

VPN zur Verwendung von MFA konfigurieren

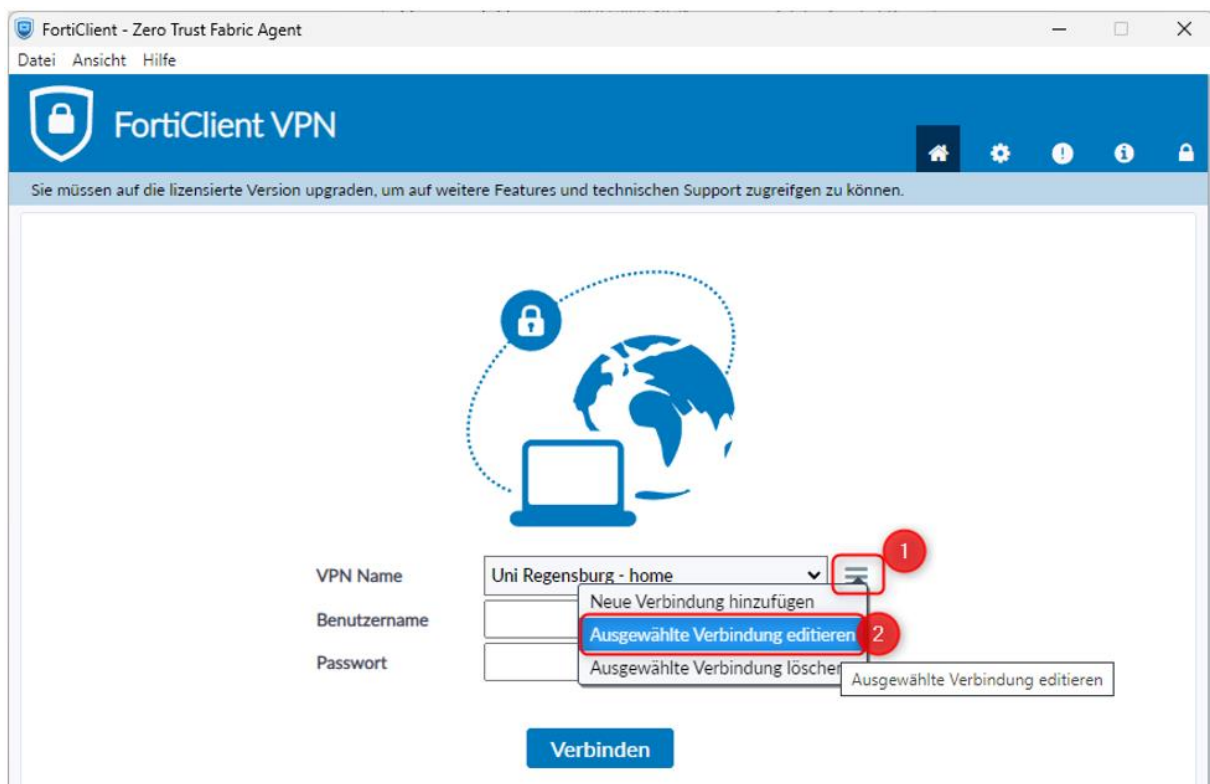
I Windows/MacOS: Konfiguration des VPN Profils im FortiClient

II Linux: Installation des openfortivpn

I Windows/MacOS: Konfiguration des VPN Profils im FortiClient

1. Öffnen Sie den FortiClient und bearbeiten Sie das gewünschte Profil, i.d.R. „**Uni Regensburg - home**“.

[Informationen zur Installation des FortiClient finden Sie unter <https://www.uni-regensburg.de/rechenzentrum/it-dienste/netzwerk-services/vpn-fuer-uni-interne-dienste>.]



2. Aktivieren Sie **Single Sign On (SSO)** sowie die Verwendung eines externen Browsers. Speichern Sie die Konfiguration durch Klick auf „**Sichern**“.

FortiClient - Zero Trust Fabric Agent

Datei Ansicht Hilfe

FortiClient VPN

Sie müssen auf die lizenzierte Version upgraden, um auf weitere Features und technischen Support zugreifen zu können.

