



OPENVPN SERVER AUF DEM DIGITAL OCEAN SERVER STAND 06/2021

DOKUMENTATION VON DANIEL KELLER



INHALTSVERZEICHNIS

1. [Digital Ocean](#)
 - 1.1. [Server mieten](#)
 - 1.2. [OpenVPN OS Instsallieren](#)
 - 1.2.1. [SSH Verbindung](#)
2. [OpenVPN](#)
 - 2.1. [Admin GUI](#)
 - 2.1.1. [Neue User](#)
 - 2.2. [Host Anteil \(Linux, Windows 10\)](#)
 - 2.2.1. [Windows Installation](#)
 - 2.2.2. [Linux Installation](#)
 - 2.2.3. [Mac Installation](#)
 - 2.3. [Kommunikation im VPN](#)
3. [Fazit](#)

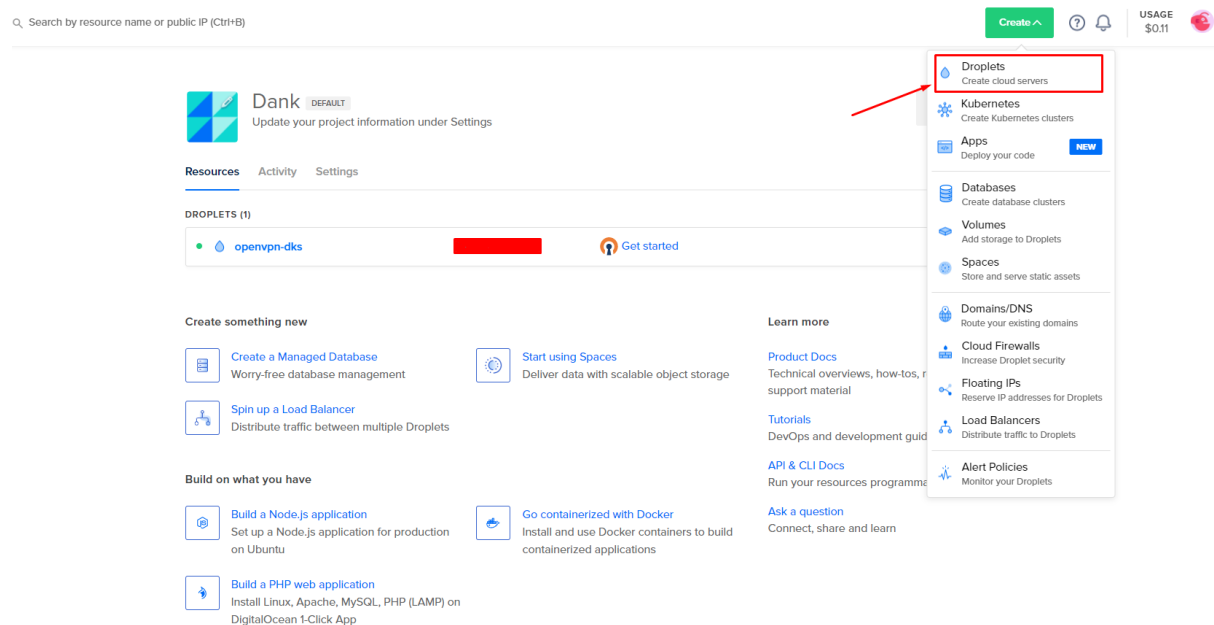
DIGITAL OCEAN

1.1 SERVER MIETEN

Als erstes registrieren wir uns bei Digital Ocean - <https://www.digitalocean.com/> . Dann wir müssen unsere Credit Karte oder PayPal verknüpfen, keine sorgen, es gibt viele Leute die DO verwenden, es ist eine gute Seite und man kann jederzeit sein Server löschen um dann nichts zahlen.

