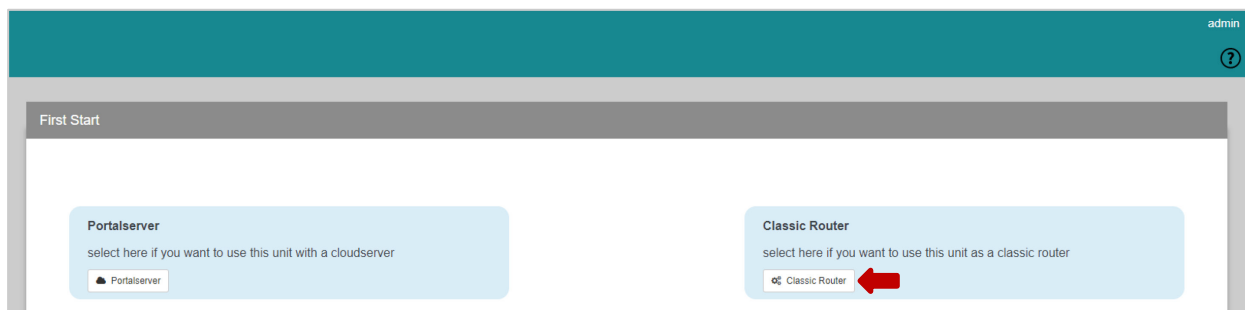
The contents of the testconnection.ovpn file are available in text format and can be edited with a standard Windows¹ editor.

We recommend opening this file parallel with the REX configuration, in order that the parameters described in the following can be immediately edited at the right place.


3 Settings in the REX 200/250

The settings described in the following must be made via the web interface of the REX. To this purpose, the REX must be accessible in the LAN via its IP address. Open the REX 200/250 web interface in a standard browser. In this example, factory settings are presumed. The IP address 192.168.0.100 must consequently be entered into the URL of the browser.

The First Start page is shown following successful web interface registration:



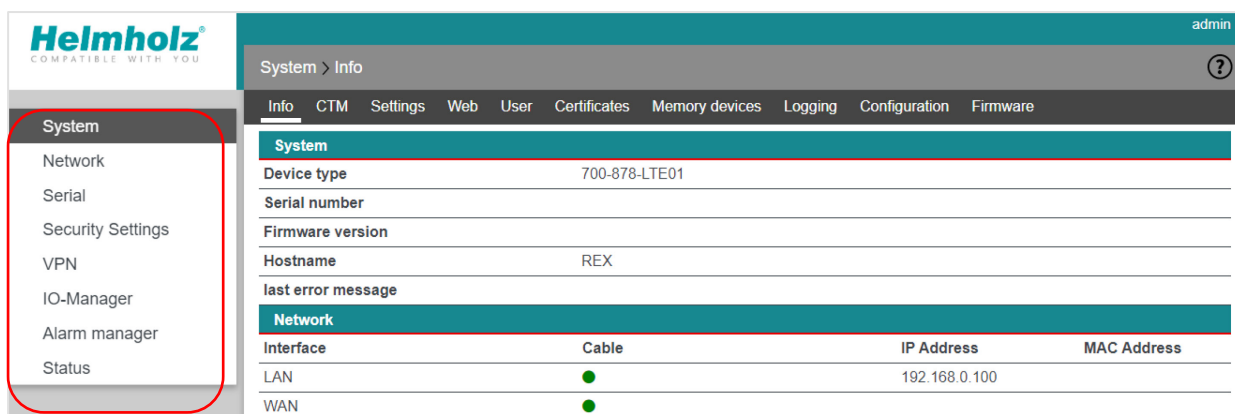
The necessary settings can be made via the selection menu of the “Classic Router”!



HINWEIS The “First Start” page is now displayed when the router is started in the delivery condition. Once activated, the renewed possibility to choose between the portal server and the classic router is only possible following a reset to factory settings.

