

# WLAN-Paramter und manuelles Einrichten

- [Parameter](#)
- [Manuelles Einrichten](#)

# Parameter

Verwenden Sie bitte ausschließlich unsere Anleitung zum WLAN einrichten. Mit unseren [Anleitungen](#) stellen Sie sicher, dass Ihr Gerät auch ohne Expertenwissen sicher und roaming-konform eingerichtet ist.

Für alle diejenigen, die doch lieber selbst Hand an die WLAN-Konfiguration legen wollen, sind hier die notwendigen Konfigurationsparameter angegeben:

| Parameter   | Einstellung   |
|---|---|
| Verschlüsselung                                     | WPA2/WPA3-Transition Mode-Enterprise mit AES  |
| Authentifizierung                                   | Protokoll 802.1X  |
| Verschlüsselung des Authentifizierungstunnels       | EAP/TTLS  |
| Äußerer Tunnel/Anonyme Identität                    | anonymous@tu-bs.de  |
| Server/Domain                                       | netauth.rz.tu-bs.de   |
| Zertifikate   | <a href="https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt">https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt</a> oder <a href="#">T-TeleSec Global Root 2</a> Es wird das TeleSec Global Root 2 als Server Zertifikat verwendet. Das Zertifikat TeleSec Global Root 2 ist meist in aktuellen Browser und Betriebssystemen bereits installiert. |
| Authentifizierung im inneren verschlüsselten Tunnel | PAP (bzw. MSCHAPv2 für die Systeme, die kein PAP unterstützen sollten)  |
| Authentifizierung/Identität (innerer Tunnel)        | Zentrale Benutzererkennung und Passwort sowie Domainangabe „tu-braunschweig.de“ (<Benutzererkennung>@tu-braunschweig.de). Ohne die Angabe <Benutzererkennung>@tu-braunschweig.de erfolgt kein Roaming an anderen Einrichtungen!   |

Wichtiger Hinweis: **Konfigurieren Sie Zertifikatsinformationen** und **deaktivieren Sie niemals die Zertifikatsprüfung** bei der WLAN-Anmeldung! Wenn Sie einen Zertifikatsfehler durch Ihr Gerät beim Anmelden an das WLAN bekommen, loggen Sie sich bitte unter keinen Umständen im WLAN ein bzw. ignorieren Sie solche Meldungen niemals! Verwenden Sie zu keinem Zeitpunkt nur Benutzererkennung und Passwort, um sich mit eduroam zu verbinden, sondern achten Sie auf die Zertifikate und konfigurieren Sie Ihre Geräte richtig und mit Bedacht.

# Manuelles Einrichten

## Manuelles Einrichten unter Linux

In dieser Anleitung erklären wir Ihnen, wie Sie manuell über die graphische Benutzeroberflächen von Ubuntu eine Verbindung mit eduroam herstellen können.

### Achtung:

Bevor Sie fortfahren, benötigen Sie noch das **Zertifikat [T-TeleSec GlobalRoot Class 2](#)**.

Zusätzlich können Sie das Zertifikat mit weiteren Zertifikaten des DFN unter folgendem [Link](#) herunterladen. Sollten Sie keine Möglichkeit haben, das Zertifikat über ein Zweitgerät herunter zu laden, können Sie sich auch an unseren IT-Service-Desk wenden. Der IT-Service-Desk ist Ihnen gerne behilflich und stellt Ihnen das Zertifikat auf einem USB-Stick zur Verfügung.

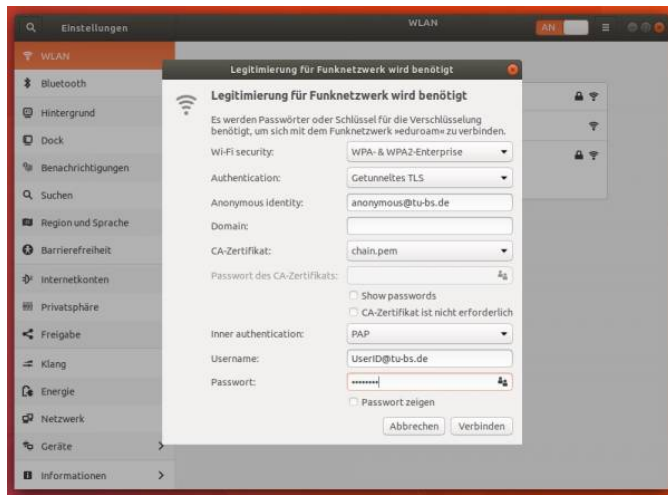


Stellen Sie sicher, dass WLAN an Ihrem Gerät aktiviert ist.

