REGIONALES RECHENZENTRUM ERLANGEN [RRZE]
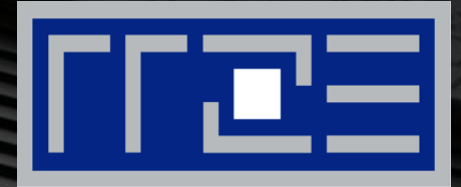
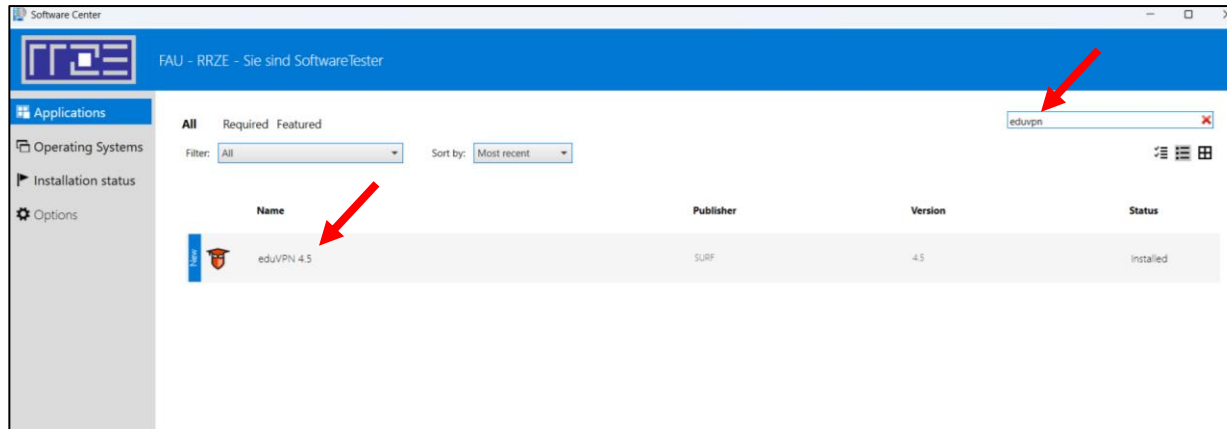## Installation and configuration of the eduVPN client

Installation on Managed Devices
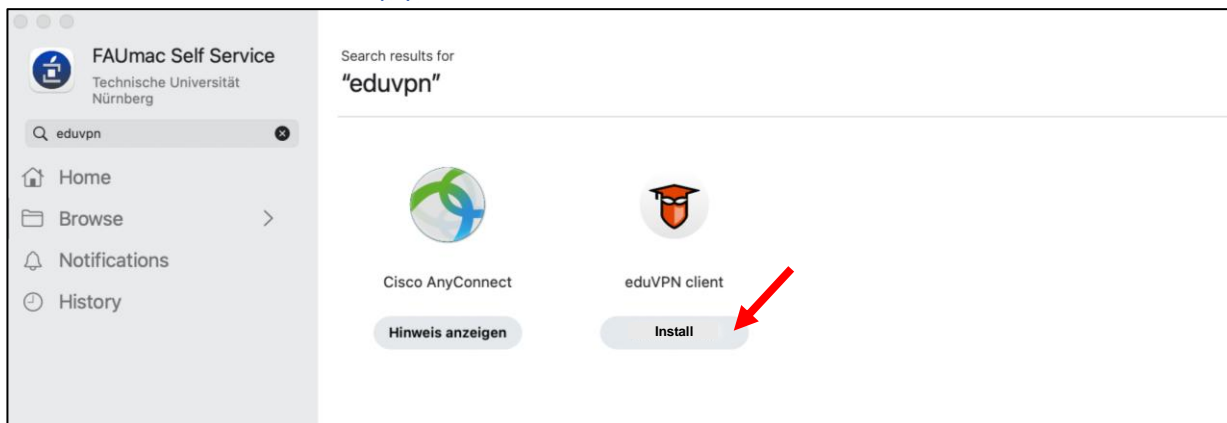
Managed Devices

WinSV/Softwarecenter (1):


FAUmac Self Service (2):

- If your computer is managed by an IZ* or if software management is handled by your institution (e.g., via WinSV (1) or FAUmac Self Service (2)), please do not install the client manually.