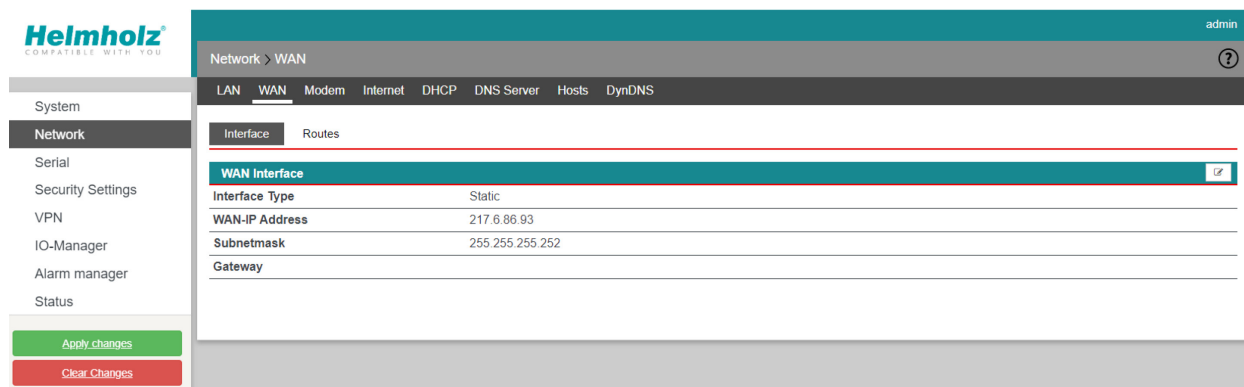
The window with the system information subsequently opens. The task sidebar is located to the left.

The router must now be manually configured for Internet access.



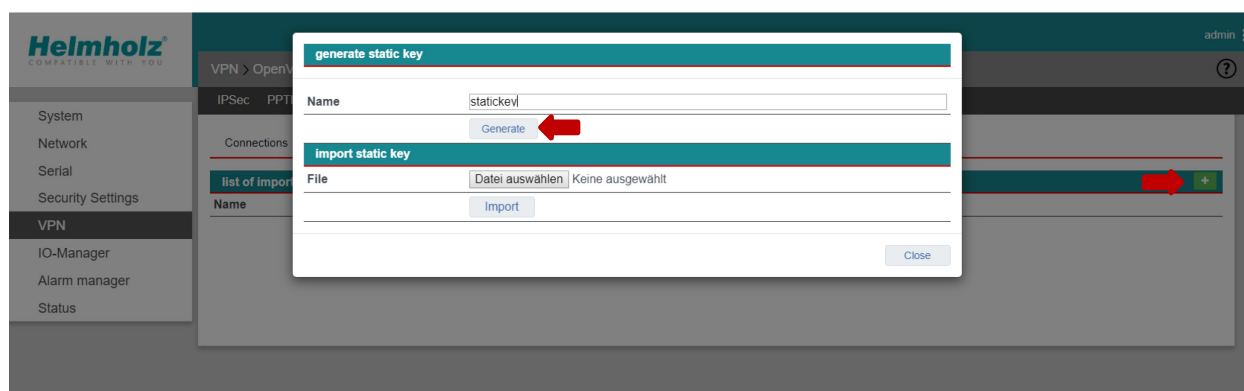
Choose “Network” in the task sidebar and then “WAN” in the menu bar. Under “Interface”, the WAN interface must be configured in keeping with the requirements at the Internet access point at the installation location.

It should be noted that the values set here only serve as an example and cannot be used for your projects!



Edit the testconnection.ovpn and enter the WAN IP address of the REX in the “remote” line (see also Chapter 4).

Choose “VPN” in the task sidebar and then “OpenVPN” in the menu bar. A key must now be generated or imported under “Static Key” via the green plus sign.



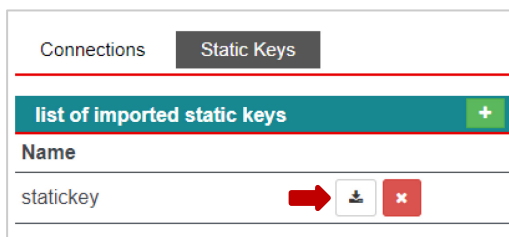
In this example, a new “stactickey” is generated (the name can be chosen freely). The entry is completed with “Close”.



