



HAM RADIO
QTH <> QTH VPN
MIT DER FRITZBOX
FRITZ!OS 7.39 & WIREGUARD
OHNE VPN-PROVIDER

INHALT

- WARUM VPN im Amateurfunk?
- Warum Wireguard & Fritz!os 7.39?
- Unterstützte Fritzboxen
- Fritz!OS Installation
- Vorbereitung für VPN
- WireGuard Verbindung einrichten
- Ersteinrichtung VPN Master
- Neue Funktion „Authenticator-APP“
- Auf der Gegenstelle
- Verwendete Hardware & Software
- Mein QTH JO61TD
- Mein QTH JO61SD
- Nach der Einrichtung
- Windows Rechner einrichten
- Option: Vereinfachte Verbindung

WARUM VPN IM AMATEURFUNK?

- VPN ist seit langer Zeit in aller Munde und die Anbieteranzahl wächst täglich. Das Hauptziel ist dabei der User mit dem Web Browser, also das Surfen. Dieser Beitrag ist **NICHT** für diese Benutzergruppe !!!
- Im Afu besteht immer öfter die Notwendigkeit der Fernsteuerung von Geräten über IP/Port , die nicht mehr über das private LAN/WLAN realisiert werden können. Nur wenige Geräte bieten Web Service (meist nicht kostenfrei) oder verlangen VPN (ICOM RS-BA1).
- Befinden sich diese Netzwerke an unterschiedlichen Orten, kann nur durch Einsatz von Routern mit öffentlichen IP Adressen/dynDNS und manueller Portfreigabe für einzelne Dienste/Gerät gearbeitet werden. Der OTH wird offen wie ein Scheunentor !!!
- Mit VPN wird einmalig die Verbindung zwischen den Standorten eingerichtet und es kann weiter wie im privaten LAN/WLAN gearbeitet werden, dabei können jedoch hohe Lizenz-/Hardwarekosten entstehen und die Einrichtung/Administration ist sehr komplex.
- Die meisten OMs besitzen einen festen Internetanschluss mit der Fritzbox, also **WARUM NICHT** mit dieser vorhandenen Technik, eine eigene, gebührenfreie VPN Verbindung aufbauen, die mit WireGuard in wenigen Minuten funktioniert?

WARUM WIREGUARD & FRITZ!OS 7.39?

- Warum FRITZ!OS 7.39 ?

Die Vorteile sind auf der Seite <https://avm.de/fritz-labor/frisch-aus-der-entwicklung/neues-und-verbesserungen/>

Meine Hauptgründe liegen in der wesentlich vereinfachten Benutzeroberfläche für VPN (IPSec oder WireGuard) und der WireGuard Unterstützung für LAN/LAN und Device/LAN Netzwerke, der DECT Unterstützung für SIM bei 6850 und App Authenticator App für Fritzbox Setup.

- Warum WireGuard ?

Zitat von AVM: „WireGuard(R) ist eine leicht verständliche und moderne VPN-Lösung. Es setzt sich zum Ziel, schneller, einfacher und schlanker als IPSec zu sein. Im Gegensatz zu IPSec und OpenVPN wird auf eine reduzierte Anzahl von (state-of-the-art) Kryptografiemethoden gesetzt. WireGuard(R) ist im Regelfall einfacher zu konfigurieren als andere Lösungen und überzeugt durch einen schnellen Verbindungsaufbau.“

UNTERSTÜTZTE FRITZBOXEN

Datum der Erstellung der Präsentation 14.08.2022

Das FRITZ! Labor in der Version 7.39 steht bereit für:

- ✓ FRITZ!Box 7530 AX (09.08.2022)
- ✓ FRITZ!Box 7590 AX, 7590, 7530 (05.08.2022)
- ✓ FRITZ!Box 6690, 6591, 6660 Cable (05.08.2022)
- ✓ FRITZ!Repeater 3000, 2400 (05.08.2022)
- ✓ FRITZ!Box 6890 LTE (15.07.2022)
- ✓ FRITZ!Box 6850 LTE (22.07.2022)

FRITZ!OS INSTALLATION

- <https://avm.de/fritz-labor/frisch-aus-der-entwicklung/frisch-aus-der-entwicklung/>
- Die Installation erfolgt vollständig separat und führt **KEINE VPN** Einrichtung aus, diese muss manuell erfolgen und benötigt anschließende Vorbereitungen
- **WICHTIG!** Nach Fritz!OS update unbedingt alle Funktionen prüfen, Internet und Telefonie testen.

VORBEREITUNG FÜR VPN

Alle Punkte gelten für VPN mit einer Fritzbox als Master, also immer wenn eine Verbindung genau zu dieser Fritzbox hergestellt werden soll.

- ✓ **öffentliche IP Adresse**

- ✓ **Feste IP Adresse oder dynDNS**

Feste IP Adressen werden selten vergeben bzw. kosten Geld. Also dynDNS einrichten, Anleitungen und Liste der freien Provider gibt es in Internet. In der Fritzbox ist eine Liste bereits vorhanden.

- ✓ **Eineindeutiger IP Adressbereich pro Standort im Gesamt-VPN**

Sollen Fritzboxen verbunden werden, dann muß jede Fritzbox ein eigenes eindeutiges Subnetz besitzen. Werden Einzelgeräte Handy/Laptop/PC mit einer Fritzbox verbunden, dann erhält jede Einzelverbindung eine IP Adresse im Bereich der Fritzbox nach dem DHCP Bereich (unbedingt berücksichtigen, wenn DHCP verwendet wird) !!!

Heimnetz --> Netzwerk --> Netzwerkeinstellungen --> weitere Einstellungen

UNBEDINGT VORAB NETZWERK und alle Clients prüfen, ob IP Änderung möglich und nach Änderung testen.

Wird einer der Punkte nicht erfüllt, dann ist eine VPN Einrichtung **NICHT** möglich.

