

Ubuntu (Linux) - VPN einrichten (OpenConnect)

Zusammenfassung

Einer VPN-Verbindung mit Bordmitteln von Debian-basierten Linux-Betriebssystemen kann wie folgt eingerichtet werden.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- Studierende
- Lehrende
- Mitarbeitende
- Wissenschaftliche Mitarbeitende und Hilfskräfte
- Einrichtungen und Gremien (z.B. Fachschaftsräte)
- Arbeitsbereiche / Gruppen (z.B. Projekte)
- Gäste der Friedrich-Schiller-Universität

Voraussetzungen

- ein aktives Nutzerkonto der Universität Jena
- aktuelles Debian-basierendes Linux-Betriebssystem
- SuperUser-Rechte auf dem Zielsystem
- Internetverbindung

Unter [VPN - Zugang zum internen Universitätsnetz \(uni-jena.de\)](#) finden Sie weitere Informationen zu Voraussetzungen und Leistungsumfang des VPN-Services.

Installation und Nutzung des VPN-Dienstes

1. Schritt: VPN-Komponenten installieren

Öffnen Sie das Terminal und tippen /kopieren Sie folgende Befehle um die neuesten Paketlisten mit deren Abhängigkeiten zu laden (hintereinander ausführen):

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

Nach Eingabe des Befehls wird das Gerätepasswort (sudo) abgefragt, wundern Sie sich nicht, dass bei Eingabe des Passwortes keine Zeichen zu sehen sind.

Anschließend müssen zusätzliche Komponenten des OpenConnect SSL Clients installiert werden. Diese sind für die Verbindung zum VPN-Gateway der Uni Jena erforderlich.

```
sudo apt-get install openconnect network-manager-openconnect network-manager-openconnect-gnome
```

Bestätigen Sie die Installation der neuen Komponenten.

Installieren Sie anschließend das Sicherheitszertifikat (hintereinander ausführen):

```
sudo -i  
cd /etc/ssl/certs  
wget https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec\_GlobalRoot\_Class\_2.pem
```

Derzeit kein Support für grafische Oberfläche bei Ubuntu



Derzeit fehlt eine notwendige Option in der grafischen Oberfläche unter Debian (Ubuntu, Mint, etc).

Die benötigte Version des network-manager-openconnect lautet 1.2.10.

Nutzen Sie daher den [Cisco AnyConnect](#) oder führen Sie OpenConnect per Kommandozeile mit den Parametern:

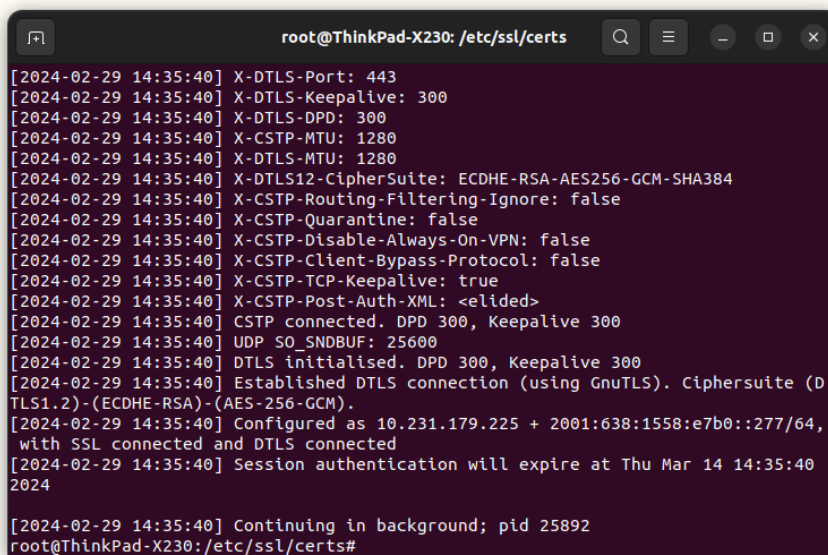
(Tipp, nutzen Sie ein neues Terminal-Fenster)

```
sudo openconnect -b --useragent 'AnyConnect' --user=ab12cde@uni-jena.de --pid-file=/var/run/vpn.pid --timestamp --syslog vpn.uni-jena.de
```

aus.

