VPNs
How to confuse your routing tables

VPNs
How to confuse your routing tables

#balccon2k17

@MacLemon

VPN

Virtual **P**rivate **N**etwork

Why?

VPN Solutions

Protocols

PPTP

Point-to-Point Tunneling Protocol

L2TP
L2TP/IPSec

Layer 2 Tunneling Protocol

IPSec IKEv1

IPSec, Internet Key Exchange v1

OpenVPN

Community Edition

IPSec IKEv2

IPSec, Internet Key Exchange v2

VPN Provider

THAT ONE PRIVACY SITE

Welcome

VPN Section

Email Section

Reviews / Blog

FAQs

Donate

Contact

About

Search...

VPN SERVICE	PRIVACY Jurisdiction	PRIVACY Logging	PRIVACY Activism	TECHNICAL Serv Conf	TECHNICAL Security	TECHNICAL Availability	BUSINESS Website	BUSINESS Pricing	BUSINESS Ethics
3Monkey									
AceVPN									
ActiVPN									
AirVPN									
Anonine									
AnonVPN									
Anonymizer									
AnonymousVPN									
Astrill									
Avast Secureline									
Avira Phantom VPN									
AzireVPN									
BeeVPN									
Betternet									
BlackVPN									
Blockless									
BolehVPN									
Boxpn									
BTGuard									
Buffered									
CactusVPN									
Celo									
ChillGlobal									
Cloak									
CrypticVPN									
CryptoHippie									
CryptoStorm									
CyberGhost									

Astril	way2stars
EarthVPN	earthvpn
GFwVPN	gfwvpn
GoldenFrog	thisisourkey
IBVPN	ibVPNsharedPSK!
IPVanish	ipvanish
NordVPN	nordvpn
PrivateInternetAccess	mysafety
PureVPN	12345678
SlickVPN	gogoVPN
TorGuard	torguard
TigerVPN	tigerVPN
UnblockVPN	xunblock4me
VPNReactor	VPNReactor

Self hosting!

VM/VPS

Hardware

Software

OpenVPN

Community Edition

```
sudo apt-get install openvpn
libssl-dev openssl easy-rsa
```

Certificate Authority

```
sudo make-cadir ~/easy-rsa

cd ~/easy-rsa
```

```
ls -l ~/easy-rsa/
total 36
lrwxrwxrwx 1 root root   28 Jan  4 09:49 build-ca -> /usr/share/easy-rsa/build-ca
lrwxrwxrwx 1 root root   28 Jan  4 09:49 build-dh -> /usr/share/easy-rsa/build-dh
lrwxrwxrwx 1 root root   31 Jan  4 09:49 build-inter -> /usr/share/easy-rsa/build-inter
lrwxrwxrwx 1 root root   29 Jan  4 09:49 build-key -> /usr/share/easy-rsa/build-key
lrwxrwxrwx 1 root root   34 Jan  4 09:49 build-key-pass -> /usr/share/easy-rsa/build-key-pass
lrwxrwxrwx 1 root root   36 Jan  4 09:49 build-key-pkcs12 -> /usr/share/easy-rsa/build-key-pkcs12
lrwxrwxrwx 1 root root   36 Jan  4 09:49 build-key-server -> /usr/share/easy-rsa/build-key-server
lrwxrwxrwx 1 root root   29 Jan  4 09:49 build-req -> /usr/share/easy-rsa/build-req
lrwxrwxrwx 1 root root   34 Jan  4 09:49 build-req-pass -> /usr/share/easy-rsa/build-req-pass
lrwxrwxrwx 1 root root   29 Jan  4 09:49 clean-all -> /usr/share/easy-rsa/clean-all
lrwxrwxrwx 1 root root   33 Jan  4 09:49 inherit-inter -> /usr/share/easy-rsa/inherit-inter
lrwxrwxrwx 1 root root   28 Jan  4 09:49 list-crl -> /usr/share/easy-rsa/list-crl
-rw-r--r-- 1 root root 7859 Jan  4 09:49 openssl-0.9.6.cnf
-rw-r--r-- 1 root root 8416 Jan  4 09:49 openssl-0.9.8.cnf
-rw-r--r-- 1 root root 8313 Jan  4 09:49 openssl-1.0.0.cnf
lrwxrwxrwx 1 root root   27 Jan  4 09:49 pkitool -> /usr/share/easy-rsa/pkitool
lrwxrwxrwx 1 root root   31 Jan  4 09:49 revoke-full -> /usr/share/easy-rsa/revoke-full
lrwxrwxrwx 1 root root   28 Jan  4 09:49 sign-req -> /usr/share/easy-rsa/sign-req
-rw-r--r-- 1 root root 2077 Jan  4 09:49 vars
lrwxrwxrwx 1 root root   35 Jan  4 09:49 whichopensslcnf -> /usr/share/easy-rsa/whichopensslcnf
```

```
sudo vim ~/easy-rsa/vars
```

```
export KEY_SIZE=4096

export EASYRSA_DIGEST="sha256"

export CA_EXPIRE=3650

export KEY_EXPIRE=365
```

```
export EASYRSA_ALGO="rsa"
```

```
export KEY_COUNTRY="SR"
export KEY_PROVINCE="Vojvodina"
export KEY_CITY="Novi Sad"
export KEY_ORG="BalCCon 2k17"
export KEY_EMAIL="vpns@balccon.org"
export KEY_OU="Balccon 2k17"
```

```
cd ~/easy-rsa/

source vars
```

```
./clean-all
./pkitool --initca
./pkitool --server server
cd keys
   openvpn --genkey --secret ta.key
cd ..
./build-dh

sudo cp server.crt server.key ca.crt \
   dh4096.pem ta.key /etc/openvpn/
```

```
ls -l keys/
-rw-r--r--  1 root root 8422 Jan  4 10:47 01.pem
-rw-r--r--  1 root root 8321 Jan  4 11:24 02.pem
-rw-r--r--  1 root root 2500 Jan  4 10:26 ca.crt
-rw-------  1 root root 3272 Jan  4 10:26 ca.key
-rw-r--r--  1 root root  245 Jan  4 10:15 dh4096.pem
-rw-r--r--  1 root root    3 Jan  4 11:24 serial
-rw-r--r--  1 root root 8422 Jan  4 10:47 server.crt
-rw-r--r--  1 root root 1785 Jan  4 10:47 server.csr
-rw-------  1 root root 3268 Jan  4 10:47 server.key
-rw-------  1 root root  636 Jan  4 10:50 ta.key
```

```
cd ~/easy-rsa/
source vars
./pkitool balccon-client
```

```
ls -l keys/balccon-client.*
-rw-r--r-- 1 root root 8321 Jan  4 11:24 balccon-client.crt
-rw-r--r-- 1 root root 1789 Jan  4 11:24 balccon-client.csr
-rw------- 1 root root 3272 Jan  4 11:24 balccon-client.key
```

balccon-client.crt
balccon-client.key
ca.crt
ta.key

```
sudo cp /usr/share/doc/openvpn/
examples/sample-config-files/
server.conf .

sudo vim server.conf
```

/etc/openvpn/server.conf

ca ca.crt
cert server.crt
key server.key
dh dh**4096**.pem

/etc/openvpn/server.conf

server 192.168.23.0 255.255.255.0

/etc/openvpn/server.conf

push "route 192.168.23.0 255.255.255.0"
push "route 192.168.0.0 255.255.255.0"

/etc/openvpn/server.conf

push "redirect-gateway def1 bypass-dhcp"

/etc/openvpn/server.conf

```
push "dhcp-option DNS 85.214.20.141"
push "dhcp-option DNS 213.73.91.35"
```

/etc/openvpn/server.conf

tls-auth ta.key 0

/etc/openvpn/server.conf

cipher AES-256-GCM
auth SHA512
tls-cipher TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
tls-version-min 1.2

ovpn --show-ciphers

ovpn --show-curves

/etc/openvpn/server.conf

comp-lzo yes

/etc/openvpn/server.conf

```
user nobody
group nogroup
```

```
sudo service openvpn restart
```

OpenVPN Clients

$ openvpn2

Network

Viscosity

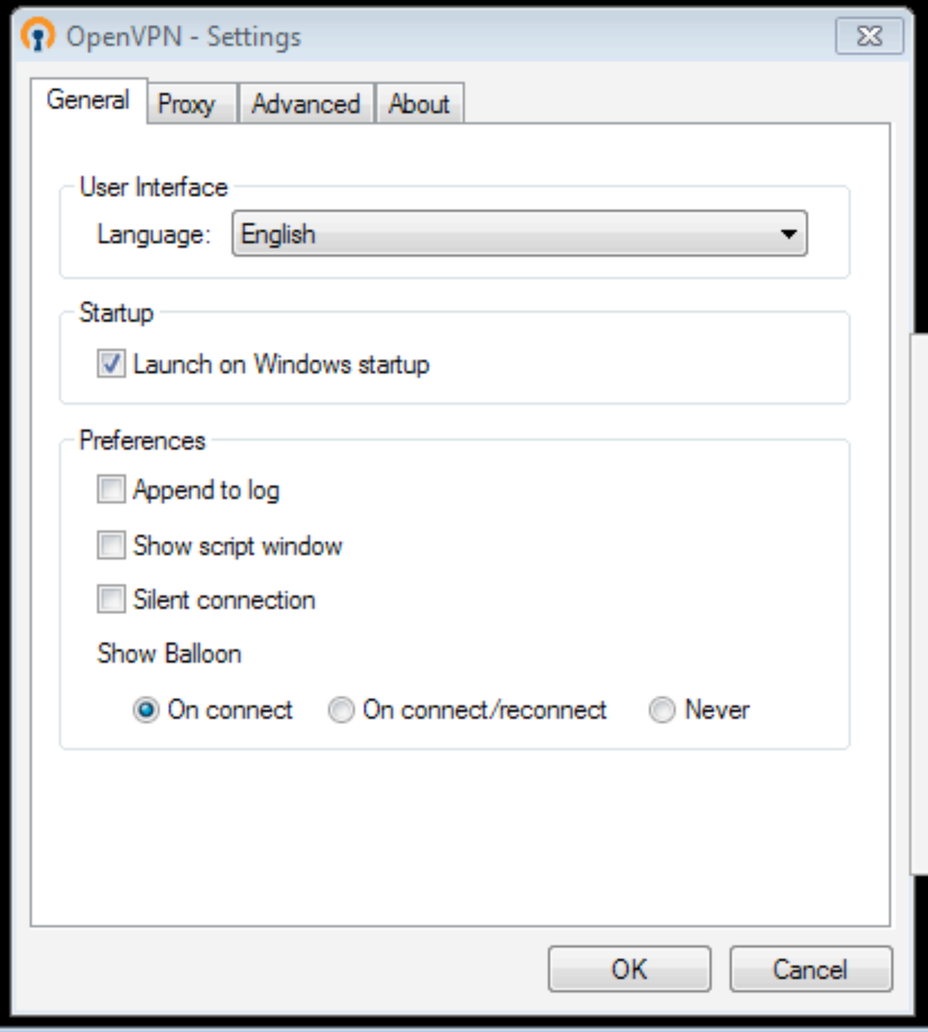
Tunnelblick

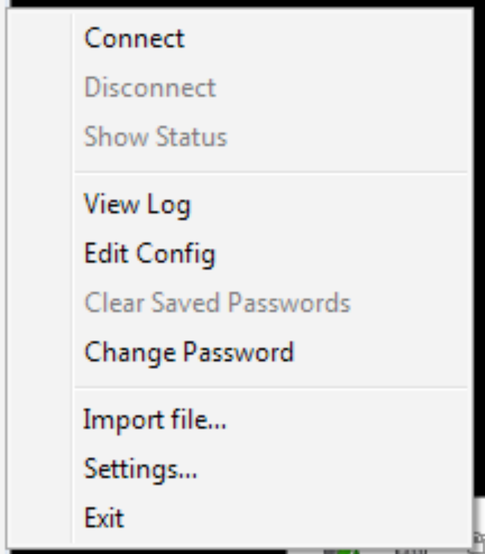
OpenVPN Connect

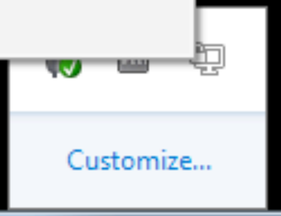
OpenVPN Connect

OpenVPN für Android

openvpn-gui.exe

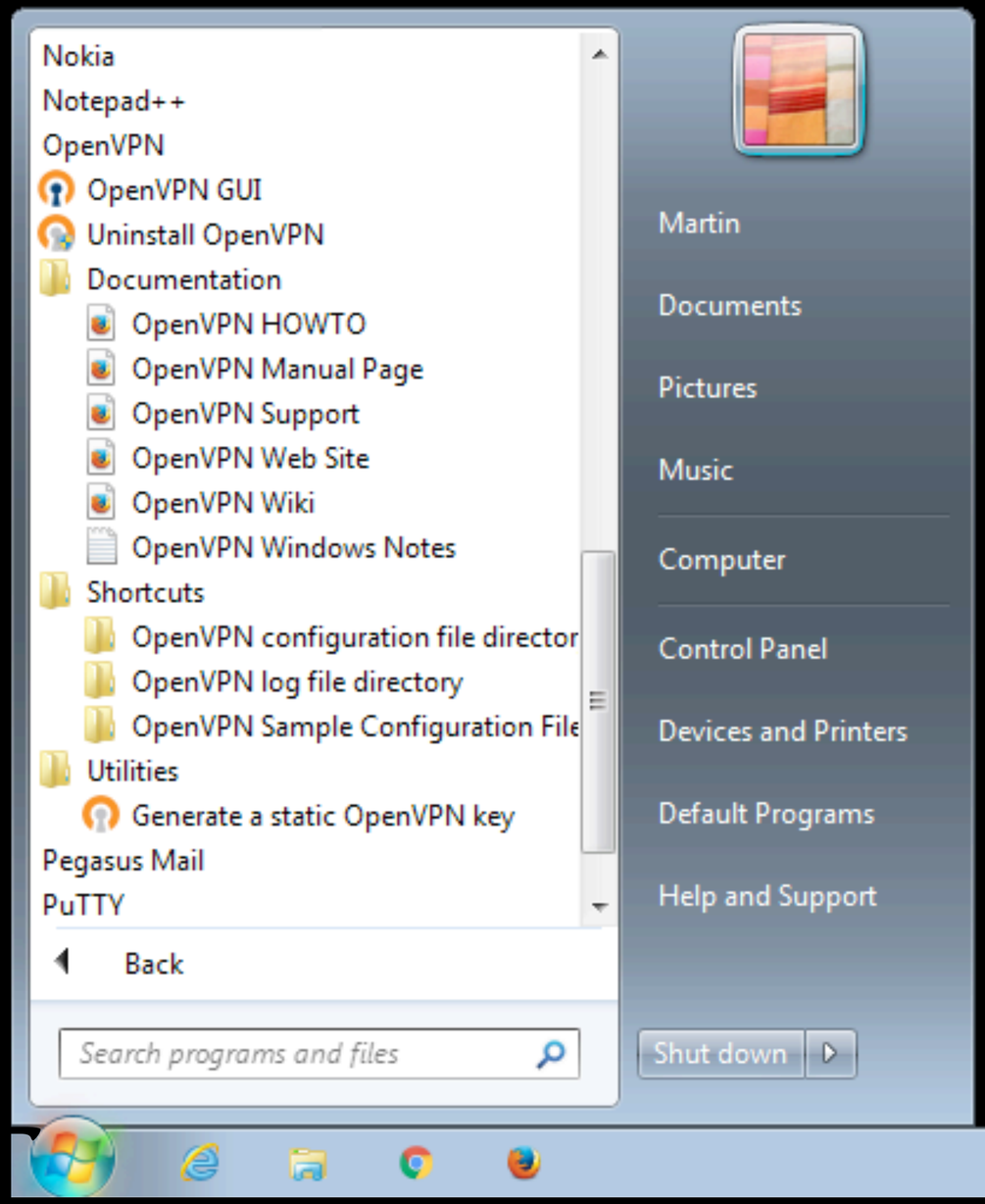

OpenVPN - Settings
General
Proxy
Advanced
About
User Interface
Language:
English
Startup
Launch on Windows startup
Preferences
Append to log
Show script window
Silent connection
Show Balloon
On connect
On connect/reconnect
Never
OK
Cancel


Connect
Disconnect
Show Status
View Log
Edit Config
Clear Saved Passwords
Change Password
Import file...
Settings...
Exit


Customize...