1.2 OPENVPN OS INSTALLIEREN

Dann wir müssen ein Droplet erstellen:



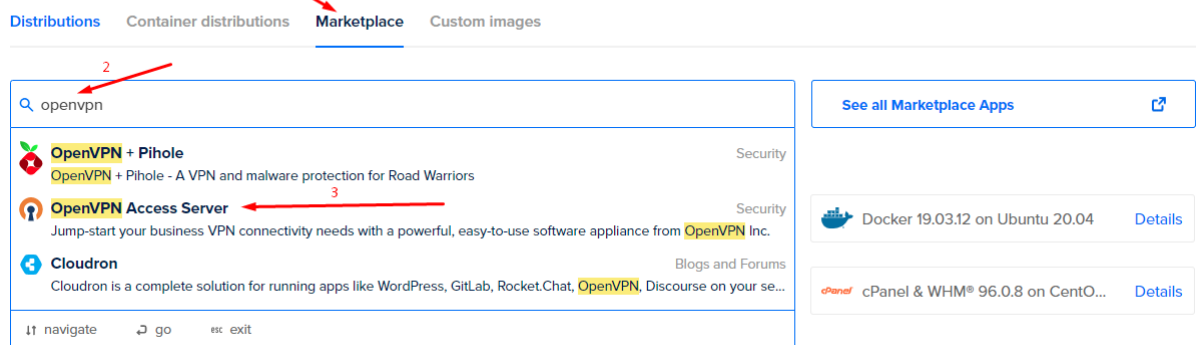
Oder wenn Sie erst bei der Seite sind und haben sich frisch angemeldet, wahrscheinlich sie sehen vereinfachte Menü mit verschiedenen Arten von Server Spezifik, da müssen wir „Virutal Machine“ auswählen.

Bei der Droplet Konfiguration es gibt paar Sachen die wir ändern müssen:

- 1) Als Distribution wir können einfach Ubuntu OpenVPN Access Server von Marketplace auswählen.

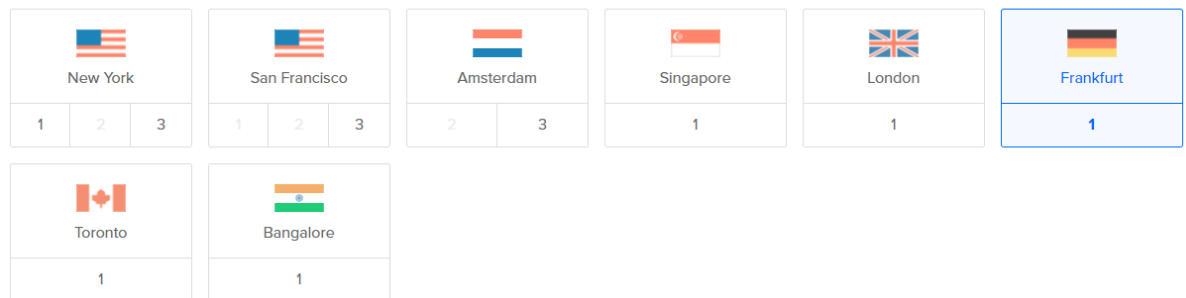
Create Droplets

Choose an image ?



- 2) Dann wir müssen unseren VPC Region auswählen. Selbstverständlich was in der Nähe von uns ist.

Choose a datacenter region



- 3) Dann wir können unseren SSH Key einsetzen, um sichere Zugriff zu haben. Wenn Sie nur üben wollen und wissen nicht was SSH ist, ist nicht prinzipiell, wählen sie dann Password aus und geben sie dort die Password ein. [SSH für Anfänger](#)

WICHTIG!!! In meinem Fall es gab SSH Problemen und ich müsste durch Web-Console von Droplet paar Sachen ändern um die SSH Verbindung zu ermöglichen, deswegen ich würde empfehlen, sowie auch erfahrene Leute, sich mit einem root Passwort zu besorgen.

Authentication ?

The screenshot shows the 'Authentication' section of the DigitalOcean interface. There are two main options: 'SSH keys' and 'Password'. The 'SSH keys' option is selected, indicated by a blue radio button. Below it, there is a section titled 'Choose your SSH keys' with three checkboxes: 'Select all', 'pCH_vpn_key' (which is checked), and 'vpnSSHkey'. A 'New SSH Key' button is located below the checkboxes. The 'Password' option is also visible, with a description: 'Create a root password to access Droplet (less secure)'.

