🔕

VPNs
Angewandte Verwirrung für Leitweg Tabellen

VPNs
Angewandte Verwirrung für Leitweg Tabellen

#lww17

@leyrer

@MacLemon

VPN

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

Warum?

VPN Lösungen

Protokolle

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
VPNJack	🟥	🟨	🟥	🟥	🟨	🟥	🟥	🟨	🟥
GoTrusted	🟥	🟥	🟥	🟥	🟨	🟥	🟥	🟨	🟥
BeeVPN	🟨	🟨	🟩	🟥	🟨	🟥	🟥	🟥	🟩
GoVPN	🟨	🟨	🟨	🟥	🟨	🟩	🟩	🟩	🟨
Hola!VPN	🟥	🟥	🟨	🟥	🟨	🟥	🟨	🟩	🟥
Hotspot Shield	🟥	🟨	🟥	🟥	🟨	🟨	🟥	🟩	🟥
LibertyShield	🟥	🟨	🟥	🟥	🟨	🟨	🟥	🟥	🟥
MyVPN.Pro	🟥	🟨	🟨	🟥	🟨	🟥	🟥	🟥	🟩
Spotflux	🟥	🟥	🟩	🟥	🟨	🟨	🟥	🟨	🟩
HideALLIP	🟥	🟨	🟩	🟥	🟥	🟨	🟥	🟩	🟥
TVWhenAway	🟥	🟨	🟨	🟥	🟨	🟥	🟩	🟥	🟩
VPN Master	🟨	🟨	🟥	🟥	🟨	🟨	🟨	🟨	🟥
Zenmate	🟨	🟨	🟩	🟥	🟨	🟥	🟨	🟨	🟥
IntelliVPN	🟥	🟨	🟥	🟥	🟨	🟥	🟨	🟨	🟩
Norton WiFi Privacy	🟥	🟨	🟥	🟥	🟨	🟥	🟥	🟩	🟩
AnonVPN	🟥	🟩	🟨	🟥	🟨	🟥	🟥	🟥	🟥
Betternet	🟨	🟥	🟨	🟥	🟨	🟨	🟩	🟩	🟩
EtherealVPN	🟥	🟨	🟩	🟥	🟨	🟥	🟥	🟨	🟥
Blockless	🟨	🟨	🟨	🟥	🟨	🟥	🟨	🟥	🟥
DotVPN	🟩	🟨	🟨	🟥	🟨	🟩	🟩	🟩	🟨
NolimitVPN	🟩	🟨	🟨	🟥	🟨	🟨	🟨	🟨	🟥
Steganos	🟨	🟨	🟥	🟥	🟨	🟥	🟩	🟨	🟩
TunnelBear	🟨	🟨	🟥	🟥	🟩	🟩	🟨	🟩	🟥
Unblock-Us	🟨	🟨	🟥	🟥	🟨	🟥	🟥	🟨	🟥
NetShade	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟩
AceVPN	🟥	🟥	🟥	🟥	🟨	🟥	🟨	🟨	🟥
Kepard	🟩	🟨	🟨	🟥	🟨	🟥	🟨	🟨	🟥
FinchVPN	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟨	🟨
LibertyVPN	🟥	🟨	🟥	🟥	🟨	🟥	🟥	🟥	🟥
LimeVPN	🟩	🟥	🟥	🟥	🟩	🟩	🟥	🟨	🟥
SunVPN	🟥	🟥	🟥	🟥	🟨	🟨	🟥	🟨	🟥
TorVPN	🟥	🟥	🟩	🟥	🟩	🟨	🟨	🟩	🟥
Unspyable	🟥	🟨	🟩	🟥	🟩	🟥	🟥	🟥	🟥
VPN Shield	🟨	🟥	🟨	🟥	🟨	🟩	🟨	🟩	🟨