HINWEIS

When settings are made, you must then “Accept changes”. The corresponding green button appears in the lower area of the task sidebar as soon as fundamental parameters have been changed via the web interface!

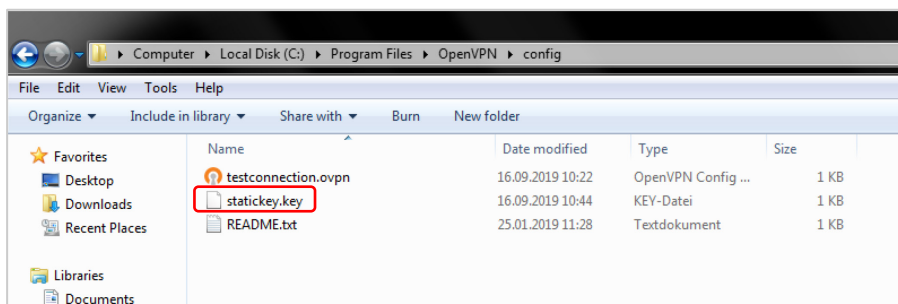
You can download the static key to your Windows¹ client PC via the symbol.



i
HINWEIS

The suggested suffix may differ depending upon the browser used. You may need to enter file name manually with the ending .key and save!

In the image you can see the final file names and the correct filing path
→ C:\Program Files\OpenVPN\config



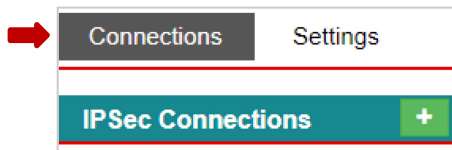
Edit the testconnection.ovpn and enter the complete path for the key just generated in the “secret” line (see also Chapter 4).

i
HINWEIS

In the case of activated UAC (User Account Control) under Windows¹ 7, an error message appears when an attempt is made to save to this directory. Should this be the case, save the file temporarily in another folder to then add it retroactively to
→ C:\Program Files\OpenVPN\config.

Confirm the query for administrator rights with “Continue”:

In order to choose the settings for the OpenVPN connections, at least the following steps must be carried out. Click on “Connections”



1) The connection name is identical with the testconnection.ovpn file! In our example, “testconnection”. When you use a different .ovpn file name, this must be entered here accordingly.

A “client - router connection” must be selected as a connection type for this example.

With “Continue” to point 2.

OpenVPN Connections

1 Connection settings 2 Network settings 3 Authentication 4 Protocol settings

Active

Connection name

Connection type

Next

Save Close

2) The IP addresses of the VPN tunnel shown here are preset in the REX and normally don't need to be changed (specifications deviating from the following illustration may be possible).

We recommend activating SNAT in order that the LAN participants connected to the REX don't require the REX LAN IP as a gateway entry.

OpenVPN Connections

1 Connection settings 2 Network settings 3 Authentication 4 Protocol settings

Local IP Address of the VPN tunnel

Peer IP Address of the VPN tunnel

Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)

Back Next

Save Close

Edit the testconnection.ovpn and enter the VPN tunnel IPs in “ifconfig” line (see also Chapter 4).

With “Continue” to point 3.

3) The appropriate selection can be made through the drop-down menus. A static key is used in this example as the authentication process.

The static key, which you have already generated, is listed in the selection line as “statickey” and must now be selected.

The screenshot displays the 'OpenVPN Connections' configuration window. At the top, a teal header reads 'OpenVPN Connections'. Below it is a progress bar with four steps: '1 Connection settings', '2 Network settings', '3 Authentication', and '4 Protocol settings'. Step 3 is highlighted in dark blue. Underneath the progress bar, there are two dropdown menus. The first is labeled 'Authentication process' and has 'static key' selected. The second is labeled 'Static Keys' and has 'statickey' selected. Below these dropdowns are two buttons: 'Back' and 'Next'. At the bottom right of the window are two buttons: 'Save' and 'Close'.

Because in our example no adjustments in the protocol settings under point 4 are necessary, the OpenVPN configuration is to this extent complete and can now be saved with “Save”.