- 4) Leistung für 5 Euro reicht für uns, wenn Sie aber den Server für andere Sachen noch benutzen wollen oder Sie möchten einfach eine starke Maschine, wählen Sie dann die beliebige Option aus.

CPU options: ☒ Regular Intel with SSD ☐ Premium Intel with NVMe SSD **NEW** ☐ Premium AMD with NVMe SSD **NEW**

\$5/mo \$0.007/hour	\$10/mo \$0.015/hour	\$15/mo \$0.022/hour	\$20/mo \$0.030/hour	\$40/mo \$0.060/hour	\$80/mo \$0.119/hour
1 GB / 1 CPU 25 GB SSD Disk 1000 GB transfer	2 GB / 1 CPU 50 GB SSD Disk 2 TB transfer	2 GB / 2 CPUs 60 GB SSD Disk 3 TB transfer	4 GB / 2 CPUs 80 GB SSD Disk 4 TB transfer	8 GB / 4 CPUs 160 GB SSD Disk 5 TB transfer	16 GB / 8 CPUs 320 GB SSD Disk 6 TB transfer

- 5) Als letztes wir umbenennen Hostname von unserem Server.

Finalize and create

How many Droplets?

Deploy multiple Droplets with the same [configuration](#).

— 1 Droplet +

Choose a hostname

Give your Droplets an identifying name you will remember them by. Your Droplet name can only contain alphanumeric characters, dashes, and periods.

openvpn-vpnServer

- 6) Dann, wir klicken auf Create Droplet. Es dauert paar Sekunden bis Maschine erstellt wird. Wenn unsere Maschine fertig ist, es wird angezeigt und sogar mit einem pop up angemeldet.

Create Droplet

- 7) Jetzt kommt die OpenVPN Installation Prozess, das machen wir im Terminal und in unsere Maschine.
- Es gibt verschiedene Wege wie man sich mit seiner Maschine verbinden kann.
- Web-Console.** Mit Web-Console wir können unsere Maschine durch Digital Ocean Seite zugreifen.

The screenshot shows the OpenStack dashboard with two droplets listed at the top:

- openvpn-vpnServer**: IP address 138.197.184.4, with a "Get started" button.
- openvpn-dks**: IP address is redacted, with a "Get started" button.

Below the droplet list, there are sections for "Create something new" (with links for Managed Database, Spaces, and Load Balancer) and "Learn more" (with links for Product Docs, Tutorials, and API & CLI Docs).

A red arrow points to the "Access console" button in the dropdown menu for the "openvpn-dks" droplet. Other options in the menu include "Add a domain", "Resize droplet", "View usage", "Enable backups", "Add tags", "Move to...", and "Destroy".

- b. **Putty**. Mit Putty wir können mit unserer Maschine durch SSH verbinden.

The screenshot shows the PuTTY Configuration dialog box. The "Session" category is selected in the left sidebar. The "Host Name (or IP address)" field is set to "ip_von_droplet" and the "Port" is "22". The "Connection type" is set to "SSH". The "Saved Sessions" list includes "Default Settings", "Fedora HV", "RBPI HomeNAS", "Ubuntu HV", "VPN ST", "WH / SSH / VPN_Serv", and "kali_vm". The "Close window on exit" option is set to "Only on clean exit".

