



BAB TECHNOLOGIE GmbH

EIBPORT 3 VPN SSL

Usage with an OpenVPN Client

Date: 11/ October 2016

EN



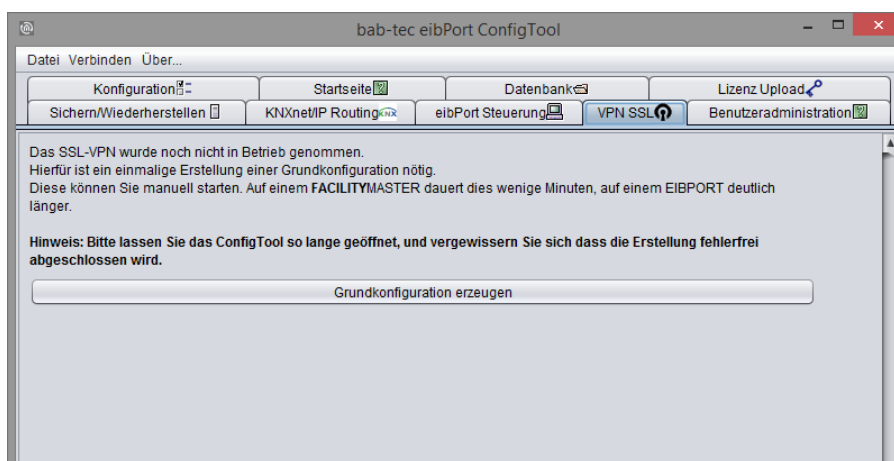
OPTIMAL DATA SECURITY

To achieve adequate data security during Internet-based access to an EIBPORT 3, we recommend using a VPN connection.

A VPN is a virtually created network between two participants that secures the connection against unauthorized access by using encryption. Additionally, the participants are connected as if they were members of the same private network.

VPN SSL SERVER

EIBPORT offers two different VPN solutions: "VPN PPTP" and "VPN SSL". For security reasons we recommend to use „VPN SSL“.



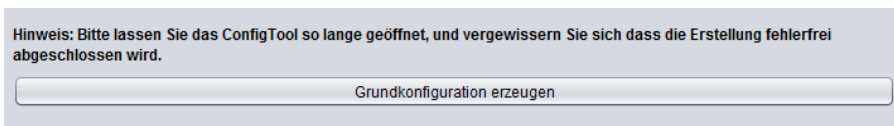
The VPN SSL service in the EIBPORT offers two functionalities:

- VPN server for a secure connection between end user devices and EIBPORT via an OpenVPN client
- Establishing a BAB **SECURELINK** connection (device serves as VPN client) to other BAB devices (**LINKMODULE**, **EIBPORT**, **FACILITYMASTER**)

Preparations

INITIALISING THE VPN SSL SERVER

To be able to use the services relevant to VPN SSL (BAB **SECURELINK**, VPN Server) in the EIBPORT, the VPN server has to be initialised once. To do so, browse the "System" menu and click on "Start basic configuration" in the "VPN SSL" menu.



Note: Initialising takes approx. 50 minutes. During this time the required certificates are generated. Do not switch off the EIBPORT while this process takes place.

After the VPN server has been successfully initialised (see above) the VPN server settings are displayed.