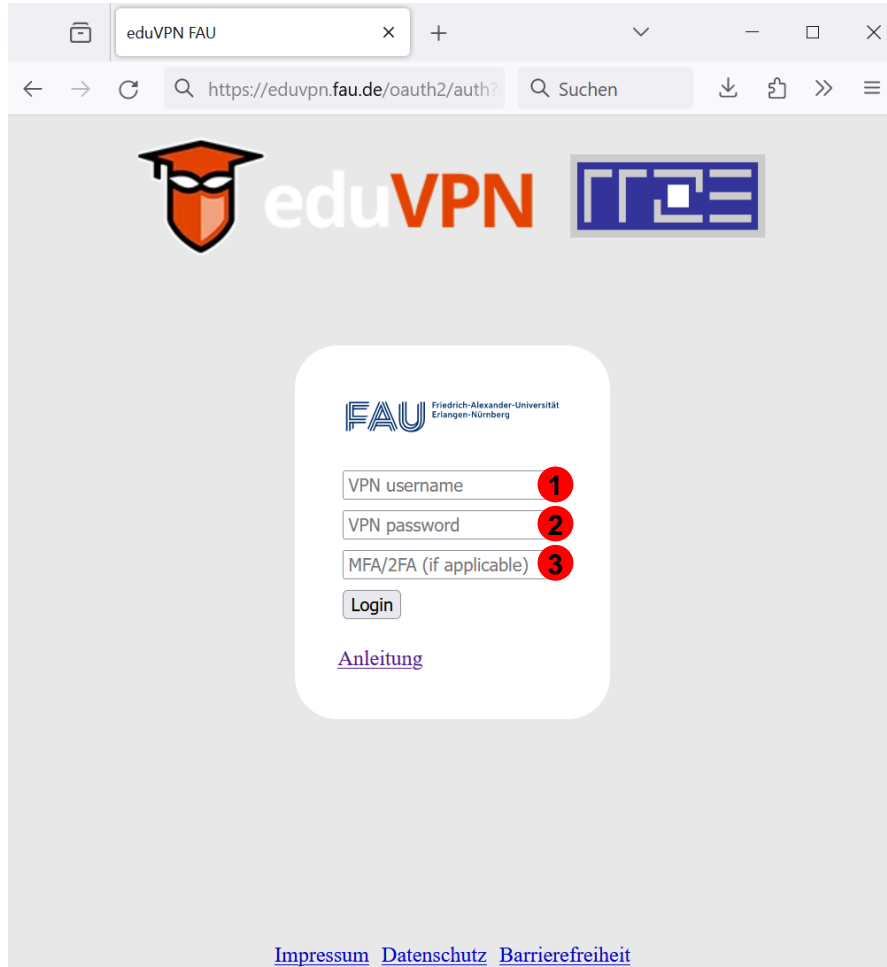- Use the installation method specified by your IT support instead.

Manual Installation and Configuration

Unmanaged / Private Devices

For devices not centrally managed / private devices:

- Download the client from the following link:https://www.eduvpn.org

Configuration
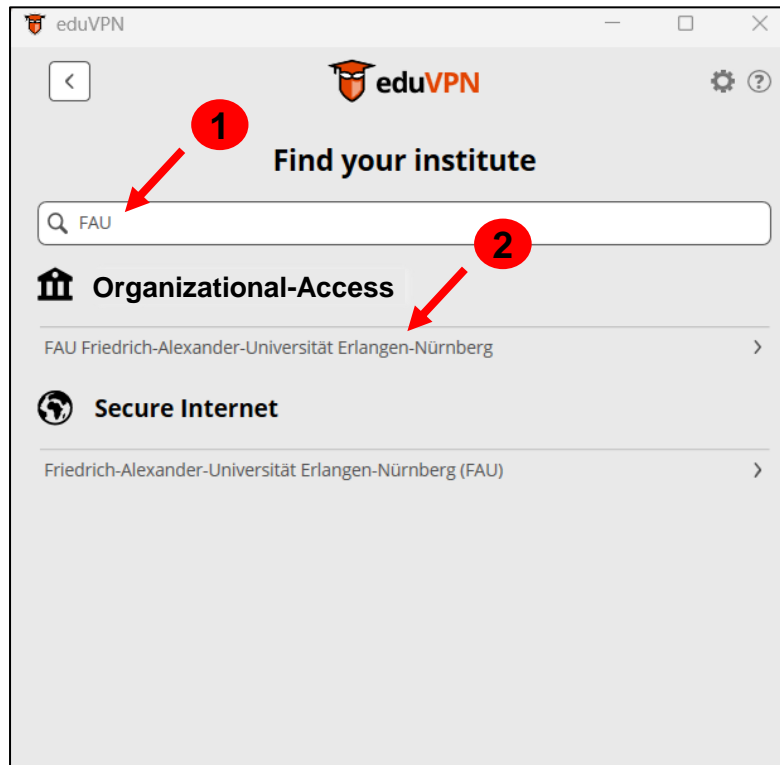
- Start „eduVPN-Client"
- Search for „FAU" (1)
- Under "Organizational-Access," click on "FAU Friedrich-Alexander-Universität Erlangen-Nürnberg" (2).
- A browser window will then open automatically.