WIREGUARD VERBINDUNG EINRICHTEN

Die nachfolgenden Seiten zeigen die Oberfläche des WireGuard Assistenten. Es stehen 2 Optionen zur Auswahl:

- **Vereinfachte Einrichtung**

Richtet eine Einzelverbindung zu Handy/Tablett oder PC ein. Auswählen Verbindungsnamen eintragen und code scannen oder speichern und fertig. Das Gerät wird in das lokale Netzwerk aufgenommen und erhält eine virtuelle IP-Adresse (nach DHCP Bereich) im lokalen Netzwerk.

- **Benutzerdefinierte Einrichtung**

Erstellt den Fritzbox Master oder die Gegenstelle benutzerdefiniert. Beide Abläufe sind in den nachfolgenden Seiten beschrieben.

FRITZ!Box 7530

Internet > Freigaben

Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden.

Willkommen im WireGuard®-Assistenten

Wie möchten Sie die WireGuard®-Verbindung erstellen?

Vereinfachte Einrichtung



Benutzerdefinierte Einrichtung

Erstellen Sie Verbindungen zwischen Netzwerken, zu einem WireGuard®-Server oder zu Dritten. Diese Verbindungen können auch gleichzeitig verwendet werden.



ERSTEINRICHTUNG VPN MASTER

Benutzerdefinierte Einstellungen festlegen

- Wurde diese WireGuard®-Verbindung bereits auf der Gegenstelle erstellt? ⓘ Ja Nein
- Soll die neue WireGuard®-Verbindung gleichzeitig zu einer bestehenden Verbindung der Gegenstelle genutzt werden? ⓘ Ja Nein
- Handelt es sich um ein Einzelgerät (Laptop, Smartphone, Tablet) oder um einen WireGuard®-fähigen Router (z.B. eine FRITZ!Box)? Einzelgerät WireGuard®-fähiger Router



Das manuelle Hinzufügen der neuen Verbindungseinstellungen wird nur erfahrenen Benutzern empfohlen.

Verbindung für einen WireGuard®-fähigen Router erstellen

Vergeben Sie einen individuellen Namen für die WireGuard®-Verbindung, um sie in der Übersicht unter diesem Namen zu finden.

Name der WireGuard®-Verbindung

Geben Sie das IP-Netzwerk der WireGuard®-Gegenstelle ein. Beachten Sie bitte, dass die Gegenstelle ein anderes Netzwerk als in Ihrem Heimnetz verwenden muss. Wenn die Gegenstelle eine manuelle IP-Adresse innerhalb des Netzwerks hat, geben Sie diese an.

Entferntes Netzwerk:

Subnetzmaske:

Um eine Datei mit den ausgewählten Einstellungen zu erstellen, klicken Sie auf „Fertigstellen“.

NEUE FUNKTION „AUTHENTICATOR-APP“

Bestätigen

Die Ausführung muss zusätzlich bestätigt werden.

1. Nehmen Sie ein an der FRITZ!Box angeschlossenes Telefon zur Hand.
2. Geben Sie ein:
3. Bestätigen Sie Ihre Eingabe mit der Verbindungstaste.
4. Hören Sie einen Quittungston und legen auf.

[Kein Telefon? Bestätigung mit FRITZ!Box-Taste oder App ▲](#)

Bestätigung mit FRITZ!Box-Taste:

- Alle LEDs an der FRITZ!Box blinken jetzt.
- Drücken Sie kurz eine beliebige Taste an der FRITZ!Box.
- Zur Bestätigung der Ausführung leuchten die LEDs an der FRITZ!Box einmal auf.

Bestätigung mit Authenticator-App auf Redmi Note 11 Pro+ 5G:

Code eingeben:

Unter "System > FRITZ!Box-Benutzer > Benutzer" können Sie die App für einzelne Benutzer einrichten oder bearbeiten.

**Konnte die Verbindung initialisiert werden, erscheint nachfolgende Seite:
Diese Seite wird nur EINMALIG angezeigt !!!
Eine Wiederholung nur nach Löschung der Verbindung möglich !!!
Für jede Verbindungserstellung wird eine *.conf Datei erzeugt, die heruntergeladen werden muss.
Also Sorgfalt was ich wo und wie speichere, die Datei ist nur für diese Verbindung gültig.
Diese Datei wird für Einrichtung der Gegenstelle benötigt.**

VPN (WireGuard®)

✓ Die WireGuard®-Verbindung wurde erfolgreich erstellt.

Einstellungen auf Ihrem Gerät manuell hinzufügen

Die nachfolgenden Einstellungen ermöglichen es Ihnen, die WireGuard®-Verbindung ebenfalls auf der WireGuard®-Gegenstelle zu hinterlegen. Nach dem Übertragen der Einstellungen auf Ihr Gerät können Sie den Fernzugriff nutzen.

Im Folgenden beschreiben wir Ihnen in kurzen Schritten, was zur Übertragung zu tun ist.

A diagram illustrating the process of transferring settings. On the left, there is a laptop icon. A green arrow points from the laptop to a document icon, which then points to a router icon on the right.

[Einstellungen herunterladen](#)

So funktioniert es:

Für die Übertragung der Einstellungen auf die Gegenstelle benötigen Sie einen Desktop oder Laptop, den Zugang zur Benutzeroberfläche der Gegenstelle und die Datei mit den Einstellungen, die hier zum Download bereitsteht.

1. Klicken Sie auf „Einstellungen herunterladen“, um die Einstellungen für Ihre WireGuard®-Verbindung nutzen zu können.
2. Öffnen Sie WireGuard® auf der Benutzeroberfläche der Gegenstelle.
3. Importieren Sie die oben angezeigte Datei und folgen Sie den weiteren Anweisungen der Software.

AUF DER GEGENSTELLE

Benutzerdefinierte Einstellungen festlegen

Wurde diese WireGuard®-Verbindung bereits auf der Gegenstelle erstellt?  Ja Nein

Einstellungen einer bestehenden WireGuard®-Verbindung importieren

Vergeben Sie einen individuellen Namen für die WireGuard®-Verbindung, um sie in der Übersicht unter diesem Namen zu finden.

Name der WireGuard®-Verbindung

Wählen Sie die Datei, aus der die WireGuard®-Einstellungen importiert werden sollen.