4 Preparation for OpenVPN connection

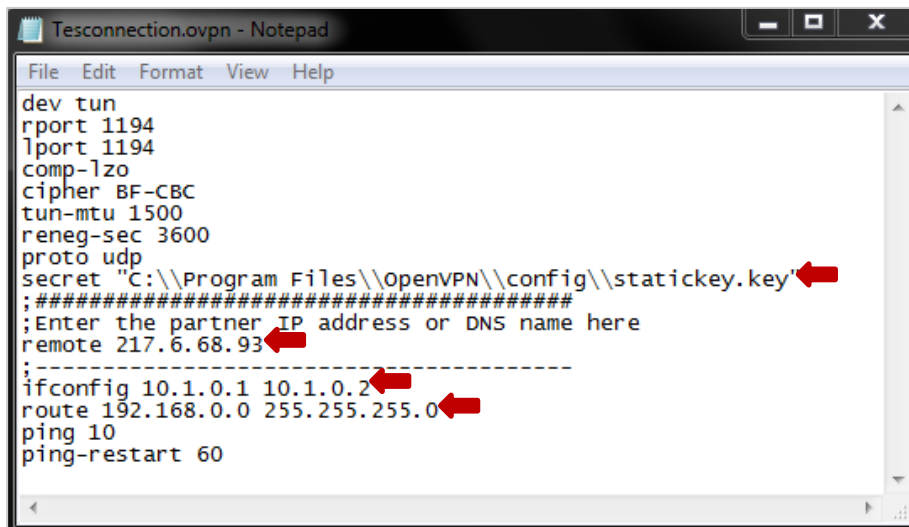
4.1 Complete connection parameters

As already commenced with in the previous chapters, all necessary adjustments of the “testconnection.ovpn” file are conclusively summarized here.

The “testconnection.ovpn” described here is available for download at our homepage and can be processed with a standard Windows¹ editor.

For this example, the following adjustments should be carried out or already have been.

- For “secret”, enter the complete path for the previously generated key. Be sure to use the method of entry with double slashes and superscript exclamation marks!
secret "C:\\Program Files (x86)\\OpenVPN\\config\\stickey.key"
- The removed IP address is entered in the “remote” line. Here you must define the Internet address to which the OpenVPN connection should be established. In our example, the WAN IP address of the REX 200/250 is entered (this IP can not be used for your application case).
- The VPN tunnel addresses are displayed in the “ifconfig”. In the event that these deviate from your settings, they must be adjusted.
- In the “route” field, indicate the network range and the subnet mask of your LAN settings from the REX. In this example, the preset factory setting IP 192.168.0.100 is taken as the basis.



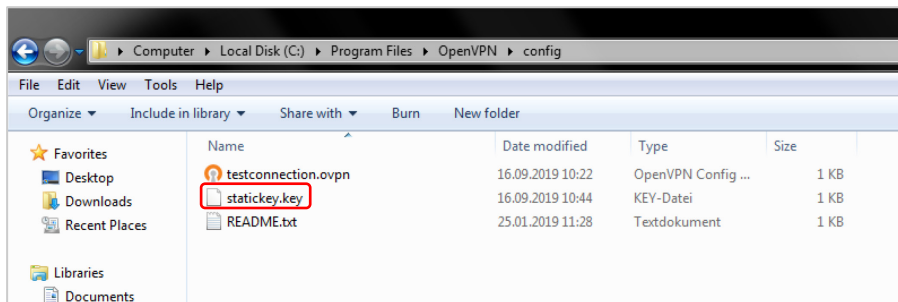
```
File Edit Format View Help
dev tun
rport 1194
lport 1194
comp-lzo
cipher BF-CBC
tun-mtu 1500
reneg-sec 3600
proto udp
secret "C:\\Program Files\\OpenVPN\\config\\stickey.key"
;#####
;Enter the partner IP address or DNS name here
remote 217.6.68.93
-----
ifconfig 10.1.0.1 10.1.0.2
route 192.168.0.0 255.255.255.0
ping 10
ping-restart 60
```



HINWEIS

OpenVPN also allows users to use a proxy server as an Internet access point. To this purpose you must convert the preset network protocol from UDP to TCP. Many proxy servers don't allow the UDP protocol. In this case, change the entry “proto udp” to “proto tcp-client” in the testconnection.ovpn file on your PC.