VPN-Verbindung bearbeiten

VPN: **SSL-VPN** | IPsec VPN | XML

Verbindungsname: Uni Regensburg - home

Beschreibung: VPN UR home - tunnel all except local LAN

Remote Gateway:

+ Füge Remote Gateway hinzufügen

☒ Port anpassen

Single Sign On Settings:

- ☒ Aktiviere Single Sign On (SSO) für den VPN Tunnel
- ☒ Verwende externen Browser als User-Agent für SAML User Authentifizierung
- ☐ Enable auto-login with Azure Active Directory

Benutzerzertifikat:

☐ Aktiviere Dual-stack IPv4/IPv6 Adresse

Beim Aufbau der Verbindung mit dem Profil „**Uni Regensburg - home**“ erfolgt künftig keine Abfrage von Benutzernamen und Passwort im FortiClient. Über „Verbinden“ erfolgt künftig die Identifikation mit MFA.

FortiClient - Zero Trust Fabric Agent

Datei Ansicht Hilfe

FortiClient VPN

Sie müssen auf die lizenzierte Version upgraden, um auf weitere Features und technischen Support zugreifen zu können.



VPN Name:

II Linux: Installation des openfortivpn

Hinsichtlich Stabilität und Performance empfiehlt das Rechenzentrum den Einsatz von „**openfortivpn**“.

1. Vorbereitung und Installation

Hinweis:

Die Installation ist etwas aufwendiger als mit dem offiziellen Client, da die neuesten Binärdateien nicht in allen Repositories verfügbar sind und der Quellcode kompiliert werden muss.

```
sudo apt update
sudo apt install build-essential git autoconf automake pkg-config libssl-dev
git clone https://github.com/adrienverge/openfortivpn.git
cd openfortivpn
git checkout v1.23.1
./autogen.sh
./configure
make
sudo make install
```

Referenz:

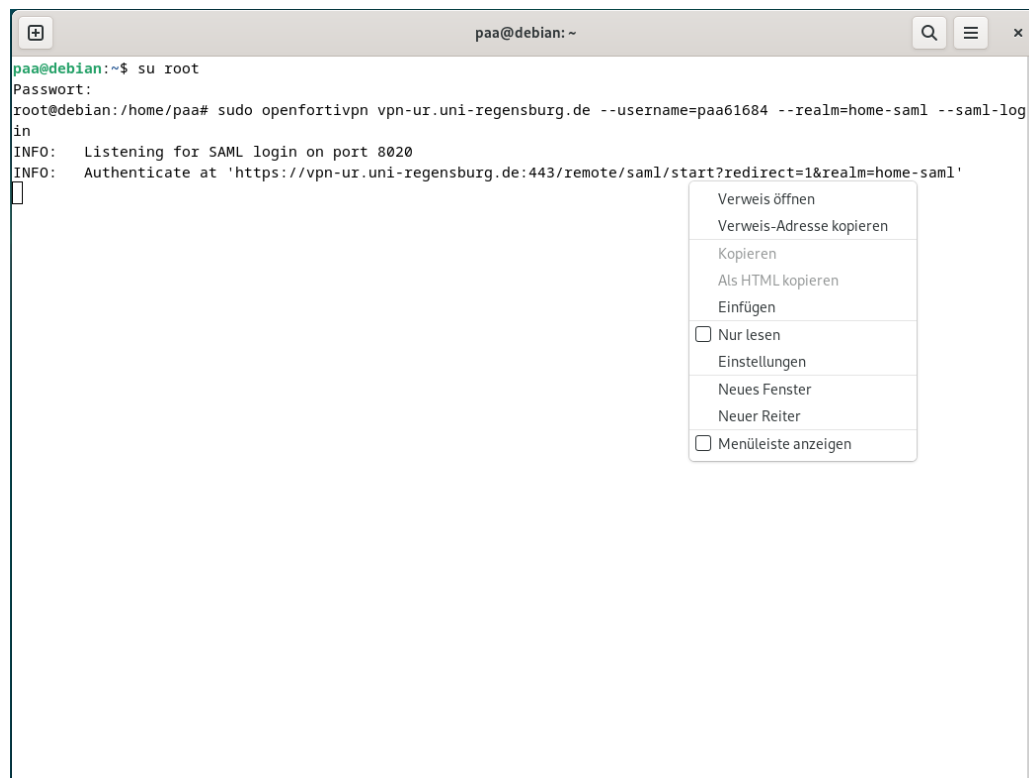
[openfortivpn - make Fortinet SSL VPN great again on Linux | nezhar.com](https://www.nezhar.com/en/make-fortinet-ssl-vpn-great-again-on-linux/)

