SP-VPN 1700
Quick guide

Scope of delivery

1. SP-VPN 1700 Server

2 Powera adapter

3 Network cabel
4. Quick guide

SP-VPN 1700 Server

SP-VPN 1700/2FA is a VPN server with two-level authentication.
SP-VPN 1700 is a VPN server with a simple authentication.

They are designed for small to medium networks and are very suitable for connecting home office workstations.

They support up to 100 VPN users.

Here you will get the most important information to get your SP-VPN 1700 Server up and running.

The SP-VPN 1700 servers have a user interface that you can open in an Internet browser.

From this user interface, you can download a PDF manual with descriptions of all the features and instructions of the SP-VPN 1700 server.

Safety

- Operate the SP-VPN 1700 server in a dry and dust-free location and provide adequate ventilation.
- The SP-VPN 1700 server is intended for indoor use. Do not allow liquids to enter the interior.
- Only remove the Schuko adapter from the socket using electrically insulated tools.
- Do not open the SP-VPN 1700 server. Opening and/or improper repairs may put you in danger.
- Disconnect the SP-VPN 1700 server from power before cleaning. Use a dry cloth for cleaning.

Connect SP-VPN 1700 server to network and start it up

Plug the network cable into the back of the SP-VPN 1700 server **(1)**. Connect the SP-VPN 1700 server to your network using the other end of the network cable.

Connect the **power supply** to the SP-VPN 1700 server **(2)** and plug it into the power outlet.

The SP-VPN 1700 server starts.

Connect computer with SP-VPN 1700 server

Immediately after starting the SP-VPN server, you can temporarily **connect via WLAN for 30 minutes** for configuration. To do this, proceed as follows:

In Windows 10:

1. In the Windows taskbar, click Start and then Settings.
2. In the Settings menu, click Network and Internet and then WLAN.
3. In the list of available connections, click on the name **CFG-SPVPN** (SSID) and then on "Connect".
4. Enter the WLAN network key **#secure4vpn** in the "Enter network security key" input field and click "Next".
5. Now the WLAN connection is established.

Under MacOS:

1. Click on the WLAN icon in the Finder bar at the top of the screen.
2. Click on the name **CFG-SPVPN** (SSID) in the context menu.
3. Enter the WLAN network key #**secure4vpn** in the "Password" input field and click "Connect".
4. Now the WLAN connection is established and its field strength is indicated by the WLAN icon.

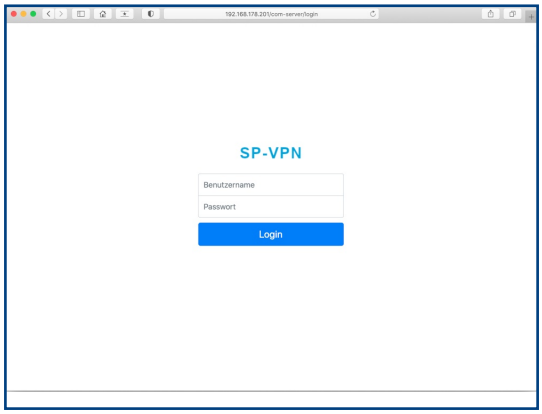
ATTENTION: The WLAN connection CFG-SPVPN is automatically switched off 30 minutes after the start of the SP-VPN server for security reasons.

Configure SP-VPN 1700 Server

To access the web application, you need a current Internet browser (Firefox, Chrome).

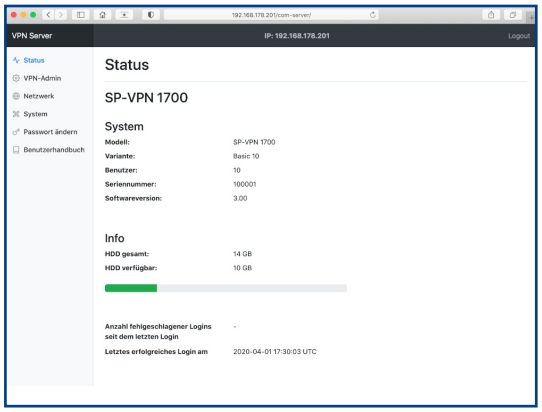
Enter the address **http://10.30.0.1** in the address bar of the browser. (Make sure that the WLAN connection with CFG-SPVPN is active)..
Then press the Enter key. Accept the security warning if necessary.

