VPN (Virtual Private Network) at the Free University of Bolzano/Bozen and EURAC

Infos regarding the usage of VPN

https://knowledge.scientificnet.org/workspace/#nd=ab7442f9-c4d0-4ffc-a4f7-1e0d84515cc9&ld=17f4d8ce-edff-4d42-ad33-d98e2cdebc35&ln=it

Instructions for MacOS X

We recommend to download and install Cisco AnyConnect from Apple Store for iOS and connect via Browser to https://vpn.scientificnet.org for Mac OSX

Unsupported Instructions for MacOS X and iOS - use at own risk!

Download, unpack (doubleclick), then doupleclick the unpacked file to install it:

vpn-scientificnet.org.networkconnect.zip

Under Network settings a new item should appear:

- VPN (IPSec)
- change username to your username
- click Connect and enter your password

Uninstalling if installation is corrupt in MacOSx

Uninstallation has to be done by running this command on terminal:

sudo /opt/cisco/vpn/bin/vpn_uninstall.sh

Should the uninstallation or reinstallation be corrupt, run this command on terminal:

sudo pkgutil –forget com.cisco.pkg.anyconnect.vpn

Instructions for iOS 9

1. Press Settings
2. Choose General
3. Nearly at the end, click VPN
4. Next click: Add VPN Configuration...
    1. **Type:** IPSec
    2. **Description:** VPN Scientificnet

3. **Server:** vpn.scientificnet.org
4. **Account:** <your-unibz-username>
5. **Password:** <your-unibz-password> or leave empty to ask every time!
6. **Group Name:** Unibz
7. **Secret:**

```
NrW2z9sj8g3kjJrzXxJwRPbIRNInWakL
```

5. Press Done in upper right corner of window
6. Status: Slide Button to the right to connect
7. Enter Password if not already entered above

Instructions for Android 7

1. Press Settings
2. Find VPN Settings, depends on Model
3. Next click: Add VPN Configuration...
    1. **Name:** Unibz VPN
    2. **Type:** IPSec Xauth PSK
    3. **Server-Address:** vpn.scientificnet.org
    4. **IPSec Identifier:** Unibz
    5. **IPSec Pre-shared Key:** NrW2z9sj8g3kjJrzXxJwRPbIRNInWakL
    6. **Account:** <your-unibz-username>
    7. **Password:** <your-unibz-password> or leave empty to ask every time!

1. Press Done
2. Status: Slide Button to the right to connect
3. Enter Password if not already entered above

Instructions for Linux using openconnect Client (recommended)

Run this command to install openconnect client and OpenConnect plugin GNOME GUI

```
sudo apt install openconnect network-manager-openconnect network-manager-openconnect-gnome
```

Once installed open Settings and go to Network, press + right of the VPN section.

Select **Cisco AnyConnect Compatible VPN (openconnect)** and fill out as shown below:

Details

1. Make available to other users: tick if you want to allow other users on your system to use the VPN

Identity

1. Name: VPN work (use a descriptive name)
2. VPN Protocol: Cisco AnyConnect
3. Gateway: vpn.scientificnet.org
4. CA Certificate: download from here , not really necessary!

The rest can be left as it is.

IPv4/IPv6

1. IPv4 Method: Automatic (DHCP)
2. DNS: ON
3. Routes: ON

Press Apply

Now you can enable the VPN connection!

Move the slider from OFF to ON, a small window should open,

make sure that for VPN Host you select: **vpn.scientificnet.org**

Enter your unibz Username, without @unibz.it and your unibz Password.

Press **Login**

If all goes well the slider should remain in ON position, if not check the Log. To verify launch this command in a terminal:

```
ifconfig | grep 172*
```

You should get a new interface –> vpn0: with an IP Address: 172.21.66.xxx

Instructions for Linux vpnc Client

1. Install vpnc

```
sudo apt-get install vpnc
```

2. For Unibz:

- Create configuration file unibz.conf. Download from here: unibz.conf

2.a For Eurac:

- Create configuration file eurac.conf. Download from here: eurac.conf

IPSec obfuscated secret needs to be on a single line.
Replace <your-windows-login> with your username.

