OPENVPN GUIDE

BUSINESS SMART CONNECT

Telekom Deutschland GmbH

Version:	1.0
Stand:	09.08.2019
Status:	Final

ERLEBEN, WAS VERBINDET.

TABLE OF CONTENTS

Introduction

For secure exchange of mobile data between customer systems and the Business Smart Connect Platform, Telekom Deutschland GmbH provides OpenVPN-service support. OpenVPN allows you to easily and inexpensively connect your servers on your own, by means of self-service.

This document presents and describes the OpenVPN set-up and configuration to successfully connect your backend to the BSC-Portal. Moreover, this document provides example set-ups and the information needed to troubleshoot issues that may arise during the set-up of the solution.

OPENVPN IN OVERALL CONTEXT

Data communication on the internet is in principle exposed to high risks if no further protective measures are taken. OpenVPN is the recommended application set-up to establish a secure data connection between the BSC-Portal and your own IT-environment.

OpenVPN allows you to reach your device from your own IT environment, since the device doesn't hold a public IP, and thus cannot be reached through the internet. Consequently, this device cannot be attacked via the internet.

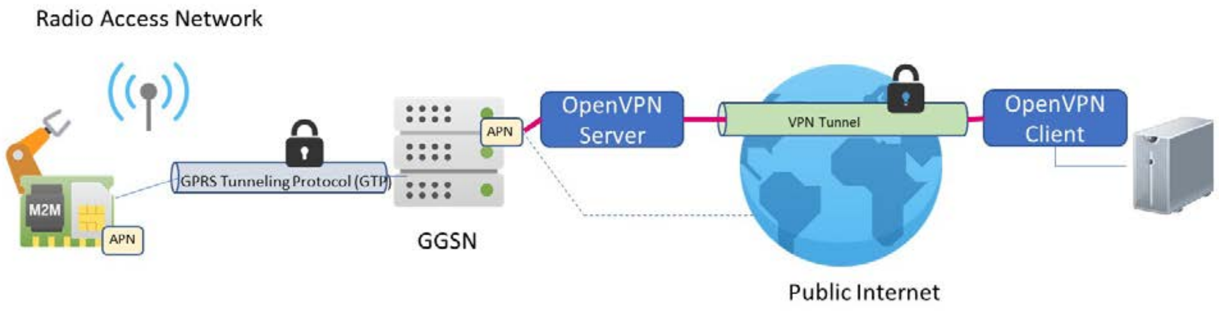


Figure 1: OpenVPN set-up in its overall context

The OpenVPN client needs to be installed on the application server, to which the data of the device shall be transmitted. The OpenVPN connection to the Business Smart Connect Portal is established by the OpenVPN client, which can be downloaded from the BSC-Portal. After the network connection and the OpenVPN connections have been established, you may check the connection with a Ping:

SIM-> Server
From the device execute a PING to the OpenVPN client's address (e.g. 10.x.x.x; the IP is always the same for the customer).

Server-> SIM
From your server execute a PING to the IP address of your device. It is a private IPv4 address which has been assigned by the Telekom network when the mobile connection is established (e.g. 100.x.x.x; the IP address is always the same for one SIM).

Note: Sometimes it may take a while until connection from device is established and several ping packet might fail, because it requires that the SIM is "online" (PDP context active), e.g. NB-IoT device is in power save mode).

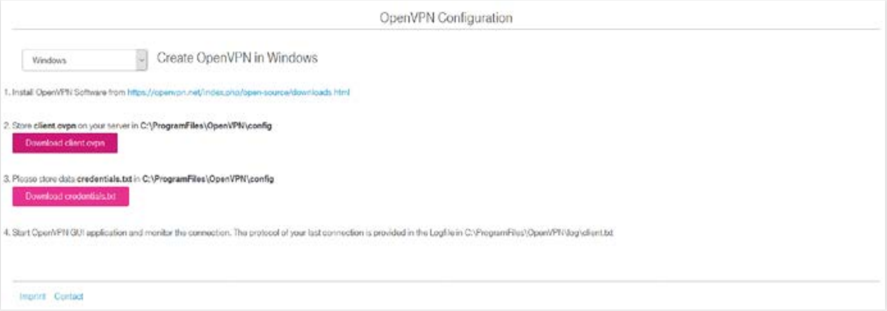
1. Configuring your OpenVPN

To configure your OpenVPN, login to the Business Smart Connect Portal. Under "Settings" of the main navigation, select the sub-menu item "OpenVPN". The configuration page of your OpenVPN will then open.

Here you can download the OpenVPN software following the provided URL to openvpn.net as well as the OpenVPN configuration file and your personal credentials file.

ACTION PAGE FOR OPENVPN CONFIGURATION

First select the operating system of your server. Different versions are available for Windows and Linux/MacOS.



