

Wireguard UI Server einrichten

- [Installation des Servers unter Debian](#)
- [Clients einrichten](#)

Installation des Servers unter Debian

Teil 1. Installation im Terminal

Abhängigkeiten installieren.

```
apt update && apt install -y wireguard curl tar iptables resolvconf
```

Hinweis:

Bei Debian 12/13 wird die resolv.conf nicht angelegt. Das heißt nach Installation von resolvconf funktioniert die Namensauflösung nicht. Daher resolv.conf anlegen mit Inhalt des google dns Servers als Beispiel

```
nameserver 8.8.8.8
```

Denn Sonst funktioniert das Update/Installationskript nicht

Falls die ufw Firewall aktiv ist, bei dieser folgenden UDP Port öffnen 51820, wenn nicht überspringen

```
ufw allow 51820/udp
```

!!Sollte der Wireguard Server hinter einem Router stehen das NAT Portforwarding UDP 51820 nicht vergessen einzurichten!!

Nun in der Systemctl Portforwarding aktivieren

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf  
echo "net.ipv6.conf.all.forwarding=1" >> /etc/sysctl.conf
```

```
sysctl -p
```

Nun das Startscript für den Wireguard WEBGUI erstellen.

In dem Systemstart wird das Programm so eingestellt das es die Datenbank zum Wireguard Server in

```
/etc/wireguard/db/ abgelegt
```

```
cat <<EOF > /etc/wireguard/start-wgui.sh
#!/bin/bash

cd /etc/wireguard
./wireguard-ui -bind-address 0.0.0.0:5000
EOF
```

ACHTUNG: Die *-bind-address* **0.0.0.0:5000** sollte aus Sicherheitsgründen, sobald der erste Tunnel steht, gegen die WireGuard Server IP-Adresse **10.252.1.0** ausgetauscht werden!

Nun das Script ausführbar machen.

```
chmod +x /etc/wireguard/start-wgui.sh
```

Nun die Systemdienste anlegen

```
cat <<EOF > /etc/systemd/system/wgui-web.service
[Unit]
Description=WireGuard UI

[Service]
Type=simple
ExecStart=/etc/wireguard/start-wgui.sh

[Install]
WantedBy=multi-user.target
EOF
```

Nun das Install / Update script erstellen, damit können wir immer die aktuellste Version downloaden.

```
cat <<EOF > /etc/wireguard/update.sh
#!/bin/bash

VER=$(curl -sI https://github.com/ngoduykhanh/wireguard-ui/releases/latest | grep "location:" | cut -d "/" -f8 | tr
```

```
-d '\r')

echo "downloading wireguard-ui \${VER}"
curl -sL "https://github.com/ngoduykhanh/wireguard-ui/releases/download/\${VER}/wireguard-ui-\${VER}-linux-
amd64.tar.gz" -o wireguard-ui-\${VER}-linux-amd64.tar.gz

echo -n "extracting "; tar xvf wireguard-ui-\${VER}-linux-amd64.tar.gz

echo "restarting wgui-web.service"
systemctl restart wgui-web.service
EOF
```

Das Script ausführbar machen und starten

```
chmod +x /etc/wireguard/update.sh
cd /etc/wireguard; ./update.sh
```

Es erscheinen folgende fehler in der Ausgabe, aber es wird trotzdem korrekt installiert

```
Ausgabe

/update.sh: Zeile 2: : Kommando nicht gefunden.
./update.sh: Zeile 4: : Kommando nicht gefunden.
downloading wireguard-ui v0.3.7
./update.sh: Zeile 7: : Kommando nicht gefunden.
extracting wireguard-ui
./update.sh: Zeile 9: : Kommando nicht gefunden.
restarting wgui-web.service
```

Wireguard conf von Systemd überwachen lassen und bei Änderung wiregaurd neustarten.
Dienst 1

```
cat <<EOF > /etc/systemd/system/wgui.service
[Unit]
Description=Restart WireGuard
After=network.target

[Service]
Type=oneshot
ExecStart=/bin/systemctl restart wg-quick@wg0.service
```

```
[Install]
RequiredBy=wgui.path
EOF
```

Dienst 2

```
cat <<EOF > /etc/systemd/system/wgui.path
[Unit]
Description=Watch /etc/wireguard/wg0.conf for changes

[Path]
PathModified=/etc/wireguard/wg0.conf

[Install]
WantedBy=multi-user.target
EOF
```

Nun alle 3 Dienste aktivieren und starten