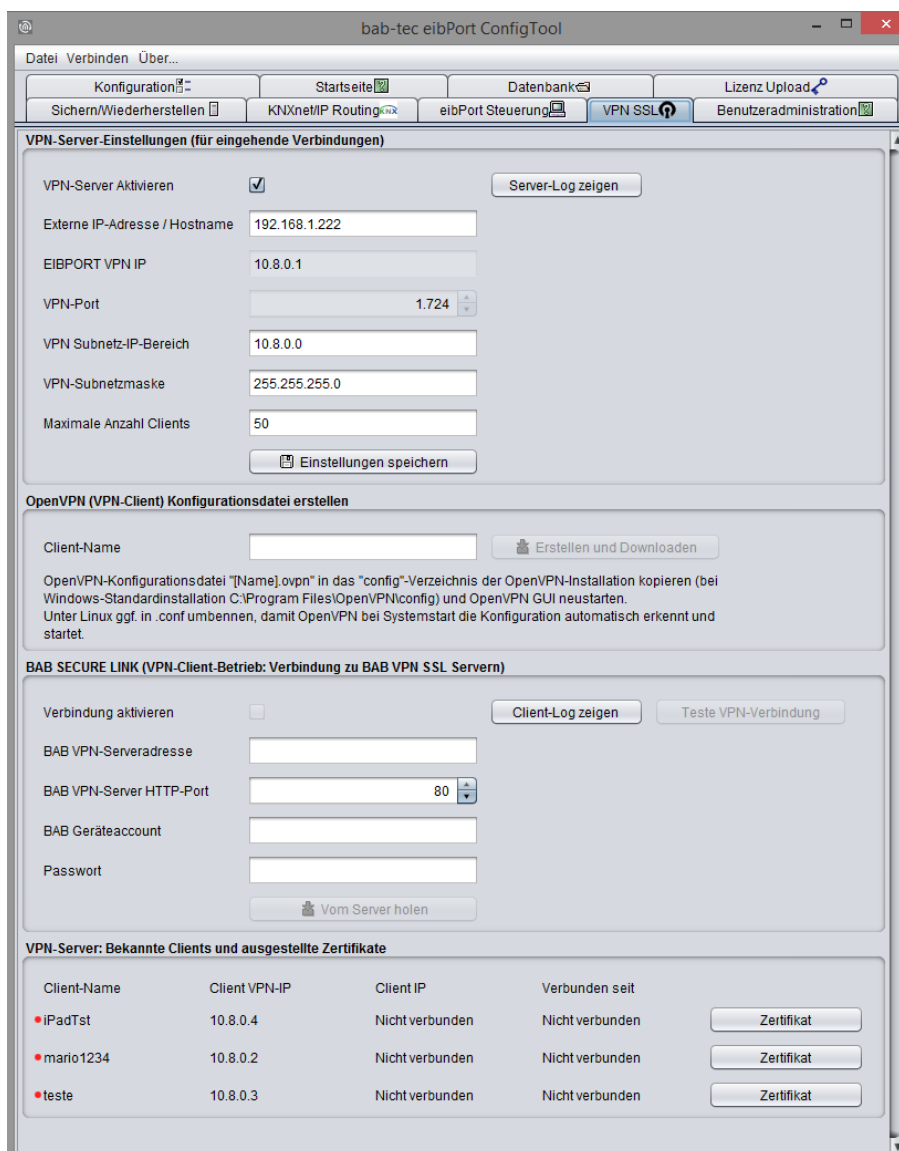


Figure 1: System – VPN SSL, Server initialised

VPN SERVER SETTINGS (FOR INCOMING CONNECTIONS)

The following parameters are available for configuring the VPN server for incoming connections:

In order to prepare the VPN SSL-Server for the usage with an OpenVPN-Client, please consider the following settings:

- *External IP address / host name:* Please enter here the address under which the EIB**PORT** can be reached from outside. If the incoming connection (a VPN client wanting to connect with the server) is from the same network, enter here the local IP address of the EIB**PORT**. If it is an external connection, the external address of the corresponding network has to be used (e. g. the external IP address of the DSL router).
- *EIB**PORT** VPN IP:* Specifies the IP address allocated to the EIB**PORT** within the VPN network.
- *VPN subnetwork IP range:* Specifies the IP range in which the VPN network is created (10.8.0.0 is set as default).

Note: The VPN server is only active after "Enable VPN server" has been highlighted and the settings have been saved.



PORT FORWARDING FOR THE VPN CONNECTION

Please note that TCP Port 1724 has to be forwarded for the usage of the VPN connection.