2. Herstellen der VPN-Verbindung

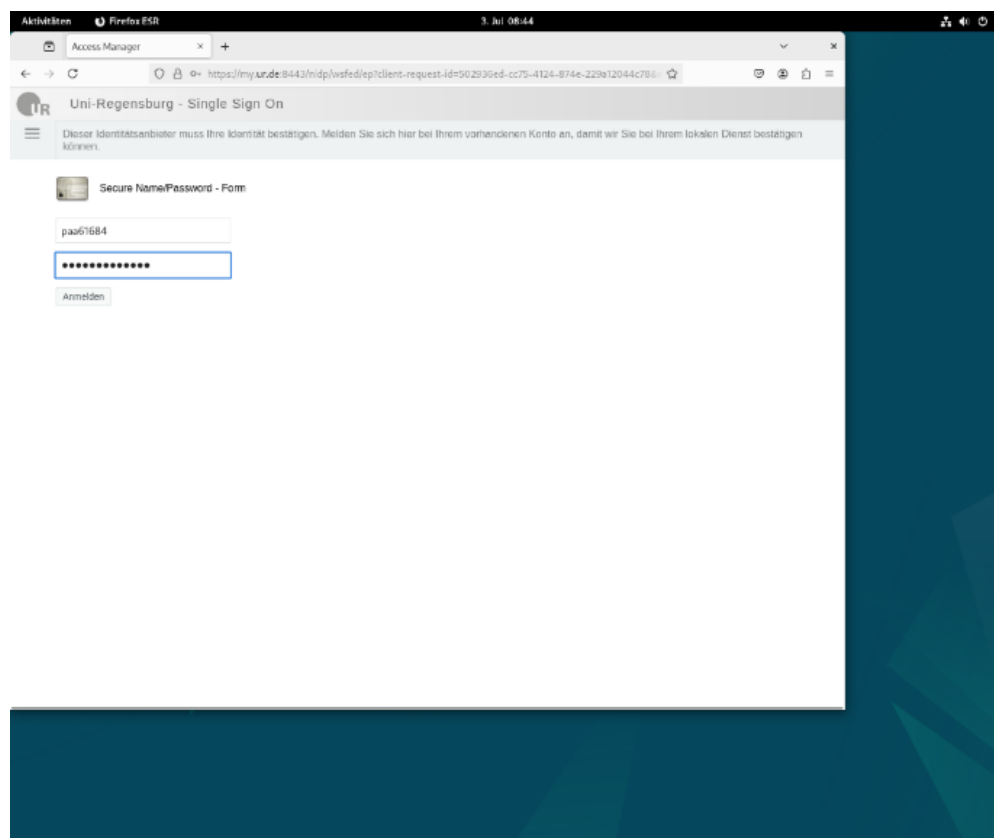
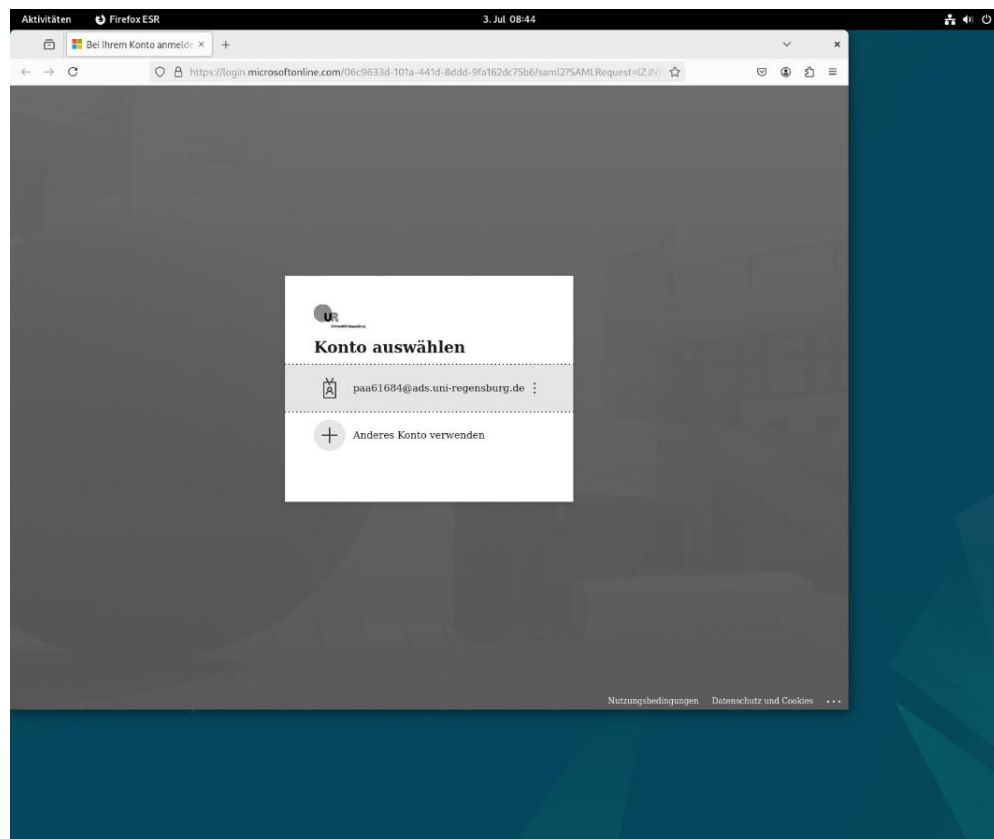
2.1 Befehl absetzen