```
touch /etc/wireguard/wg0.conf
systemctl enable wgui.{path,service} wg-quick@wg0.service wgui-web.service
systemctl start wgui.{path,service}
```

Nun können wir auf den Wireguard Server über die Weboberfläche zugreifen.

<http://ipadresse:5000>

Standard Anmeldedaten :

Benutzername : admin

Kennwort : admin

In der alten version über die Datei!!!!

Diese ändern wir ab in der Datei /etc/wireguard/db/server/users.json

```
nano /etc/wireguard/db/server/users.json
```

Inhalt, einfach neues Passwort setzen

```
{
  "username": "admin",
  "password": "<neues passwort>"
}
```

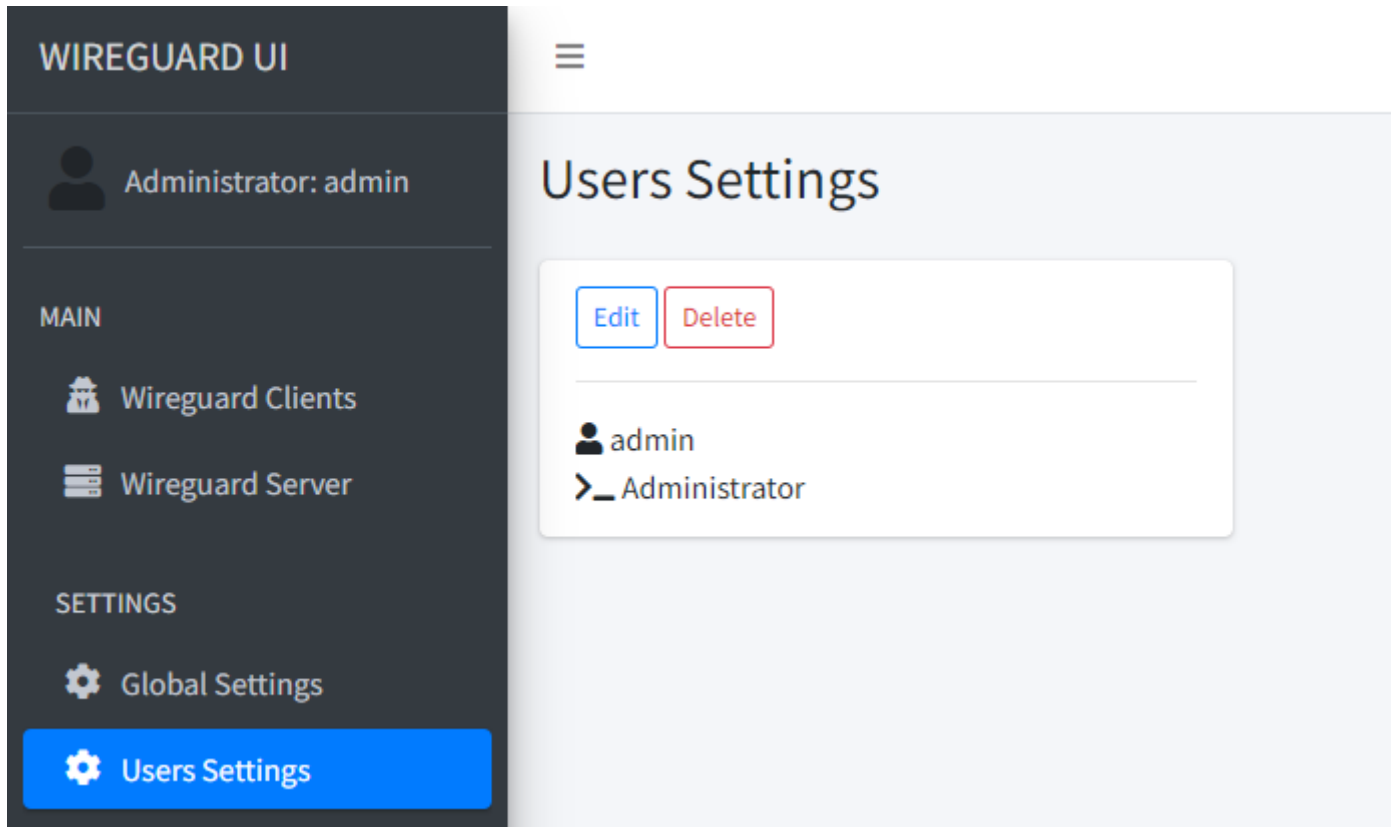
}

In der neuen Version endlich über GUI.

Auf User Setting und dann Edit.

Endlich können auch mehrere Benutzer erstellt werden ;-)

Über den Button new user oben rechts



Nun neues Passwort vergeben und auf save klicken

Edit user admin



Name

Password

 Admin

Teil 2. Email sender Einrichten (Optional)

Wenn man gerne die Files per Email versendet möchte müssen in der Service Datei folgende Environment Variablen angelegt werden

Die Service datei editieren