3Monkeys	1	3.5	0	2	2.5	2	0	7	3	Switzerland	Cooperative	No	No		Yes	Yes	Yes	No	No
AceVPN	4	3	0	3.5	2.5	4	0	0	0	USA	Five	Yes			Yes		Yes	No	No
ActiVPN	1	2	0	2	2.5	0	0	1	3	France	Nine	No						Email	Yes
AirVPN	1	2	0	1	0	0	1	0	0	Italy	Fourteen	No	No					Email	Yes
Anonine	4	3	1	2	2.5	0	11	4	1	UK	Five	Yes	No		Yes		Yes	Email	Yes
AnonVPN	4	1	2	0	2.5	0	0	7	4	USA	Five	Yes	No		No		No	Email	No
Anonymizer	4	1	2	1	2.5	3	13	2	1	USA	Five	Yes	No			No	No	Email	No
AnonymousVPN	0	3	2	2	2.5	0	2	4	0	Seychelles	No	No	No		Yes	Yes		Email	No
AnVill	0	3	4	2.5	1.5	2	0	4	0	Seychelles	No	No			Yes		Yes	No	Yes
Avast Secureline	1	3.5	4	1	1.5	2	3	4	2.5	Czech Republic	Cooperative	No			Yes	Yes	Yes	No	No
Avira Phantom VPN	1	2	0	0	1.5	2	0	1	1.5	Germany	Fourteen	No	No			Yes	No	No	No
AzireVPN	1	0	0	0	1.5	1	1	2	0	Sweden	Fourteen	No	No	No	No	No	No	Email	Yes
BestVPN	1	2	1	0	1.5	0	10	0	0	Denmark	Nine	No						Email	Yes
Betternet	2	3	2	0	2.5	3	3	0	0	Canada	Five	No			Yes	Yes		Yes	No
BlackVPN	0	0	0	2	0	0	4	0	0	Hong Kong	No	No	No	No	No	No	No	Email	Yes
BlazingVPN	3	0	0	2	0.5	2	4	0	0		Not Disclosed	Not Disclosed	No	No	No	No	No	Email	Yes
Blockless	2	2	2	4	2.5	0	6	7	3	Canada	Five	No						Email	No
BolehVPN	0	0	0	0.5	0	0	5	4	0	Malaysia	No	No	No	No	No	No	No	Email	Yes
Boxpn	0	2	1	2	2.5	0	9	4	4	Seychelles	No	No						Email	Yes
BTGuard	4	1.5	1	1	1.5	4	5	0	3	USA	Five	Yes	No				No	Email	Yes
Buffered	1	3.5	2	2	1.5	2	6	4	3.5	Hungary	Cooperative	No	No		Yes	Yes	Yes	Email	No
CactusVPN	0	0	4	2.5	0	1	4	2	0	Moldova	No	No	No	No	No	No	No	No	Yes
Celo	2	3	4	1	1.5	0	5	3	1	Australia	Five	No	No		Yes		Yes	No	Yes
ChillGlobal	1	2.5	0	1	2.5	4	13	0	1	Germany	Fourteen	No	No		Yes			No	No
Cloak	4	3.5	0	2	2.5	3	2	2	1	USA	Five	Yes	See Note		Yes	Yes	Yes	No	No
CrypticVPN	4	0.5	1	2	2.5	2	1	0	1	USA	Five	Yes	No		No	No	No	Email	Yes
CryptoHippie	4	2	0	1.5	0	3	1	0	0	USA	Five	Yes	See Note	No		Yes		Yes	Yes
CryptoStorm	1	1.5	0	0	1.5	4	4	6	0	Iceland	Cooperative	No	No				No	Yes	Yes
CyberGhost	0	1	1	2.5	1.5	2	10	4	0	Romania	No	No	No		No		No	Email	Yes
DatioVPN	0	2	0	2	2.5	2	11	6	0	Panama	No	No	No					No	No
DefenseVPN	2	2	0	2.5	2.5	0	3	1	3	Barbados	See Note	Owned	No					No	No
DissembleVPN	3	2	1	2	0	2	2	4	0		Not Disclosed	Not Disclosed	No					Yes	Yes
DotVPN	0	2.5	2	4	2.5	1	3	0	2	Hong Kong	No	No					Yes	Email	No
EarthVPN	0	2.5	1	2.5	2	0	4	3	4	Northern Cyprus	No	No	No				Yes	Yes	Yes
EtherealVPN	3	2	1	0	2.5	4	13	0	3		Not Disclosed	Not Disclosed						Email	Yes
ExpressVPN	2	2	1	0	0.5	0	0	4	4.5	British Virgin Islands	See Note	Owned	No	No	Yes	Yes	No	Email	Yes
Faceless.ME	0	3	0	2	2.5	0	12	6	0	Cyprus	No	No			Yes		Yes	No	No
FinchVPN	0	3.5	1	2.5	3	2	7	4	1	Malaysia	No	No	No		Yes	Yes	Yes	Email	Yes
FlowVPN	3	3	2	2	2.5	0	3	3	0		Not Disclosed	Not Disclosed			Yes		Yes	Email	No
FlyVPN	3	3	0	2	2.5	2	5	4	0		Not Disclosed	Not Disclosed			Yes		Yes	No	No
FoxyProxy	4	2	1	1	2.5	2	3	0	0	USA	Five	Yes	No	No		Yes		Email	No
