

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 IPv4-Netzwerk: . . .

Subnetzmaske: . . .

IPv6-Adresse (/64):

Geben Sie die DNS-Domains der WireGuard®-Gegenstelle ein, um die Heimnetz-Geräte der Gegenstelle mit ihrem Namen zu adressieren.

DNS-Domains

Erweiterte Einstellungen zum Netzwerkverkehr

- Gesamten IPv4-Netzwerkverkehr über die VPN-Verbindung senden**
Aktivieren Sie diese Option, wenn diese FRITZ!Box sämtliche IPv4-Internetanfragen über die VPN-Verbindung zur WireGuard®-Gegenstelle senden soll.
- NetBIOS über diese Verbindung zulassen**
NetBIOS erlaubt es, einen Namen für Geräte netzwerkweit zu registrieren. Das ist besonders für Microsoft Windows Datei- und Druckerfreigaben wichtig.
- Nur bestimmte Geräte im Heimnetz sollen über diese WireGuard®-Verbindung erreichbar sein:**

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

[< Zurück](#) [Fertigstellen](#) [Abbrechen](#)

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.



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.

Wenn Sie die Einrichtung der WireGuard®-Verbindung auf der Gegenstelle vorgenommen haben, können Sie diese Ansicht schließen. Die neue Verbindung wird Ihnen dann auf der Übersicht aller WireGuard®-Verbindungen angezeigt.

2 [Schließen](#)

2. WireGuard-Konfiguration der Fritzbox anpassen

Internet > Freigaben



Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise finden Sie auf unserem [VPN Service-Portal](#).

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

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung
WireGuard Netzwerk-Verbindung				
<input checked="" type="checkbox"/>	NOT38_UDM	192.168.200.0/24		
<input checked="" type="checkbox"/>	FUE_NOT38	192.168.190.0/24		
WireGuard Geräte-Verbindung				
<input checked="" type="checkbox"/>	FUE_STANDARD	192.168.178.203/32 fdfe:4874:ae31::203/128		22.09.2025, 08:01:35

Verbindung hinzufügen

WireGuard®-Einstellungen Ihrer FRITZ!Box

Die FRITZ!Box speichert über angelegte WireGuard®-Verbindungen alle notwendigen Informationen in Form einer Einstellungsdatei. Wenn eine vertrauenswürdige Gegenstelle eine Verbindung zu Ihrer FRITZ!Box einrichten möchte, können Sie diese Einstellungsdatei von der Gegenstelle erweitern lassen.



WireGuard®-Einstellungen anzeigen

WireGuard®- Einstellungen Ihrer FRITZ!Box

Nutzen Sie diese Angaben, um auf einer Ihnen bekannten Gegenstelle eine Verbindung zu dieser FRITZ!Box einzurichten.



Die Einstellungsdatei enthält vertrauliche Informationen über Ihre FRITZ!Box sowie die Zugangsdaten für alle eingerichteten WireGuard®-Gegenstellen. Nutzen Sie daher die Einstellungsdatei nur auf Gegenstellen, denen Sie vertrauen. Die Weitergabe der Einstellungsdatei an Dritte kann unter Umständen zu Missbrauch führen.

Einstellungen

Öffentlicher Schlüssel

[REDACTED]



Internet-Adresse Ihrer FRITZ!Box

[REDACTED]



IPv4-Adresse

192.168.178.1



IPv4-Subnetzmaske

255.255.255.0



IPv6-Adresse (/64)

fdfe:4874:ae31::3e37:12ff:fe81:33db



```
[Interface]
PrivateKey = [REDACTED]
ListenPort [REDACTED]
Address = 192.168.178.1/24,fdfe:4874:ae31::3e37:12ff:fe81:33db/64
DNS = 192.168.178.1,fdfe:4874:ae31::3e37:12ff:fe81:33db
DNS = fritz.box,192.168.190.1,fritz.box,192.168.200.1
```

```
[Peer]
PublicKey = [REDACTED]
PresharedKey = [REDACTED]
```

Einstellungsdatei herunterladen

Schließen

Text aus Konfigurationsanzeige kopieren und als Datei (z.B. „wg_config_FB.conf“) speichern:

```
[Interface]
PrivateKey = xxx
ListenPort = xxx
Address = 192.168.178.1/24,fdfe:4874:ae31::3e37:12ff:fe81:33db/64
DNS = 192.168.178.1,fdfe:4874:ae31::3e37:12ff:fe81:33db
DNS = fritz.box,192.168.190.1,fritz.box,192.168.200.1

[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.178.203/32,fdfe:4874:ae31::203/128
PersistentKeepalive = 25
[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.190.0/24
PersistentKeepalive = 25
[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.200.0/24
PersistentKeepalive = 25
```

Modifikation der Konfiguration durchführen

- Nicht anzupassende Peers (andere VPN-Verbindungen der FritzBox) löschen
- DNS-Eintrag vereinfachen
- AllowedIPs für Peer erweitern (hier muss jedes Netzwerk der UDM, das erreicht werden soll eingetragen werden)

```
[Interface]
PrivateKey = xxx
ListenPort = xxx
Address = 192.168.178.1/24
DNS = 192.168.178.1

[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.200.0/24, 192.168.60.0/24
PersistentKeepalive = 25
```

Zuvor erstellte Verbindung löschen

Internet > Freigaben



Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise finden Sie auf unserem [VPN Service-Portal](#).