The login window appears in the browser window.



Access to the web application is protected.
The user name is "**admin**" and the initial password in the delivery state is "**admin**".
After successful authentication, the status page of the SP-VPN 1700 server appears.

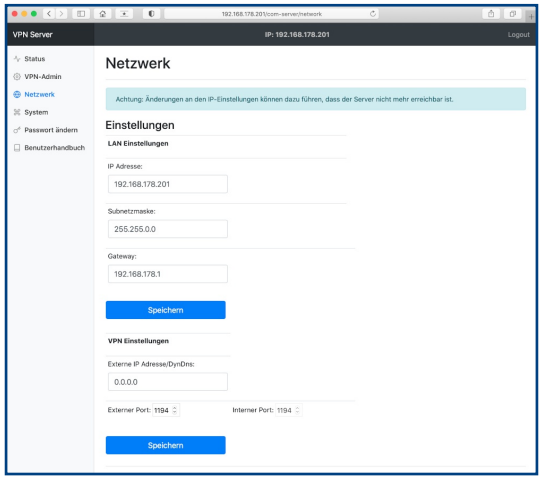
ATTENTION: We recommend changing the initial password to prevent unauthorized access. Instructions for changing the password are described in the manual.



In the section "Network" you can adjust your IP address, subnet mask and gateway in the **LAN settings**.

At **VPN settings** you enter your **external IP address** or your **DynDns address**, as well as an **external port**. Both must be released later at the router (e.g. at the Fritzbox) by **port forwarding**.
Save the VPN settings.

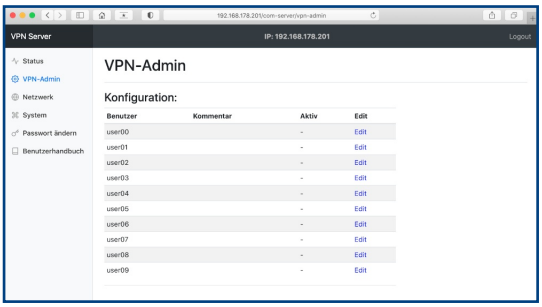
Now the WLAN connection CFG-SPVPN can be terminated. The SP-VPN server can now be reached at the address specified in LAN settings.



VPN user configuration

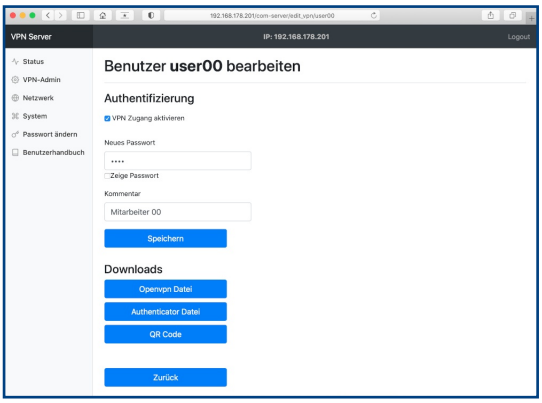
1. VPN Admin Settings

Log in to the SP-VPN 1700 server. In the section "**VPN-Admin**" you will find the available VPN users. Click on "**Edit**" in the line of the user "user00".



On the "**Edit user00**" page, activate "**Activate VPN access**". In the "**New password**" field you can enter a new password and in the "Comment" field you can enter a comment.

"**Save**" saves the settings and activates the VPN access for user user00.



2. download the configuration files

Save the files "**Openvpn file**", "Authenticator file "*) and "QR Code "*) by clicking on them. The "Openvpn file" is needed for the OpenVPN client or tunnel view, "**Authenticator file**" and "**QR Code**" for the two-step authenticator.

*) Only SP-VPN Server/2FA

Clicking "**Back**" will take you back to the VPN Admin page where you can continue configuring VPN users.