OpenVPN
GUI


00:36


Nokia
Notepad++
OpenVPN
OpenVPN GUI
Uninstall OpenVPN
Documentation
OpenVPN HOWTO
OpenVPN Manual Page
OpenVPN Support
OpenVPN Web Site
OpenVPN Wiki
OpenVPN Windows Notes
Shortcuts
OpenVPN configuration file director
OpenVPN log file directory
OpenVPN Sample Configuration File
Utilities
Generate a static OpenVPN key
Pegasus Mail
PuTTY
Back
Search programs and files
Martin
Documents
Pictures
Music
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down

C:\Users\[USERNAME]
\OpenVPN\config\balccon.ovpn

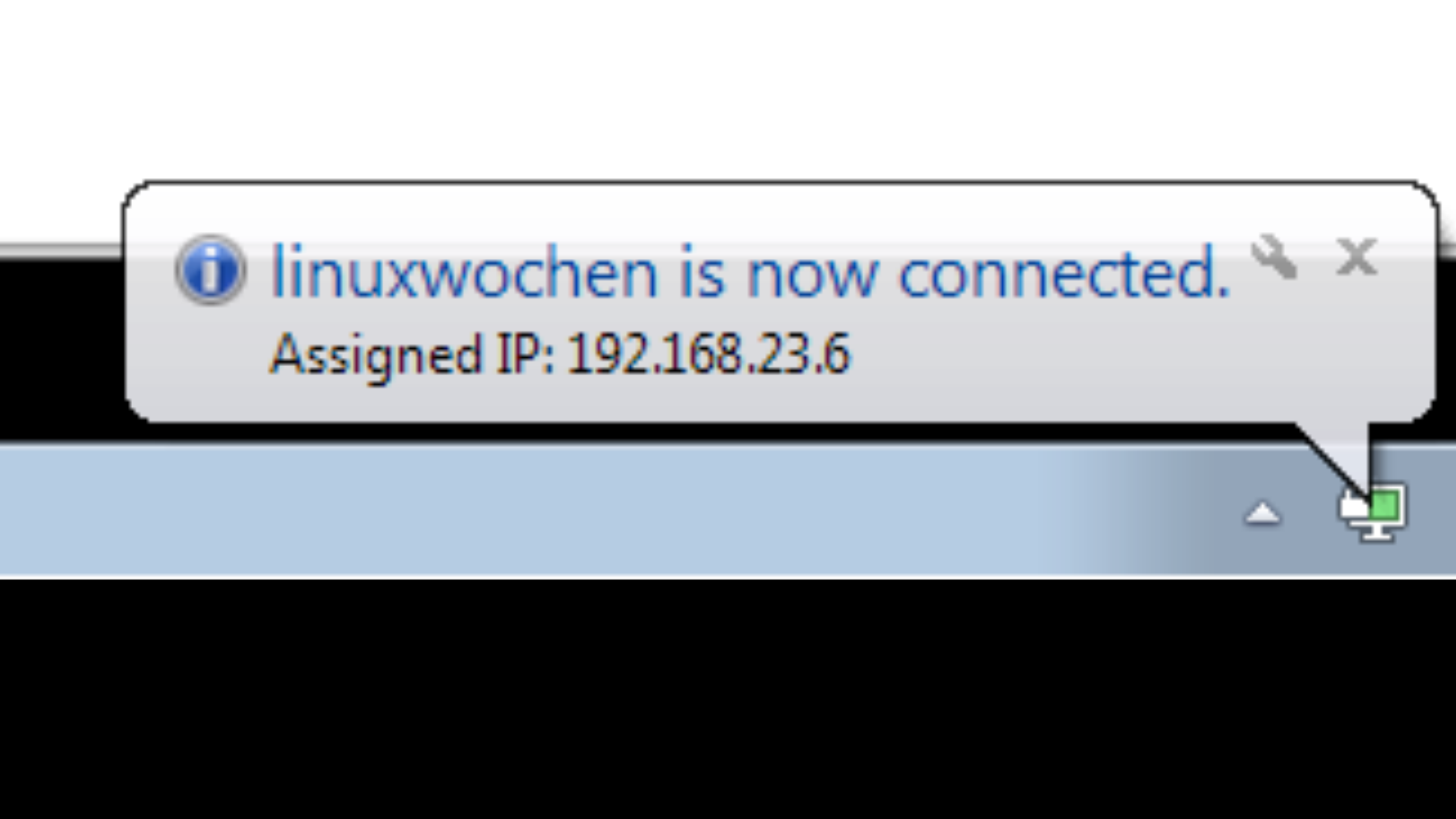
remote openvpn.example.com 1194

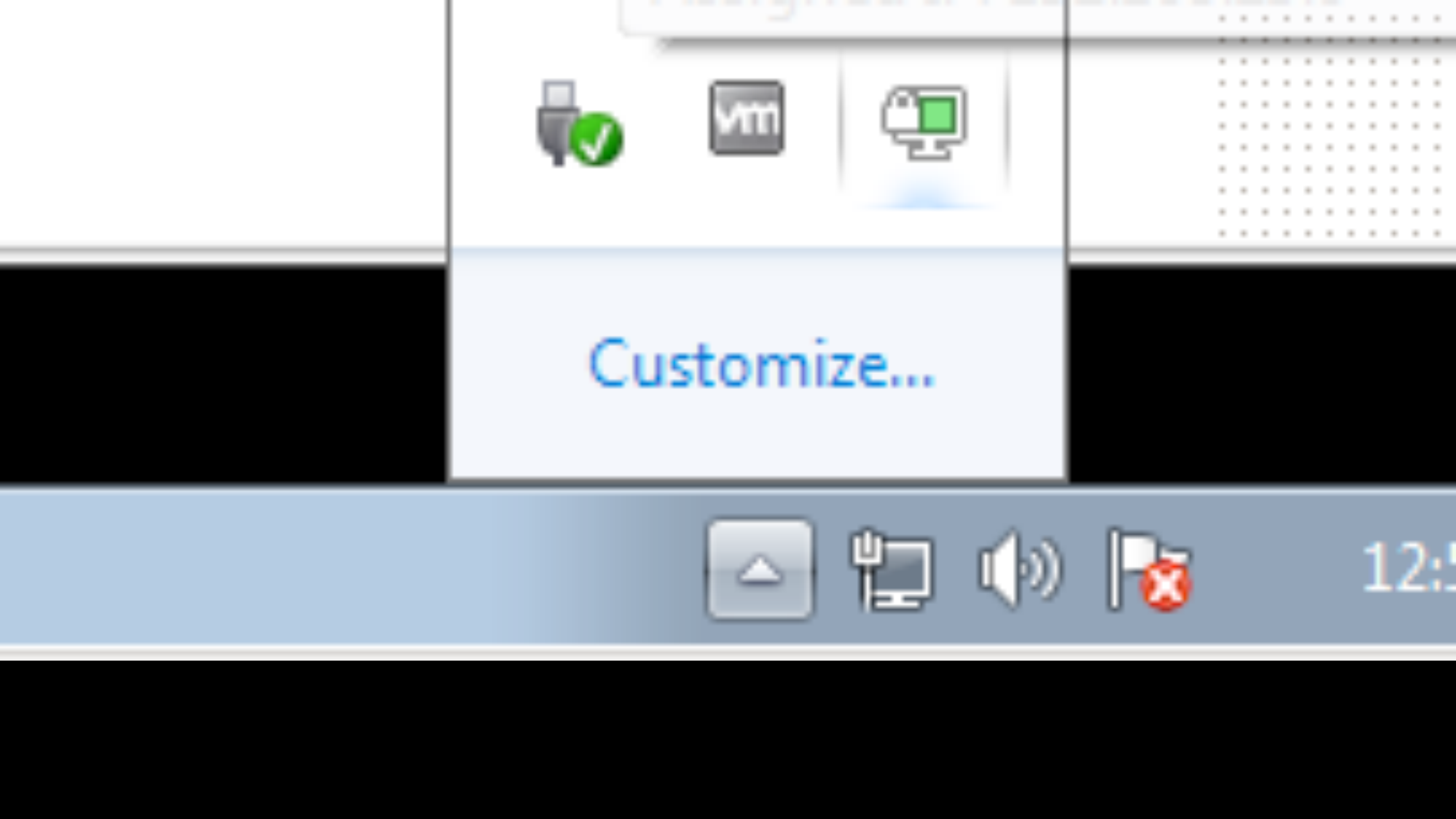
C:\Users\[USERNAME]
\OpenVPN\config\balccon.ovpn

```
ca ca.crt
cert balccon-client.crt
key balccon-client.key
tls-auth ta.key 1
```

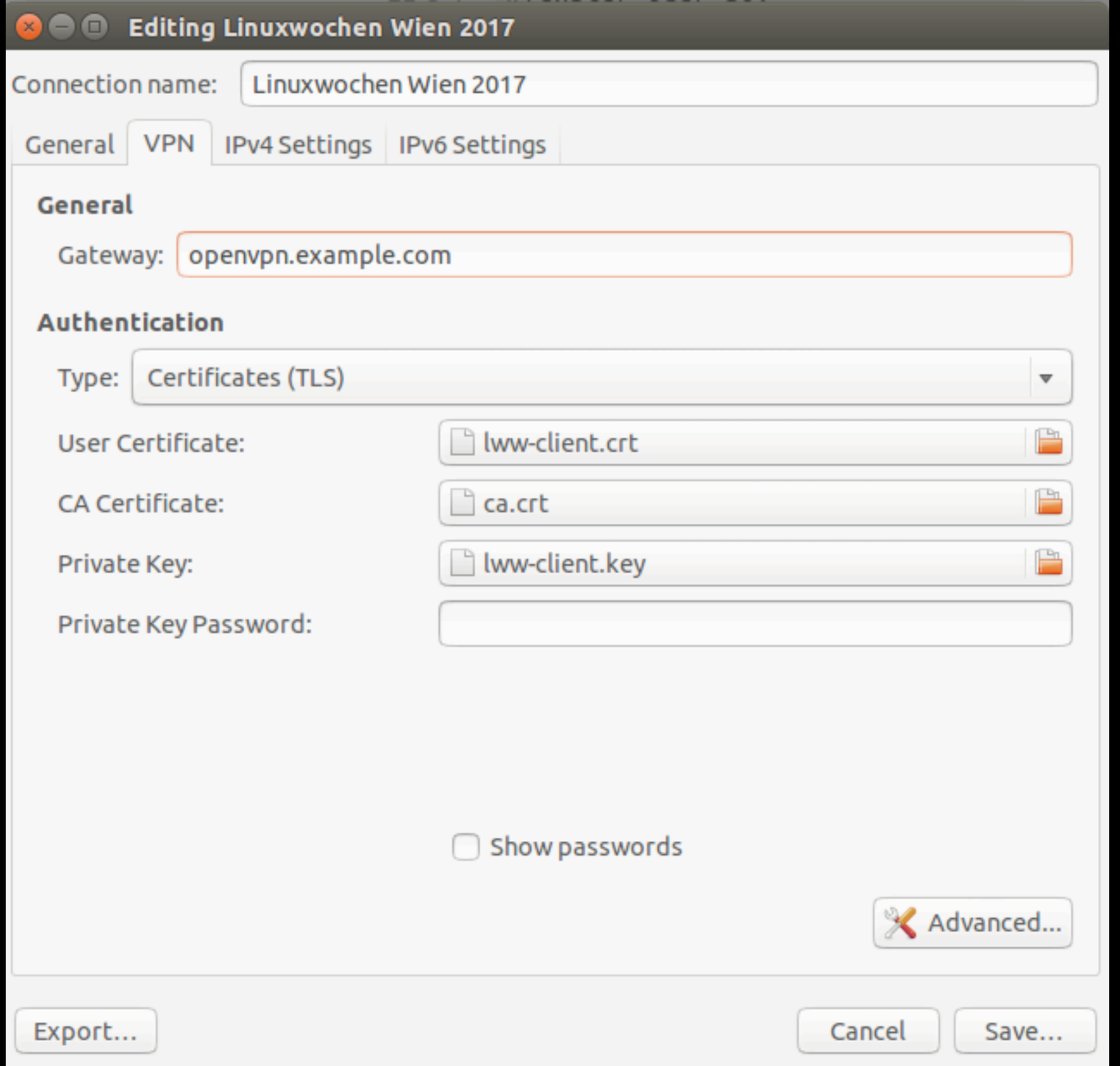
C:\Users\[USERNAME]
\OpenVPN\config\balccon.ovpn