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

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung
WireGuard Netzwerk-Verbindung				
<input checked="" type="checkbox"/>	● NOT38_UDM	192.168.200.0/24		
<input checked="" type="checkbox"/>	● FUE_NOT38	192.168.190.0/24		
WireGuard Geräte-Verbindung				
<input checked="" type="checkbox"/>	● FUE_STANDARD	192.168.178.203/32 fdfe:4874:ae31::203/128		22.09.2025, 08:01:35

Verbindung hinzufügen

WireGuard®-Einstellungen Ihrer FRITZ!Box

Die FRITZ!Box speichert über angelegte WireGuard®-Verbindungen alle notwendigen Informationen in Form einer Einstellungsdatei. Wenn eine vertrauenswürdige Gegenstelle eine Verbindung zu Ihrer FRITZ!Box einrichten möchte, können Sie diese Einstellungsdatei von der Gegenstelle erweitern lassen.

WireGuard®-Einstellungen anzeigen

Übernehmen

Verwerfen

Mit angepasster Konfiguration, Verbindung wieder hinzufügen

Internet > Freigaben



Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise finden Sie auf unserem [VPN Service-Portal](#).

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

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung
WireGuard Netzwerk-Verbindung				
<input checked="" type="checkbox"/>	● FUE_NOT38	192.168.190.0/24		
WireGuard Geräte-Verbindung				
<input checked="" type="checkbox"/>	● FUE_STANDARD	192.168.178.203/32 fdfe:4874:ae31::203/128		22.09.2025, 08:01:35

Verbindung hinzufügen

WireGuard®-Einstellungen Ihrer FRITZ!Box

Die FRITZ!Box speichert über angelegte WireGuard®-Verbindungen alle notwendigen Informationen in Form einer Einstellungsdatei. Wenn eine vertrauenswürdige Gegenstelle eine Verbindung zu Ihrer FRITZ!Box einrichten möchte, können Sie diese Einstellungsdatei von der Gegenstelle erweitern lassen.

WireGuard®-Einstellungen anzeigen

Übernehmen

Verwerfen

Willkommen im WireGuard®-Assistenten

Welche WireGuard®-Verbindung möchten Sie erstellen?

Einzelgerät verbinden

Richten Sie eine WireGuard®-Verbindung zu dieser FRITZ!Box für ein Smartphone, Tablet oder einem einzelnen Computer ein.



Netzwerke koppeln oder spezielle Verbindungen herstellen

Richten Sie eine WireGuard®-Verbindung zwischen zwei FRITZ!Box-Netzwerken, dieser FRITZ!Box und einem VPN-Anbieter, dieser FRITZ!Box und einem WireGuard®-Server oder andere spezielle WireGuard®-Verbindungen ein.



Für eine Verbindung zweier FRITZ!Box-Produkte (LAN-LAN) erstellen Sie hier die WireGuard®-Verbindung und importieren Sie diese auf der zweiten FRITZ!Box.

Weiter >

Abbrechen

Benutzerdefinierte Einstellungen festlegen

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

< Zurück

Weiter >

Abbrechen

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 **1**

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

2

wg_config_FB.conf

Erweiterte Einstellungen zum Netzwerkverkehr

Gesamten IPv4-Netzwerkverkehr über die VPN-Verbindung senden

Aktivieren Sie diese Option, wenn diese FRITZ!Box sämtliche IPv4-Internetanfragen über die VPN-Verbindung zur WireGuard®-Gegenstelle senden soll.

3

NetBIOS über diese Verbindung zulassen

NetBIOS erlaubt es, einen Namen für Geräte netzwerkweit zu registrieren. Das ist besonders für Microsoft Windows Datei- und Druckerfreigaben wichtig.

Nur bestimmte Geräte im Heimnetz sollen über diese WireGuard®-Verbindung erreichbar sein:

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

< Zurück

Fertigstellen

Abbrechen

4

Als entferntes Netz wird nun auch das gewünschte Netzwerk zu UDM angezeigt (wichtig für Routing) in der Fritzbox

Internet > Freigaben



Portfreigaben

FRITZ!Box-Dienste

DynDNS

VPN (IPSec)

VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise finden Sie auf unserem [VPN Service-Portal](#).

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

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung
WireGuard Netzwerk-Verbindung				
<input checked="" type="checkbox"/>	NOT38_UDM	192.168.200.0/24 192.168.60.0/24		
<input checked="" type="checkbox"/>	FUE_NOT38	192.168.190.0/24		
WireGuard Geräte-Verbindung				
<input checked="" type="checkbox"/>	FUE_STANDARD	192.168.178.203/32 fdfe:4874:ae31::203/128		22.09.2025, 08:01:35

[Verbindung hinzufügen](#)

WireGuard®-Einstellungen Ihrer FRITZ!Box

Die FRITZ!Box speichert über angelegte WireGuard®-Verbindungen alle notwendigen Informationen in Form einer Einstellungsdatei. Wenn eine vertrauenswürdige Gegenstelle eine Verbindung zu Ihrer FRITZ!Box einrichten möchte, können Sie diese Einstellungsdatei von der Gegenstelle erweitern lassen.