OpenVPN Configuration

Windows — Create OpenVPN in Windows

1. Install OpenVPN Software from https://openvpn.net/index.php/open-source/downloads.html

2. Store **client.ovpn** on your server in **C:\ProgramFiles\OpenVPN\config**

3. Please store data **credentials.txt** in **C:\ProgramFiles\OpenVPN\config**

4. Start OpenVPN GUI application and monitor the connection. The protocol of your last connection is provided in the Logfile in C:\ProgramFiles\OpenVPN\log\client.txt

Figure 2: Configuring OpenVPN

A) OpenVPN Software Installation

The OpenVPN client must be installed on the customer application (application server) to which the data of the device will be transferred. You have the possibility to download the OpenVPN software. For the selected operating system, a link or note appears to download the OpenVPN software. For Windows following link can be followed to install OpenVPN software: https://openvpn.net/index.php/open-source/downloads.html

B) Download client configuration file

To configure the OpenVPN client for Windows, you can download a configuration file and save it in the config-folder. By clicking on the "Download client ovpn" you can download the file for Windows. For Linux / MacOS click on "Download client.conf".

C) Download credentials

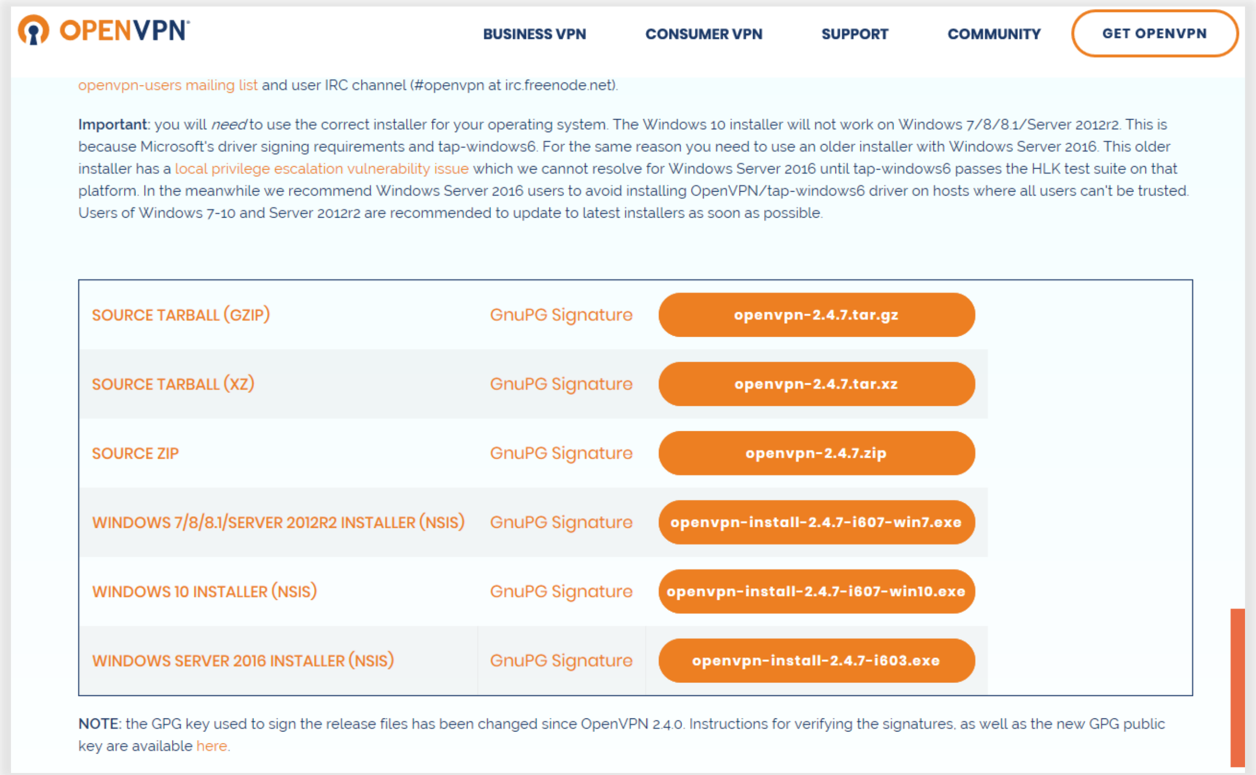
In addition to the client, you will also need your user credentials to successfully create an OpenVPN session. You can download your credentials by clicking on "Download credentials.txt". Your user credential file is then downloaded, and you can then store it in your folder.

The next two sections will guide you through the steps for successfully installing OpenVPN in Windows and Linux/MacOS.