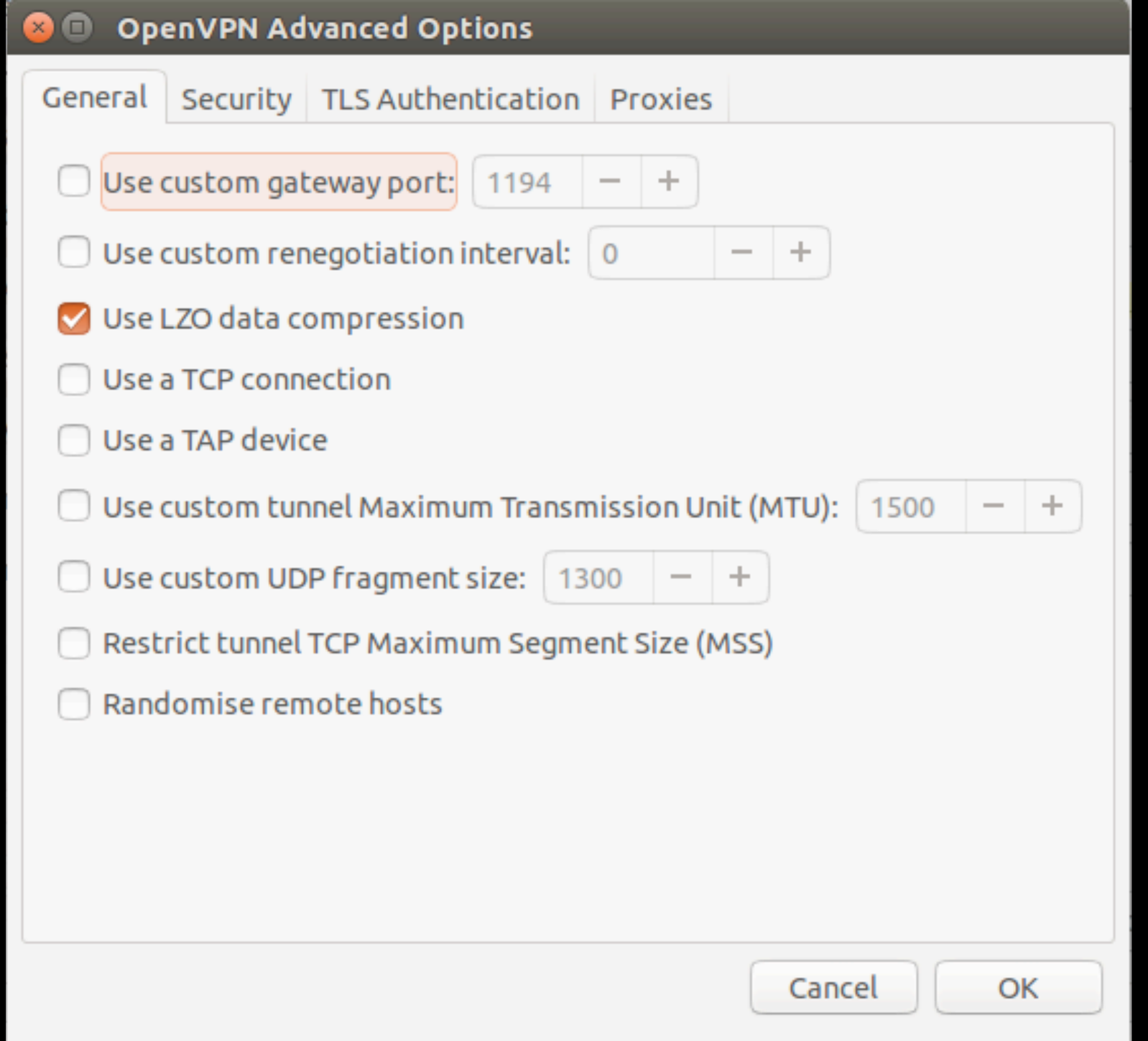
cipher AES-256-GCM
auth SHA512
comp-lzo yes

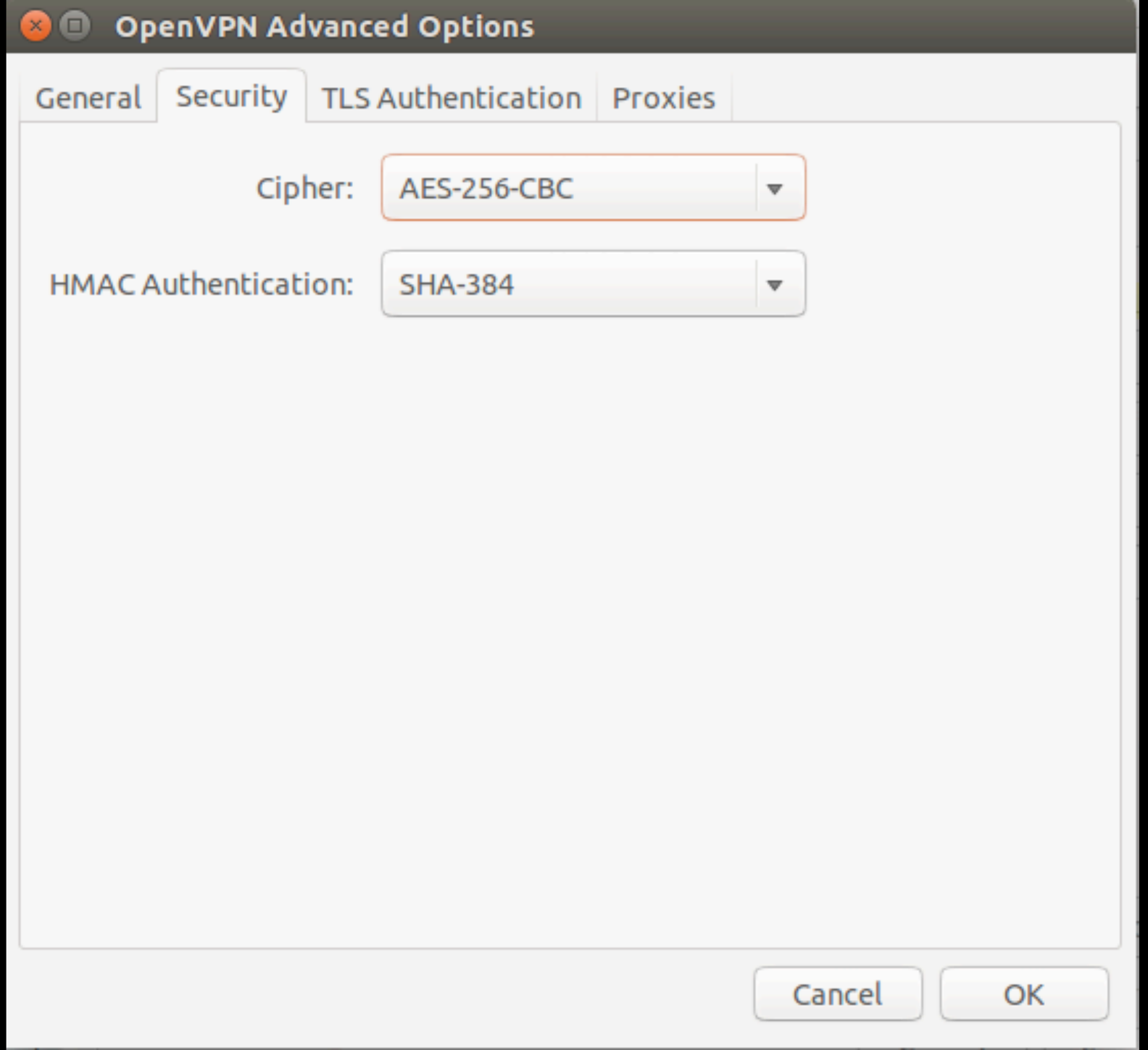

linuxwochen is now connected.
Assigned IP: 192.168.23.6

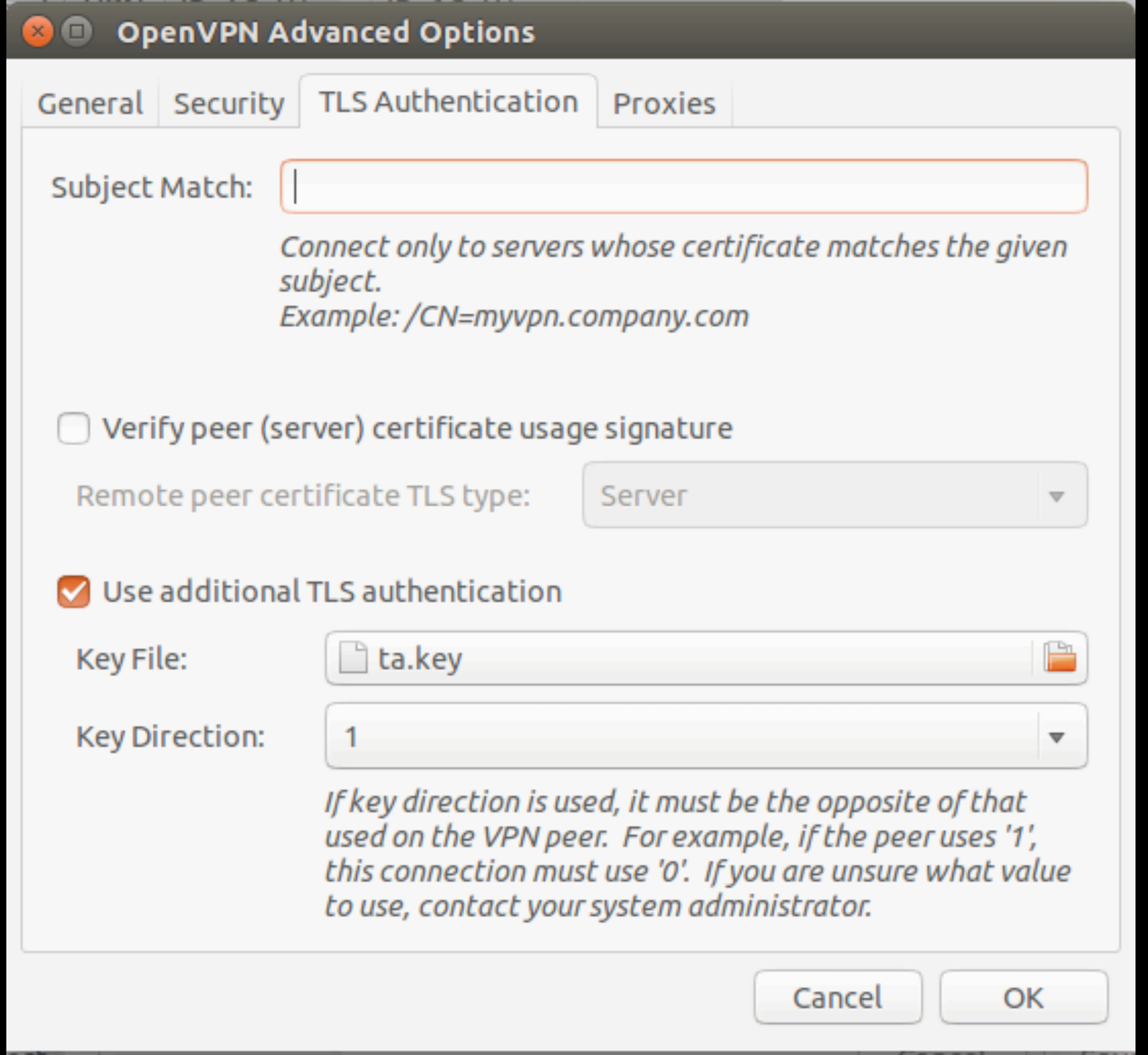

Customize...

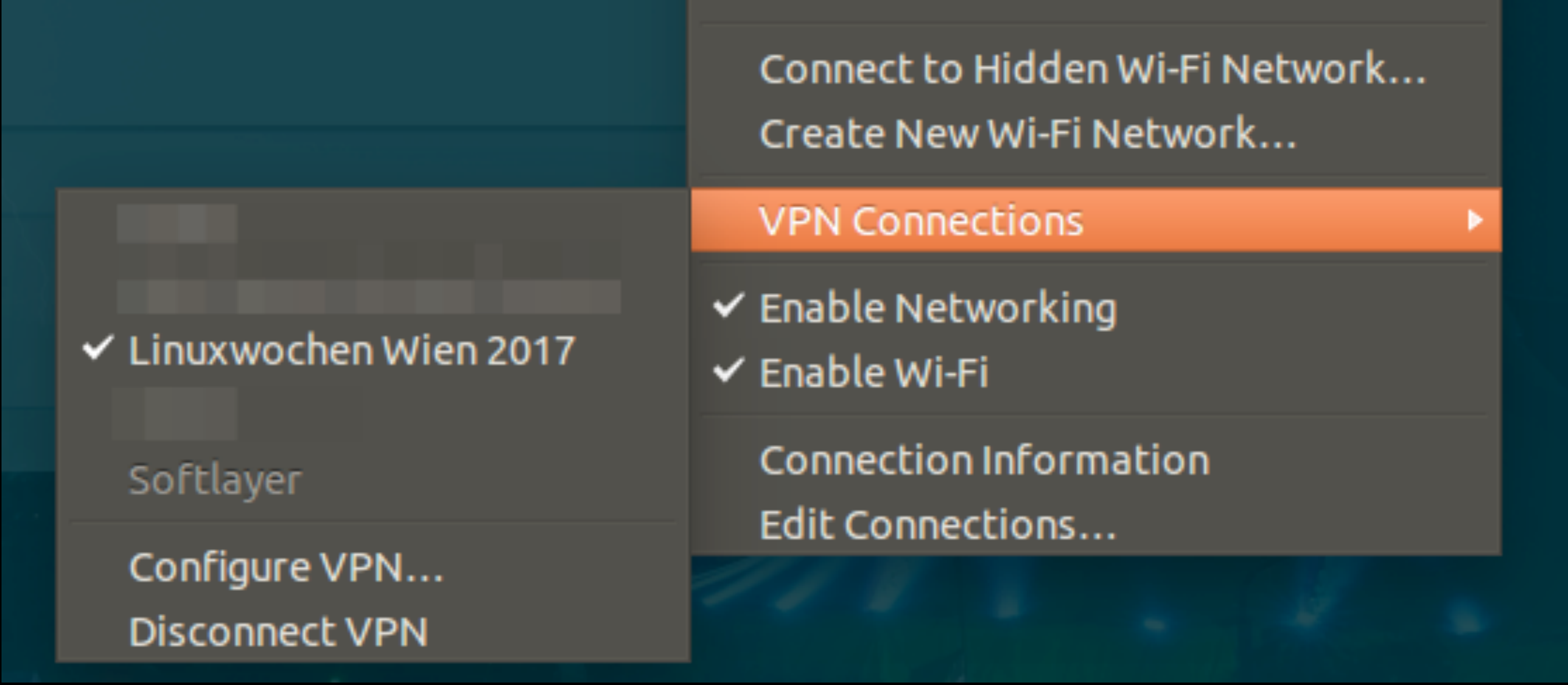
```
sudo apt-get install \
  network-manager-openvpn
```

