

## Unifi servers

### Server names

usg-vpn.sb.dfki.de and usg-vpn2.sb.dfki.de

We recommend to setup VPN connection profiles for both servers, there is no automated load balancing.

### Client OS and software

- MacOS (native built-in client)
- Linux
- Windows (native built-in client)

### Setup

#### MacOS

- Preferences > Network -> add
- Interface VPN, VPN type: "L2TP over IPSec, choose a connection service name
- Server Address usg-vpn.sb.dfki.de or usg-vpn2.sb.dfki.de
- Account Name your DFKI according to the scheme abcd01
- Click "Authentication Settings" and add the "Shared Secret" to "Machine Authentication": DFKI-VPN
- Leave "GroupName" empty, choose whether to store your user password ("User Authentication")
- Click "Advanced Options", Session Options: activate "Send all traffic over VPN connection"

#### Windows

- Settings -> Network and Internet -> VPN -> + Add VPN connection
- VPN provider: "Windows (integrated)"
- Connection name: your choice (e.g.: "DFKI VPN")
- Server Address: usg-vpn.sb.dfki.de or usg-vpn2.sb.dfki.de
- VPN type: "L2TP/IPSec with preinstalled key"
- Preinstalled key: DFKI-VPN
- Login information type: "User name and password"
- Click on "Save". The window closes and the settings are visible again.
- Now click on "Change adapter options" in the right sidebar under "Related settings".
- Right click on the VPN connection just created, then "Properties"
- Select "Security" tab
- Under "Authentication" and "Allow the following protocols2 **only** select Microsoft Chap Version 2 (MS-CHAP-v2)
- click on "OK" and establish the connection. Log in with myDFKI user name according to the scheme "abcd01". We recommend a LAN(Ethernet) connection.

#### Linux

Setup package specific, please use the setup parameters given above.

## Cisco VPN server

Server name

vpn.dfki.de

Client OS and software

- MacOS (native built-in client)
- Linux (any IPsec Xauth PSK capable package)
- Windows (additional Cisco AnyConnect necessary)

Setup

### Mac OS

- Preferences > Network -> add
- Interface VPN, VPN type: Cisco IPSec, choose a connection service name
- Server Address vpn.dfki.de
- Account name : DFKI account abcd01
- Authentication Settings: Group Name = Wavelan
- Shared Secret = Wavelan

### Windows

- Installation Cisco AnyConnect required (download in Teams site team available)
- Server Address vpn.dfki.de

### Linux

Setup package specific, please use the parameters

- VPN server: *vpn.dfki.de*
- Group access identifier: Select group (e.g. Wavelan for non split tunnel)
- Group password: corresponds to the name of the group profile (here: Wavelan)
- Username: User name of the myDFKI account
- Password: Password of the myDFKI account