VPN Client Software Installations

1. Installation of the VPN client

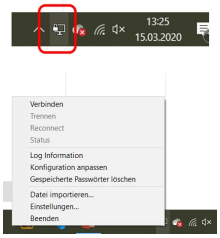
The following open source client programs are recommended for establishing the VPN connection.
(Administrator rights required)

On Windows 10:

OPENVPN

Download the **OpenVPN** software. (https://openvpn.net/index.php/open-source/downloads.html)
To start the installation, double-click the installation file and follow the requirements.

Import OpenVPN file:
Start OpenVPN on your PC and import (by right-clicking on the icon) the file downloaded under "**Openvpn file**" (user00.ovpn).



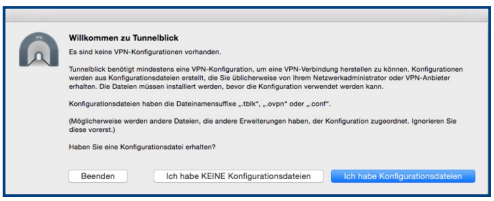
Proceed accordingly for further VPN users.

On macOS:

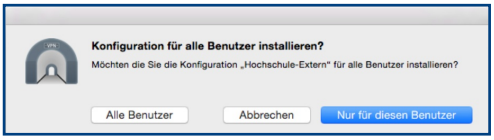
Tunnelblick free software for OpenVPN on macOS

Download the **Tunnelblick** software (https://tunnelblick.net/downloads.html).
To start the installation, double-click the installation file and follow the requirements.

Import of the OpenVPN file:
During the installation, in response to the question "Did you receive a configuration file?", select "**I have configuratioins files**" and then confirm with Ok.



Double-click the file downloaded under "**Openvpn file**" (user00.ovpn) and select "**Only for this user**" in the following dialog.



Proceed accordingly for other VPN users.

2. Installation of an OATH Authenticator (two-step authentication) (Not for SP-VPN 1700 Light Server).

Using Google Authenticator APP as an example.

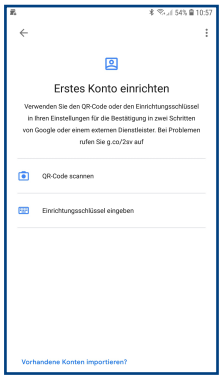
Google Authenticator

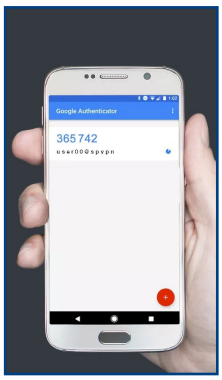
For two-step authentication, we recommend using a mobile device. Google Authentificator is available for free for Android in the Google Play Store and for Apple in the App Store.

Install the Google Authenticator on your mobile device.

Launch the app.

Select "**Scan QR Code**" and scan the QR code in the file downloaded under "QR Code" (e.g. "user00.qrcode.png").





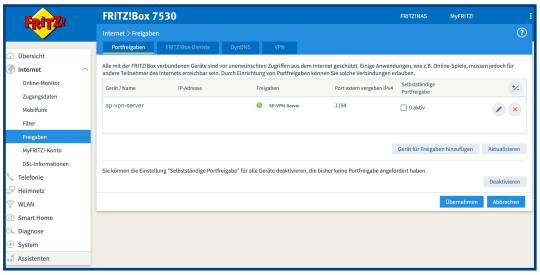
Alternatively, you can **enter a setup key**. As a key, take the first line from the file downloaded under "**Authenticator File**" (e.g. "user00.google_authenticator.txt").

With "**Add account**" the account for the user is connected. Proceed accordingly for additional VPN users.

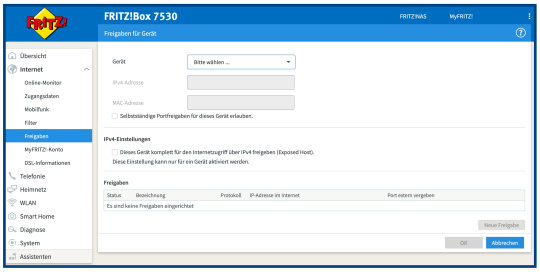
Enable port forwarding

Using the example of a FRITZ!Box 7350.