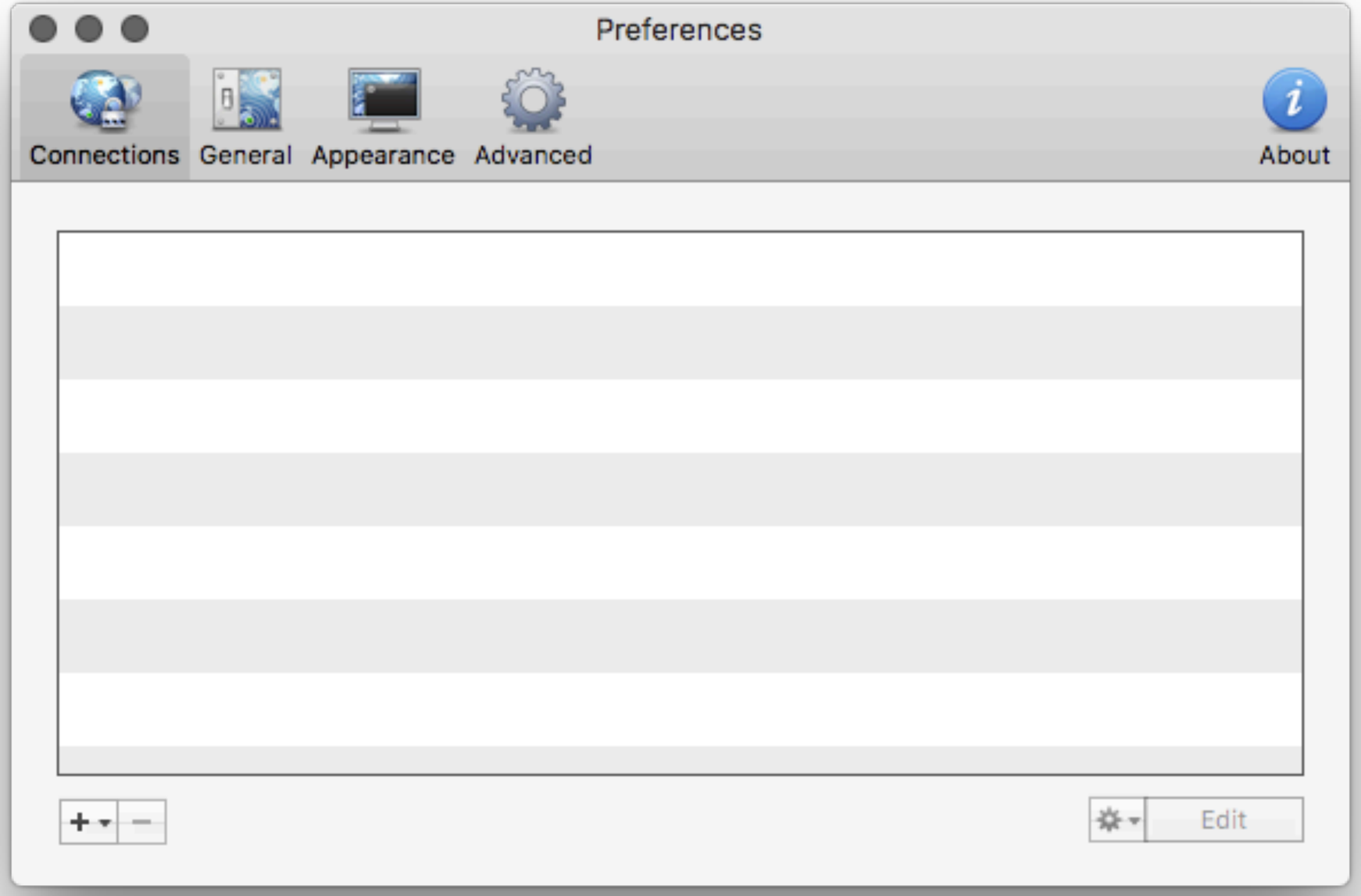

Editing Linuxwochen Wien 2017
Connection name:
Linuxwochen Wien 2017
General
VPN
IPv4 Settings
IPv6 Settings
General
Gateway:
openvpn.example.com
Authentication
Type:
Certificates (TLS)
User Certificate:
lww-client.crt
CA Certificate:
ca.crt
Private Key:
lww-client.key
Private Key Password:
Show passwords
Advanced...
Export...
Cancel
Save...

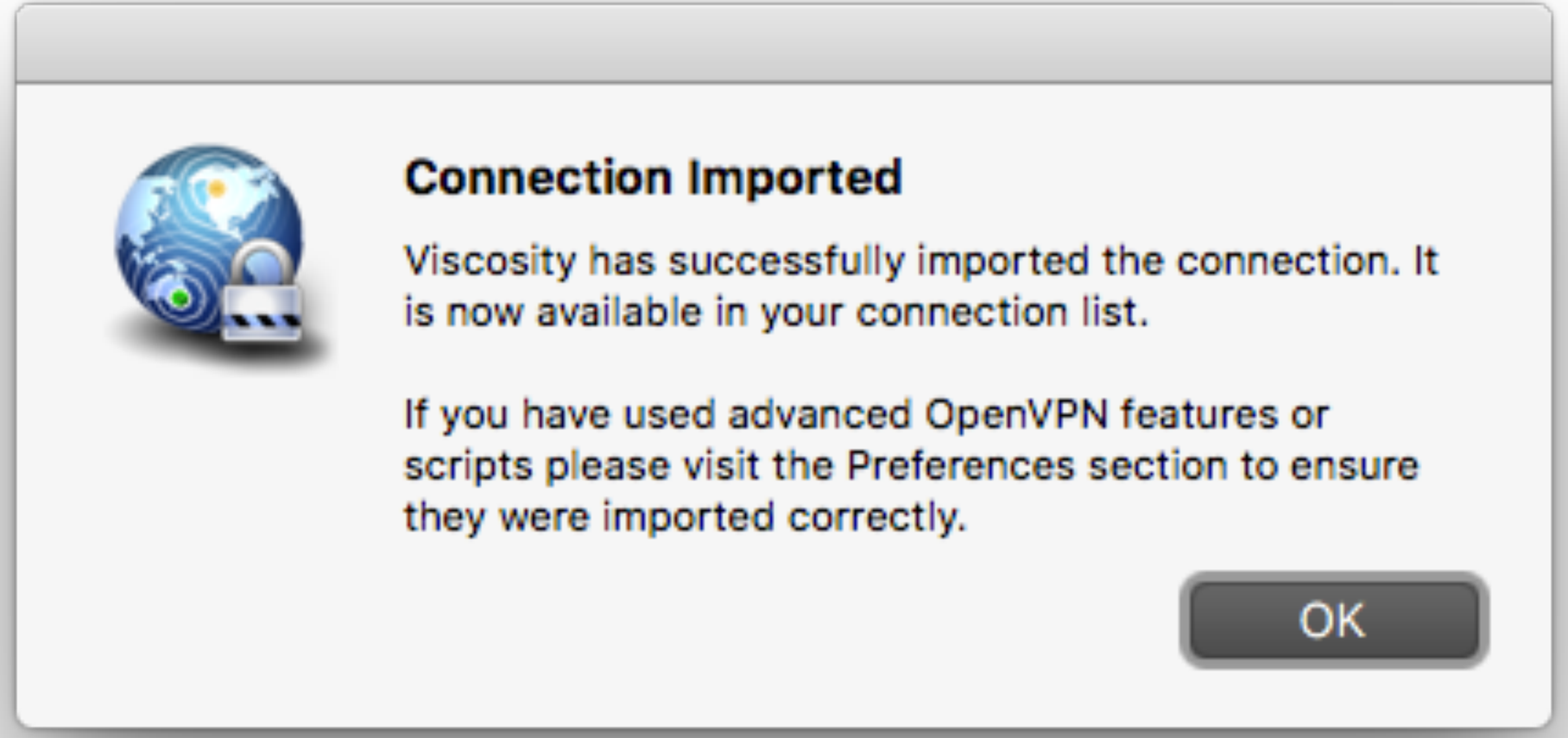

OpenVPN Advanced Options
General
Security
TLS Authentication
Proxies
Use custom gateway port:
1194
Use custom renegotiation interval:
0
Use LZO data compression
Use a TCP connection
Use a TAP device
Use custom tunnel Maximum Transmission Unit (MTU):
1500
Use custom UDP fragment size:
1300
Restrict tunnel TCP Maximum Segment Size (MSS)
Randomise remote hosts
Cancel
OK

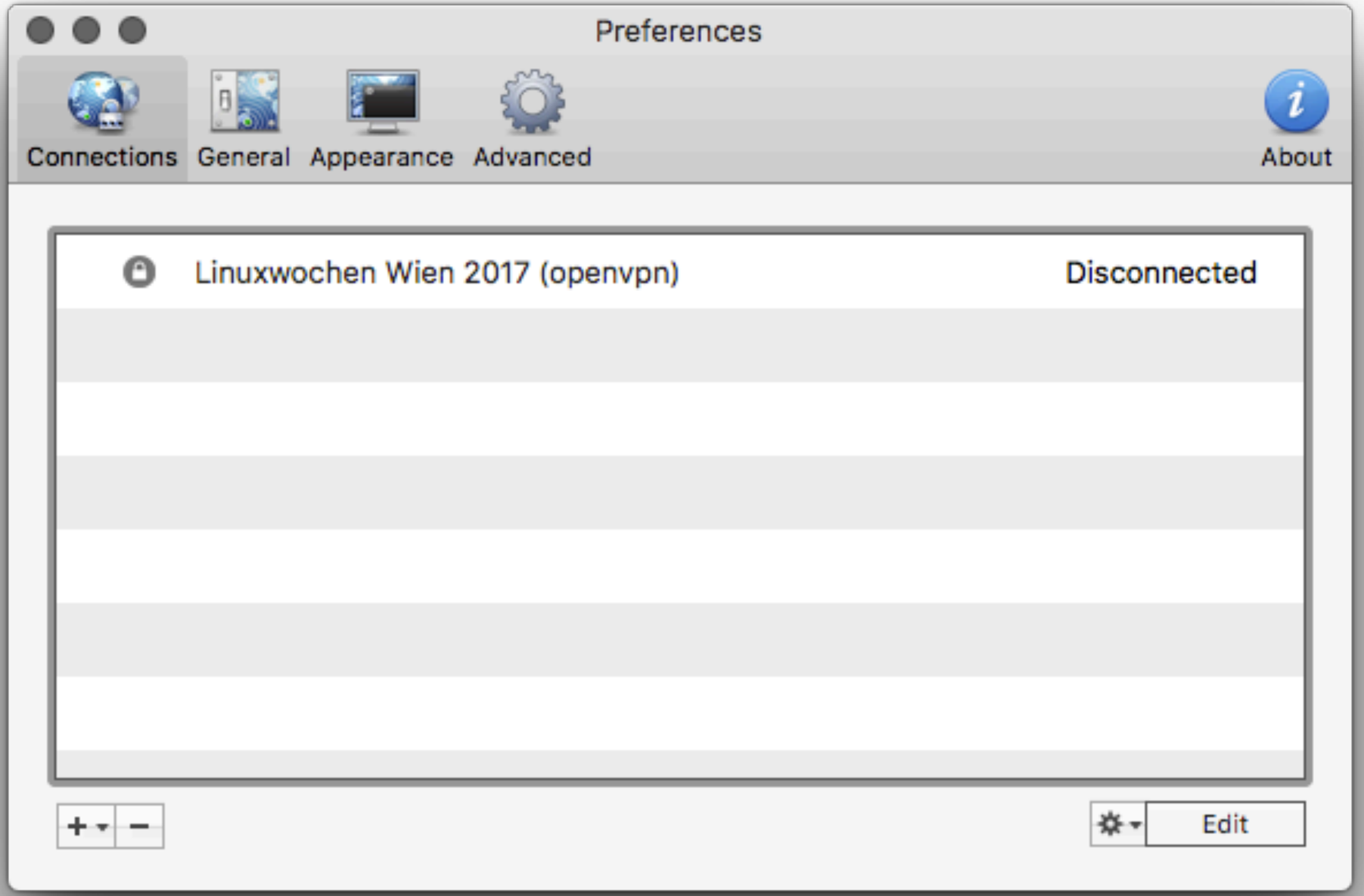

OpenVPN Advanced Options
General
Security
TLS Authentication
Proxies
Cipher:
AES-256-CBC
HMAC Authentication:
SHA-384
Cancel
OK


OpenVPN Advanced Options
General
Security
TLS Authentication
Proxies
Subject Match:
Connect only to servers whose certificate matches the given subject.
Example: /CN=myvpn.company.com
Verify peer (server) certificate usage signature
Remote peer certificate TLS type:
Server
Use additional TLS authentication
Key File:
ta.key
Key Direction:
1
If key direction is used, it must be the opposite of that used on the VPN peer. For example, if the peer uses '1', this connection must use '0'. If you are unsure what value to use, contact your system administrator.
Cancel
OK

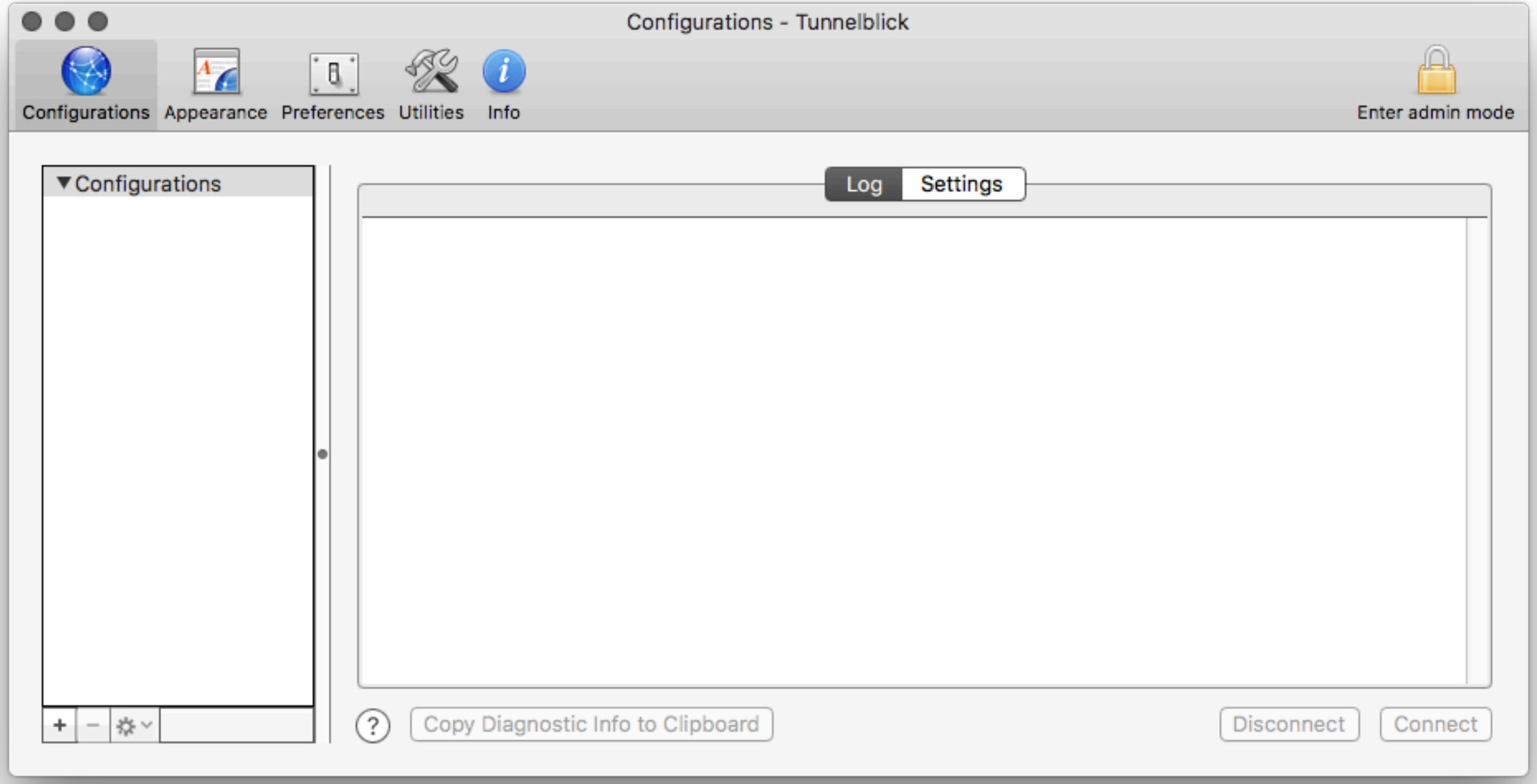

Connect to Hidden Wi-Fi Network...
Create New Wi-Fi Network...
VPN Connections
Enable Networking
Enable Wi-Fi
Connection Information
Edit Connections...
Linuxwochen Wien 2017
Softlayer
Configure VPN...
Disconnect VPN