Keine Datei ausgewählt

Um die ausgewählten Einstellungen anzuwenden, klicken Sie auf „Fertigstellen“.

VERWENDETE HARDWARE & SOFTWARE

Diese Anleitung wurde mit den Fritzboxen :

7530 (QTH jo61td mit DSL Vodafone)

und

6850 LTE (QTH jo61sd mit 4g-o2)

Beide mit

FRITZ!OS: 7.39-98873 BETA

Installiert und erfolgreich getestet.

Ergebnis auf den Folgeseiten:

MEIN QTH JO61TD

FRITZ!Box 7530

Internet > Freigaben

Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden.

WireGuard®-Verbindungen zwischen der FRITZ!Box und anderen Geräten

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung	Gesamter Datenverkehr
WireGuard Netzwerk-Verbindung					
<input checked="" type="checkbox"/>	 WGserverDSL	172.20.60.0 /24	46.114.203.105:41009	17.08.2022, 14:27:42	Nein

MEIN QTH JO61SD

FRITZ!Box 6850 LTE

MyFRITZ!

Internet > Freigaben

Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden.

WireGuard®-Verbindungen zwischen der FRITZ!Box und anderen Geräten

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung	Gesamter Datenverkehr
WireGuard Netzwerk-Verbindung					
<input checked="" type="checkbox"/>	 WGvonServer	172.20.61.0 /24	88.76.247.111:50589 [REDACTED]	17.08.2022, 14:29:47	Nein

NACH DER EINRICHTUNG

Wenn die Verbindung auf beiden Fritzboxen aktiviert (grün) ist, wurde die LAN2LAN VPN Verbindung erfolgreich eingerichtet.

Nun beginnt die eigentliche Arbeit mit den Windows PCs.

Viele Rechner in privaten Netzwerken laufen unter Windows (7..11) und auf diesen sind die HAM Apps installiert.

Auf allen Rechner sollte auch eine Firewall eingerichtet und aktiv sein und hier liegt eines der Hauptprobleme. Das nächste Problem liegt in der Netzwerkeinstellung öffentlich und privat.

Öffnen wir den Explorer und klicken Netzwerk, dann sehen wird das zweite Netzwerk NICHT. Auch ein Ping auf eine Windows-PC IP-Adresse in der Gegenstelle ist nicht möglich. Wer das sieht, glaubt nicht mehr an eine erfolgreiche VPN Einrichtung.

https://avm.de/service/wissensdatenbank/dok/FRITZ-Box-7590/67_Netzwerkgerate-werden-uber-VPN-Verbindung-nicht-angezeigt/

Wir geben im Browser die entfernte lokale IP-Adresse der Fritzbox ein und sehen es funktioniert doch.

WINDOWS RECHNER EINRICHTEN

Bevor wir beginnen sollten wir wissen was wir wollen und was wir haben und was ist für den HAM Betrieb notwendig ?

- Welche HAM HW & SW befindet sich am jeweiligen QTH ?
- Welche HAM HW & SW ist an den QTH gebunden und nicht beweglich ?

Mein Status HAM HW fest und beweglich:

QTH JO61SD	QTH JO61TD
IC 7100 HF und VHF/UHF Antennen, , DXPatrol MK4 100kHz..2GHz SDR Umschalter noch manuell	IC 7000, X200, CQ100 DXPatrol TRX 12W, 120cm Spiegel, DXPatrol MK4 100kHz..2GHz SDR, Loop
Fritzbox 6850 LTE SubNet: 172.20.60.0/24	Fritzbox 7530 DSL SubNet: 172.20.61.0/24, dynDNS Strato
Windows10, G01LHE-HAM, RS-BA1 Gateway ..60.20 Windows10, G01LHE-JO61SD, RS-BA1 Client ..60.21	Windows11, G01LHEW03, RS-BA1 Client ..61.100 Windows11, G01LHEL03, Laptop DHCP, QTH beliebig

- Was ist weiter vorhanden und was wird geplant

JO61SD	JO61TD
<p>GigaCube Vodafone mit eigenem Netzwerk für Überwachungsanlage, HomeMatic IP und CCU3, Shelly 4 PM zur Drehstromüberwachung und Steuerung</p>	<p>Fritzbox stellt Internet Verbindung für BR200 bereit, dahinter befindet sich die komplette Domain mit Windows Server 2019, SQL Server, MySQL Server, RAID, Web Server und die Windows11 Workstations.</p>
<p>Auslagerung der kostenpflichtigen Systeme in VPN. Einbau von CM4 IO Modulen zur Antennensteuerung über VPN. HAM Arbeitsplatz auf Windows11 und neuer HW. Komplette SDR Überarbeitung.</p>	<p>Bereitstellung von Datenbanken und File Server Bereichen für VPN Clients . Einrichtung eines Intranets im VPN. VPN bleibt Workgroup und hat keinen Domainzugriff. Komplette SDR Überarbeitung und Antennenumschaltung und Loop-Abstimmung mit CM4.</p>

Was folgt aus dem Istzustand und den geplanten Erweiterungen ?

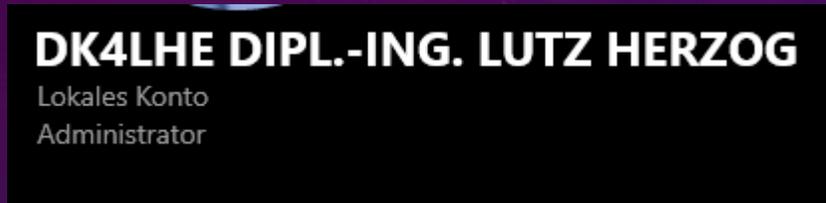
- Der bidirektionale Datenverkehr zwischen 172.20.60.0/24 und 172.20.61.0/24 muß auf IP/Port mit TCP und UDP möglich sein
- Windows Datei- und Druckerfreigabe
- QTH Administration per Remotedesktop und Test-Tools(Ping(IP), Telnet(TCP), portqry(UDP))

Was sind die nächsten Schritte, die VPN LAN/LAN Verbindung ist aktiv:

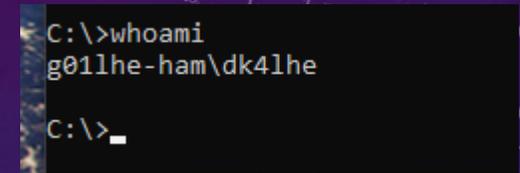
1. pro QTH wird ein Windows PC gewählt Ich wähle G01LHE-HAM (172.20.60.20) und G01LHEW03 (172.20.61.100) beide mit Kontoeinstellungen: lokales Konto Administrator
2. Auf beiden PCs wird die Netzwerkverbindung auf privat gesetzt, feste IP verwenden (manuell oder in Fritzbox immer diese IP verwenden), IP-Adressen mit Benutzername und Kennwort sicher aufbewahren
3. Datei- und Druckerfreigabe aktivieren
4. Rechner in gleiche Arbeitsgruppe (bei mir DK4LHE-VPN)
5. Remotedesktop aktivieren mit Authentifikation
6. Auf jeden Rechner einen Ordner erstellen und Freigabe einrichten auf Administratorebene mit Vollzugriff
7. Windows Defender Firewall kontrollieren und anpassen:
Kontrolle der zugelassenen Apps auf Auswahl Privat bei Remotedesktop
8. Firewall >> Erweiterte Einstellungen Eingehende und Ausgehende Regeln anpassen:
Lokaler Port: 137 UDP, 138 UDP, 139 TCP und 445 TCP mit Remoteadresse „Lokales Subnetz“
Bereich mit 2. VPN Subnetz erweitern (bei mir G01LHE-HAM 172.20.60.20 mit Subnetz von G01LHEW03 172.20.61.100, also 127.20.61.0/24 erweitern)
Protokoll: ICMPv4 mit Remoteadresse „Lokales Subnetz“ ebenfalls erweitern

Nachfolgend die Beispiele für G01LHE-HAM 172.20.60.20 im Subnetz 172.20.60.0/24

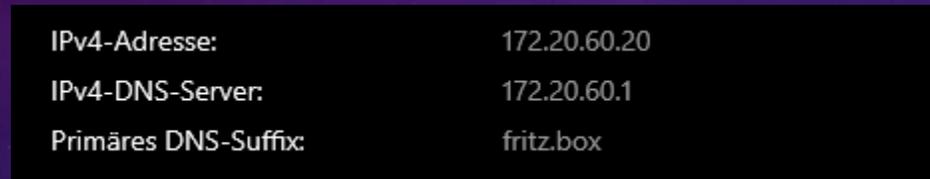
1. Konto



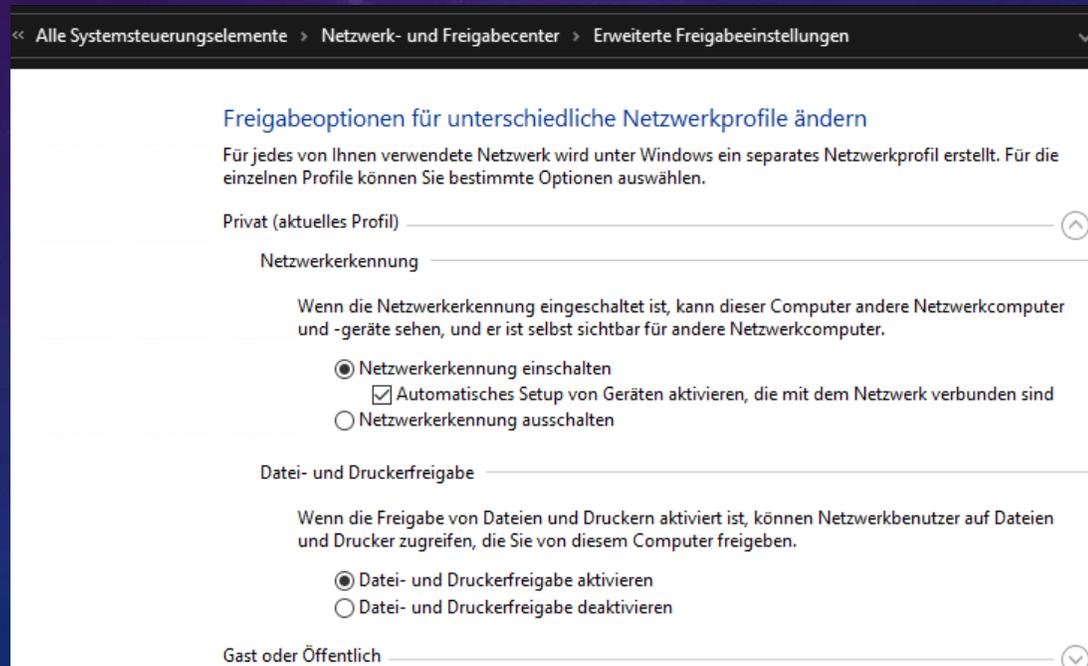
Mit whoami in CMD testen.
Dass ist der Remotedesktop
Username.