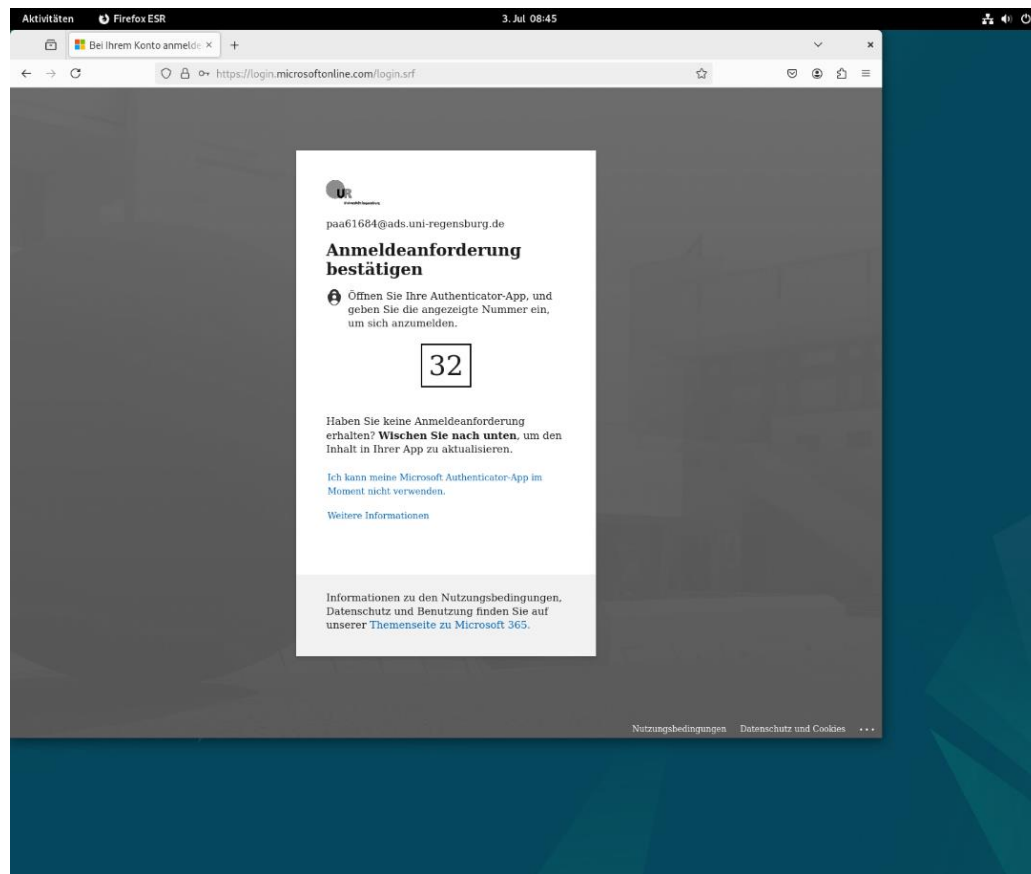
```
sudo openfortivpn vpn-ur.uni-regensburg.de --username=abc12345 --realm=home --saml-login
```

2.2 URL mit „Rechtsklick – Verweis öffnen“ aufrufen



2.3 Anmeldung am Microsoft Konto (MFA erforderlich)





2.4 Verbindung schlägt zunächst fehl, kann aber durch erneutes Ausführen des obenstehenden Befehls (2.1) aufgebaut werden. Dabei muss der Browsergeöffnet bleiben.