Log in to your Internet router and go to "**Shares**" in the "**Internet**" section.
Go to "**Add device for sharing**".



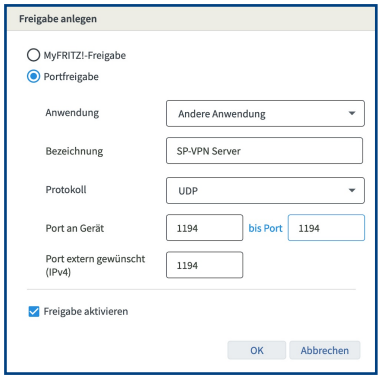
Select the SP-VPN server under "**Device**" or enter the IP address of the SP-VPN server.
Go to "**New share**"



In the "**Create share**" dialog, select "**Port share**" and specify "**Other application**" for Application.

Assign a name and select the protocol "**UDP**".
For "**Port to device**", select **1194 to 1194**. For "**Port desired externally**", enter the external port specified in SP-VPN Server.

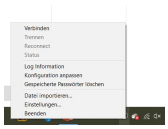
Activate "**Enable sharing**" and close the dialog with "**OK**". Confirm the changes in "**Release for device**" with "**OK**".

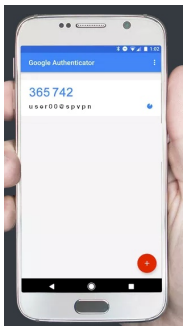


Port forwarding is now enabled.

Establish VPN connection

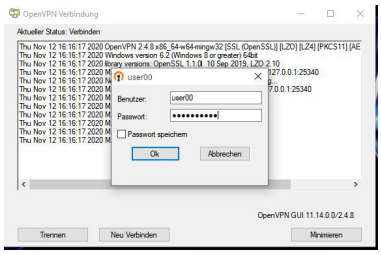
The VPN client and an authenticator (SP-VPN 1700/2FA only) are required to establish the VPN connection.





Under Windows 10:
Start OpenVPN and go (by right-clicking on the icon) to connect.
Enter the username (e.g. "user00"), as password enter the password assigned under "VPN User Configuration" .

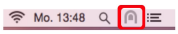
(SP-VPN 1700/2FA only)
Start the Microsoft Authentificator on your smartphone and append the **6 digit number sequence** for the VPN user (e.g. "user00") to the password (e.g. "secret_passwort365742").

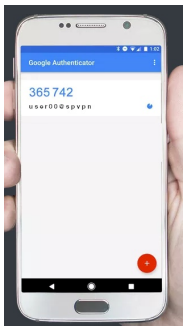


With "**Ok**" the connection is established.
Proceed accordingly for further VPN users.

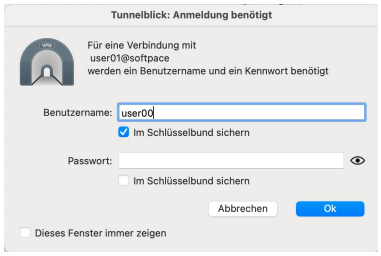
Info: The OATP password is valid for 30 seconds.

On macOS:
Click on the tunnel vision icon in the menu and go to "user00" connect.
Enter the user name (e.g. "user00"), as password enter the password assigned under "VPN User Configuration" .





(SP-VPN 1700/2FA only)
Start the Microsoft Authenticator on your smartphone and append the **6 digit number sequence** for the VPN user (e.g. "user00") to the password (e.g. "secret_passwort365742").



With "**Ok**" the connection is established.
Proceed accordingly for further VPN users.

Info: The OATP password is valid for 30 seconds.

Disposal

Der SP-VPN 1700 Server darf gemäß europäischen Vorgaben nicht über den Hausmüll entsorgt werden. Bringen Sie sie nach der Verwendung zu den Sammelstellen der Kommune.

Contact

www.softpace.net

Softpace GmbH
Parkstrasse 27 / 82008 Unterhaching

Legal

Legal information and license terms can be found in the user interface under Manual.

CE Declaration of Conformity

CE Hereby Softpace declares that the device is in compliance with the essential requirements and other relevant provisions of Directives 2014/53/EU, 2009/125/EC and 2011/65/EU.