```
nano /etc/systemd/system/wgui-web.service
```

Das SMTP PASSWORT muss leer gesetzt werden.
und in die Passwort Datei muss das Passwort

Variable	Mögliche optionen
<code>SMTP_AUTH_TYPE</code>	Die SMTP authentication Typen. : <code>PLAIN</code> , <code>LOGIN</code> , <code>NONE</code>
<code>SMTP_ENCRYPTION</code>	Dieencryption Methode. : <code>NONE</code> , <code>SSL</code> , <code>SSLTLS</code> , <code>TLS</code> , <code>STARTTLS</code> jenachdem was für ein Port gesetzt wurde

Inhalt hinzufügen

```
[Unit]  
Description=WireGuard UI
```

```
[Service]
Type=simple
ExecStart=/etc/wireguard/start-wgui.sh
Environment="SMTP_HOSTNAME=<smtpserver>"
Environment="SMTP_PORT=465"
Environment="SMTP_USERNAME=<benutzername>"
Environment="SMTP_PASSWORD="
Environment="SMTP_PASSWORD_FILE=/etc/wireguard/smtppass"
Environment="SMTP_AUTH_TYPE=LOGIN"
Environment="SMTP_ENCRYPTION=SSL"
Environment="EMAIL_FROM_ADDRESS=<emailadresse>"
Environment="EMAIL_FROM_NAME="Anzeigename"