Preferences
Connections
General
Appearance
Advanced
About
Edit


Connection Imported
Viscosity has successfully imported the connection. It is now available in your connection list.
If you have used advanced OpenVPN features or scripts please visit the Preferences section to ensure they were imported correctly.
OK


Preferences
Connections
General
Appearance
Advanced
About
Linuxwochen Wien 2017 (openvpn)
Disconnected
Edit


Details
Linuxwochen Wien 2017 (openvpn)
Connected
Status
24 seconds
Connected Time
192.168.23.10
Client IP
84.113.130.37
Server IP
42 KB
0 KB
In: 2 KB/s
Out: 1 KB/s


Configurations - Tunnelblick
Configurations
Appearance
Preferences
Utilities
Info
Enter admin mode
Configurations
Log
Settings
Copy Diagnostic Info to Clipboard
Disconnect
Connect


Tunnelblick
Linuxwochen Wien 2017 (openvpn)
Connected 01:20
In: 6.51 KB/s 420 KB
Out: 9.87 KB/s 205 KB
Disconnect
Connect

Troubleshooting Tips

/etc/openvpn/server.conf

mtu-test

balccon-client/213.225.11.140:2533 NOTE: Empirical MTU test completed

[Tried,Actual]

local->remote=[1585,1585]

remote->local=[1585,1585]

openvpn[8177]: NOTE: Empirical MTU test completed
[Tried,Actual]
local->remote=[1557,1445]
remote->local=[1557,1557]

openvpn[8177]: NOTE: This connection is unable to accomodate a UDP packet size of 1557. Consider using --fragment or --mssfix options as a workaround.

MSS = MTU - 40

/etc/openvpn/server.conf

fragment 1405

mssfix

/ OpenVPN

Community Edition

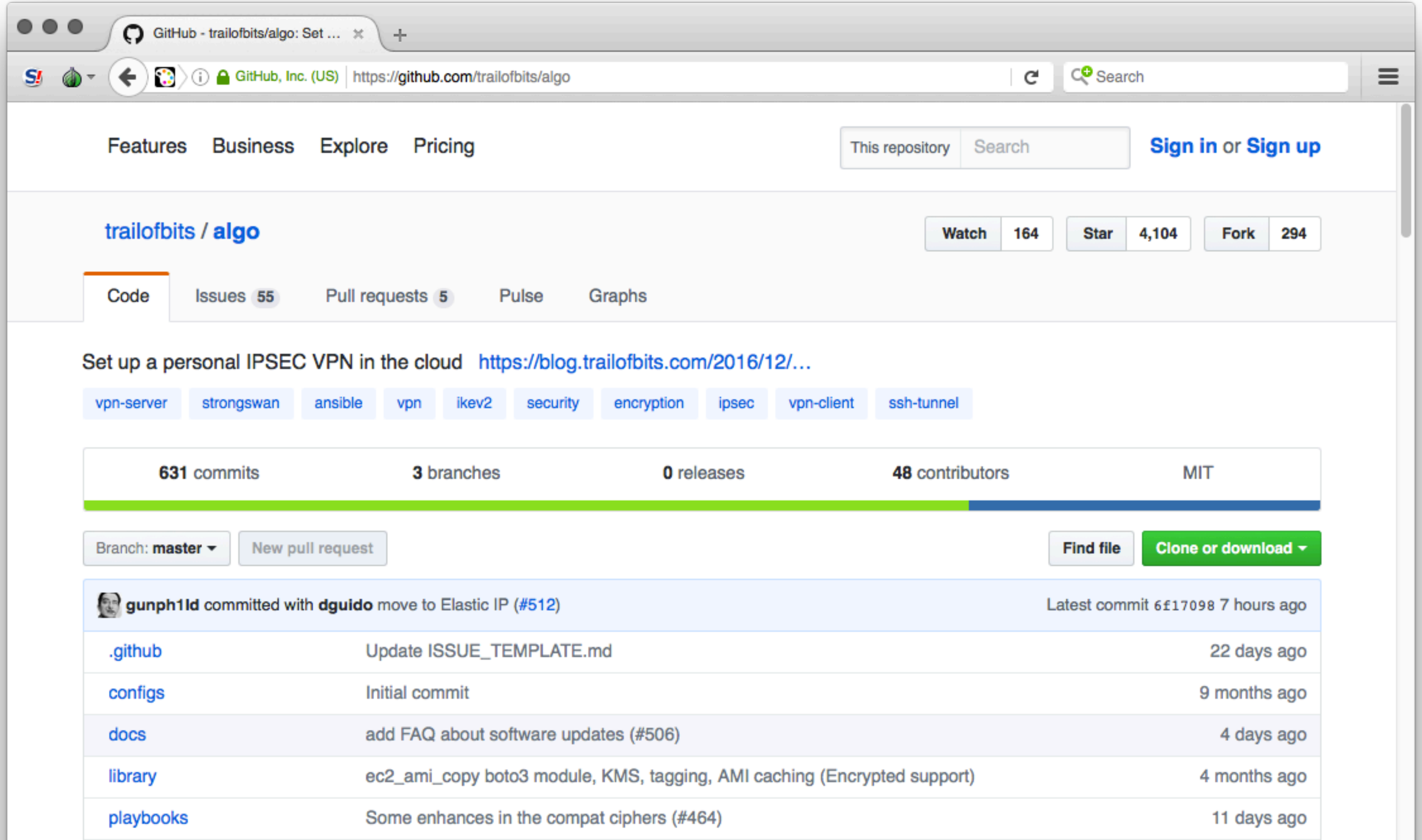
<‘(((^(((><

The Middle of the Talk

For certain definitions of „middle“.

IPSec, IKEv2

AlgoVPN


GitHub - trailofbits/algo: Set …
GitHub, Inc. (US)
https://github.com/trailofbits/algo
Search
Features Business Explore Pricing
This repository Search
Sign in or Sign up
trailofbits / algo
Watch 164
Star 4,104
Fork 294
Code Issues 55 Pull requests 5 Pulse Graphs
Set up a personal IPSEC VPN in the cloud https://blog.trailofbits.com/2016/12/…
vpn-server strongswan ansible vpn ikev2 security encryption ipsec vpn-client ssh-tunnel
631 commits 3 branches 0 releases 48 contributors MIT
Branch: master
New pull request
Find file
Clone or download
gunph1ld committed with dguido move to Elastic IP (#512)
Latest commit 6£17098 7 hours ago
.github Update ISSUE_TEMPLATE.md 22 days ago
configs Initial commit 9 months ago
docs add FAQ about software updates (#506) 4 days ago
library ec2_ami_copy boto3 module, KMS, tagging, AMI caching (Encrypted support) 4 months ago
playbooks Some enhances in the compat ciphers (#464) 11 days ago