2. Netzwerk auf privat und IP Adresse von Fritzbox, dort fest eingestellt.

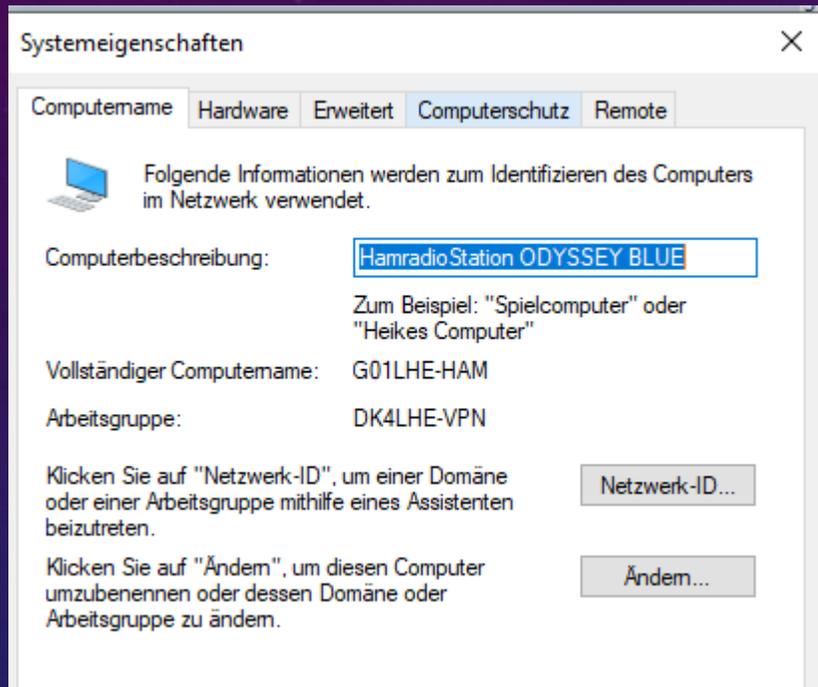


3. Datei- und Druckerfreigabe

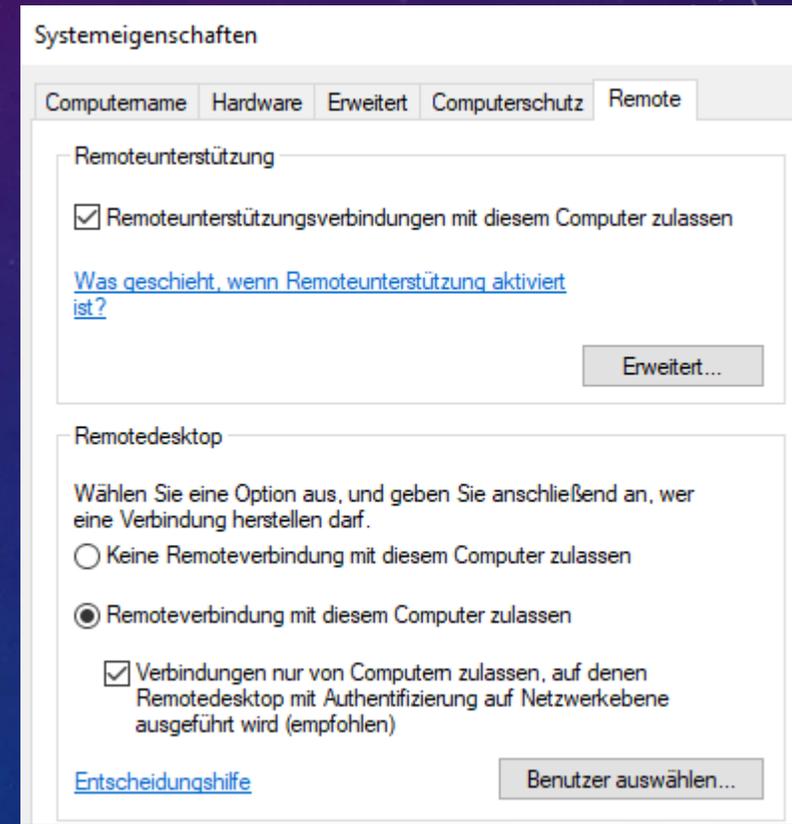


Aktion: Systemsteuerung >> System

4. Rechner in gleiche Arbeitsgruppe (bei mir DK4LHE-VPN)

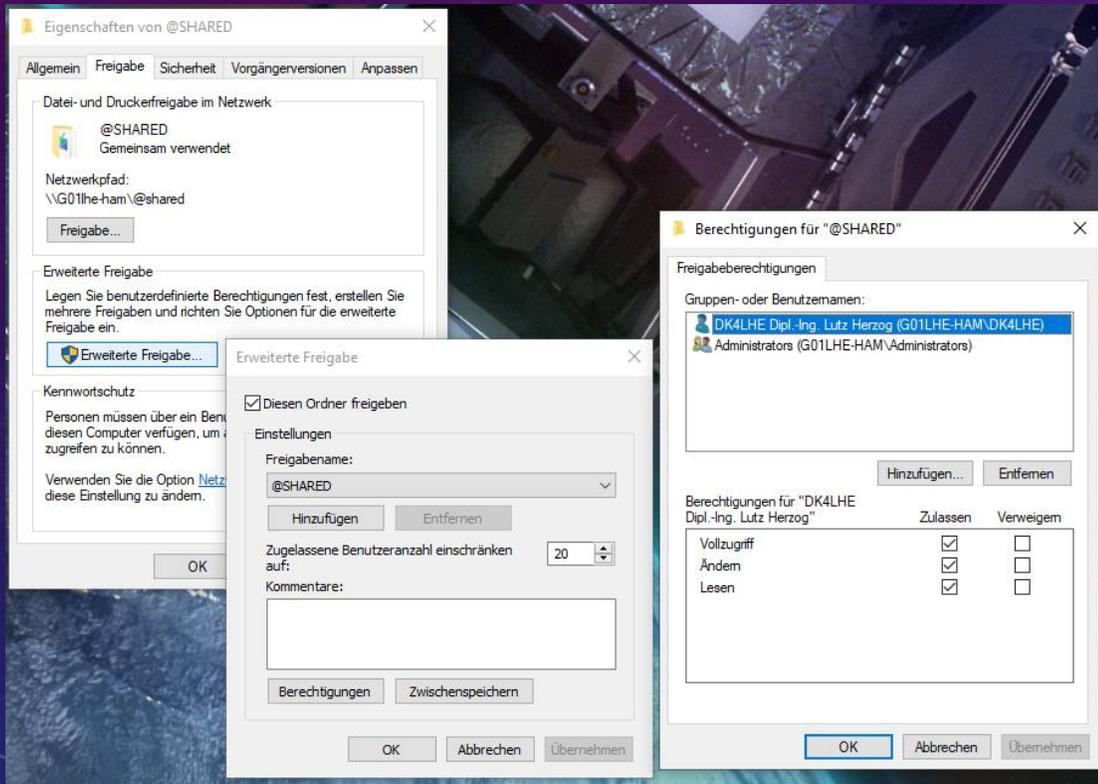


5. Remotedesktop aktivieren mit Authentifikation



Aktion: Ordner im Root Laufwerk anlegen und rechte Maus Eigenschaften >> Freigabe