- 8) In meinem Fall ich werde durch Web-Console zugreifen und ich erkläre später warum. Wenn wir haben uns im Web-Console angemeldet, erscheint diese Text was sie auf dem Bild sehen. **Da müssen wir „yes“ eingeneben, ansonsten bricht die Installation ab.** Dann alle anderen Sachen die erscheinen wir lassen leer und einfach mit „Enter“ durchklicken, weil alles für uns schon passend eingesetzt ist.

```
support questions or issues specifically related to the OpenVPN Access
Server product. To file a ticket, go to our website at http://openvpn.net
/
and sign in using the account that was registered and used to purchase th
e
license key(s). You can then access the support ticket system through our
website and submit a support ticket. Tickets filed in the ticketing syste
m
are answered on a best-effort basis. OpenVPN Inc. staff
reserve the right to limit responses to users of our demo / expired
licenses, as well as requests that substantively deviate from the OpenVPN
Access Server product line. Tickets related to the open source version of
OpenVPN will not be handled here.
11. Purchasing a license key does not entitle you to any special rights or
privileges, except the ones explicitly outlined in this user agreement.
Unless otherwise arranged prior to your purchase with OpenVPN,
Inc., software maintenance costs and terms are subject to change after yo
ur
initial purchase without notice. In case of price decreases or special
promotions, OpenVPN Inc. will not retrospectively apply
credits or price adjustments toward any licenses that have already been
issued. Furthermore, no discounts will be given for license maintenance
renewals unless this is specified in your contract with OpenVPN Inc.

Please enter 'yes' to indicate your agreement [no]: yes_
```

- 9) Jetzt führen wir paar Standart Befehle für Linux, die uns mit Updates besorgen:

```
apt-get update
apt-get upgrade
```

1.2.1 SSH VERBINDUNG

- 3) Und jetzt um die SSH Verbindung zu ermöglichen wir müssen eine Zeile im SSH Config ändern. Dafür geben wir – `sudo nano /etc/ssh/sshd_config`

```
root@openvpn-vpnServer:~# sudo nano /etc/ssh/sshd_config
```

Dort müssen wir den Port finden und auf irgendeine beliebige ändern. Was tcp und udp hat.

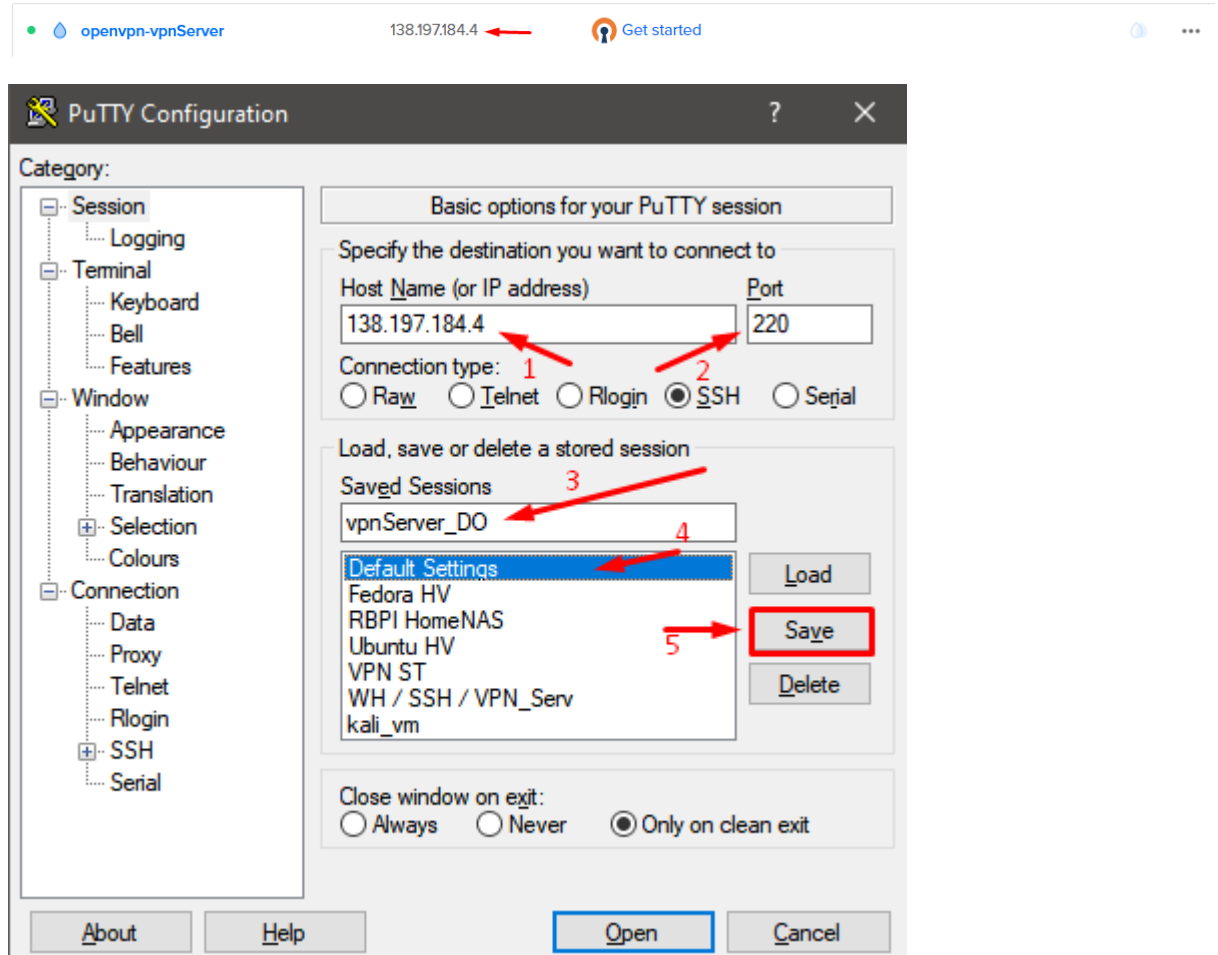
[Liste von Ports](#)

```
#      $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $
#
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
#
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
#
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.
Port 220
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
[ Read 122 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Um das abzuspeichern wir drücken `Ctrl + S` und um rauszugehen `Ctrl + X`. Jetzt starten wir SSH Service neue mit zwei Befehle `service ssh restart` und `service sshd restart` und können dann mit VM durch Putty verbinden.