CREATE AN OPENVPN (VPN CLIENT) CONFIGURATION FILE

- Assign a unique name for the configuration file of the desired device in the field „Create OpenVPN (VPN Client) Configuration File“. Then download the file by pressing „Create and Download“.

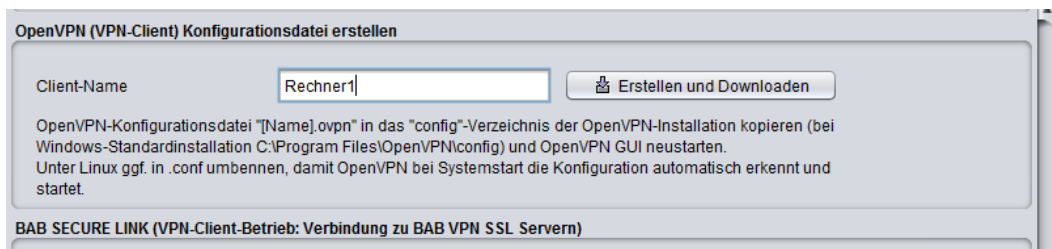


Figure 2: VPN SSL – Create and Download OpenVPN file

INSTALL THE OPENVPN CLIENT SOFTWARE ON THE DESIRED DEVICE

Please download the correct OpenVPN-Client software for your operation system and install it:

- Windows: „OpenVPN GUI“ (at www.openvpn.net)
- MAC OS: „Tunnelblick“ (at www.tunnelblick.net)
- Android: „OpenVPN for Android“ (from the Google PlayStore)
- iOS: „OpenVPN“ (from the iOS AppStore)

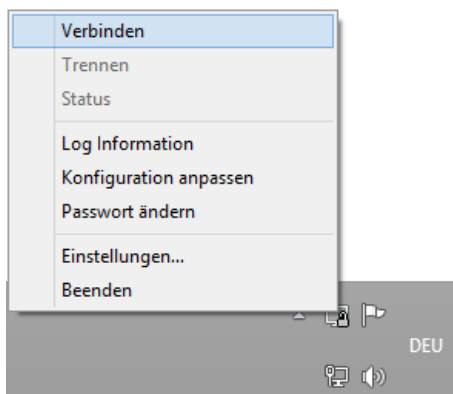
Setup

CREATE OPENVPN (VPN CLIENT) CONFIGURATION FILE

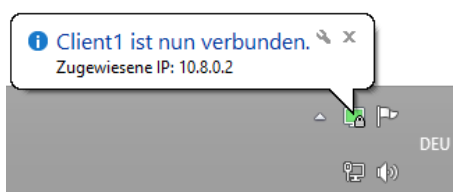
- Copy the OpenVPN configuration file '[Name].ovpn' into the 'config' directory of the OpenVPN client installation (for Windows-„OpenVPN GUI“ the default path is: „C:\Program Files\OpenVPN\config“).
- Then start „OpenVPN GUI“ via Windows Start menu. The OpenVPN GUI icon will appear in the Windows System Tray



- You can now establish the connection using the context menu of the icon (right-click the icon)



- A successfully established connection will be indicated by a notification pop-up and by the icon turning green



The EIBPORT is now available at the “EIBPORT VPN IP” (see above, standard 10.8.0.1).

VERBINDUNG MIT MAC OS HERSTELLEN

- After you have installed Tunnelblick (see above), the Tunnelblick icon will appear in your menu bar. You can drag the downloaded configuration file with your mouse onto the Tunnelblick icon.



- This will open an additional dialogue which allows you to establish the connection.



- Click on „Verbinden“. The connection will be established. A successful connection is indicated by the Tunnelblick symbol turning active and the font becoming green.