6. Auf jeden Rechner einen Ordner erstellen und Freigabe einrichten auf Benutzerebene mit Vollzugriff



6. Windows Defender Firewall kontrollieren und anpassen:

In der Liste der zugelassenen Apps muss Name: „Remotedesktop“ und Privat: ausgewählt wurden sein. Zum ändern die Schaltfläche „Einstellungen ändern“ klicken. Werden Apps manuell hinzugefügt oder wurden Apps bereits installiert, immer kontrollieren, ob das Netzwerk „Privat“ aktiviert ist. Bei mobilen Geräten, die auch in öffentlichen Netzwerken betrieben werden sollen, muss auch entsprechend verfahren werden, dann sind zusätzlich auch die Bereichserweiterungen in den erweiterten Einstellungen zu regeln. HINWEIS! Privat ist privat, also mobile Geräte vor Nutzung im eigenen VPN auf privates Netzwerk umschalten.

Startseite der Systemsteuerung

Den PC mithilfe der Windows Defender Firewall schützen

Mithilfe der Windows Defender Firewall kann verhindert werden, dass Hacker oder Schadsoftware über das Internet bzw. über ein Netzwerk Zugriff auf den PC erhalten.

Private Netzwerke Verbunden

Heim- oder Arbeitsplatznetzwerke mit Personen und Geräten, die bekannt und vertrauenswürdig sind

Windows Defender Firewall-Zustand: **Ein**

Eingehende Verbindungen: Alle Verbindungen mit Apps blockieren, die nicht in der Liste zugelassener Apps vorhanden sind

Aktive private Netzwerke: **Network 4**

Benachrichtigungsstatus: Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird

Gast oder öffentliche Netzwerke Nicht verbunden

Kommunikation von Apps durch die Windows Defender Firewall zulassen

Klicken Sie zum Hinzufügen, Ändern oder Entfernen zugelassener Apps und Ports auf "Einstellungen ändern".

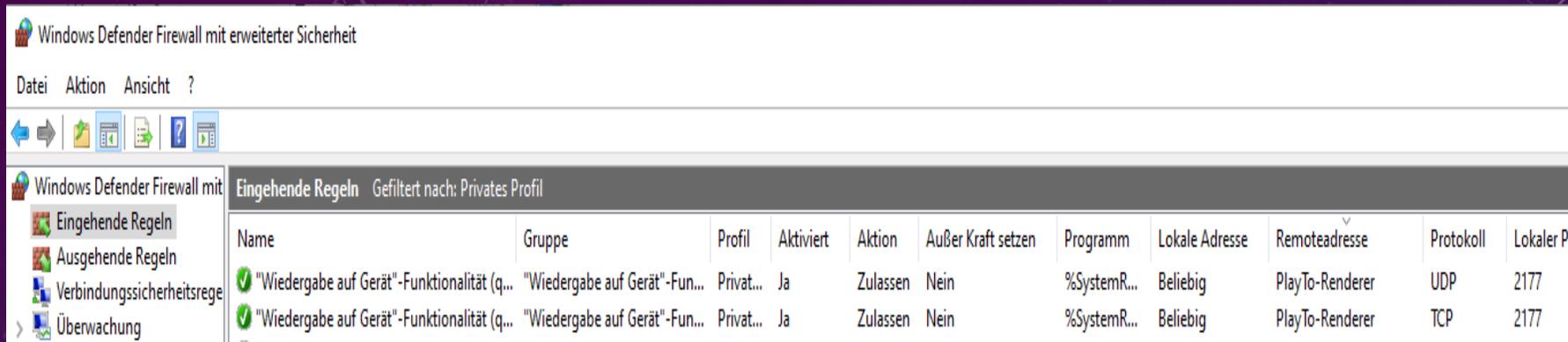
Welche Risiken bestehen, wenn die Kommunikation einer App zugelassen wird? Einstellungen ändern

Zugelassene Apps und Features:

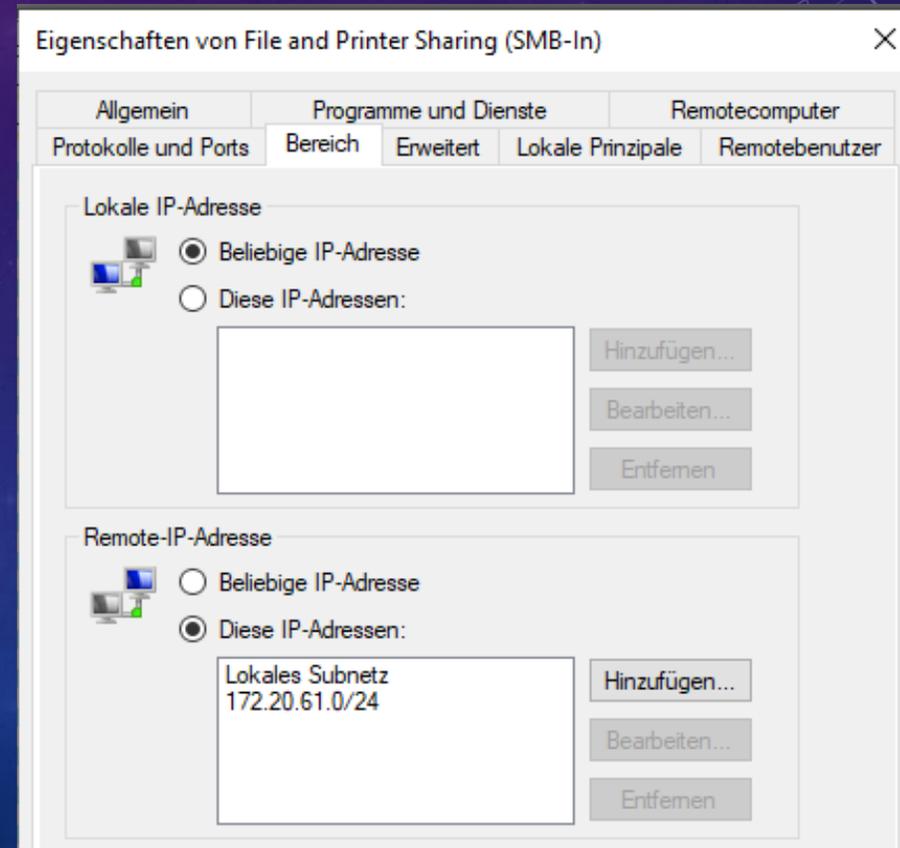
Name	Privat	Öffentlich
<input checked="" type="checkbox"/> Remotedesktop	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remotedesktop (WebSocket)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remotedienstverwaltung	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remote-Ereignisprotokollverwaltung	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remoteereignisüberwachung	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remoteherunterfahren	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remoteunterstützung	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remoteverwaltung geplanter Aufgaben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remotevolumeverwaltung	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Routing und RAS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Schlüsselverwaltungsdienst	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Secure Socket Tunneling-Protokoll	<input type="checkbox"/>	<input type="checkbox"/>