Navigieren Sie zu „Wählen Sie ein Netzwerk aus“ (oben rechts unter dem Netzwerksymbol).

Wählen Sie in der Übersicht der verfügbaren Funknetzwerke eduroam aus (siehe Abbildung links).

Nach Auswahl der SSID eduroam öffnet sich ein Einstellungsfenster, dass Sie nach den Vorgaben in den folgenden Abbildungen ausfüllen müssen.



Wie links in der Abbildung zu sehen, müssen Sie unter „Authentication“ „Getunneltes TLS“ oder auch TTLS auswählen. Als „Anonymous Identity“ wird der Benutzer anonymous@tu-braunschweig.de eingetragen.

In der Zeile „CA certificate“ muss das zuvor heruntergeladene „TU-Braunschweig Zertifikat“ angegeben werden. Bitte beachten Sie, dass die **Datei die Endung .pem** haben muss.

Zuletzt ist in den Einstellung „Inner authentication“ PAP auszuwählen. Bei Benutzername muss die jeweilige Benutzerkennung (nicht Ihre E-Mail-Adresse) in dem Format **<Benutzerkennung>@tu-braunschweig.de** gefolgt von Ihrem „Passwort“ eingegeben werden.

Nach Abschluss der Einstellungen können Sie die Konfiguration mit „Verbinden“ bestätigen.

# Networkmanager

Falls das SecureW2 JoinNow Skript oder die Konfiguration per grafischer Oberfläche je nach Distribution und Paketsituation fehlschlagen, können Sie die Verbindung zu eduroam mit folgender Beispielkonfiguration für den Networkmanager herstellen.

Wichtige Hinweise für Mehrbenutzerkonfigurationen:

1. Wenn diese Konfiguration unter /etc/NetworkManager/system-connections/ angelegt wird (root-Rechte) sollten Sie bedenken, dass das im Feld „[802-1x] password=“ hinterlegte **persönliche** Kennwort Ihrer Benutzerkennung für Nutzer mit **superuser**-Rechten am Gerät **einsehbar** ist.
2. Unter „[connection] permissions=user:<Nutzernamen>;“ angegebene Nutzer können diese Verbindung verwenden. Bitte bedenken Sie, dass die Authentifizierung im eduroam dann mit den angegebenen persönlichen Zugangsdaten erfolgen würde. **Diese Verwendung entspricht nicht den Nutzungsordnungen** der persönlichen Benutzerkennung am Gauß-IT-Zentrum. Ausnahme hierfür sind Accounts für technische Geräte, wie z.B. WLAN-fähige Messgeräte oder Drucker mit t-Nummern.

```
[connection]
id=eduroam
uuid=<uuid des Verbindungsprofils>
type=wifi
permissions=user:<Nutzername(n)>;
secondaries=

[wifi]
mac-address=<MAC(Physikalische)-Adresse des WLAN-Adapters>
mac-address-blacklist=
mac-address-randomization=0
mode=infrastructure
seen-bssids=
ssid=eduroam

[wifi-security]
group=
key-mgmt=wpa-eap
pairwise=
proto=

[802-1x]
altsubject-matches=
anonymous-identity=anonymous@tu-braunschweig.de
ca-cert=/etc/ssl/certs/TUCertChain.pem
domain-suffix-match=netauth.rz.tu-bs.de
eap=ttls;

identity=<GITZ Benutzerkennung>@tu-braunschweig.de
password=<GITZ Kennwort>
phase2-altsubject-matches=
# mschapv2 oder pap
phase2-autheap=pap

[ipv4]
dns-search=
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
ip6-privacy=0
method=auto
```