For Unibz:

```
sudo vi /etc/vpnc/unibz.conf
```

```
########################################
IPSec gateway vpn.unibz.it
IPSec ID Unibz
IPSec obfuscated secret
06294C134E0BEBDA4B449B56BFD305D35D12DABF4044EDB6794926C2CA6D5AEDFE6342DF190E
566EB11215DDC1591D5CB6ABEBEB593693C6D0B2077D78034B6AFEEA3221E77F4C9858DD711A
A8DE58F6
Xauth username your-windows-login
# e.g. Xauth username fmoser (not fmoser@unibz.it)
########################################
```

apply this rights:

```
sudo chmod 600 /etc/vpnc/unibz.conf

sudo chown root.root /etc/vpnc/unibz.conf
```

```
sudo ls -l /etc/vpnc/unibz.conf
-rw------- 1 root root 250 2009-05-02 15:54 /etc/vpnc/unibz.conf
```

For Eurac:

```
sudo vi /etc/vpnc/eurac.conf
```

```
########################################
IPSec gateway vpn.scientificnet.org
IPSec ID Eurac
IPSec obfuscated secret
56A1CD68CC3AD33B48DB0F727ADDBC0A354DE3287D15C8526ED4CEDE4BC2ACDD1BB2460BC235
4671A405F6150EA7C294C4DBC4CF9FFE45873BECAD3A2A738C5053BE34F709D592B50AD5BC47
2CDFF350
Xauth username your-windows-login
# e.g. Xauth username fmoser (not fmoser@eurac.edu)
########################################
```

apply this rights:

```
sudo chmod 600 /etc/vpnc/eurac.conf

sudo chown root.root /etc/vpnc/eurac.conf
```

```
sudo ls -l /etc/vpnc/eurac.conf
-rw------- 1 root root 250 2009-05-02 15:54 /etc/vpnc/eurac.conf
```

3. Start vpnc

For Unibz:

```
sudo vpnc-connect --domain unibz unibz
```

This will first ask for your sudo password and then your <unibz-password>

For Eurac:

```
sudo vpnc-connect --domain eurac eurac
```

This will first ask for your sudo password and then your <eurac-password>

4. Stop vpnc

```
sudo vpnc-disconnect
```

Possible errors

If you get the following error: **vpnc-connect: no response from target**
try adding the line below to your configuration file (unibz.conf)

NAT Traversal Mode cisco-udp

When one attempts to connect to their VPN after installing and configuring vpnc on Ubuntu Oneiric, the following error occurs:

```
root@ubuntu:~# vpnc-connect
Error: either "to" is duplicate, or "ipid" is a garbage.
```

It appears that the Ubuntu package vpnc comes with an old version of vpnc-script.
This script is what sets up all the addresses and routes for you. The OpenConnect project provides an updated / revised release of this script. Download the latest copy from here.
Replace the vpnc-script script that comes with the Ubuntu vpnc package: /etc/vpnc/vpnc-script

---

Access via ssh not possible, MTU value to high!

In some cases the MTU value is too high, which results in an very strange situation: ping works, but

ssh hangs at this point:

... debug1: sending SSH2_MSG_KEX_ECDH_INIT debug1: expecting SSH2_MSG_KEX_ECDH_REPLY

There are 2 bug reports for this:

https://bugs.launchpad.net/ubuntu/+source/network-manager/+bug/1110787
https://bugs.launchpad.net/ubuntu/+source/openssh/+bug/1254085

and a possible solution/workaround for Linux Mint:

https://community.hide.me/threads/setup-problem-on-linux-mint-17.1839/

Check the current MTU value:

```
ip link | grep mtu
```

Set MTU value on interface eth0 to 1392

```
/sbin/ifconfig eth0 mtu 1392
```

Allow local (LAN) access when using VPN (MacOS)

Decode Group Password

cisco vpnclient password decoder

Instructions for Linux Cisco AnyConnect Client

Installation

1. Open with your browser (tested with firefox 11.0) the following URL:

https://vpn.scientificnet.org

2. Enter your Username and password, then press **Login**

3. A “Warning - Security” Windows opens: This will install the Cisco AnyConnect Client in /opt/cisco of your Platform.

4. Press **Run** on the “Warning - Security” Window

5. In order to install Cisco AnyConnect, Admin (sudo) rights are required; a Window opens,

enter your local password.