[WireGuard®-Einstellungen anzeigen](#)

Übernehmen

Verwerfen

3. VPN-Client in der UDM einrichten

The screenshot displays the UniFi Network Controller interface for configuring a VPN Client. The interface is dark-themed and includes a sidebar on the left with navigation options: Overview, WiFi, Networks, Internet, VPN (highlighted with a yellow '2'), CyberSecure, Policy Engine, Profiles, System, UDM Pro, Control Plane, and Identity. The main content area has tabs for Teleport, VPN Server, VPN Client (highlighted with a yellow '3'), and Site-to-Site VPN. The VPN Client tab is active, showing an 'Outbound VPN' section with the text: 'Securely connect to external VPN providers and forward selected traffic using Policy-Based Routing.' Below this text is a 'Create VPN Client' button (highlighted with a yellow '4'). A yellow '1' is placed near the bottom left of the sidebar, and a yellow '2' is placed near the 'VPN' menu item. At the bottom of the sidebar, there are three notification cards: 'Give feedback directly to the UniFi R&D team here.', 'Share Site Details' (with a checkmark and a play button), and 'Activate Professional Support for Phone Assistance. Click Here'. The bottom of the sidebar shows the version 'Network 9.4.19'.

< **Configuration** ● Valid

VPN Type WireGuard OpenVPN

Name NOT38_UDM

Setup File Manual

Configuration File ⓘ **1** [wg_config.conf](#)

Device Wizard ⓘ Off Device Network **2**

WE1 Hauptnetzwerk × **3**

Edit (1)

Content Wizard ⓘ Off Domain IP Region

i Device and Content Wizard automatically creates a Policy-Based Route.

Kill Switch ⓘ

Connection ● Not Established

Private Key ⓘ [Redacted]

Public Key ⓘ [Redacted] Copy

IP Address	Netmask
192.168.200.1	24

IP / Hostname	Port
[Redacted]	[Redacted]

Server Address ⓘ [Redacted]

Public Server Key ⓘ [Redacted]

Pre-Shared Key ⓘ [Redacted]

Primary DNS Server ⓘ 1.1.1.1

Secondary DNS Server

Apply

VPN-Client wird als in der Zone-Based-Firewall (ZBF) im Bereich „External“ geführt. Dafür Firewall-Einstellungen und Routing-Policy einrichten.

Source	Destination	Destination								
		Internal	External	Gateway	VPN	Hotspot	DMZ	Haus Allgemein	TKM	
Internal	Internal	Allow All	Allow All (3)	Allow All (2)	Allow All	Allow All	Allow All	Allow Return (2)	Allow All (2)	
External	External	Allow Return (5)	Allow Return (3)	Allow Return (5)	Allow Return (3)	Allow Return (3)	Allow Return (3)	Allow Return (3)	Allow Return (3)	
Gateway	Gateway	Allow All	Allow All	-	Allow All	Allow All	Allow All	Allow All	Allow All	
VPN	VPN	Allow All	Allow All (2)	Allow All	Allow All	Allow All	Allow All	Block All	Block All	
Hotspot	Hotspot	Allow Return (4)	Allow All (6)	Allow Return (9)	Allow Return (3)	Block All (3)	Block All (2)	Block All (2)	Block All (2)	
DMZ	DMZ	Allow Return	Allow All (2)	Allow Return	Allow Return	Block All	Block All	Block All	Block All	
Haus Allgemein	Haus Allgemein	Block All	Allow All (3)	Allow All (2)	Block All	Block All	Block All	Block All	Block All	
TKM	TKM	Allow Return (3)	Allow All (2)	Allow All (2)	Block All	Block All	Block All	Block All	Block All (8)	

Allow VPN (External) to Internal

Source Zone: External

Source: Any (IP selected)

IP Address / Subnet: 192.168.178.0/24

Action: Allow

Auto Allow Return Traffic:

Destination Zone: Internal

Destination: Any

IP Version: Both

Protocol: All

Connection State: All

Schedule: Always

Allow VPN (External) to Internal (Return)

Source Zone: Internal

Source: Any

Source Port: Any

Action: Allow

Destination Zone: External

Destination: 192.168.178.0/24

Destination Port: Any

IP Version: Both

Protocol: All

Connection State: -

ID: 30000

Configure Firewall Policy

Diese Routing-Policy hat die UDM beim Erstellen der VPN-Verbindung bereits angelegt.

NOT38_UDM ✕

Name
NOT38_UDM

Interface/VPN Tunnel ⓘ
NOT38_UDM ▾

Kill Switch ⓘ

Source ⓘ
 Any Device / Network
🌐 WE1 Hauptnetz... ✕
[Edit \(1\)](#)

Destination ⓘ
 Any IP Domain Region