When you have adjusted the entries described above, save the file under → C:\Program Files\OpenVPN\config ab.

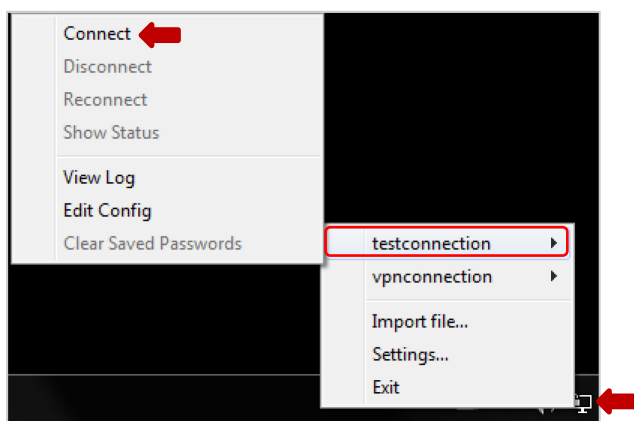


4.2 Establish and end tunnel connection

After all files have been filed in the \config folder, the OpenVPN GUI can be started in the Windows¹ client.

Other prerequisites are that the previously configured REX 200/250 is connected at the WAN interface and can be reached via the Internet.

In the Windows¹ task bar, a new symbol (preferably in the lower right area) was added during the OpenVPN installation.



Right-click on the OpenVPN icon in order to open the software context menu. Choose your “testconnection” and go to “Connect” in the next drop-down window with the left mouse button.

OpenVPN will now attempt to establish a VPN connection to the other previously configured connection point. This can be recognized in that the OpenVPN symbol changes to the yellow state.

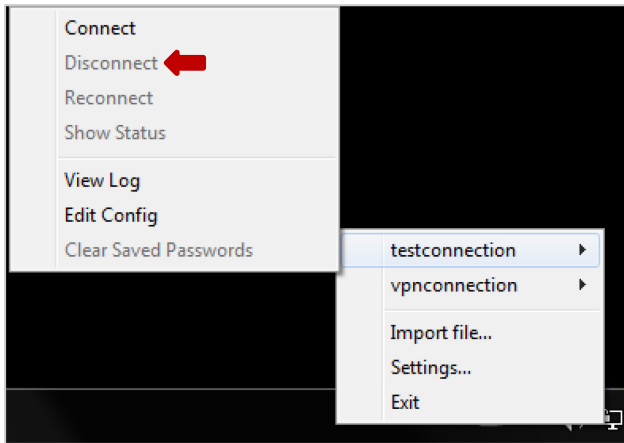


Please note that the VPN connection can only be established when no other port barriers are active in the involved firewalls. The successfully established tunnel connection is displayed for you in the form of a green OpenVPN symbol.



In this example you can now reach the LAN IP address of the removed REX 200/250 and, for example, open the web interface with the URL: <http://192.168.0.100>. Other TCP-IP participants connected to the LAN ports can be reached in the same way or remote maintenance can be realized.

If you would like to disconnect, click with the right mouse button on the OpenVPN symbol and select “Disconnect”. The icon will now change color from green to gray and the tunnel connection is terminated.



5 Appendix

Here the content of the testconnection.ovpn used in this white paper for copying and further processing in a text editor:

```
dev tun
rport 1194
lport 1194
comp-lzo
cipher BF-CBC
tun-mtu 1500
reneg-sec 3600
proto udp
secret "C:\\Program Files (x86)\\OpenVPN\\config\\stickey.key"
#####
;Enter the partner IP address or DNS name here
remote 217.6.68.93
;-----
ifconfig 10.1.0.1 10.1.0.2
route 192.168.0.0 255.255.255.0
ping 10
ping-restart 60
```

1 Windows is a registered trademark of Microsoft Corporation.