[Install]
WantedBy=multi-user.target
```

Danach den Systemd daemon neustarten

```
systemctl daemon-reload
```

Nun die Passwortfile erstellen

```
nano /etc/wireguard/smtppass
```

Inhalt

```
absolutgeheimesmtppasswort
```

Nun den Dienst neustarten

```
service wgui-web restart
```

Nun kann man über die GUI die Datei wegsenden.
Dazu bei dem Client auf den Button Email klicken

Wireguard Clients

Download

QR code

Email

More



[blurred]



[blurred]



2022/12/01 09:38:46



2024/10/30 19:25:10



DNS disabled

IP Allocation

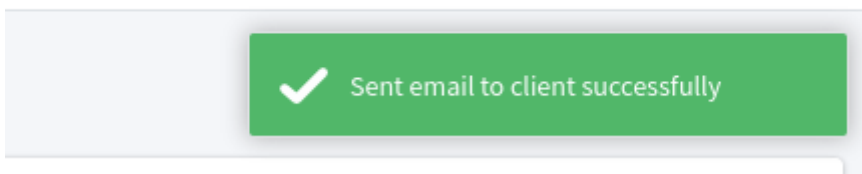
Nun entweder hinterlegte Adresse nutzen, oder andere eingeben dann auf send

Send config to client ✕

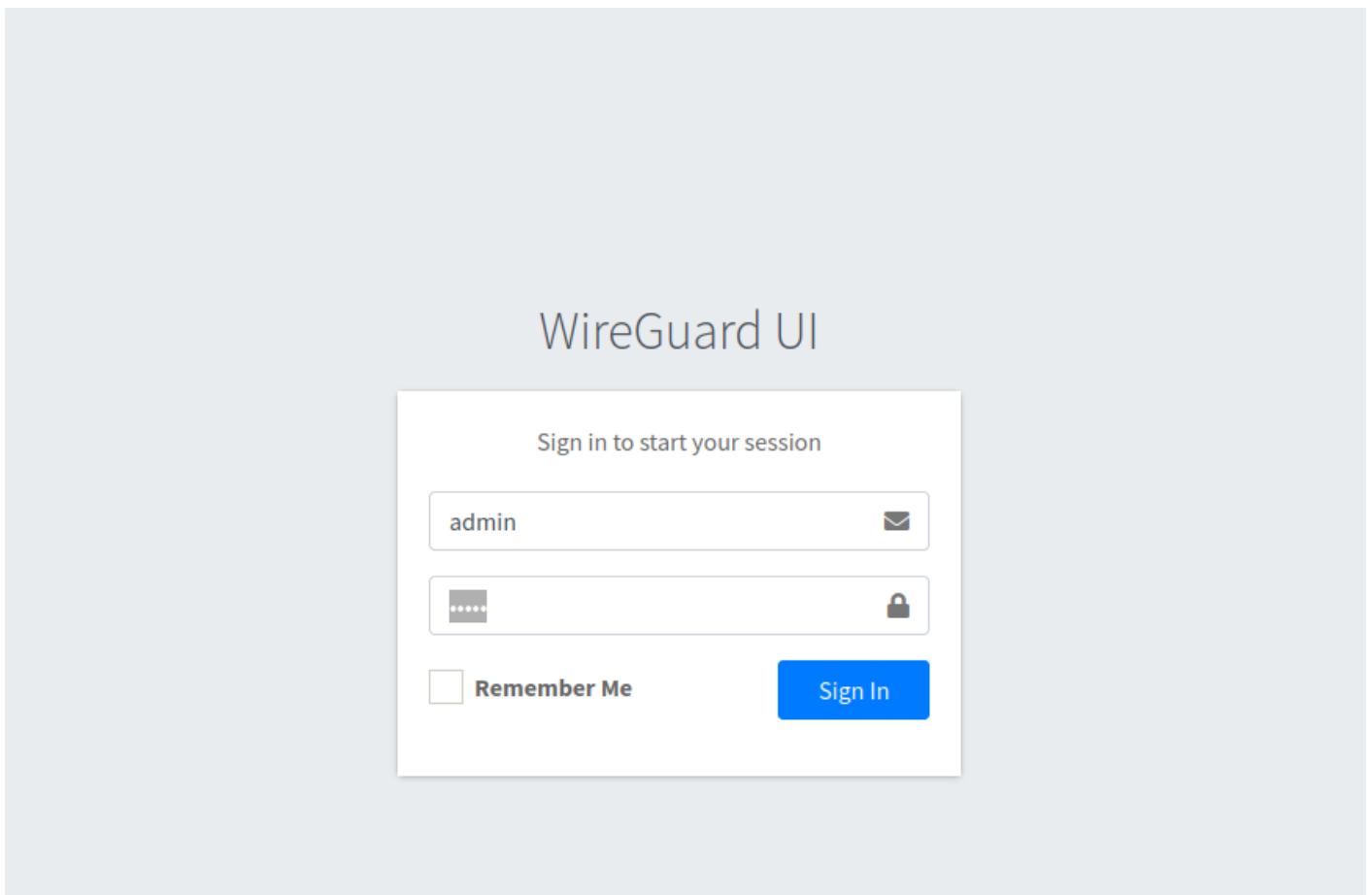
Email address

Die Email wurde erfolgreich gesendet

[+ New Client](#) [Logout](#)



Teil 3. Weiter in der Webgui



Nach dem Einloggen links auf den Menüpunkt Global Settings.

WIREGUARD UI

admin

MAIN

- Wireguard Clients
- Wireguard Server

SETTINGS

- Global Settings**

UTILITIES

- Status
- WoL Hosts

Global Settings

Wireguard Global Settings

Endpoint Address

 [Suggest](#)

DNS Servers

 [Add More](#)

MTU

Persistent Keepalive

Wireguard Config File Path

[Save](#)

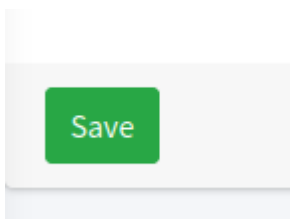
Help

- 1. Endpo**
The publ
the publi
- 2. DNS S**
The DNS
- 3. MTU**
The MTU
(e.g PPPc
Leave bla
- 4. Persist**
By defaul
and/or fir
Persist
Leave bla
- 5. Wiregt**
The path

Die Endpoint Address mit dem DNS namen oder Public ip tauschen.
um die Public IP rauszubekommen, im Terminal.