FreedomIP	3	3.5	1	2	2.5	2	3	4	1		Not Disclosed	Not Disclosed			Yes	Yes	Yes	Email	Yes
Freedome	0	3	2	2	0	2	4	4	0	Finland	No	No				Yes	Yes	Yes	No
FreeVPN Ninja	3	2	0	2	2.5	2	1	0	0		Not Disclosed	Not Disclosed						Yes	Yes
FrootVPN	1	0	1	2	2.5	2	1	1	4	Sweden	Fourteen	No	No	No	No	No	No	Email	Yes
FrostVPN	4	3	4	2.5	2.5	0	5	6	0	USA	Five	Yes	No		Yes	Yes		No	Yes
GetFlix	2	2	0	1	2.5	2	9	4	2.5	Canada	Five	No						No	No
GhostPath	4	2	1	2	2.5	2	1	7	4	USA	Five	Yes						Email	Yes
GoTrusted	4	3	0	0.5	2.5	0	0	6	3	USA	Five	Yes			Yes	Yes		No	No
GoVPN	1	2.5	2	0	2.5	1	2	0	2	Germany	Fourteen	No	No				Yes	Email	No
Hide.me	0	2	1	1	1.5	0	5	4	4	Malaysia	No	No	No					Email	Yes
HideALL.IP	3	2	1	0	4	2	11	2	0		Not Disclosed	Not Disclosed						Email	Yes
HideIPVPN	4	1.5	4	2.5	2.5	1	9	3	4	USA	Five	Yes					No	No	Yes
HideMyAss	4	3.5	1	2.5	3	2	6	3	3	UK	Five	Yes	No		Yes	Yes	Yes	Email	Yes
Hide Me IP	4	2	1	2	2.5	2	6	2	4	USA	Five	Yes						Email	Yes
HolaVPN	3	6	2	0	2.5	0	5	3	4		Not Disclosed	Not Disclosed	Yes		Yes		Yes	Email	No
Hotspot Shield	4	2.5	4	0	2.5	3	7	0	3	USA	Five	Yes					Yes	No	Yes
HotVPN	3	2	1	2	2.5	0	10	6	0		Not Disclosed	Not Disclosed						Email	Yes
IBVPN	0	2	4	1.5	1.5	2	0	3	0.5	Romania	No	No	No					No	Yes
Identity Cloaker	1	2.5	0	2	1.5	2	12	0	0	Czech Republic	Cooperative	No	No			Yes		No	No
IncognitoVPN	4	2.5	0	2	2.5	0	2	0	6	USA	Five	Yes	No	No	Yes		Yes	No	No
In-Disguise	0	2	1	2.5	2.5	2	1	7	0	Belize	No	No						Email	Yes
Insorg	3	2	1	2	2.5	2	13	0	3		Not Disclosed	Not Disclosed	No					Email	Yes
Integrity.st	1	1.5	4	2	1.5	0	0	6	0	Sweden	Fourteen	No	No				No	No	Yes
IntellVPN	3	2.5	0	0	2.5	0	5	4	0		Not Disclosed	Not Disclosed					Yes	No	No
Internetz.me	1	1	0	2	1.5	1	0	7	3	Germany	Fourteen	No	No		No	No		Email	Yes
IntroVPN	3	3	1	2	1.5	4	3	6	1		Not Disclosed	Not Disclosed	No	No	Yes	Yes	Yes	Email	Yes
IPinator	4	2.5	0	1	2.5	0	7	3	4	USA	Five	Yes	No			Yes		No	No
IPredator	1	3.5	0	0.5	2.5	3	0	0	0	Sweden	Fourteen	No	No		Yes	Yes	Yes	Email	Yes
IPVanish	4	2	1	0.5	1.5	0	7	0	0	USA	Five	Yes	No					Email	Yes
Ironsocket	0	3.5	1	1.5	0.5	0	5	4	3	Hong Kong	No	No	No		Yes	Yes	Yes	Email	Yes
Ivacy	0	2	4	1	2.5	0	5	6	4	Hong Kong	No	No	No					No	Yes
IVPN	2	0	0	0	0	0	1	0	0	Gibraltar	See Note	Owned	No	No	No	No	No	Email	Yes
Kepard	0	2	2	3.5	2.5	0	4	0	4	Moldova	No	No						Email	No
LeVPN	0	3	1	1.5	1.5	2	6	0	4	Hong Kong	No	No	No	No	Yes	Yes	Yes	Email	Yes
LibertyShield	4	2.5	4	0	2.5	2	11	0	3	UK	Five	Yes					Yes	No	Yes
LibertyVPN	4	2	0	3	2.5	4	10	0	4.5	USA	Five	Yes						No	No
LimeVPN	0	3	4	3	1	0	17	0	4	Hong Kong	No	No	No		Yes	Yes		No	Yes
LiquidVPN	4	0	3	0	0	0	4	0	4	USA	Five	Yes	No	No	No	No	No	No	Yes
Lokun	1	2.5	0	1	2.5	0	0	3	0	Iceland	Cooperative	No			Yes			Email	Yes
Mullvad	1	0	0	0	0	0	1	2	0	Sweden	Fourteen	No	No	No	No	No	No	Yes	Yes
My Expat Network	4	2	0	2	3	3	4	7	0	UK	Five	Yes						No	No
MyIP.io	4	2	0	1	2.5	4	5	6	2	USA	Five	Yes	No					No	No
My Private Network	0	1.5	0	1	1.5	2	0	3	1.5	Hong Kong	No	No	No	No	Yes	No		Email	Yes