Achtung. "ab12cde" muss mit Ihrem Loginkürzel ersetzt werden!

Nach Eingabe des Befehls wird das Gerätepasswort (sudo) abgefragt, wundern Sie sich nicht, dass bei Eingabe des Passwortes keine Zeichen zu sehen sind. Anschließend wird Ihr Passwort des URZ-Logins abgefragt.



```
root@ThinkPad-X230: /etc/ssl/certs
[2024-02-29 14:35:40] X-DTLS-Port: 443
[2024-02-29 14:35:40] X-DTLS-Keepalive: 300
[2024-02-29 14:35:40] X-DTLS-DPD: 300
[2024-02-29 14:35:40] X-CSTP-MTU: 1280
[2024-02-29 14:35:40] X-DTLS-MTU: 1280
[2024-02-29 14:35:40] X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384
[2024-02-29 14:35:40] X-CSTP-Routing-Filtering-Ignore: false
[2024-02-29 14:35:40] X-CSTP-Quarantine: false
[2024-02-29 14:35:40] X-CSTP-Disable-Always-On-VPN: false
[2024-02-29 14:35:40] X-CSTP-Client-Bypass-Protocol: false
[2024-02-29 14:35:40] X-CSTP-TCP-Keepalive: true
[2024-02-29 14:35:40] X-CSTP-Post-Auth-XML: <elided>
[2024-02-29 14:35:40] CSTP connected, DPD 300, Keepalive 300
[2024-02-29 14:35:40] UDP SO_SNDBUF: 256000
[2024-02-29 14:35:40] DTLS initialised. DPD 300, Keepalive 300
[2024-02-29 14:35:40] Established DTLS connection (using GnuTLS). Ciphersuite (D
TLS1.2)-(ECDHE-RSA)-(AES-256-GCM).
[2024-02-29 14:35:40] Configured as 10.231.179.225 + 2001:638:1558:e7b0::277/64,
with SSL connected and DTLS connected
[2024-02-29 14:35:40] Session authentication will expire at Thu Mar 14 14:35:40
2024
[2024-02-29 14:35:40] Continuing in background; pid 25892
root@ThinkPad-X230:/etc/ssl/certs#
```

Der VPN-Dienst läuft nach erfolgreichem Login im Hintergrund

Die verlässlichste Variante, das VPN zu beenden ist ein Neustart des Systems.

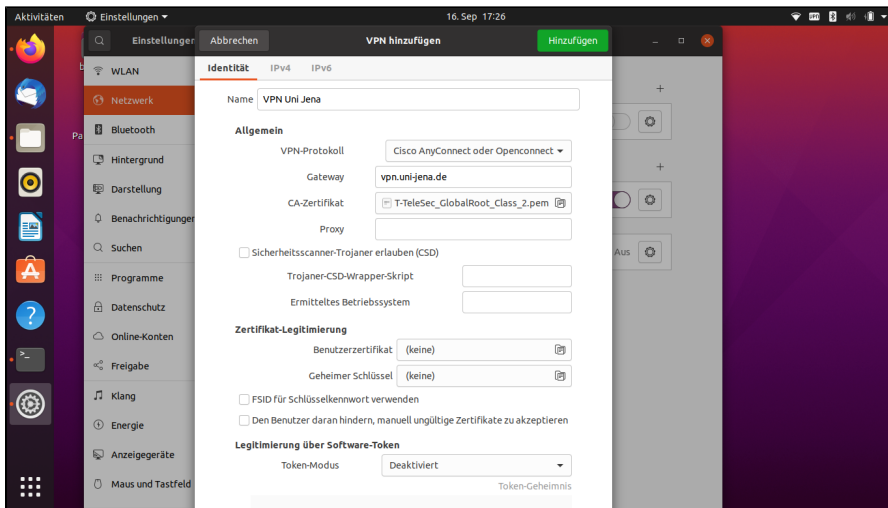
2. Schritt: VPN-Profil über den nativen Network-Manager konfigurieren

```
sudo openconnect -b --useragent 'AnyConnect' --user=ab12cde@uni-jena.de --pid-file=/var/run/vpn.pid --timestamp --syslog vpn.uni-jena.de
```