```
curl ifconfig.me
```

DNS Server auf 8.8.8.8 setzen und MTU rauslöschen.und auf save klicken



und dann apply Config klicken

[+ New Client](#)

[✓ Apply Config](#)

[Logout](#)

Dann sehe das ganze so aus als Beispiel

Global Settings

Wireguard Global Settings

Endpoint Address

Suggest

DNS Servers

8.8.8.8 x Add More

MTU

MTU

Persistent Keepalive

15

Firewall Mark

Firewall Mark

Table

auto

Wireguard Config File Path

/etc/wireguard/wg0.conf

Save

Nun auf den Menüpunkt links Wireguard Server.

Nun mittels terminal und ip a herausfinden welche Netzwerkkarte für lan es gibt.

Ausgabe

ip a

```
ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
link/ether 2a:xx:xxx:xx:85 brd ff:ff:ff:ff:ff:ff  
altname enp0s18
```

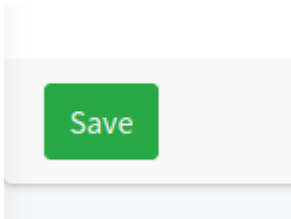
Nun bei Postup folgendes eintragen (die ens18 durch eure Netzwerkkarte ersetzen)

```
iptables -A FORWARD -i %i -j ACCEPT; iptables -A FORWARD -o %i -j  
ACCEPT; iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
```

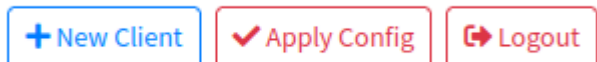
Nun bei Postdown folgendes eintragen (die ens18 durch eure Netzwerkkarte ersetzen)

```
iptables -D FORWARD -i %i -j ACCEPT; iptables -D FORWARD -o  
%i -j ACCEPT; iptables -t nat -D POSTROUTING -o ens18 -j MASQUERADE
```

Nun auf save



und apply config klicken



Dann sieht das ganze so aus.

WIREGUARD UI

admin

MAIN

- Wireguard Clients
- Wireguard Server**

SETTINGS

- Global Settings

UTILITIES

- Status
- WoL Hosts

Wireguard Server Settings

Interface

Server Interface Addresses

10.252.1.0/24 x Add More

Listen Port

51820

Post Up Script