MyVPN.Pro	4	2	2	0	1.5	0	11	0	0	USA	Five	Yes						Email	No
Netshade	4	6	0	4	2.5	3	4	4	0	USA	Five	Yes	Yes		Yes		Yes	No	No
Newshosting	4	2	4	2	1.5	0	0	6	1	USA	Five	Yes	No					No	Yes
NEXTGenVPN	0	2	1	1.5	2.5	4	11	0	1	Seychelles	No	No						Email	No
NolimitVPN	0	2.5	2	4	2.5	3	4	4	4	Singapore	No	No	No		Yes			Email	No
NordVPN	0	0.5	0	0.5	0.5	0	4	1	0	Panama	No	No	No		No	No	No	Email	Yes
Norton WiFi Privacy	4	2	0	0	2.5	0	7	1	0	USA	Five	Yes						No	No
NVPN	0	2	1	2	1.5	2	2	6	1	Bosnia	No	No						Email	Yes
OctaneVPN	4	1.5	1	2	2.5	0	4	3	3	USA	Five	Yes			No	Yes	No	Email	Yes
OneVPN	0	1.5	1	1	1.5	0	9	4	6	Hong Kong	No	No	No				No	Email	Yes
Opera (Browser) VPN	1	7	2	2	2.5	3	4	0	0	Norway	Nine	No	Yes	Yes	Yes	Yes	Yes	Yes	No
OverPlay	4	2	2	1	2.5	2	0	0	3	UK	Five	Yes						Email	No
oVPN.com	1	0	0	0	0	1	3	0	0	Sweden	Fourteen	No	No	No	No	No	No	Yes	Yes
oVPN.to	3	1	0	0.5	0	0	0	6	0		Not Disclosed	Not Disclosed	No		No	No		Email	Yes
Perfect Privacy	1	1.5	0	0.5	0.5	0	4	0	3.5	Switzerland	Cooperative	No	No				No	Email	Yes
PirateParty.ca	2	2	3	2	2.5	0	5	7	0	Canada	Five	No						No	Yes
Private Internet Access	4	0.5	1	0.5	1	0	4	3	3.5	USA	Five	Yes	No	No	No		No	Email	Yes
PrivatePackets.io	2	2	2	0.5	2.5	1	2	0	0	British Indian Ocean	See Note	Owned	See Note	See Note	See Note	See Note	See Note	Email	No
PrivateTunnel	4	2	4	2	2.5	3	2	0	0	USA	Five	Yes						No	Yes
PrivateVPN	1	2	1	2	0	0	7	6	4	Sweden	Fourteen	No						Email	Yes
Proxy.sh	0	2	1	1	0	0	7	0	4	Seychelles	No	No	No					Email	Yes
ProXPN	1	1	4	2	0	2	5	3	0	Netherlands	Nine	No	No		No		No	No	Yes
PRQ	1	2	2	1	2.5	0	7	4	0	Sweden	Fourteen	No						Email	No
PureVPN	0	3	4	0.5	1.5	0	3	4	0	Hong Kong	No	No	No		Yes	Yes		No	Yes
RA4W VPN	4	2	1	2	2.5	2	7	0	1	USA	Five	Yes	No					Email	Yes
RogueVPN	2	2	1	2.5	1.5	2	4	4	4	Canada	Five	No						Email	Yes
RoutVPN	1	3	4	2	1.5	3	3	6	0	Netherlands	Nine	No				Yes	Yes	No	Yes
SaferVPN	0	3.5	1	2	3	0	7	4	3	Israel	No	No	No		Yes	Yes	Yes	Email	Yes
SecureVPN.com	3	2.5	0	2	2.5	2	9	0	6		Not Disclosed	Not Disclosed					Yes	No	No
SecureVPN.to	3	0	1	1	0	0	1	6	0		Not Disclosed	Not Disclosed	No	No	No	No	No	Yes	Yes
SecurityKISS	0	3.5	1	1	4	2	0	7	0	Ireland	No	No			Yes	Yes	Yes	Email	Yes
Seed4.Me	0	3	1	2.5	2.5	2	6	0	0	Taiwan	No	No	No		Yes		Yes	Email	Yes
Seedboxes.cc	0	2	4	2	2.5	0	5	7	1	Cyprus	No	No						No	Yes
ShadeYou	1	2	1	2	2.5	3	0	2	0	Netherlands	Nine	No						Email	Yes
SlickVPN	4	1	1	1	1.5	0	4	1	0	USA	Five	Yes	No		No		No	Email	Yes
Smart DNS Proxy	0	2	0	1.5	2.5	2	9	0	2	Seychelles	No	No						No	No
SmartVPN	0	3	4	2	2.5	2	5	7	4	Morocco	No	No	No		Yes	Yes		No	Yes
SpotBus	4	0	1	0	2.5	3	11	4	0	USA	Five	Yes	Yes					Email	Yes
Steganos	1	1.5	0	4	1.5	0	3	6	0	Germany	Fourteen	No					No	No	No
StrongVPN	4	2	1	2	2.5	2	3	7	0.5	USA	Five	Yes	No					Email	Yes
SwitchVPN	2	2.5	1	2.5	2.5	2	12	2	4	India	No	Yes	No		Yes	Yes	No	Yes	Yes
SumRando	0	3	4	2	1.5	0	0	7	3	Mauritius	No	No	No		Yes	Yes		No	Yes
SunVPN	4	6	0	2	1.5	2	12	0	3	USA	Five	Yes	Yes		Yes		Yes	No	Yes