Details... Entfernen

Andere App zulassen...



8. Lokaler Port: 137 UDP, 138 UDP, 139 TCP und 445 TCP mit Remoteadresse „Lokales Subnetz“ Bereich mit 2. VPN Subnetz erweitern und Protokoll: ICMPv4 (opt. ICMP v6) mit Remoteadresse „Lokales Subnetz“ ebenfalls erweitern. Doppelklick auf Listeneintrag und „Bereich“ wählen.



Alle Änderungen in Eingehende und Ausgehende Regeln: „Lokales Subnetz“ ist erweitert.

Ausgehende Regeln Gefiltert nach: Privates Profil					
Name	Profil	Remoteadresse	Aktiviert	Protokoll	Remoteport
Kernnetzwerkdiagnose – ICMP-Echoanfo...	Privat...	Lokales Subnetz, 172.20.61.0/24	Nein	ICMPv4	Beliebig
✓ File and Printer Sharing (SMB-Out)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	TCP	445
✓ File and Printer Sharing (NB-Session-Out)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	TCP	139
✓ File and Printer Sharing (NB-Name-Out)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	UDP	137
✓ File and Printer Sharing (NB-Datagram-O...	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	UDP	138
✓ File and Printer Sharing (Echo Request - I...	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	ICMPv4	Beliebig

Eingehende Regeln Gefiltert nach: Privates Profil					
Name	Profil	Remoteadresse	Aktiviert	Protokoll	Lokaler Port
✓ Netzwerkerkennung (NB-Name eingehe...	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	UDP	137
Kernnetzwerkdiagnose – ICMP-Echoanfo...	Privat, Öffe...	Lokales Subnetz, 172.20.61.0/24	Nein	ICMPv6	Beliebig
Kernnetzwerkdiagnose – ICMP-Echoanfo...	Privat, Öffe...	Lokales Subnetz, 172.20.61.0/24	Nein	ICMPv4	Beliebig
✓ File and Printer Sharing (SMB-In)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	TCP	445
✓ File and Printer Sharing (NB-Session-In)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	TCP	139
✓ File and Printer Sharing (NB-Name-In)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	UDP	137
✓ File and Printer Sharing (NB-Datagram-In)	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	UDP	138
✓ File and Printer Sharing (Echo Request - I...	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	ICMPv6	Beliebig
✓ File and Printer Sharing (Echo Request - I...	Privat	Lokales Subnetz, 172.20.61.0/24	Ja	ICMPv4	Beliebig

Die Seiten zeigten alle Einstellungen für PC G01LHE-HAM 172.20.60.20 mit Subnetz 172.20.60.0/24 also mit Subnetz 172.20.61.0/24 erweitert. Alle Einstellungen sind genauso auf PC G01LHEW03 172.20.61.100 mit Subnetz 172.20.61.0/24 aber mit Subnetz 172.20.60.0/24 zu erweitern.

Mit anderen Worten die Bereichserweiterung muss immer die Gesamtanzahl der VPN Subnetze darstellen.

Werden Port Regeln hinzugefügt, immer Bereich prüfen !!!

Alle weiteren PCs im Netzwerk sind analog zu behandeln !!!