AlgoVPN

Features

AlgoVPN

Antifeatures

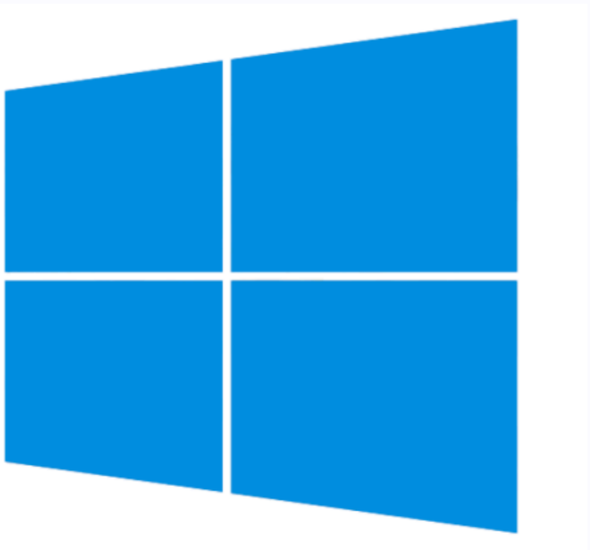
Ubuntu Server 16.04 LTS

AlgoVPN
Server Installation

```
linuxwochen@wien:~$
linuxwochen@wien:~$
```

IPSec, IKEv2 Clients

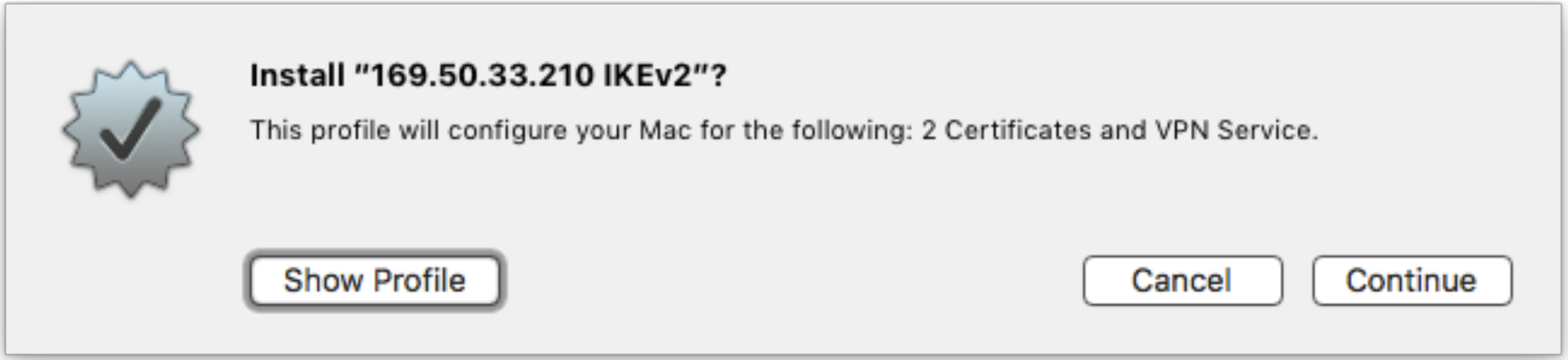

10

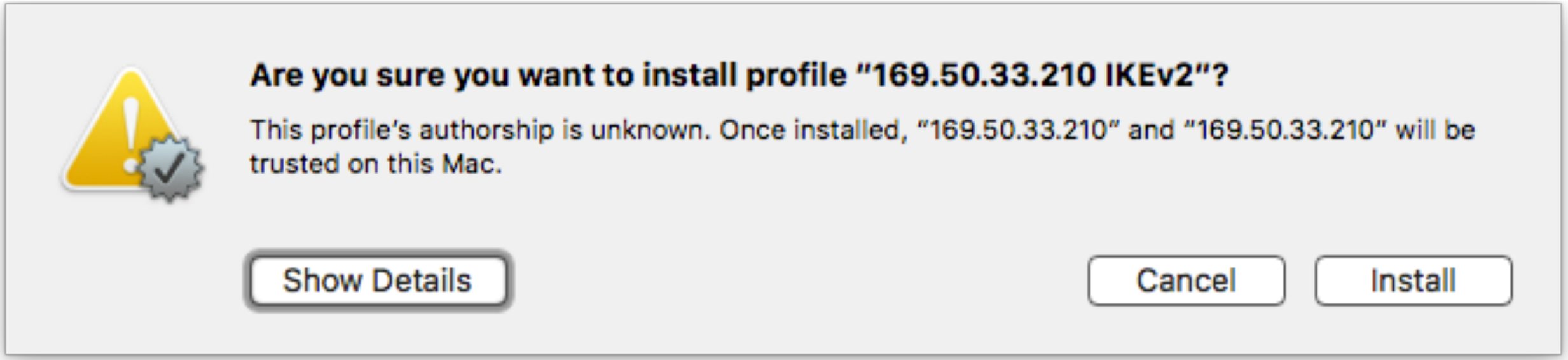


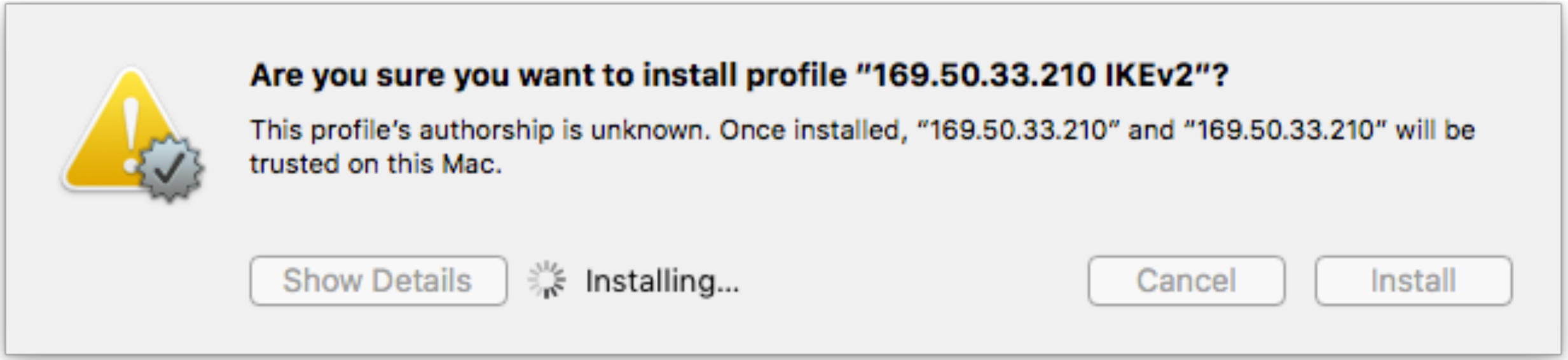
Client Installation

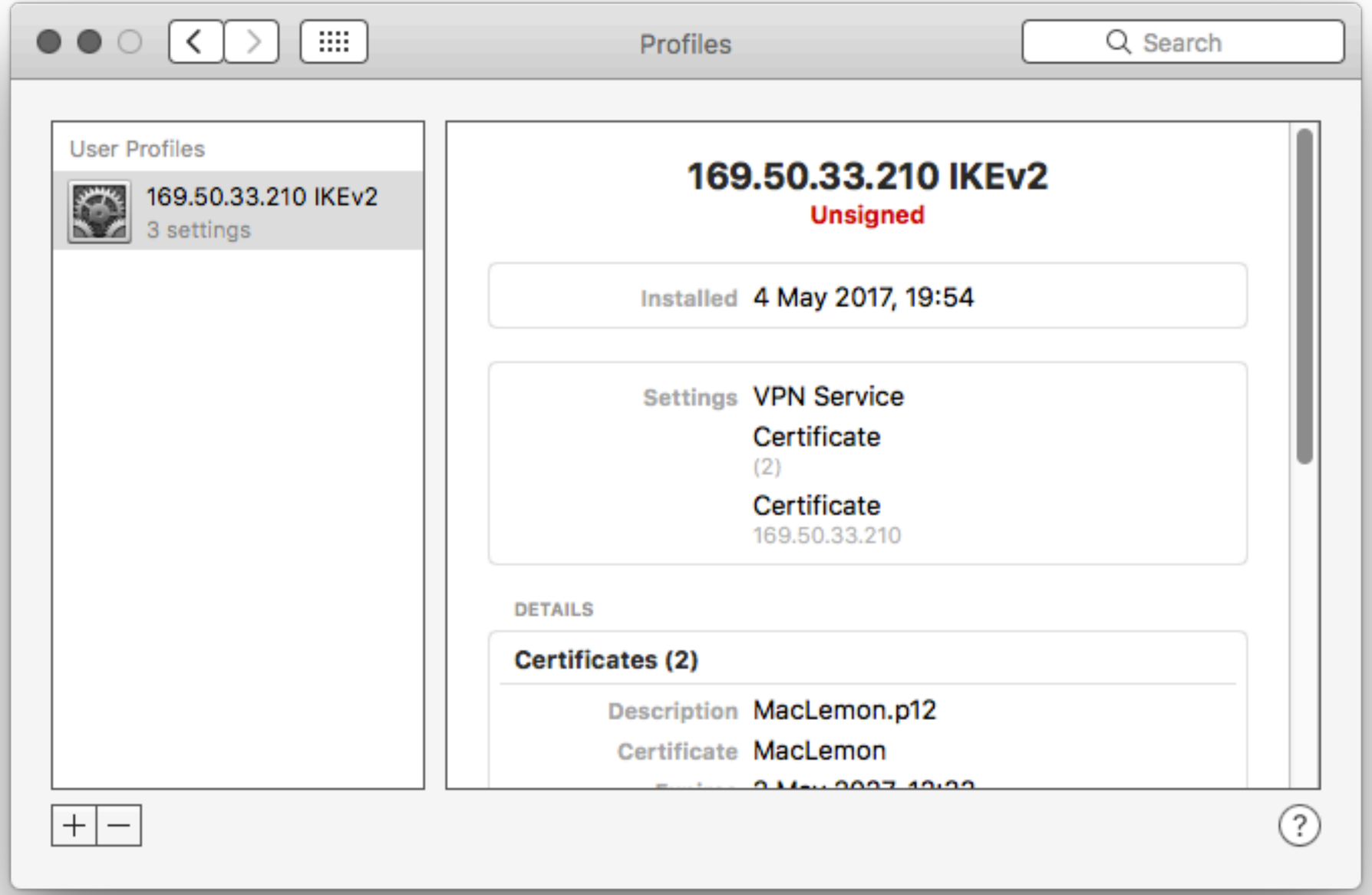
macOS

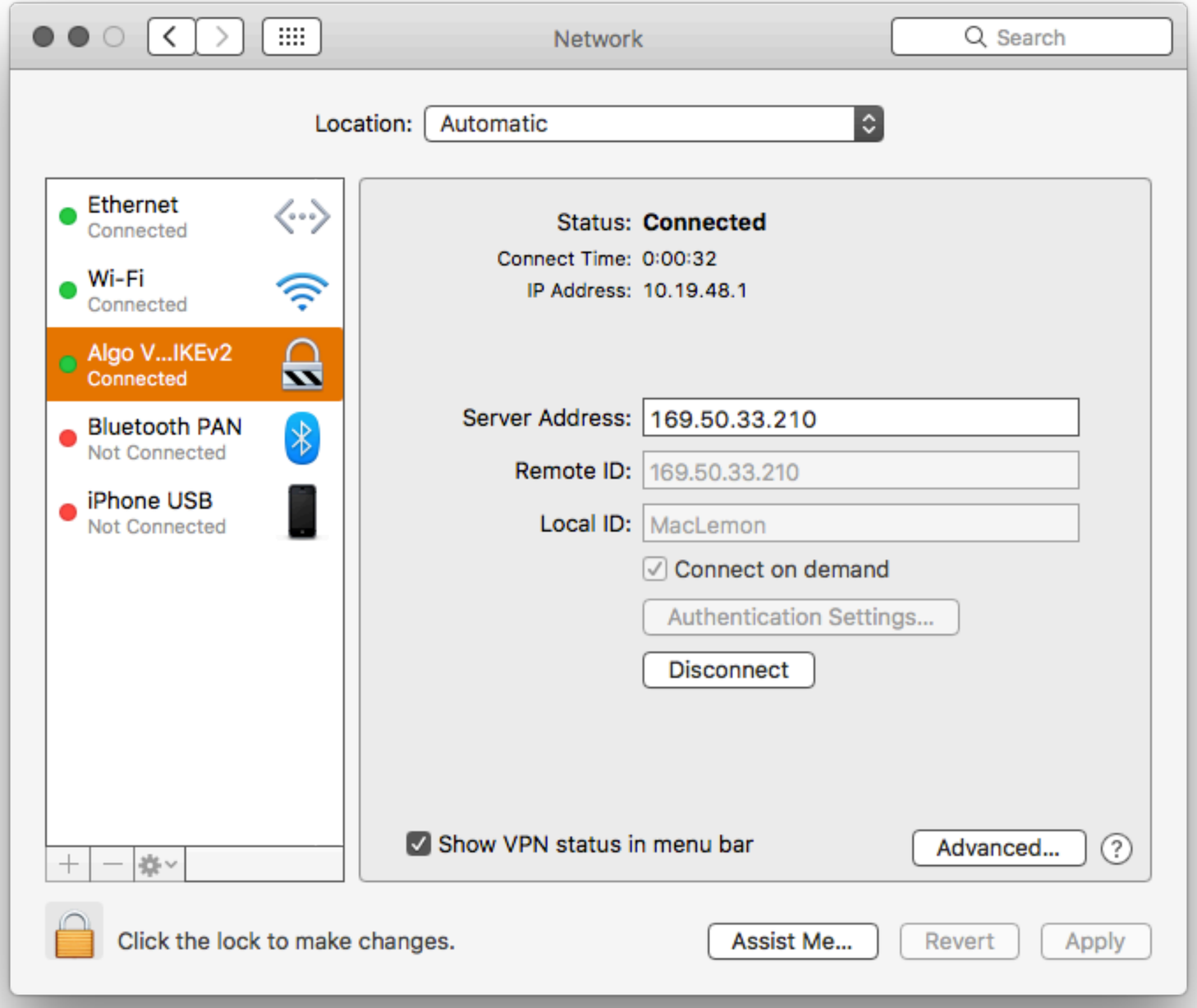
Balccon.mobileconfig


Install "169.50.33.210 IKEv2"?
This profile will configure your Mac for the following: 2 Certificates and VPN Service.
Show Profile
Cancel
Continue

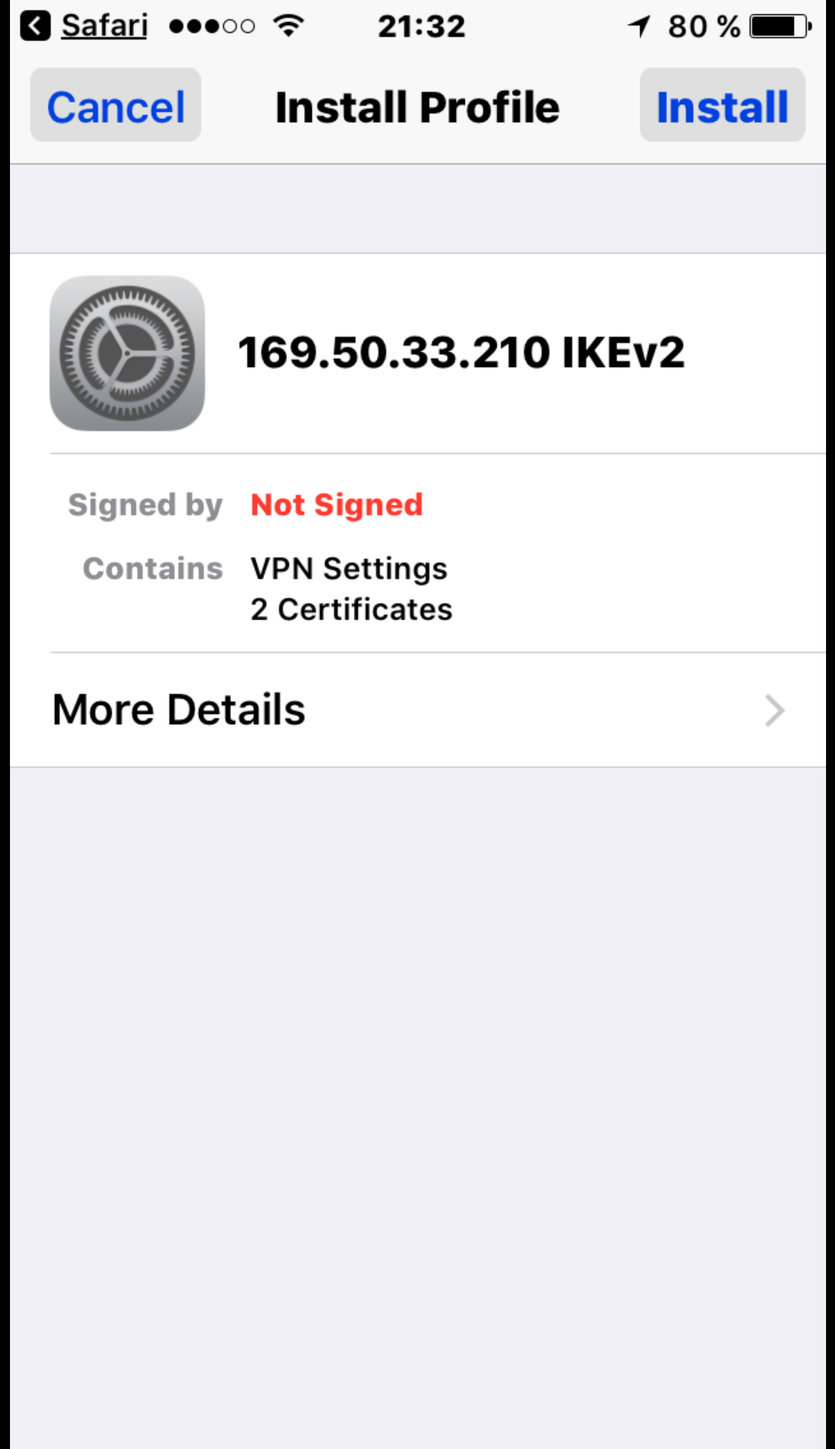

Are you sure you want to install profile "169.50.33.210 IKEv2"?
This profile's authorship is unknown. Once installed, "169.50.33.210" and "169.50.33.210" will be trusted on this Mac.
Show Details
Cancel
Install

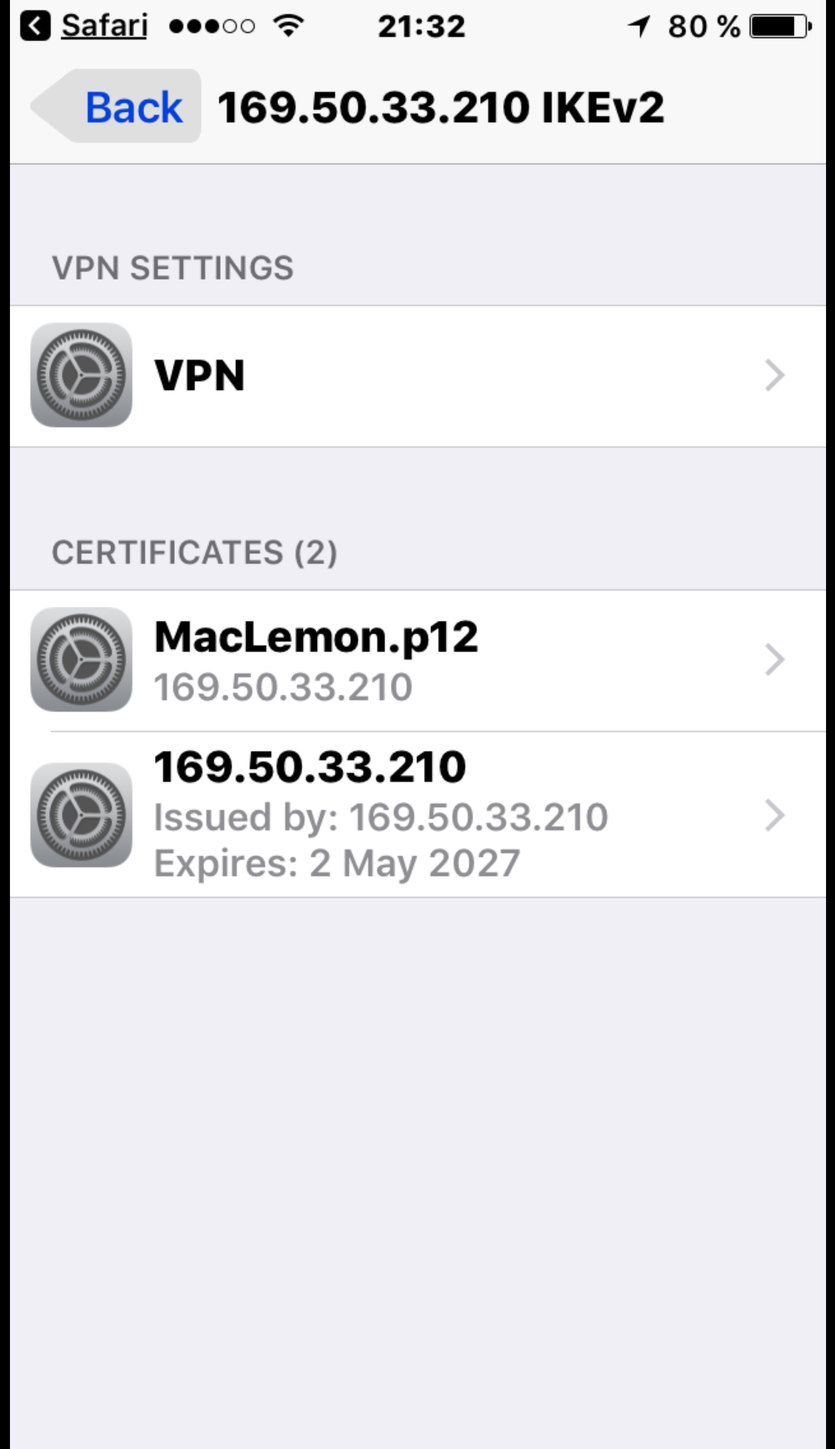

Are you sure you want to install profile "169.50.33.210 IKEv2"?
This profile's authorship is unknown. Once installed, "169.50.33.210" and "169.50.33.210" will be trusted on this Mac.
Show Details
Installing...
Cancel
Install