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

Selbst hosten!

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="AT"
export KEY_PROVINCE="VIE"
export KEY_CITY="Vienna"
export KEY_ORG="Linuxwochen Demo"
export KEY_EMAIL="linuxwochen@example.com"
export KEY_OU="Linuxwochen Wien"
```

```
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 lww-client
```

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

lww-client.crt

lww-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 dh4096.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-CBC
auth SHA384
tls-cipher TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
```

/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

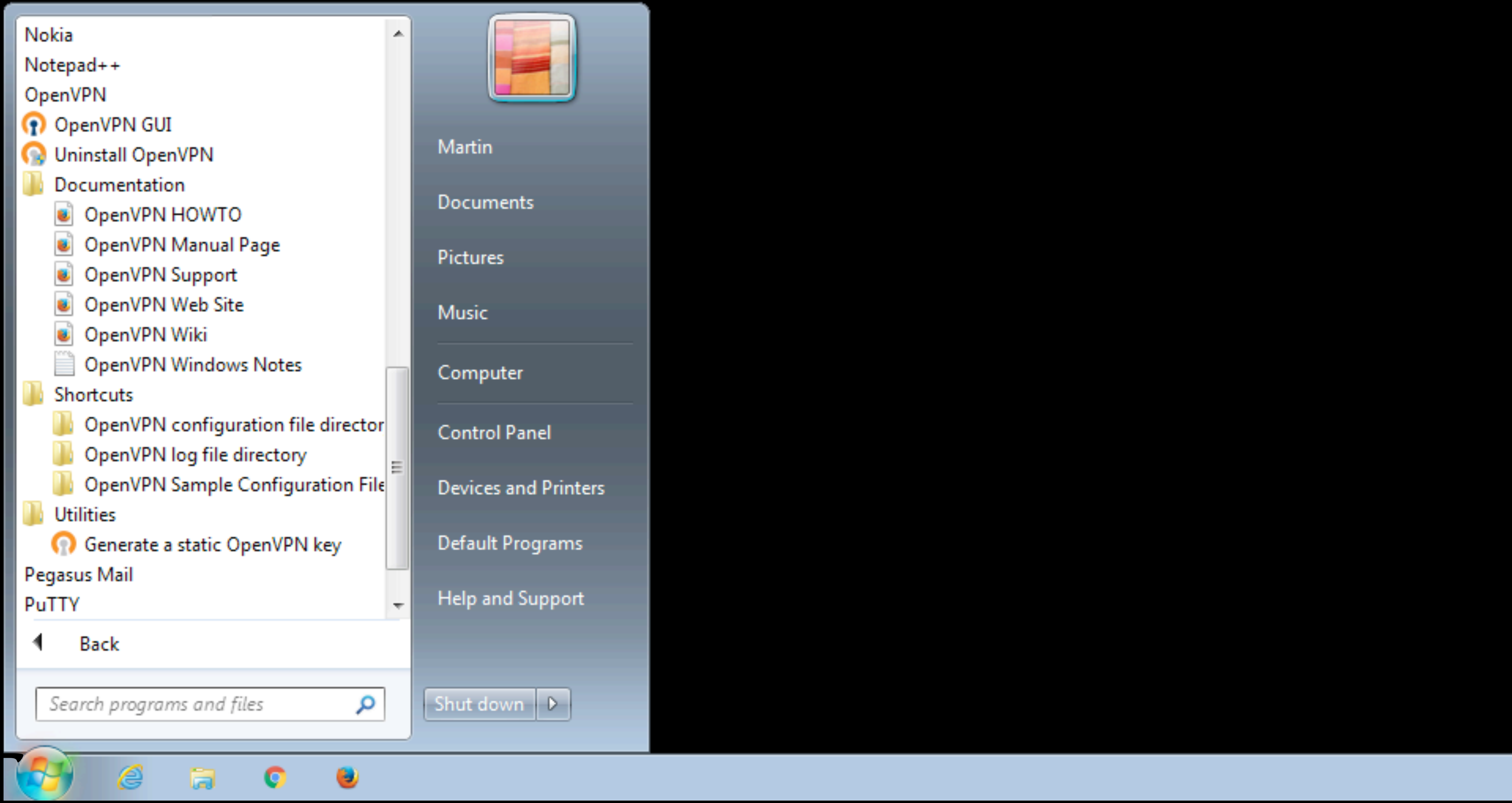
□ Show script window

□ 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\[BENUTZERNAME]\OpenVPN\config\linuxwochen.ovpn

```
remote openvpn.example.com 1194
```

C:\Users\[BENUTZERNAME]\OpenVPN\config\linuxwochen.ovpn

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

```
C:\Users\[BENUTZERNAME]\OpenVPN\config\linuxwochen.ovpn
```

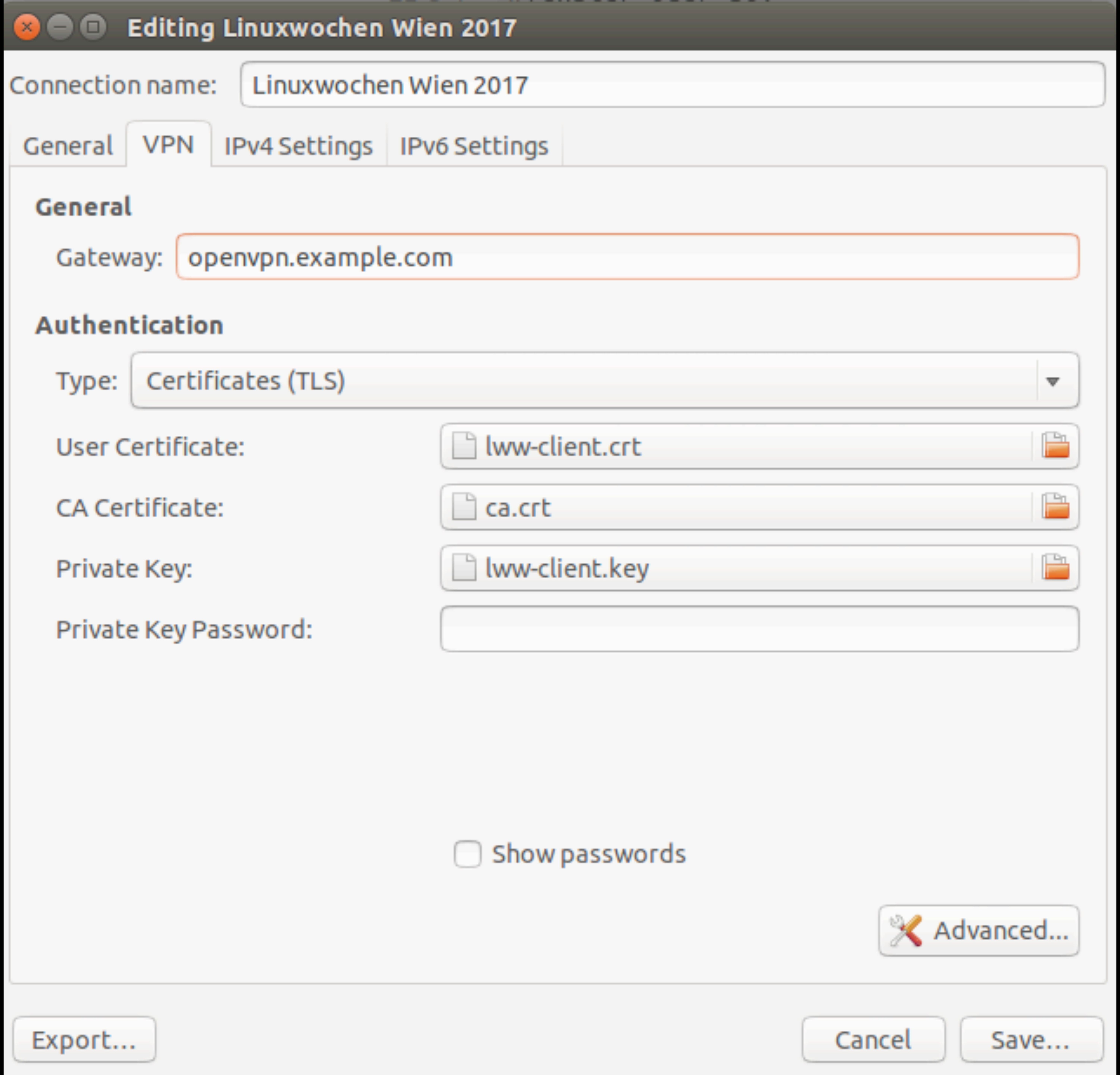
```
cipher AES-256-CBC
auth SHA384
comp-lzo yes
```