```
> -i %i -j ACCEPT; iptables -A FORWARD -o %i -j ACCEPT; iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
```

Post Down Script

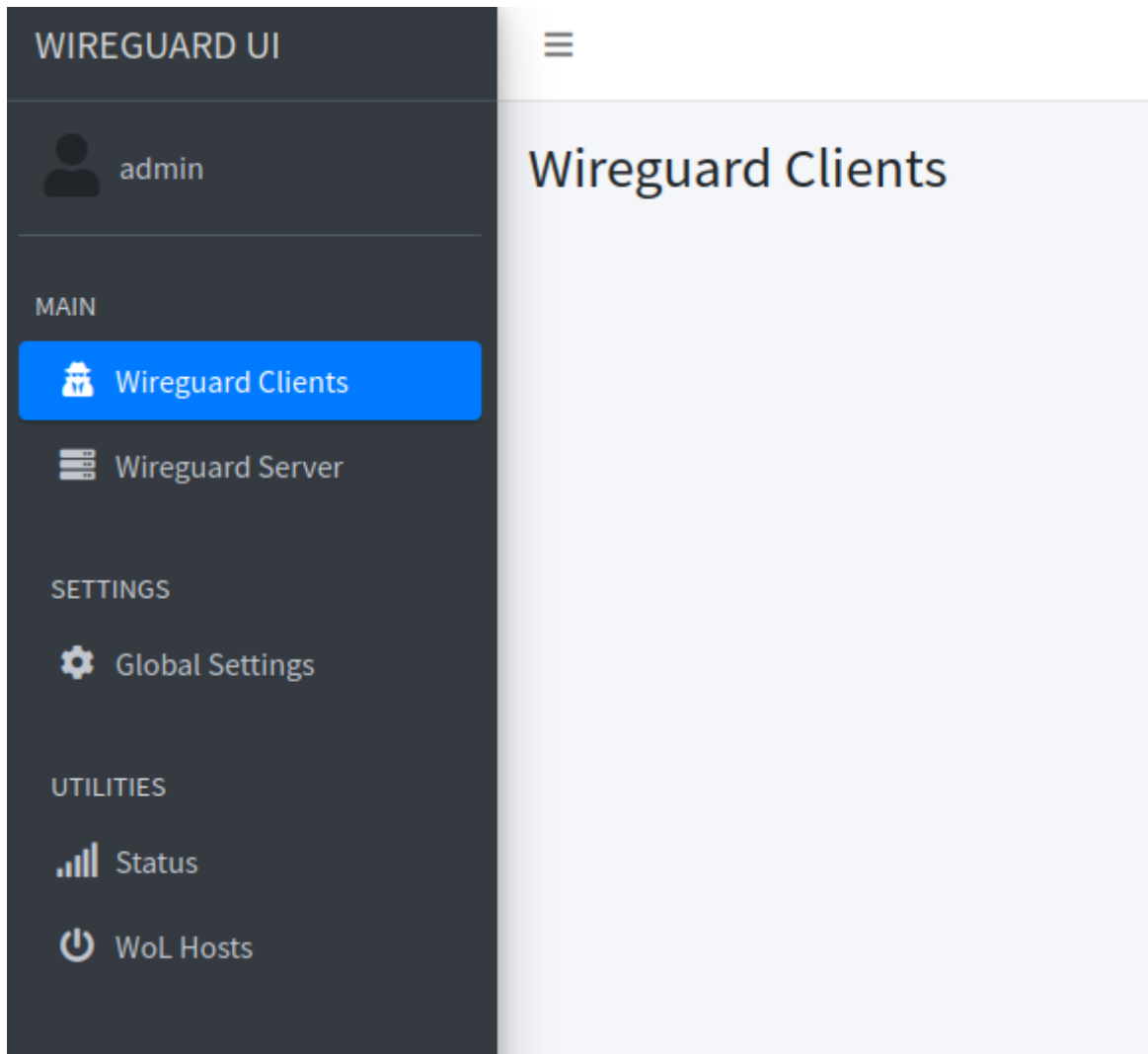
```
> -i %i -j ACCEPT; iptables -D FORWARD -o %i -j ACCEPT; iptables -t nat -D POSTROUTING -o ens18 -j MASQUERADE
```

Save

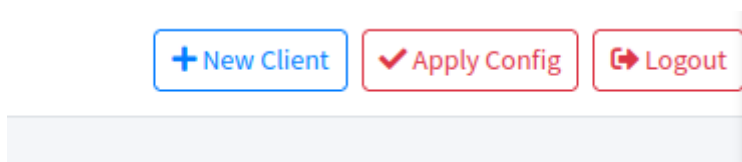
Damit ist die Installation abgeschlossen

Clients einrichten

In der Weboberfläche einloggen dann im Menü links auf Wireguard Clients gehen



Nun oben rechts auf New Client klicken.



Nun folgendes Ausfüllen:

Name : Name des Clients

Email : Email des Clients

IP-Allocations (so lassen nichts ändern)

Allowed IPs. Alles rauslöschen und 10.252.1.0/24 eintragen und als zweiten werd euer netzt was Ihr

erreichen wollt in diesem Fall 192.168.178./24
Use server DNS : haken raus

Dann sehe das ganze so aus:

New Wireguard Client ×

Name

Email

IP Allocation

10.252.1.1/32 x [Add More](#)

Allowed IPs i

10.252.1.0/24 x 192.168.178.0/24 x [Add More](#)

Extra Allowed IPs i

Use server DNS

Enable after creation

▶ **Public and Preshared Keys i**

Nun wieder auf apply Config oben rechts

Nun steht in der liste unser Client in der Liste.

Über Download wird die wireguard conf downgeloaded und über QR Code der Code angezeigt

The screenshot displays the Wireguard UI interface. On the left is a dark sidebar with the title 'WIREGUARD UI' and a user profile 'admin'. The sidebar is divided into sections: 'MAIN' with 'Wireguard Clients' (highlighted in blue) and 'Wireguard Server'; 'SETTINGS' with 'Global Settings'; and 'UTILITIES' with 'Status' and 'WoL Hosts'. The main content area is titled 'Wireguard Clients' and features a toolbar with buttons for 'Download', 'QR code', 'Email', and 'More'. Below the toolbar, a client entry 'Mein Client' is shown with a list of actions: 'Email vom client', two timestamps '2022/12/01 09:38:46', and 'DNS disabled'. Underneath, the 'IP Allocation' is '10.252.1.1/32' and 'Allowed IPs' are '10.252.1.0/24' and '192.168.178.0/24'.

Damit ist unser Client eingerichtet und einsatzbereit.

Wer einen Postfix konfigurieren möchte, kann auch die Email senden funktion nutzen.