1.1 Installing OpenVPN in Windows

OpenVPN configuration takes place in three steps:

Step 1:
As a first step, please install the OpenVPN software. You can find it in the OpenVPN configuration area within your customer account. (see chapter 1)



openvpn-users mailing list and user IRC channel (#openvpn at irc.freenode.net).

Important: you will *need* to use the correct installer for your operating system. The Windows 10 installer will not work on Windows 7/8/8.1/Server 2012r2. This is because Microsoft's driver signing requirements and tap-windows6. For the same reason you need to use an older installer with Windows Server 2016. This older installer has a local privilege escalation vulnerability issue which we cannot resolve for Windows Server 2016 until tap-windows6 passes the HLK test suite on that platform. In the meanwhile we recommend Windows Server 2016 users to avoid installing OpenVPN/tap-windows6 driver on hosts where all users can't be trusted. Users of Windows 7-10 and Server 2012r2 are recommended to update to latest installers as soon as possible.

SOURCE TARBALL (GZIP)	GnuPG Signature	openvpn-2.4.7.tar.gz
SOURCE TARBALL (XZ)	GnuPG Signature	openvpn-2.4.7.tar.xz
SOURCE ZIP	GnuPG Signature	openvpn-2.4.7.zip
WINDOWS 7/8/8.1/SERVER 2012R2 INSTALLER (NSIS)	GnuPG Signature	openvpn-install-2.4.7-I607-win7.exe
WINDOWS 10 INSTALLER (NSIS)	GnuPG Signature	openvpn-install-2.4.7-I607-win10.exe
WINDOWS SERVER 2016 INSTALLER (NSIS)	GnuPG Signature	openvpn-install-2.4.7-I603.exe

NOTE: the GPG key used to sign the release files has been changed since OpenVPN 2.4.0. Instructions for verifying the signatures, as well as the new GPG public key are available here.

Figure 3: OpenVPN Software, example of free third-party software

Step 2:
In a second step, download client.ovpn and store it on your server in folder C:\Program Files\OpenVPN\config.

Step 3:
Download the file credentials.txt from “Configuration” section in the customer portal and save it in "C:\Program Files\OpenVPN\config"

Step 4:
Start your OpenVPN Application and monitor your connection.

For a log on your last connection open the logfile in C:\Program Files\OpenVPN\log\client.txt
(may also be C:\Users\<IHRPROFIL>\OpenVPN\log\client.txt)

1.2 Installing OpenVPN in Linux/MacOS

Install OpenVPN with `sudo apt-get install openvpn`; for “Ubuntu” or using “Homebrew” for MacOS with `brew install openvpn`

Download „client.conf“ from customer portal (Configuration -> OpenVPN Configuration -> Linux/macOS -> Download client.conf).

* Optional: Add line in client.conf just for debugging purpose. *

```
        log /var/log/openvpn_Telekom.log
```

Copy <client.conf> to /etc/openvpn.

Download „credentials.txt“ from customer portal (Configuration -> OpenVPN Configuration -> Linux/macOS -> 3. Save the following file credentials.txt ...).

Copy <credentials.txt> also in /etc/openvpn.

Start the OpenVPN connection with new configuration.

```
sudo service openvpn restart
```

Note: Homewbrew is not standard provided by MacOS. You can also use alternative software with GUI (e.g. Tunnelblick)

Note: The OpenVPN client version provided from the software repository of your Linux distribution might not be the latest version that is available on openvpn.net. During installation of the OpenVPN client there might be additional software automatically installed to fulfill dependencies. For troubleshooting help you may want to visit the openvpn.net Wiki or support forum.

2. Common Questions

This chapter covers the most frequently asked questions and problems related to the use of OpenVPN.

2.1 How to locate the OpenVPN log files

OpenVPN creates log files that contains the connection details of the tunnel (e.g. establishing the tunnel). Analyzing log files helps you with trouble shooting.

To view the log files for the OpenVPN Connect Client for Windows, you should go to the following location:

```
C:\Program Files (x86)\OpenVPN Technologies\OpenVPN
Client\etc\log\openvpn_(unique_name).log
```

Log files in Linux distributions can be viewed with the command cd/var/log. OpenVPN log files can be found in the following location:

```
/var/log/syslog
```

Note: if you followed the steps in chapter 1.2, you have the log file under `/var/log/openvpn_Telekom.log`

The OpenVPN Connect Client for Mac:

```
/Library/Application Support/OpenVPN/log/openvpn_(unique_name).log
```

Macintosh may not show you this folder in finder as it only shows you certain things and hides others. So, to get to the "/Library" folder, open Finder and in the menu at the top choose Go, followed by Go to folder and then enter the path /Library to get into that directory. You can then go to the correct folder and look up the log file. Please also note that the OpenVPN Connect Client for Macintosh will have permissions set on the log file so that you cannot normally open it.