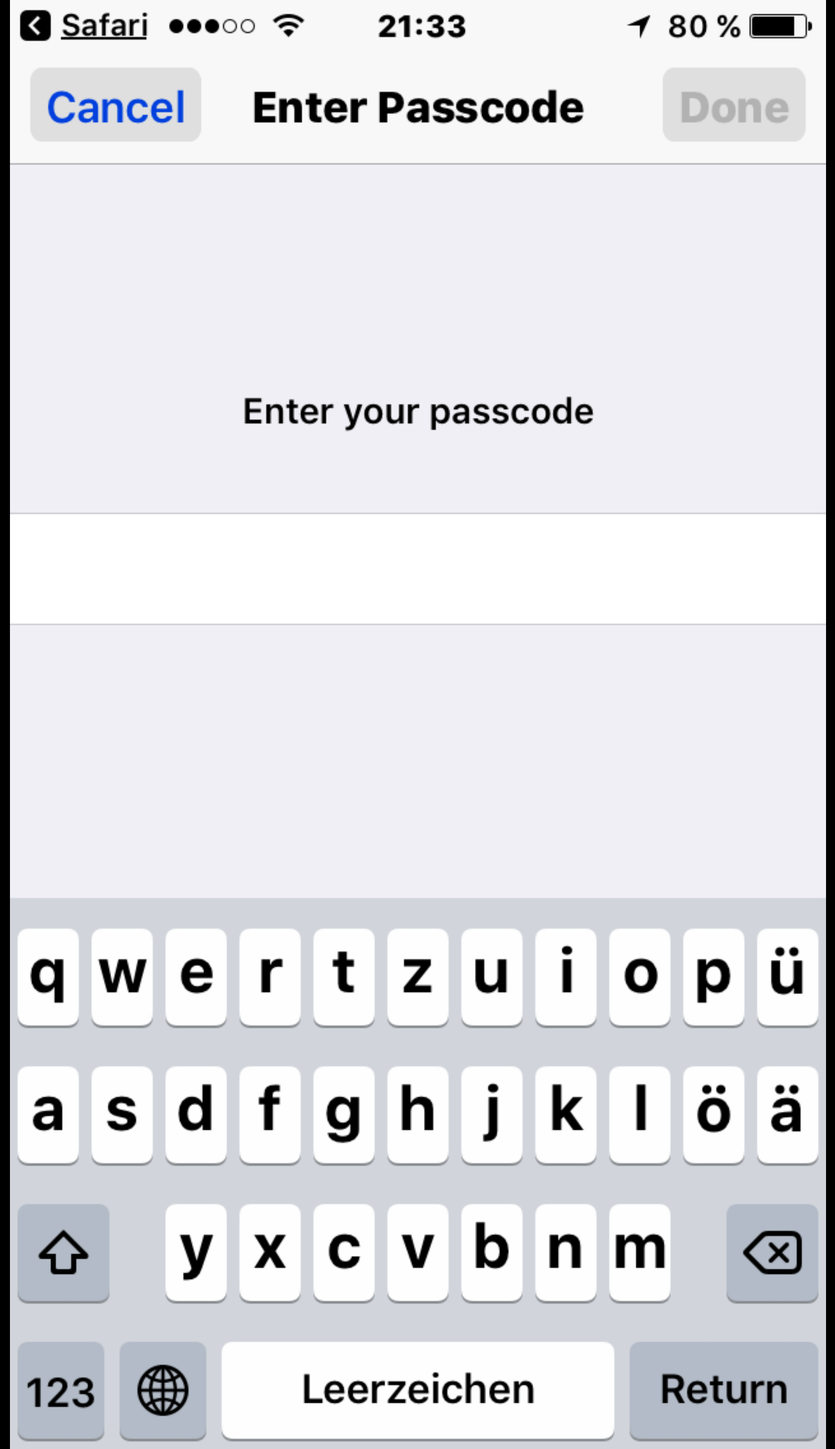

Profiles
Search
User Profiles
169.50.33.210 IKEv2
3 settings
169.50.33.210 IKEv2
Unsigned
Installed 4 May 2017, 19:54
Settings VPN Service
Certificate
(2)
Certificate
169.50.33.210
DETAILS
Certificates (2)
Description MacLemon.p12
Certificate MacLemon

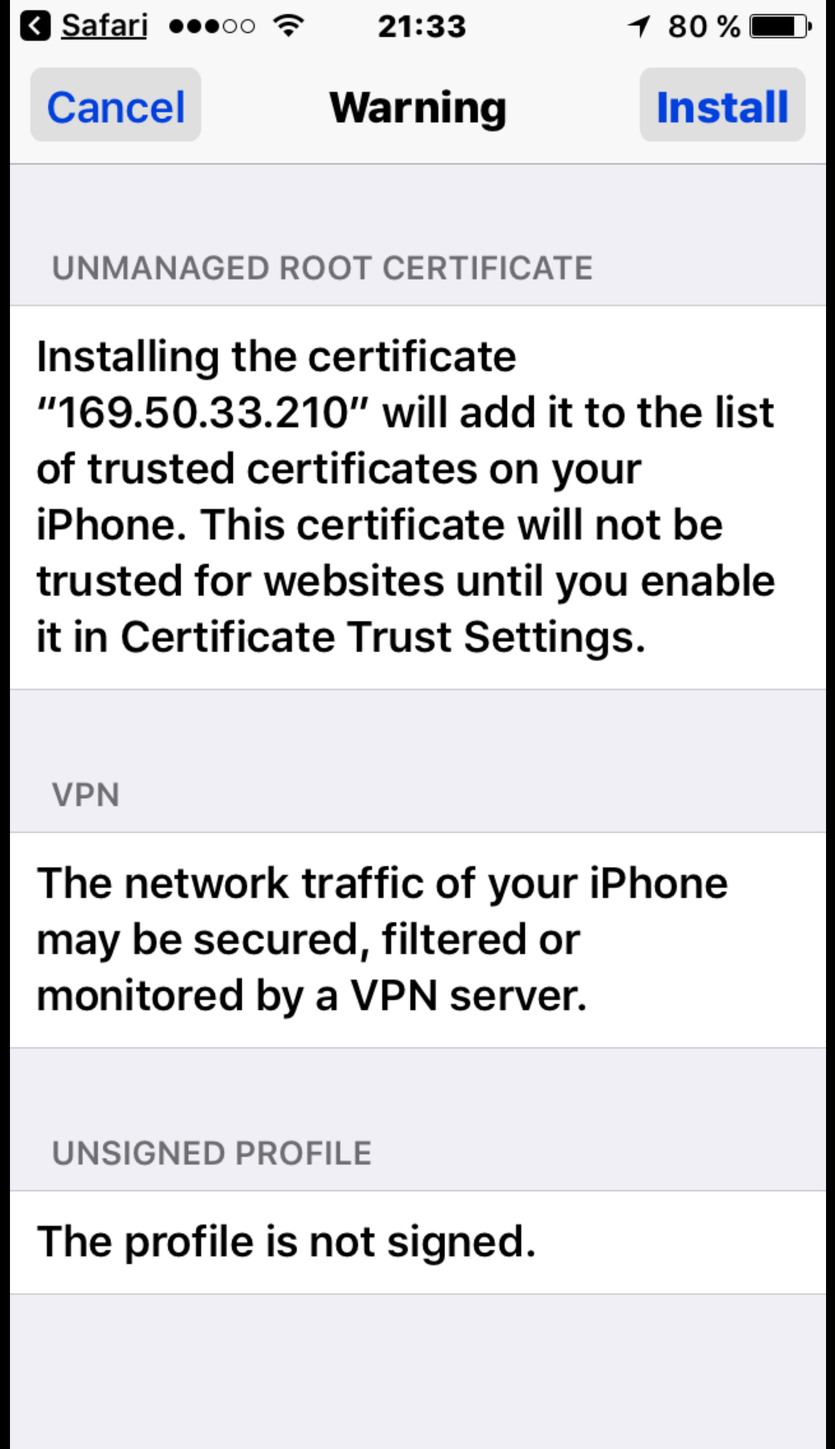

Network
Search
Location:
Automatic
Ethernet
Connected
Wi-Fi
Connected
Algo V...IKEv2
Connected
Bluetooth PAN
Not Connected
iPhone USB
Not Connected
Status: Connected
Connect Time: 0:00:32
IP Address: 10.19.48.1
Server Address: 169.50.33.210
Remote ID: 169.50.33.210
Local ID: MacLemon
Connect on demand
Authentication Settings...
Disconnect
Show VPN status in menu bar
Advanced...
Click the lock to make changes.
Assist Me...
Revert
Apply

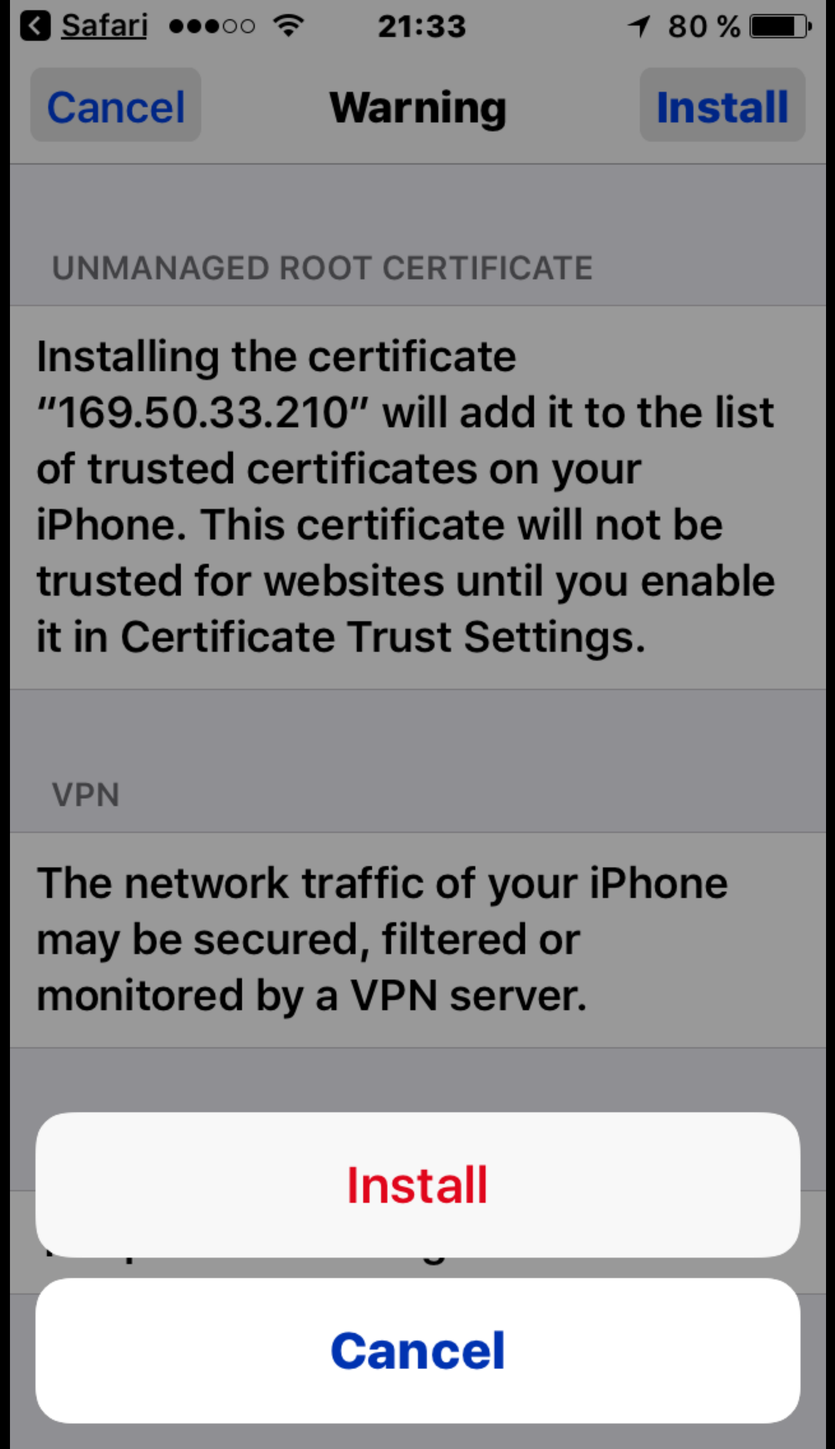
iOS

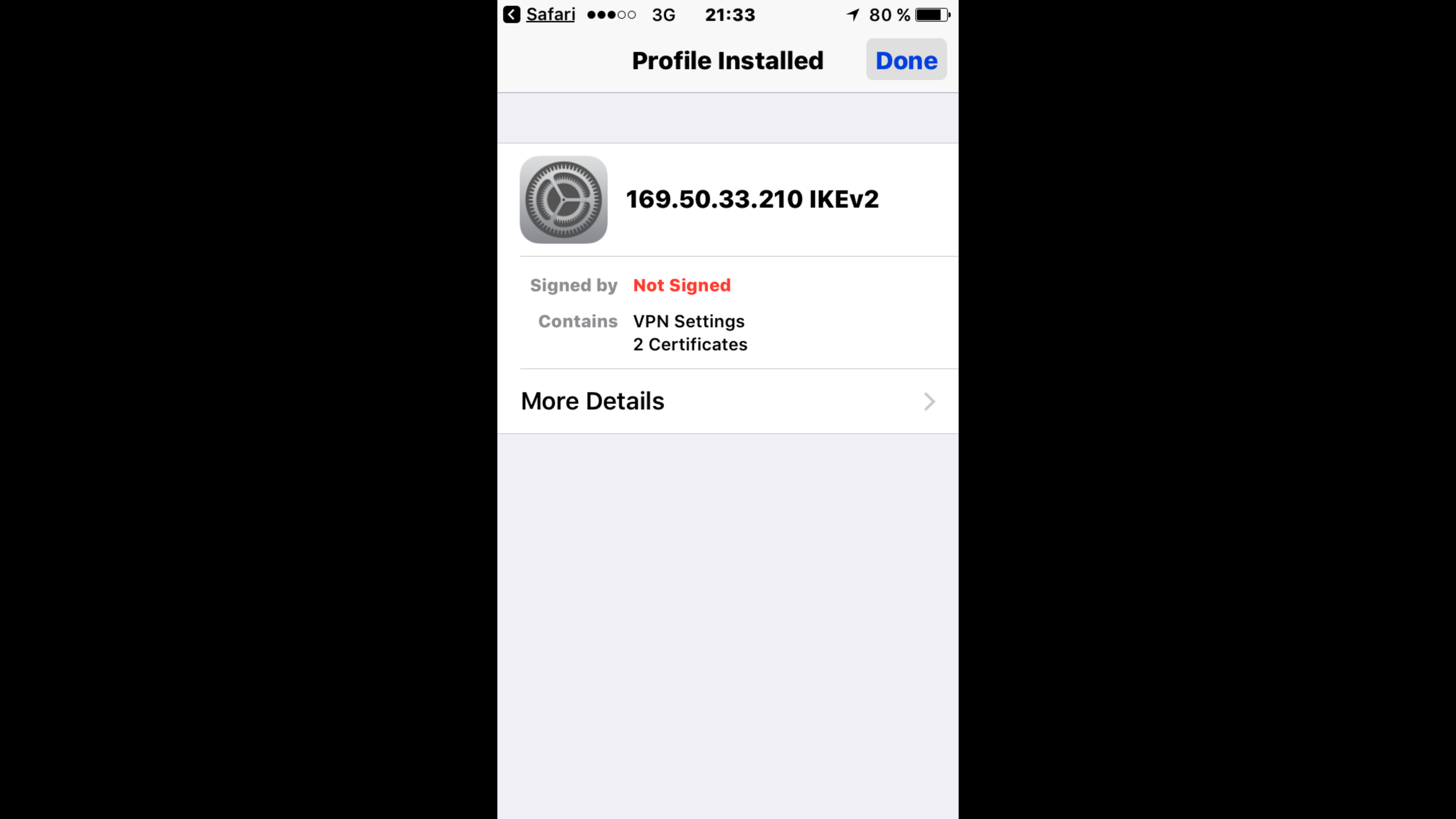

Safari
21:32
80 %
Cancel
Install Profile
Install
169.50.33.210 IKEv2
Signed by
Not Signed
Contains
VPN Settings
2 Certificates
More Details