Configuration

- Enter your IdM unsername in the browser window(1).
- Enter your IdM password (2).
- If you have activated MFA in the IdM portal, enter your second factor (3).
- Click „Login".

Configuration
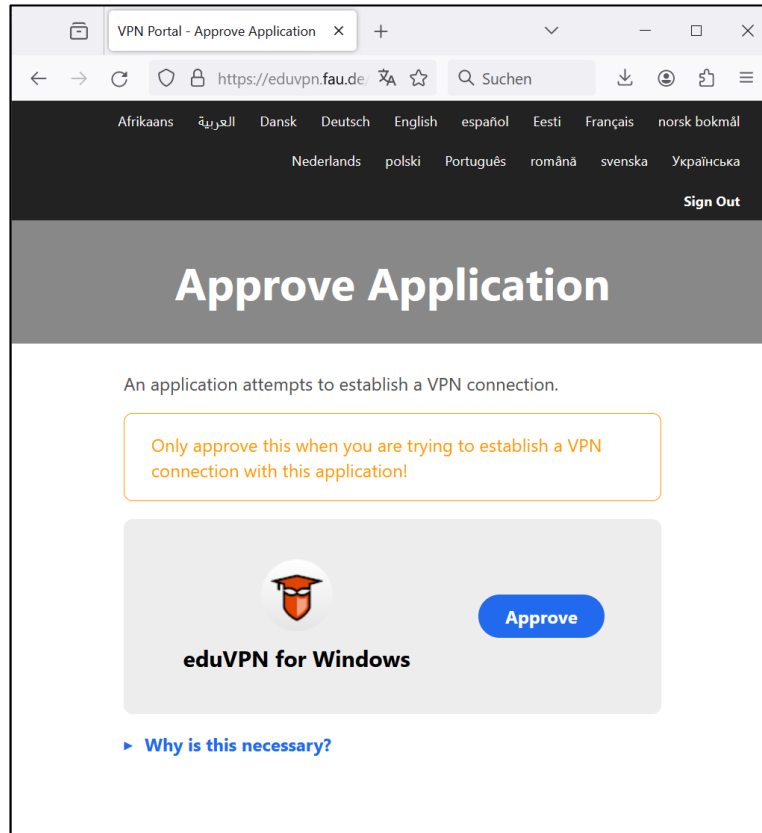
- Click "Approve" to complete the process.
- You can then close the browser window and return to eduVPN.

