VPN – Linux Ubuntu 22.4.1

VPN is short for **V**irtual **P**rivate **N**etwork and helps create a secure and encrypted connection via the public internet. A condition for setting up such a connection is an existing internet connection. Furthermore, the protocol should not be blocked by the local provider.

In addition to the encryption, the client is allocated an IP-address from the address range of the University of Bonn once a VPN connection is established. Thereby, you gain access to services that are otherwise restricted to University computers.

A VPN connection can only be created after successful **authentication** with the **Uni-ID of the University of Bonn**.

This VPN connection is necessary in the following cases:

- using the BONNET WiFi at the University of Bonn
- using the majority of literature databases and electronic journals (eMedia) from home or otherwise
- working from home

Please not that a service might be restricted further and that a VPN is not always sufficient for access.

Content of this manual:

Current version: 02/2025

Setting up the VPN:

To set up the VPN access, download and install the client. Depending on the connection you want, enter one of the following addresses into the client.

- **external** connections/ from home:

  unibn-vpn.uni-bonn.de
- **internal** connections from within the university network:

  unibn-wlan.uni-bonn.de

Attention! These are server addresses and not website links. Thus, they have to be entered into the **address bar of the VPN client** and not into the browser.

The distributions given here are those under which the instructions have been tested. In case of major changes, we will adapt the instructions.
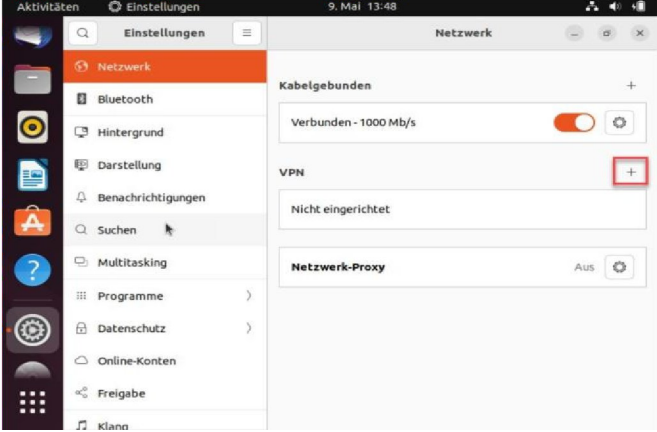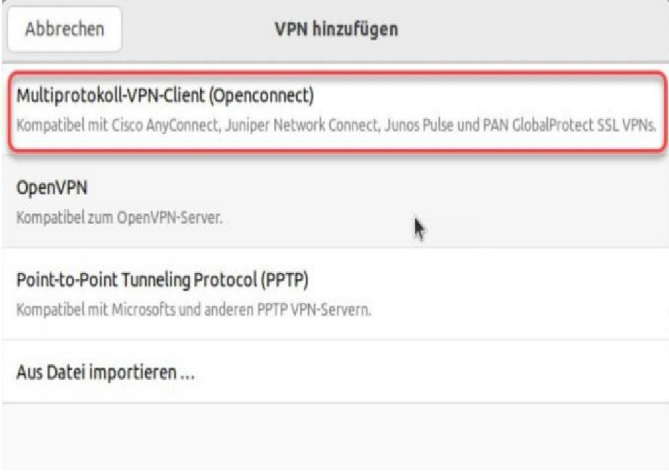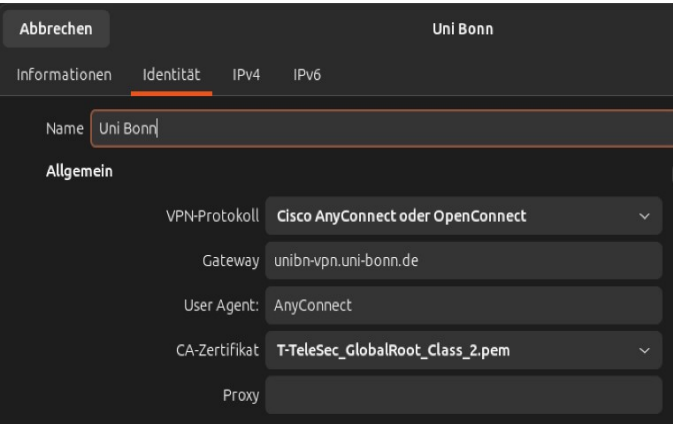
Instructions using openConnect.

Downloading and installing the VPN client
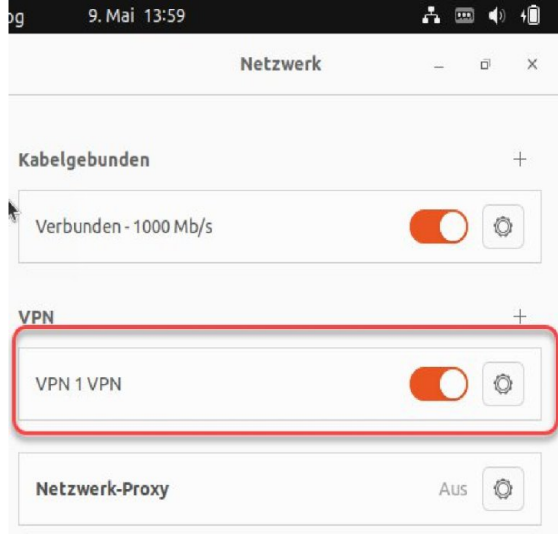
Prerequisites

- A valid Uni-ID of the University of Bonn n
- A stable internet connection (WiFi/ mobile or network cable)

1	Opening a terminal window using e.g. <STRG><ALT><T> .

2	Entering the following command:
	`sudo apt install network-manager-openconnect`
	`sudo apt install network-manager-openconnect-gnome`

3	Enter the admin password and install.
4	Now restart the computer.

Current version: 02/2025

5	Select the settings for the "**Network**" via "**Activities/ System Settings**" and click the +-symbol next to VPN.	
6	Select **"Multiprotokoll-VPN-Client (Openconnect)"**.	
7	Use the following settings: **Name**: any **VPN protocol**: Cisco AnyConnect or OpenConnect **Gateway** (for external connections): **unibn-vpn.uni-bonn.de** **CA-certificate**: select via search under /etc/ssl/certs/T-TeleSec_GlobalRoot_Class_2.perm The field "**User Agent**" should also pop up here, and should be filled with "**AnyConnect**".	

Current version: 02/2025

	If this field is not shown, please enter the following into the terminal and repeat the installation steps from the beginning: `sudo apt remove openconnect` If the field still does not pop up, your system does not support it and you will have to log in via the command line.	
8	Leave everything else as is and add the connection save the button "**Add**".	

Using the VPN client

1	Now the VPN connection can be easily turned on and off via the switch.	
2	For the authentification enter the Uni-ID (without @uni-bonn.de) and the password and click the button "**Connect**".	

Further notices:

If you want to use the VPN client within the university network, e.g. To use certain services, you will have to add another VPN connection according to the instruction above. Every input is the same except that now: **unibn-wlan.uni-bonn.de** has to be entered as gateway.

Current version: 02/2025