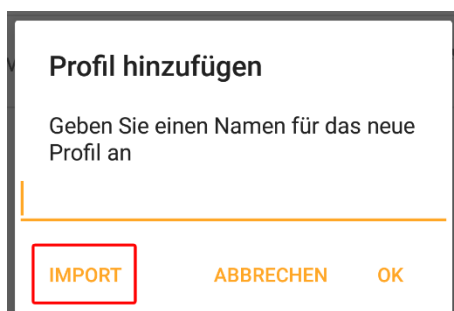
The EIBPORT is now available at the “EIBPORT VPN IP” (see above, standard 10.8.0.1).

ESTABLISH A VPN CONNECTION WITH ANDROID DEVICES

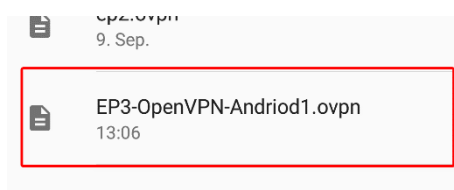
- After you have installed the app mentioned under “Preparations”, please transfer this file to your Android system. We recommend using a USB connection.
- Start the app. You can import OpenVPN configuration files by tapping the “Plus” symbol.



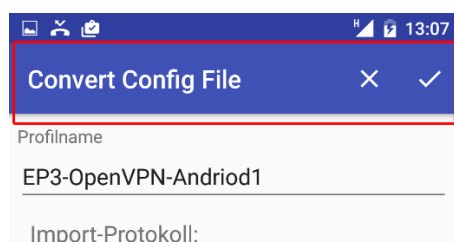
- Click on “Import VPN Profile” to access the download folder of your Android device.



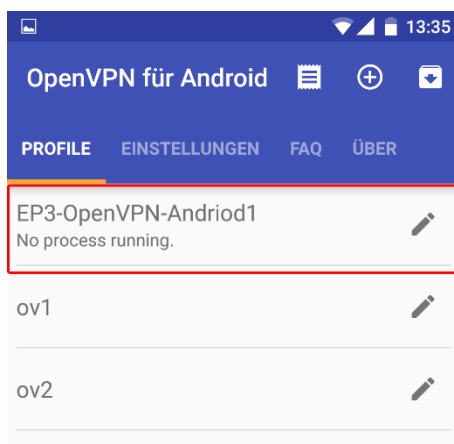
- Then select the correct configuration file from the download folder.



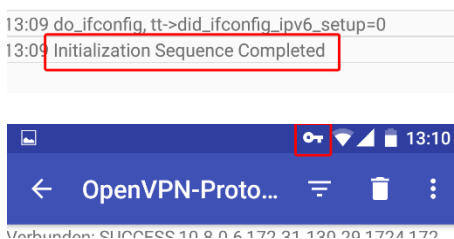
- The app first needs to convert the file. Confirm this process by tapping the check mark.



- Afterwards, you can establish the connection by simply tapping the corresponding list entry.



- A successful connection will then be indicated through log messages and a key symbol in the status bar.



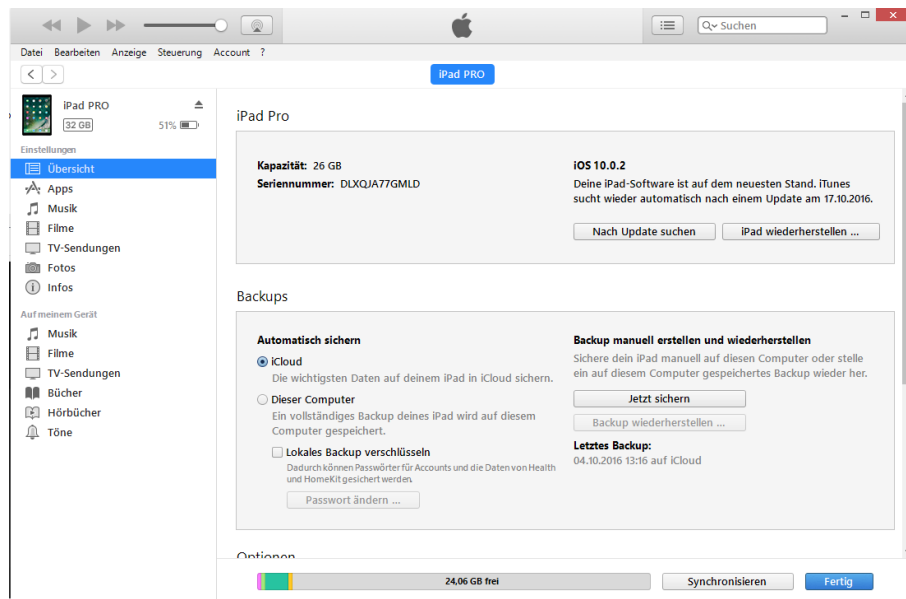
The EIBPORT is now available at the “EIBPORT VPN IP” (see above, standard 10.8.0.1).