```
root@openvpn-vpnServer:~# service ssh restart
root@openvpn-vpnServer:~# service sshd restart
root@openvpn-vpnServer:~#
```


- 4) Jetzt können wir mit VM durch Putty verbinden. Dafür geben wir in putty unsere public IPv4 Adresse(1) von dem Droplet ein, **nicht private**. Und früher gewählter Port(2). Dann wir geben den Namen für unsere Verbindung(3), wählen Default Settings(4) aus und Klicken auf Save(5) um das dann als Profil zu haben, damit wir nicht jeder mal die Daten neue eingeben sollten.



Dann haben wir unsere VM geöffnet und geben unsere Anmeldedaten ein.
Ab jetzt wir haben eine ständige und sichere SSH Verbindung zur VM, um dann später sich mit ufw, iptables, fail2ban oder andere Sicherheits Features einfach und bequem zu besorgen.

2 OPENVPN

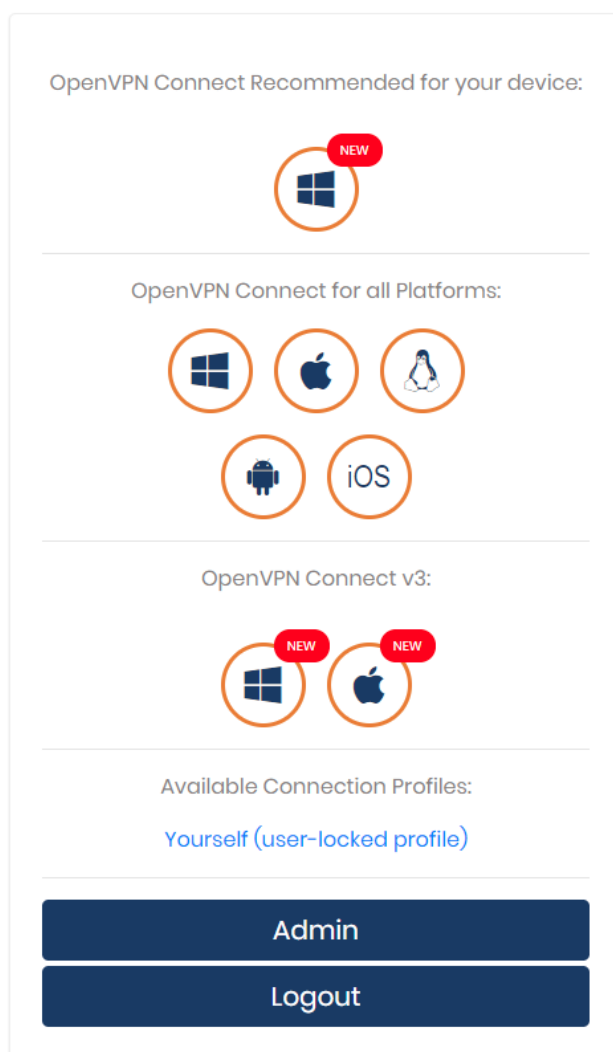
2.1 ADMIN GUI

Als erstes wir müssen Password für unsere Admin user einsetzen. Damit geben wir auf unserem Server so ein Befehl – `passwd openvpn` . Damit ändern wir password für openvpn user.

Um Admin Panel zuzugreifen, wir öffnen unseren Web Browser und geben dort https://public_ip_address_von_droplet `https://138.197.184.4` und klicken auf Enter.

Dann wir gehen durch ein Sicherheitsmeldung und sehen unsere Panel, da loggen wir als **openvpn** user.

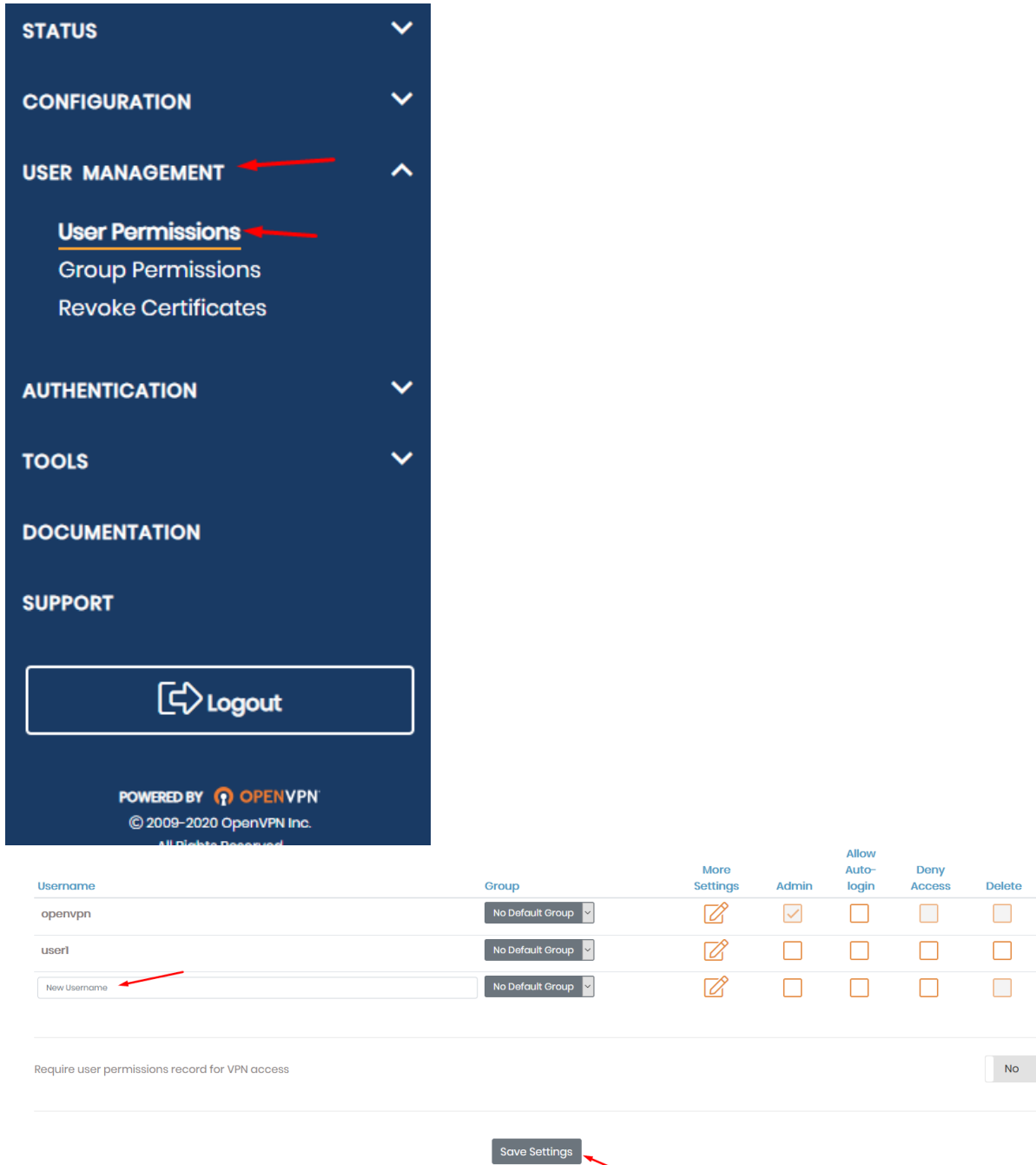
In diesem Panel wir können OpenVPN Software für Windows oder Mac herunterladen. Wenn wir weiter in Admin panel gehen wollen, klicken wir auf Admin und loggen uns mit dem openvpn user nochmal an.



2.2 HOST ANTEIL

2.1.1 NEUE USER EINFÜGEN UND NEUE PROFIL DATEI

Um den neuen User zu erstellen gehen wir in Admin Panel in User Management -> User Permissions und in Box «New Username» geben wir die Name unseres Users. Dann ganz unten, wie klicken auf «Save Settings» um das abzuspeichern. Jetzt klicken wir auf «Refresh» und bei unserem neuen User gehen ins „More Settings“ und dort kann man die Password eingeben. Jetzt wir haben anderen User erstellt