Das ist das Resultat für G01LHE-HAM →

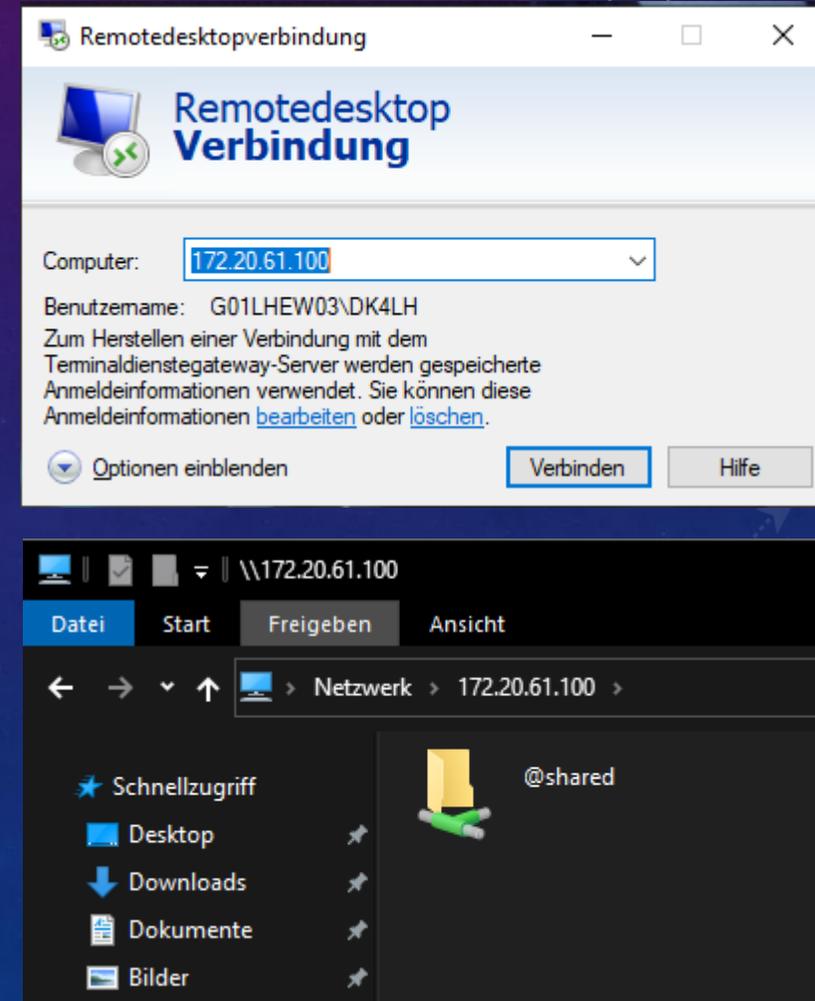
```
C:\Users\ODYSSEY>ping 172.20.61.100

Ping wird ausgeführt für 172.20.61.100 mit 32 Bytes Daten:
Antwort von 172.20.61.100: Bytes=32 Zeit=57ms TTL=126
Antwort von 172.20.61.100: Bytes=32 Zeit=60ms TTL=126
Antwort von 172.20.61.100: Bytes=32 Zeit=71ms TTL=126
Antwort von 172.20.61.100: Bytes=32 Zeit=63ms TTL=126

Ping-Statistik für 172.20.61.100:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 57ms, Maximum = 71ms, Mittelwert = 62ms

C:\Users\ODYSSEY>ping 172.20.61.1

Ping wird ausgeführt für 172.20.61.1 mit 32 Bytes Daten:
Antwort von 172.20.61.1: Bytes=32 Zeit=78ms TTL=63
Antwort von 172.20.61.1: Bytes=32 Zeit=68ms TTL=63
Antwort von 172.20.61.1: Bytes=32 Zeit=53ms TTL=63
Antwort von 172.20.61.1: Bytes=32 Zeit=68ms TTL=63
```



OPTION: VEREINFACHTE VERBINDUNG

Willkommen im WireGuard®-Assistenten

Wie möchten Sie die WireGuard®-Verbindung erstellen?

Vereinfachte Einrichtung



The diagram illustrates a simplified connection setup. On the left is a laptop icon. A green arrow points from the laptop to a server icon on the right. Above the arrow is a key icon, and below it is the text 'VPN', representing the VPN tunnel.

WireGuard®-Verbindung erstellen

Vergeben Sie einen individuellen Namen für die WireGuard®-Verbindung, um sie in der Übersicht unter diesem Namen zu finden.

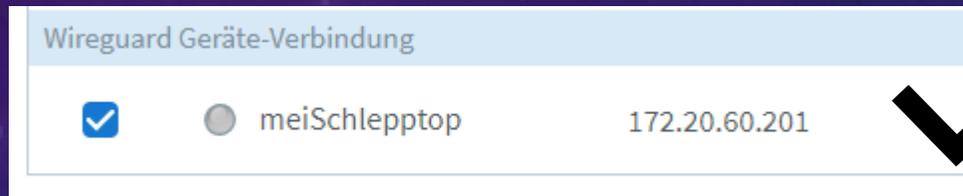
Name der WireGuard®-Verbindung

Fehlermeldung

Der Name der Verbindung enthält ungültige Zeichen. Bitte korrigieren Sie die Eingabe.

OK

Beim Namen keine Umlaute!
Beispiel mit korrekter Eingabe. ->



War der Name korrekt erscheint die Seite mit generierten Verbindungsdaten als QR Code und Download Link.

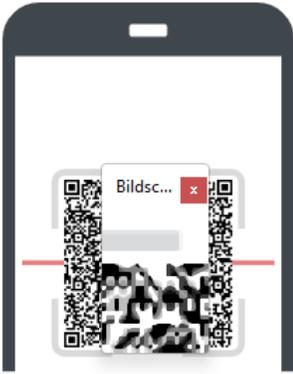
Diese Seite wird nur EINMALIG angezeigt !!!

Eine Wiederholung nur nach Löschung der Verbindung möglich !!!

Für jede Verbindungserstellung wird eineindeutiger Code erzeugt.

Also Sorgfalt was ich wo und wie speichere.

Smartphone oder Tablet



So funktioniert es:

Für die Verwendung mit einem Smartphone oder Tablet benötigen Sie die WireGuard®-App und den oben angezeigten QR-Code.

1. Installieren Sie die WireGuard®-App über den jeweiligen App-Store auf dem bevorzugten Gerät.
2. Starten Sie WireGuard®, tippen Sie auf das Plus „+“ und anschließend auf „aus QR-Code erstellen“.
3. Scannen Sie mit der Kamera Ihres Geräts den oben angezeigten QR-Code ein.
4. Folgen Sie den weiteren Anweisungen in der WireGuard®-App.

Desktop oder Laptop


[Einstellungen herunterladen](#)

So funktioniert es:

Für die Verwendung mit einem Desktop oder Laptop benötigen Sie die WireGuard®-Software und die oben bereitgestellte Einstellungen.

1. Klicken Sie auf „Einstellungen herunterladen“, um die Einstellungen für Ihre WireGuard®-Verbindung nutzen zu können.
2. Installieren Sie die WireGuard®-Software für das Betriebssystem Ihres Desktops oder Laptops.

[Software auf **www.wireguard.com** finden](#) [🔗](#)

3. Starten Sie WireGuard® und klicken Sie auf „Tunnel aus Datei importieren“.
4. Importieren Sie die oben angezeigte Datei und folgen Sie den weiteren Anweisungen der Software.

<https://www.wireguard.com/install/>

 WireGuard

Installation

Quick Start

Interworkings ▾

Installation

Windows [7, 8.1, 10, 11, 2008R2, 2012R2, 2016, 2019, 2022]

macOS [app store]

Installation

 Windows [7, 8.1, 10, 11, 2008R2, 2012R2, 2016, 2019, 2022 - v0.5.3]

[Download Windows Installer](#)

[Browse MSIs](#)



73 Lutz