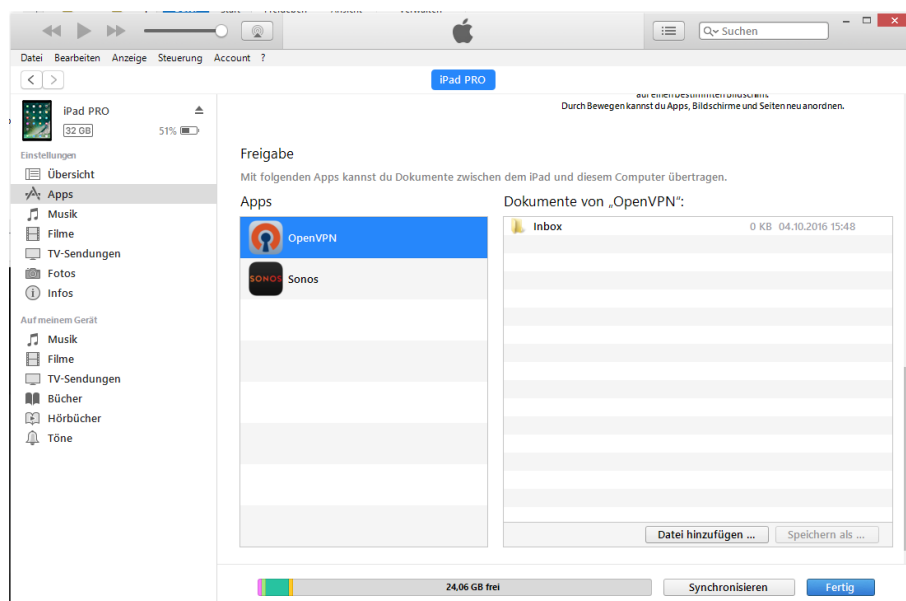
ESTABLISH A VPN CONNECTION WITH IOS DEVICES

Note: At least EIBPORT firmware 3.4.4 required

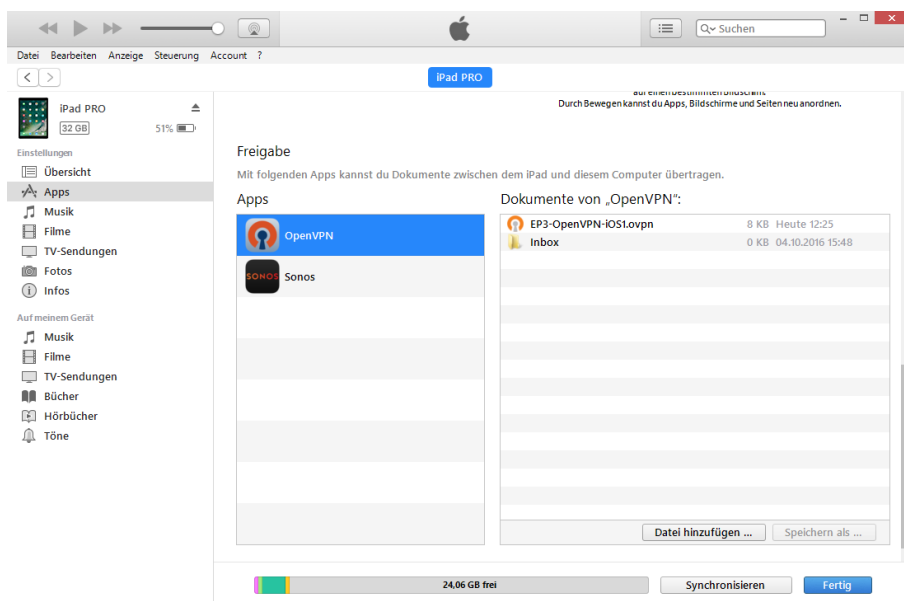
- Start iTunes and select the device view