The screenshot shows the OpenVPN Admin Panel interface. On the left is a dark blue sidebar with the following menu items: STATUS, CONFIGURATION, USER MANAGEMENT (highlighted with a red arrow), User Permissions (highlighted with a red arrow), Group Permissions, Revoke Certificates, AUTHENTICATION, TOOLS, DOCUMENTATION, and SUPPORT. At the bottom of the sidebar is a 'Logout' button and a footer that reads 'POWERED BY OPENVPN © 2009-2020 OpenVPN Inc. All Rights Reserved'.

The main content area displays a table of users with the following columns: Username, Group, More Settings, Admin, Allow Auto-login, Deny Access, and Delete. The table contains three rows: 'openvpn' (Admin checked), 'user1', and a new user entry with 'New Username' in the input field (highlighted with a red arrow). Below the table is a checkbox for 'Require user permissions record for VPN access' (set to 'No') and a 'Save Settings' button at the bottom (highlighted with a red arrow).

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user1	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="New Username"/>	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Require user permissions record for VPN access


Um die cleint.ovpn Profil für den User zu bekommen wir müssen als dieser User anmelden. Genau wie wir damals uns mit dem openvpn angemeldet haben. **WICHTIG!!!** Nicht im Admin URL, im normalen URL .

Jetzt haben Sie die Profil Datei für den neuen User.






2.2.1 OPENVPN WINDOWS INSTALLATION