Configuration
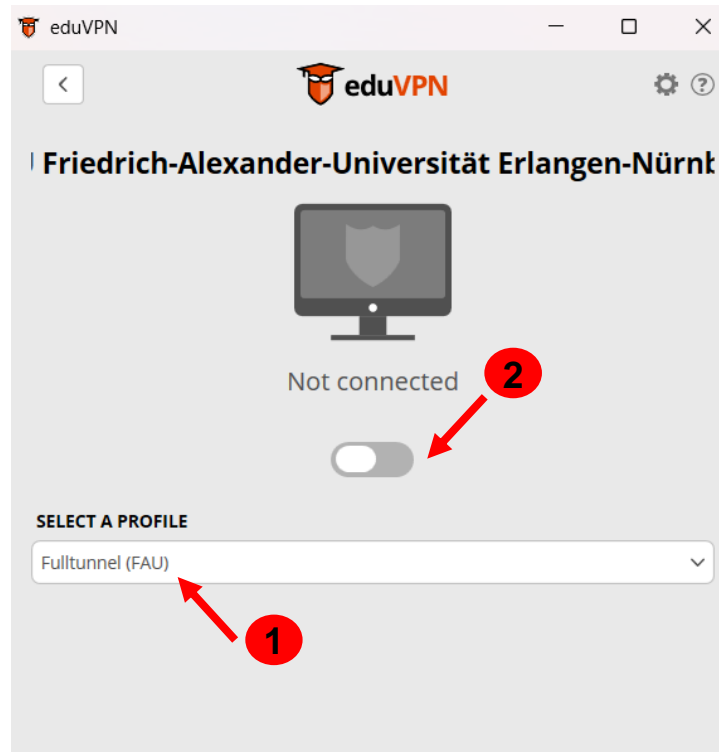
- Under „Select a profile" select either the full tunnel or the split tunnel (1) (see the Info-VPN slide for details).

- Click the „slider" to establish the connection (2).

Configuration
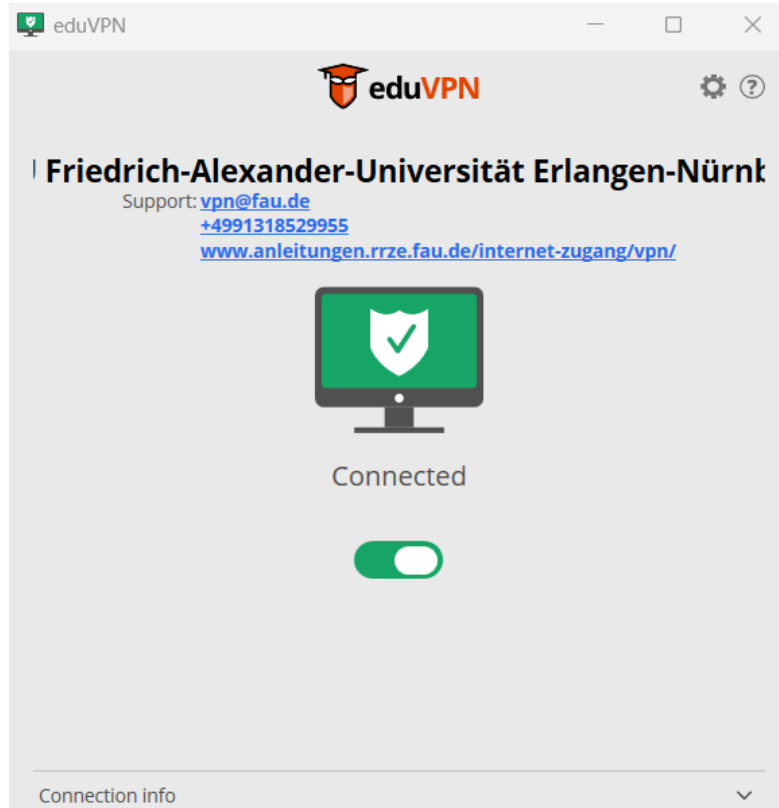
- The connection has been successfully established.

- The login remains valid on this device for one week.
- During this time, you can connect to or disconnect from the VPN at any moment using the slider.
- You do not need to log out—the slider's position is preserved even after restarting the computer.

FAU-Full-Tunnel

- This setting sends all IP data packets through the tunnel to the FAU VPN server. Internet access remains possible, but all traffic is routed "through" FAU. For access to certain electronic resources, this rerouting is essential to prove your affiliation with FAU. With this profile, you can also conceal your internet activity when using public or guest networks.

FAU-Split-Tunnel

- Use this setting only if you need to access FAU services and must also communicate directly with other internet services. Data sent to destinations within FAU will be routed through the secure tunnel, while all other internet traffic will go directly to its destination as usual. However, this setting carries an increased risk of infecting FAU or institute systems with malware.

More information: https://www.rrze.fau.de/internet-e-mail/internet-zugang/vpn/