(zum Vergrößern auf das Bild klicken)

Unter Einstellungen (bei Ubuntu) finden Sie links einen Menüpunkt "Netzwerk" unter diesem ist der Abschnitt "VPN" zu finden. Über das kleine "+" können neue Verbindungen eingerichtet werden.

Jetzt ist der durch die Installation von OpenConnect hinzugekommene Punkt "Multiprotocol-VPN-Client (OpenConnect)" auszuwählen.



(zum Vergrößern auf das Bild klicken)

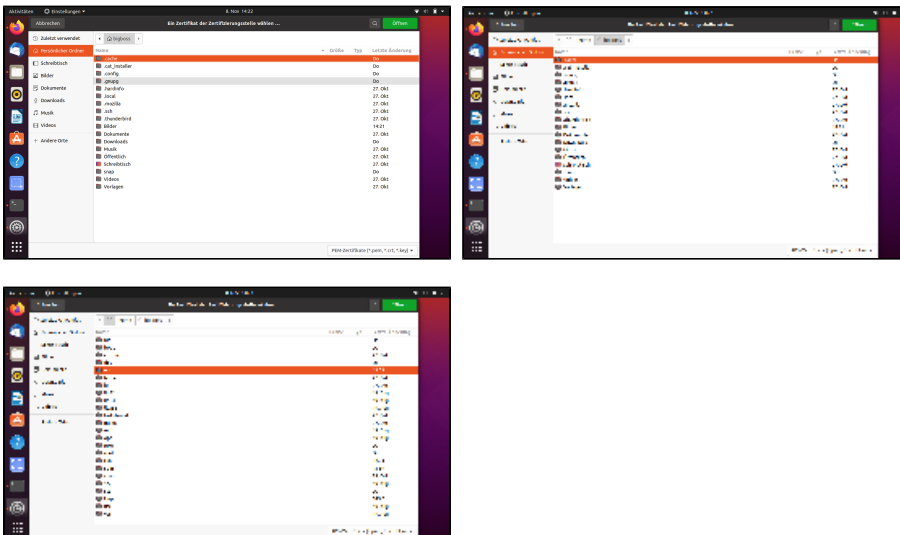
Anschließend kann der Name für dieses VPN-Profil vergeben werden. Weiterhin sollten die Einstellungen wie abgebildet lauten:

- VPN-Protokoll: Cisco AnyConnect oder OpenConnect
- Gateway: vpn.uni-jena.de
- CA-Zertifikat: /etc/ssl/certs/T-TeleSec_GlobalRoot_Class_2.pem

Sollte das Zertifikat nicht an diesem Speicherort zu finden sein, kann es über das Terminal nachinstalliert werden:

```
sudo -i
cd /etc/ssl/certs
wget https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.pem
```

(Befehle hintereinander ausführen)