Damit wir OpenVPN benutzen könnten klicken wir erst auf Windows Logo und laden Version für Windows herunter. Danach installieren wir Soft wie auch immer, und dann wir öffnen OpenVPN und sehen GUI. Dort gibt es schon vorhandene Zertifikat um mit unserem VPN zu verbinden. Wir schalten den Schalter ein und loggen als openvpn user ein. Jetzt haben wir die Verbindung mit unserem VPN Server!



OpenVPN Connect Recommended for your device:



OpenVPN Connect for all Platforms:

OpenVPN Connect v3:





Available Connection Profiles:


[Yourself \(user-locked profile\)](#)

Admin

Logout

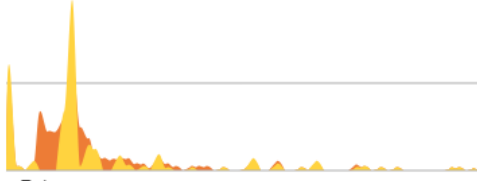
**OpenVPN Profile**
openvpn@138.197.184.4 [client (1)] 

CONNECTED


**OpenVPN Profile**
openvpn@138.197.184.4 [client (1)]


CONNECTION STATS

4.1KB/s




0B/s

BYTES IN
14 B/S 

 **BYTES OUT**
5 B/S

DURATION
00:01:01

PACKET RECEIVED
0 sec ago

YOU
openvpn 

2.2.2 OPENVPN LINUX INSTALLATION

Als erstes auf unserem Linux Host, wir müssen paar Vorbereitungs Befehle eingeben: `sudo apt install apt-transport-https`

Dann wir installieren `openvpn sudo apt-get install openvpn`.

Dann bei der Konfiguration von openvpn nach der Installation, wir gehen einfach durch, weil alles schon richtig steht.

Jetzt müssen wir eine vorbereitete Datei von openvpn Profil editieren. *Wie man Dateien aus Windows in Linux überträgt erfahren sie selbst, aber das Programm dafür ist [WinSCP](#).* Das Profil müssen wir in `/etc/openvpn/` reinkopieren, es wird so gemacht `cp von/wo/client.ovpn nach/wo/`. Und dann editieren wir es mit `nano /das/weg/client.ovpn`.

Jetzt suchen wir Zeile `auth-user-pass` `auth-user-pass` und als Parameter `/etc/openvpn/auth.txt` eingeben und speichern es mit `Ctrl + S` und `Ctrl + X`.

Jetzt müssen wir so eine Datei erstellen, dafür geben wir so ein Befehl ein – `touch /etc/openvpn/auth.txt` und editieren es mit `nano /etc/openvpn/auth.txt`, dort fügen wir die User Namen von Profil was wir erstellt haben und Password dafür, Datei wird so aussehen:



```
user1
password
```

[Read 0 lines]

Dann speichern wir das wieder ab.

Jetzt um sich zu verbinden geben wir ein Befehl `openvpn --config /etc/openvpn/client.ovpn --daemon`. Und wenn sie haben richtige Profil Datei und richtige Anmeldedaten eingegeben, soll es eine Verbindung sein. Man kann das auch im Admin Panel überprüfen, im „Status“ -> „Current Users“.

2.2.3 MAC INSTALLATION

Mac – mac selsbt 😊

<https://openvpn.net/client-connect-vpn-for-mac-os/>

oder

<https://tunnelblick.net/>

VERBINDUNG INNERHALB DES VPNS

Um Geräte Innerhalb des VPNs zu verbinden müssen wir in Admin Panel paar Sachen einschalten.

Im User Management bei Users wen wir im Netz „sichtbar“ und „pingbar“ machen wollen, sollen wir im Acces Control bei „Select adressing method“ „Use Routing“ auswählen und bei „Allow Acces From“ «all other VPN clients» auswählen. So können wir z.B aus dem Büro, Schule oder Uni im Netz von unserer Wohnung zugreifen.

Access Control

Select addressing method:

Allow Access To these Networks:

Allow Access From:

Allow Access From:

☐ Use NAT ☒ Use Routing

☐ all server-side private subnets

☒ all other VPN clients

WICHTIG!!! Vergießen Sie nicht das alles dann abzuspeichern. Ganz unten „Save Settings“ und dann „Update Running Server“

FAZIT

In dieser Dokumentation ich habe euch gezeigt wie man OpenVPN Server auf dem Digital Ocean Droplet einstellen kann. Wie setzt man neuen Users ein, wie ändern man Passwörter. Wie Installiert man OpenVPN auf verschiedene Clients wie Linux oder Windows. Und wie man sich mit Droplet durch SSH Verbinden kann. Es gibt natürlich Sachen die man noch zeigen könnte, wie man configs fürs clients ändern, ufw, fail2ban aber das alles ist ein anderes Thema.

Hoffentlich das hat euch geholfen und das war mehr Interessant als nervig zu machen.