6. The Cisco AnyConnect is installed and running, you can close the URL.



Launching Cisco AnyConnect GUI

This allows you to connect and disconnect the VPN service.

```
/opt/cisco/anyconnect/bin/vpnui
```

Please note the vpnagentd must be running for this

- ps auxww | grep vpn

```
root      1759  0.0  0.3  17984  7644 ?        S    12:58   0:00
/opt/cisco/anyconnect/bin/vpnagentd
```

Launching Cisco AnyConnect NON-GUI

This allows you to connect and disconnect the VPN service.

- /opt/cisco/anyconnect/bin/vpn

```
Cisco AnyConnect Secure Mobility Client (version 3.0.5080) .

Copyright (c) 2004 - 2011 Cisco Systems, Inc.
All Rights Reserved.


  >> state: Disconnected
  >> state: Disconnected
  >> notice: Ready to connect.
  >> registered with local VPN subsystem.
VPN> connect vpn.unibz.it
connect vpn.unibz.it
  >> contacting host (vpn.unibz.it) for login information...
  >> notice: Contacting vpn.unibz.it.
VPN>
  >> Please enter your username and password.
    0) clientless
    1) scientificnetwork
Group: [clientless]

Username: <your-username>
Password:
```

```
  >> state: Connecting
  >> notice: Establishing VPN session...
  >> notice: Checking for profile updates...
  >> notice: Checking for product updates...
  >> notice: Checking for customization updates...
  >> notice: Performing any required updates...
  >> state: Connecting
  >> notice: Establishing VPN session...
  >> notice: Establishing VPN - Initiating connection...
  >> notice: Establishing VPN - Examining system...
  >> notice: Establishing VPN - Activating VPN adapter...
  >> notice: Establishing VPN - Configuring system...
  >> notice: Establishing VPN...
  >> state: Connected
  >> notice: Connected to vpn.unibz.it.
VPN>exit
```

Uninstalling the AnyConnect Client

The client comes with an uninstallation script

- sudo /opt/cisco/vpn/bin/vpn_uninstall.sh

However it doesn't actually uninstall everything properly, it removes files but leaves behind directories.
You can clean up what it leaves behind by deleting the directory /opt/cisco/ and /opt/.cisco/

- sudo rm -r /opt/cisco /opt/.cisco

Per-user configuration is stored in your home directory in a file called .anyconnect

Install openconnect-sso macOS with SAML

If you don't want to use Cisco Anyconnect on the Apple Mac, you can install openconnect and openconnect-sso for using SAML!

Requirements: Python3

Install brew

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Install openconnect and pipx

```
brew install openconnect pipx
```

```
pipx ensurepath
```

Install pipx

```
pip install --user pipx
```

Install openconnect-sso

```
pipx install "openconnect-sso[full]"
pipx ensurepath
```

Launch openconnect-sso

```
/Users/user/.local/bin/openconnect-sso --server vpn.scientificnet.org/saml
```

```
...
...
[info     ] Loading page                    [webengine]
url=https://vpn.scientificnet.org/+CSCOE+/saml/sp/login?tgname=ScientificNet
workSouthTyrol-SAML&acsamlcap=v2
[info     ] Terminate requested.            [webengine]
[info     ] Exiting browser                 [webengine]
[info     ] Browser exited                  [openconnect_sso.browser.browser]
[info     ] Response received               [openconnect_sso.authenticator]
id=success message=
[sudo] password for <local-username>:

Connected to 193.106.xxx.xxx:443
SSL negotiation with vpn.scientificnet.org
Server certificate verify failed: signer not found
Connected to HTTPS on vpn.scientificnet.org
Got CONNECT response: HTTP/1.1 200 OK
CSTP connected. DPD 30, Keepalive 20
Connected as 172.xx.xx.xx + 2a02:27e8:10:741:0:dacc:0:2/64, using SSL, with
DTLS in progress
Established DTLS connection (using GnuTLS). Ciphersuite (DTLS1.2)-(ECDHE-
RSA)-(AES-256-GCM).
Error: any valid prefix is expected rather than "dev".
```

A browser-window will ask for your username and password, next it will ask for the PIN which you need to generate with an Authenticator!

Last thing to enter is the sudo password to enable the network interface.

From:
https://wiki.inf.unibz.it/ - **Engineering-Tech Wiki**

Permanent link:
https://wiki.inf.unibz.it/doku.php?id=auth:howto:linux:vpnclient&rev=1651846925

Last update: **2022/05/06 16:22**