VPN Access to the UIBK network

ZID offers VPN access to the internal uibk network (138.232.x.x; Class B) which is necessary for some services (License Servers, Mounting Shared Folders, Library Access, ...).

Note: for some services an additionally authentication against the zid firewall is necessary: https://fwauth-tech.uibk.ac.at.

Web-Access

https://vpn.uibk.ac.at

Tools and Settings

Name	Description
VPNC	vpnc is a VPN client for the Cisco 3000 VPN Concentrator, creating a IPSec-like connection as a tunneling network device for the local system (man vpnc)
OpenConnect	OpenConnect is a VPN client, that utilizes TLS and DTLS for secure session establishment, and is compatible with the CISCO AnyConnect SSL VPN protocol (https://openconnect.github.io/)
AnyConnect	Software provided by Cisco. The ZID recommends using AnyConnect.
Advanced Settings	
Additional Resources	

VPNC

Settings:

```
Gateway: vpn1.uibk.ac.at
User: c703XXX
Pass: YourC703XXX-Password
Group name: uibk.ac.at
Group password: vpn2001-zugang
```

The username is your c-Number and user password is your password.

On Ubuntu system (version > 10.11) you have to restart the network-manager (or best just reboot your system) before you can connect with gnome vpnc network manager.

Installation on Debian based systems:

```
aptitude install network-manager-vpnc network-manager-vpnc-gnome vpnc
```

should install all necessary tools.

To configure vpn, just add a new vpn connnection → choose cisco compatible vpn (vpnc)

Openconnect

There is also a vpn client called openconnect: again there is a Debian package:

```
aptitude install openconnect
```

You can then start a VPN connection with [1)]

```
/usr/bin/openconnect vpn.uibk.ac.at
```

AnyConnect

visit https://vpn.uibk.ac.at in a browser.

Just logon with your credentials

```
username = c703xxx
password = your uibk password
```

Start AnyConnect.

After the initial installation a new 'AnyConnect' menu entry should appear in

```
applications -> internet
```

This entry starts a new vpn session.

Advanced Settings

VPN Split-Tunneling and Session Timeout

you can append and combine following options to your c-number:

Option	Description
_split	aktivate Split-Tunneling. Only traffic to the university IP's is using the VPN-Tunnel. Other traffic is direct.
_long	Extend the max. Session Timeout: 2 days instead of 10h

E.g.: using `cXXXXX_split_long` provides a long-session split-tunnel vpn connection.

Additional Resources in German

Installation, FAQ: VPN-Zugang zum INNET

1)
With pre-wheezy Debian, you additionally have to download a script called `vpn-script` -

downloadable from

```
http://www.infradead.org/openconnect/vpnc-script.html
```

to start the vpn-connection:

```
/usr/bin/openconnect --script vpnc-script vpn.uibk.ac.at
```