To bypass this, right click the log file and choose the "Get info" option in the menu. Then at the bottom, under "Sharing & Permissions", you will be able to use the yellow padlock icon to unlock the settings and to give everyone read access. Then you will be able to open the log file with a right click and selecting "Open with" and then choosing something like Text editor to view the contents of the log file.

2.2 Why to update the routing table for OpenVPN regularly

After placing the first order, you will also be assigned one full/22 IP subnet mask. This IP-range supports a total of 1022 SIM cards. Once your number of SIM cards exceeds this amount, a new subnet mask will be added by the Business Smart Connect Platform.

The OpenVPN client pulls the information for all required routes from the BSC-platform during the initialization of the connection. To ensure that all new Subnets are included into the local routing tables, we recommend you restart the OpenVPN client when you deploy your newly ordered SIM cards.

2.3 How to solve a potential route subnet conflict

The OpenVPN log entry „potential route subnet conflict" means that your SIM cards have IP addresses that are also in your local network. There are two ways to resolve this conflict.

Firstly, you can include a "redirect gateway local" option in the OpenVPN configuration file. Secondly, you can change the addresses of your local LAN. You do this by changing your router's configuration. Depending on your router, you must either specify the first three numbers of the LAN (e.g. 157.168.77) or specify the address of the router itself (e.g. 157.168.77.1).

2.4 My OpenVPN connection dropped suddenly. What could be the reason?

The most common reason is that your credentials are in use for another connection. Our OpenVPN client supports one active connection to the OpenVPN server.

You can help diagnose the problem by checking your log files. A continuous reconnection and dropping of the connection indicate this problem. Also, please check if another user is also trying to establish an OpenVPN connection with your credentials.

2.5 How to solve a HTTPS time-out of your OpenVPN connection

HTTPs connections to your application Server may time out when connecting through OpenVPN. Changing the MTU size for the network interface may solve the issue. Changing the MTU size to 1300 should help. You can add the following line in file "client.conf" before the line `proto udp`:

```
tun-mtu 1300
```

2.6 How to prevent authentication issues

If you use certain OpenVPN versions, you might run into failed authentication attempts. The reason for this is that certain OpenVPN versions do not support a password length exceeding 128 characters.

For example, it is known in the "OpenVPN 2.4.6 arm-openwrt-linux-gnu" on OpenWRT with PKCS#11 disabled. Recompiled OpenVPN after patching the support for longer passwords solves the problem. The Bug is known in the OpenVPN community and can be found at: https://community.openvpn.net/openvpn/ticket/712

3. Example set-ups OpenVPN with IoT-Devices

This section describes the communication of an IoT device with a Linux-based server. For the example we used and Raspberry 3 Model B (Debian Buster) connected to a Quectel BG96 EVK as IoT device and Laptop running Ubuntu 18.04 as server.

3.1 Ubuntu server configuration

The Ubuntu server hosts the OpenVPN client. Details on how the installation of the client is done can be obtained from Section 1.2. To check if the connection has been setup properly, the command

```
ip -brief address
```

can be used, which will yield an output like this:

```
lo                UNKNOWN       127.0.0.1/8 ::1/128
wlp2s0            UP            10.51.13.126/20 fe80::bdd0:364b:2418:ca95/64
docker0           DOWN          172.17.0.1/16
tun0              UNKNOWN       10.64.160.33 peer 10.64.160.34/32
fe80::3bd2:ab34:df15:256c/64
enx00051be1fabf   DOWN
```

The first column lists all available network interfaces and the third column their assigned IP addresses. The network interface for the OpenVPN connection is

`tun0` with the IP address `10.64.160.33`

This IP address can be used to send data to the Ubuntu server.

3.2 Raspberry Pi configuration

The Quectel EVK is connect with USB-cable to the Raspberry Pi and switched on. To access it, a serial terminal is required. Putty for instance, can be installed via the package manager:

```
sudo apt-get install putty
```

a connection can be established by using the connection parameters:

```
Baudrate: 115200
Databits: 8
Parity: N
Stopbits: 1
```

Connect the serial terminal to the BG96 and check if the response to the command “AT” is “OK”. After this use the following sequence to send a PING to the Ubuntu server:

```
at+cfun=0
OK
at+cgdcont=1,"IP","iot.telekom.net"
OK
at+cfun=1
OK
at+cops=1,2,"26201"
OK
at+qiact=1
OK
at+qping=1,"IP ADDRESS OF UBUNTU SERVER"
OK
+QPING: 0,"10.64.160.33",32,386,255
+QPING: 0,"10.64.160.33",32,216,255
+QPING: 0,"10.64.160.33",32,202,255
+QPING: 0,"10.64.160.33",32,217,255
+QPING: 0,4,4,0,202,386,255
```