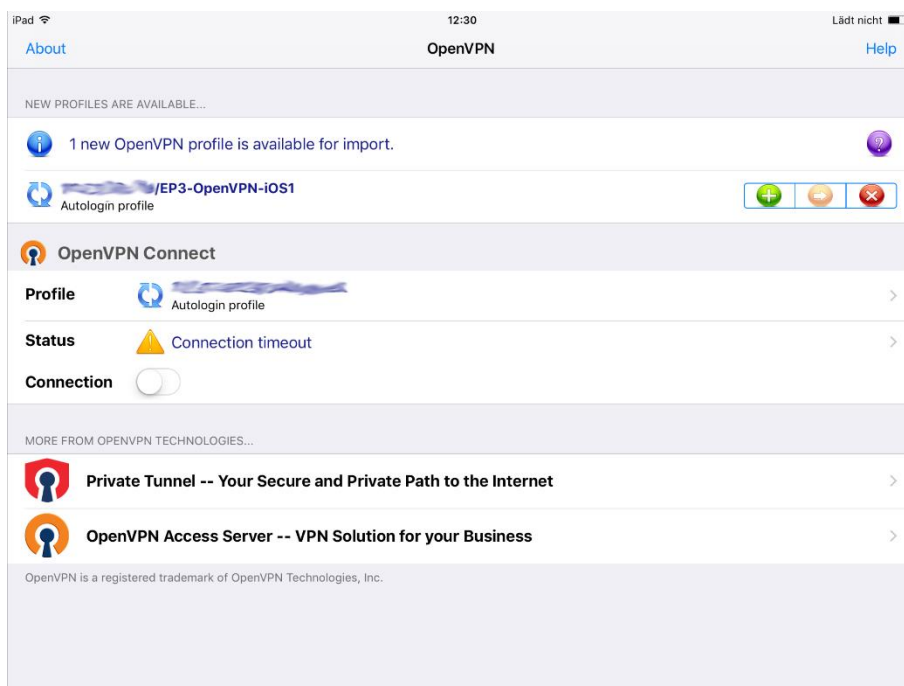
- Under „Apps“ you get access to the file system shares of certain apps. The „OpenVPN“ app will appear here once installed.