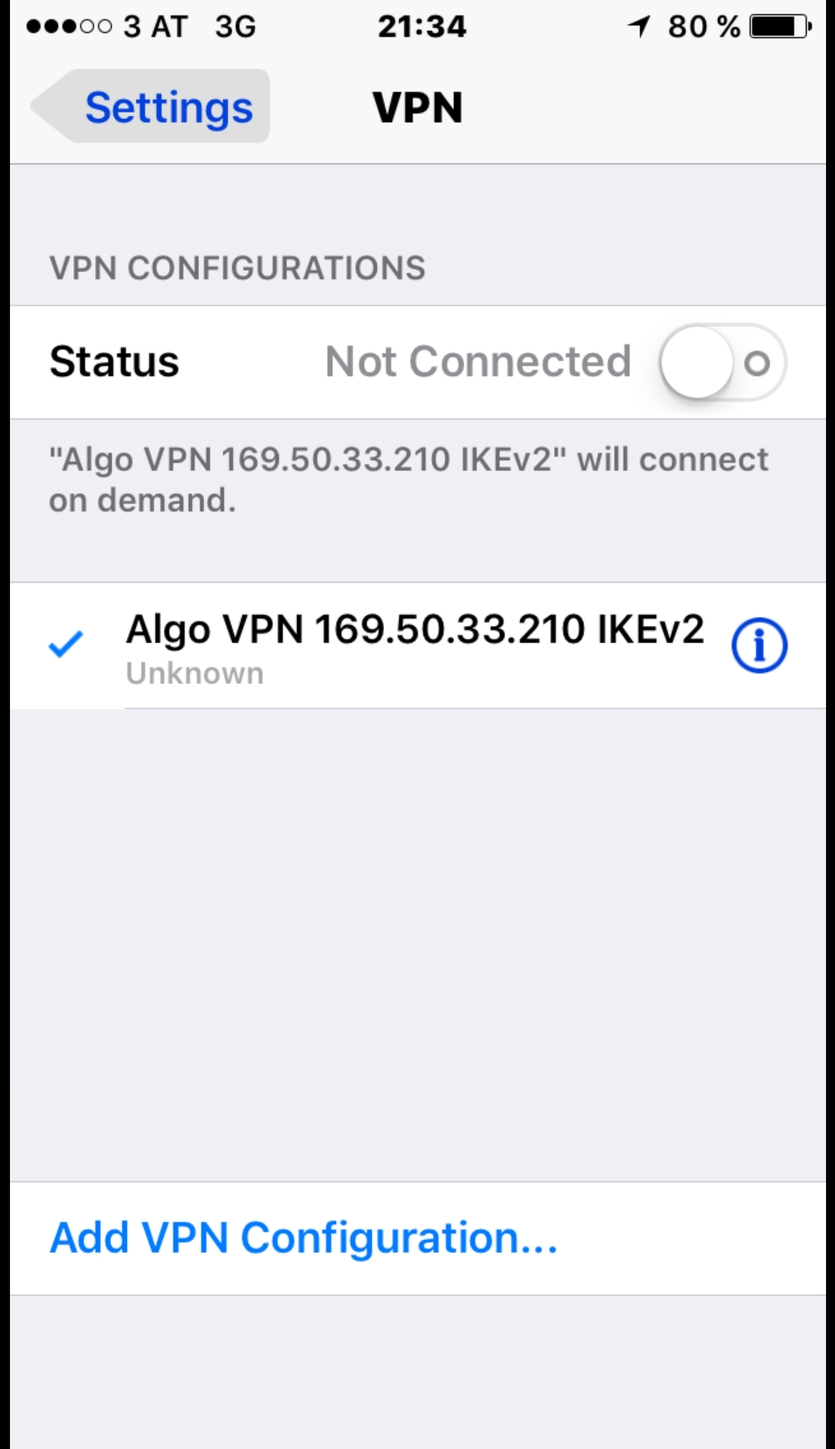

Safari
21:32
80 %
Back
169.50.33.210 IKEv2
VPN SETTINGS
VPN
CERTIFICATES (2)
MacLemon.p12
169.50.33.210
169.50.33.210
Issued by: 169.50.33.210
Expires: 2 May 2027

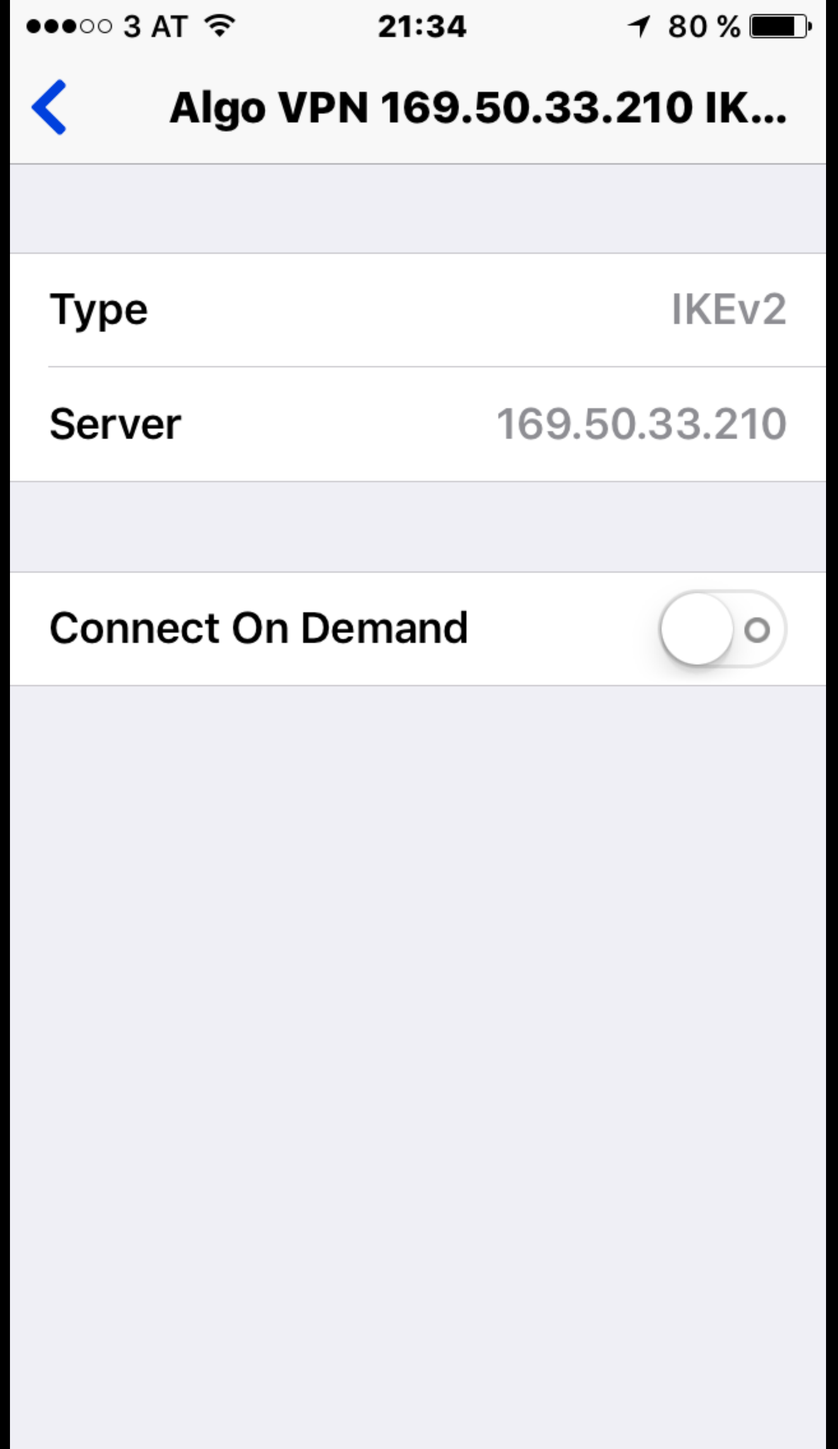

Safari
21:33
80 %
Cancel
Enter Passcode
Done
Enter your passcode
q w e r t z u i o p ü
a s d f g h j k l ö ä
y x c v b n m
123
Leerzeichen
Return

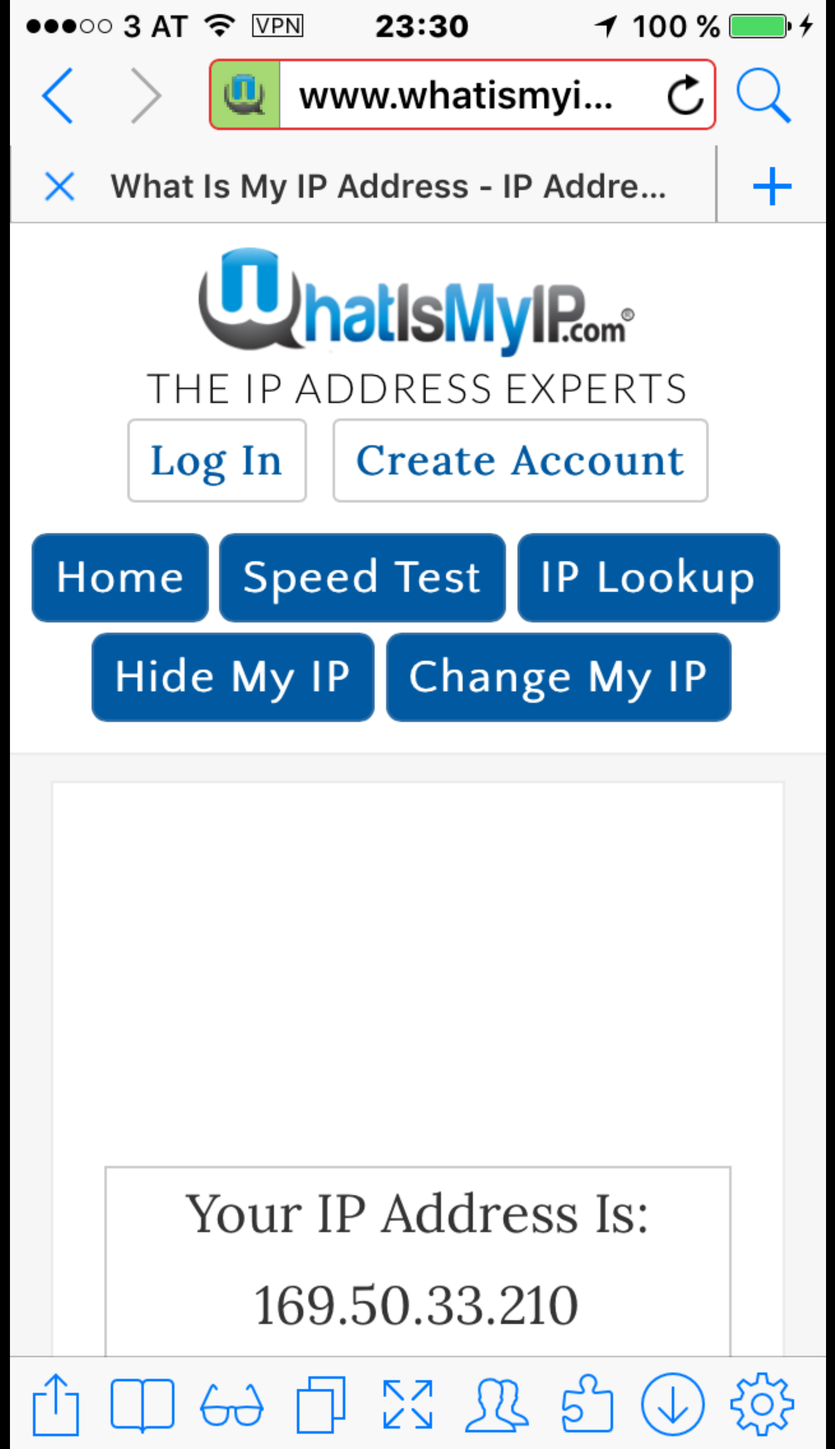

Safari
21:33
80 %
Cancel
Warning
Install
UNMANAGED ROOT CERTIFICATE
Installing the certificate “169.50.33.210” will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.
VPN
The network traffic of your iPhone may be secured, filtered or monitored by a VPN server.
UNSIGNED PROFILE
The profile is not signed.


Safari
21:33
80 %
Cancel
Warning
Install
UNMANAGED ROOT CERTIFICATE
Installing the certificate “169.50.33.210” will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.
VPN
The network traffic of your iPhone may be secured, filtered or monitored by a VPN server.
Install
Cancel


Safari ●●●○○ 3G 21:33 80 %
Profile Installed
Done
169.50.33.210 IKEv2
Signed by
Not Signed
Contains
VPN Settings
2 Certificates
More Details


●●●○○ 3 AT 3G
21:34
80 %
Settings
VPN
VPN CONFIGURATIONS
Status
Not Connected
"Algo VPN 169.50.33.210 IKEv2" will connect on demand.
Algo VPN 169.50.33.210 IKEv2
Unknown
Add VPN Configuration...


●●●○○ 3 AT
21:34
80 %
Algo VPN 169.50.33.210 IK...
Type
IKEv2
Server
169.50.33.210
Connect On Demand


3 AT
VPN
23:30
100 %
www.whatismyi...
What Is My IP Address - IP Addre...
WhatIsMyIP.com
THE IP ADDRESS EXPERTS
Log In
Create Account
Home
Speed Test
IP Lookup
Hide My IP
Change My IP
Your IP Address Is:
169.50.33.210

/Algo VPN

Other VPN solutions

Just obscure inspiration…

SSH Layer 2 VPN

SSHuttle

SSH -D

DynamicForward

The end

#balccon2k17

@MacLemon

Thanks