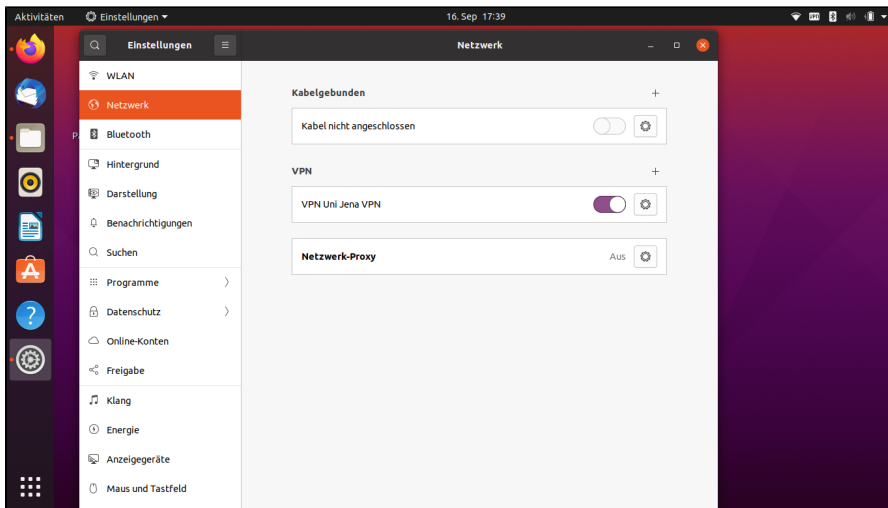


(zum Vergrößern auf das Bild klicken)

In das Root-Verzeichnis "/" (vergleichbar mit Festplatte C:\ unter Windows) gelangen Sie über das Festplattensymbol, welches Sie über den kleinen Pfeil links neben dem Namen Ihres Nutzerprofils sichtbar machen können.

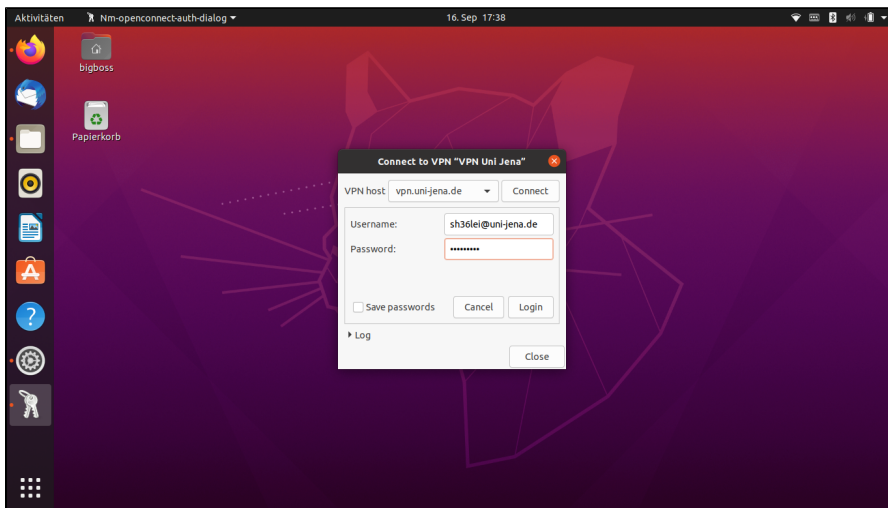
Über die Schaltfläche "Hinzufügen" ist das neue VPN-Profil gespeichert.

3. Schritt: VPN-Verbindung über eingerichtetes Profil aufbauen



(zum Vergrößern auf das Bild klicken)

Unter "Netzwerk" in den "Einstellungen" wird das jüngst eingerichtete Profil angezeigt. Über den Schalter kann die VPN-Verbindung aufgebaut werden.



(zum Vergrößern auf das Bild klicken)

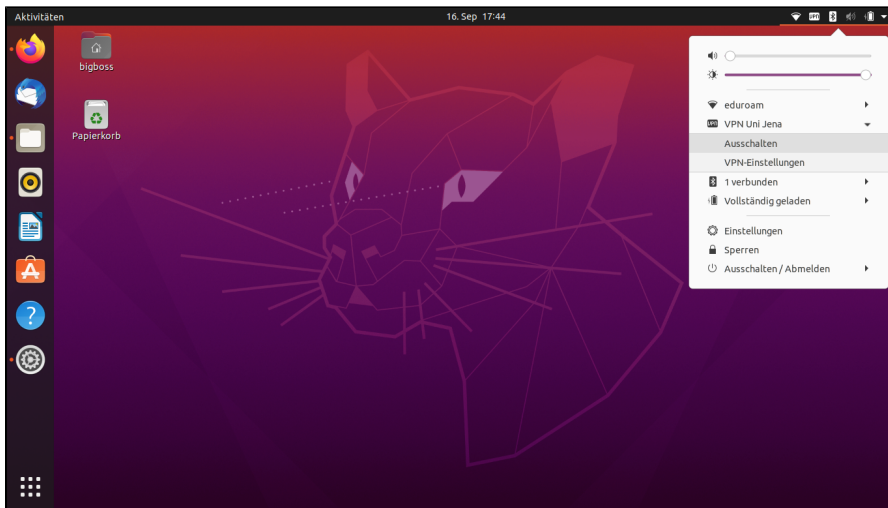
Bei der Abfrage der Credentials (Anmelde-Informationen) ist folgendes Schema zu beachten:

- Username: sh36lei@**uni-jena.de**
- Password: password

Nutzername und Passwort sind hier beispielhaft angegeben, ersetzen Sie diese bitte mit Ihren.

Nach einem Klick auf **[Login]** sind Sie mit dem VPN der Friedrich-Schiller-Universität Jena verbunden und können auf interne Inhalte zugreifen.

4. (optional) Schritt: VPN-Verbindung Schnellzugriff - Trennen /Verbinden



(zum Vergrößern auf das Bild klicken)

Über den kleinen Pfeil rechts oben ist das aktuelle VPN-Profil schnell zu erreichen und kann hier ein- und ausgeschaltet werden.



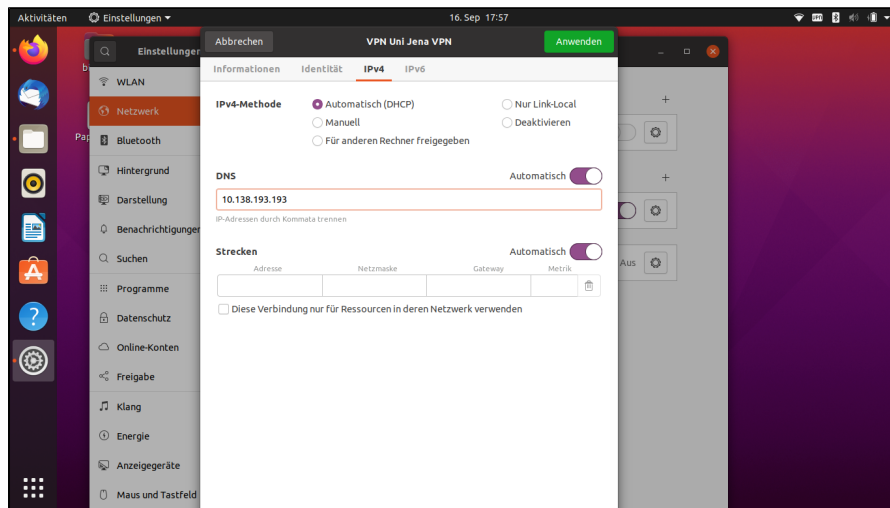
Es kann zu DNS-Problemen mit dem "openconnect Plugin" kommen.

Leider werden die Uni-DNS Server, die korrekt mittels "X-CSTP-DNS: 10.138.193.193" Header an den openconnect-Client übermittelt werden, nicht ins eigene System übernommen.

Das Problem tritt bei Archlinux mit dem NetworkManger-Plugin und auch der CLI-Version von openconnect auf. Auch ein aktuelles Ubuntu 20.04 zeigt mit dem NM-openconnect das gleiche Problem. Somit können dann universitätsinterne Server nicht aufgelöst und damit nicht erreicht werden.

Ein möglicher Workaround ist, im IPv4 Tab der Verbindungseinstellungen (siehe Abbildung) des VPN Profils unter "DNS Server" die Uni-DNS Server händisch einzutragen.

Dann werden diese auch beim Verbinden mit dem VPN im System übernommen und der Zugriff auf universitätsinterne Server ist per VPN möglich.



(zum Vergrößern auf das Bild klicken)

Titel: "Ubuntu (Linux) - VPN einrichten (OpenConnect)"

Stand: 11.11.2021