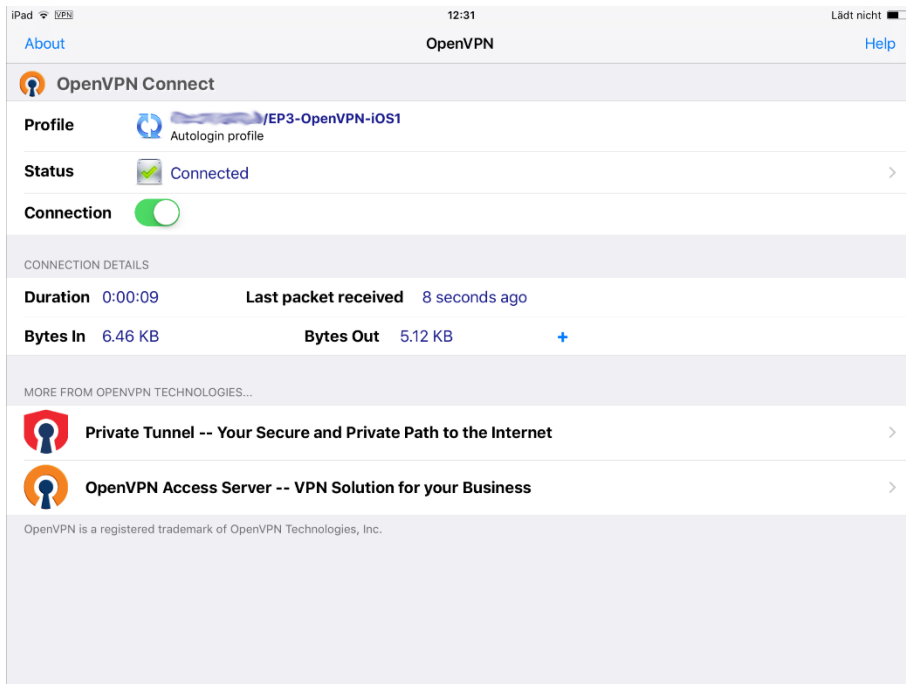
- Use the “Add file” button to copy the OpenVPN configuration file to documents of the OpenVPN app.



- The file will then appear in the app, marked as available for import.



- Tap the green plus symbol to import the configuration file. Afterwards, the configuration can be used to establish a connection.



- The VPN connection can be activated using the switch next to „Connection“. As soon as it has been established, a green check mark appears next to „Status“, and the duration will be shown under „Connections Details“.

The EIBPORT is now available at the “EIBPORT VPN IP” (see above, standard 10.8.0.1).

REVOKE AND LOOK AT CERTIFICATES

This list contains all configuration files that have been created.

| Client-Name | Client VPN-IP | Client IP | Verbunden seit | |
|-------------|---------------|-----------------|--------------------------|------------|
| Rechner1 | 10.8.0.5 | [REDACTED] | Wed Mar 23 15:42:26 2... | Zertifikat |
| iPadTst | 10.8.0.4 | Nicht verbunden | Nicht verbunden | Zertifikat |
| mario1234 | 10.8.0.2 | Nicht verbunden | Nicht verbunden | Zertifikat |
| teste | 10.8.0.3 | Nicht verbunden | Nicht verbunden | Zertifikat |

Figure 3: OpenVPN – list of known clients

If a connection is active, the corresponding values are shown in "Client IP" and "Connected since".

Certificate

Each connected client has been allocated its own certificate by the configuration file. The certificate can be displayed using the "Certificate" button, downloaded ("Download") or blocked ("Block").

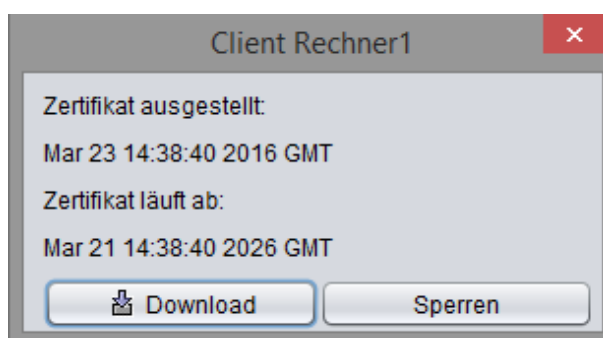


Figure 4: OpenVPN Client – displaying the certificate

Block client

To block a connected client, use the "Block" function in the "Certificate" menu. The client connection will be interrupted immediately. To be able to use the client again, the block has to be deleted and a configuration file has to be re-created.

- Open "Certificate" again. Click on "Delete". You can then load a configuration file for the same client name in the Certificate window.