linuxwochen is now connected.

Assigned IP: 192.168.23.6

Customize...
12:5

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



Editing Linuxwochen Wien 2017

Connection name: Linuxwochen Wien 2017

General

Gateway: openvpn.example.com

Authentication

Type: Certificates (TLS)

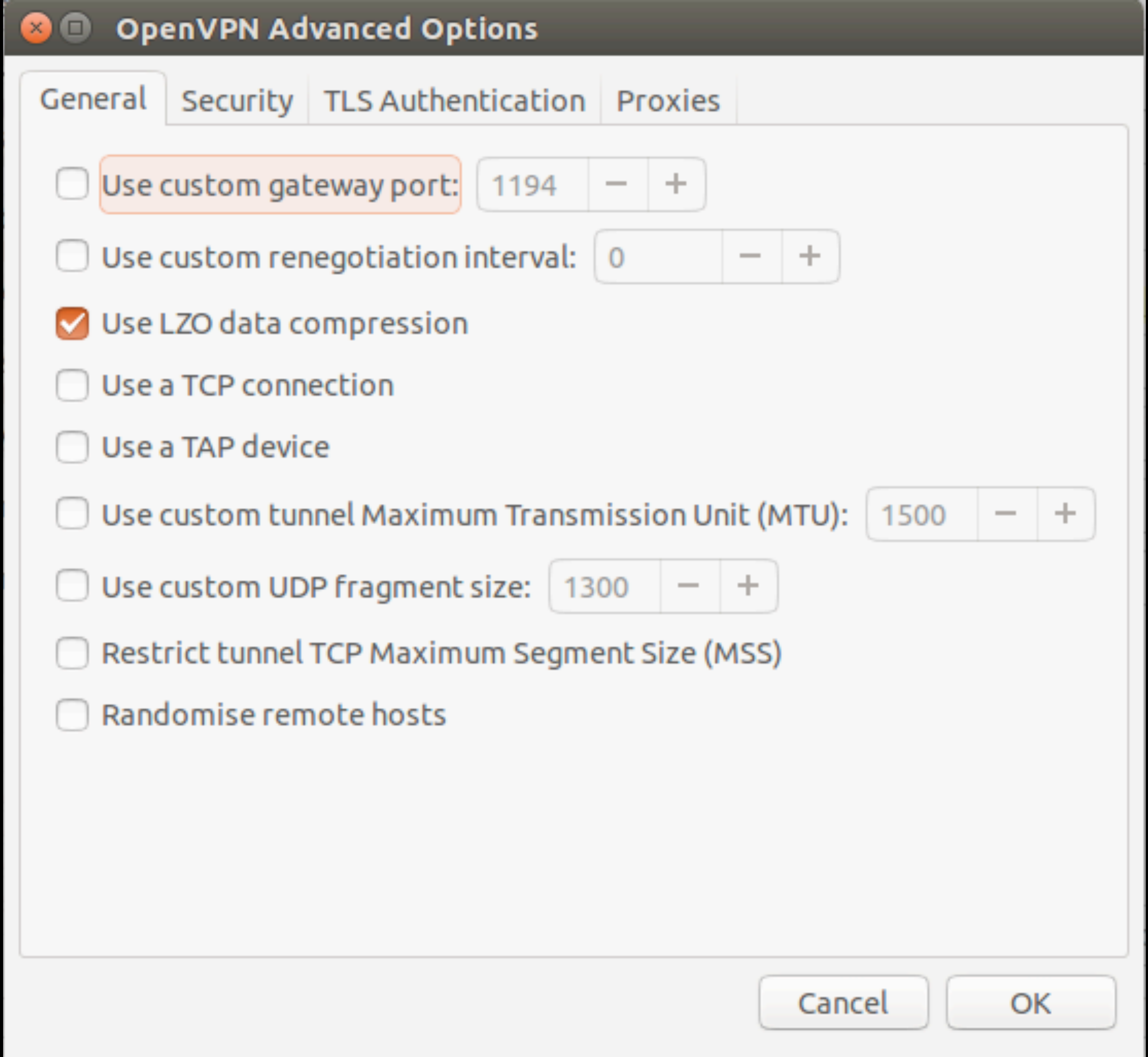
User Certificate: lww-client.crt

CA Certificate: ca.crt

Private Key: lww-client.key

Private Key Password:

☐ Show passwords



OpenVPN Advanced Options

□ Use custom gateway port: 1194

□ Use custom renegotiation interval: 0

☑ Use LZO data compression

□ Use a TCP connection

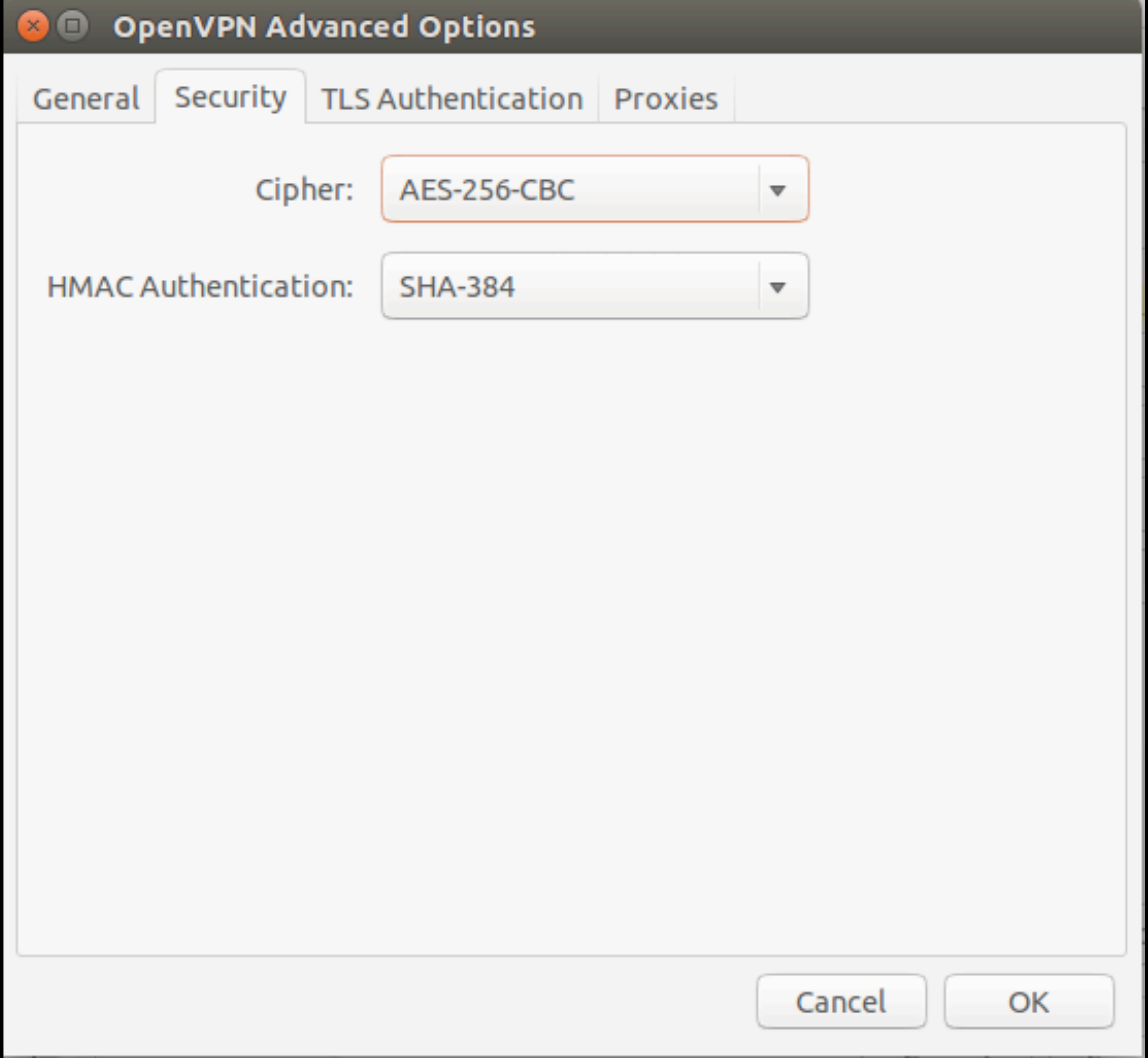
□ Use a TAP device

□ Use custom tunnel Maximum Transmission Unit (MTU): 1500

□ Use custom UDP fragment size: 1300

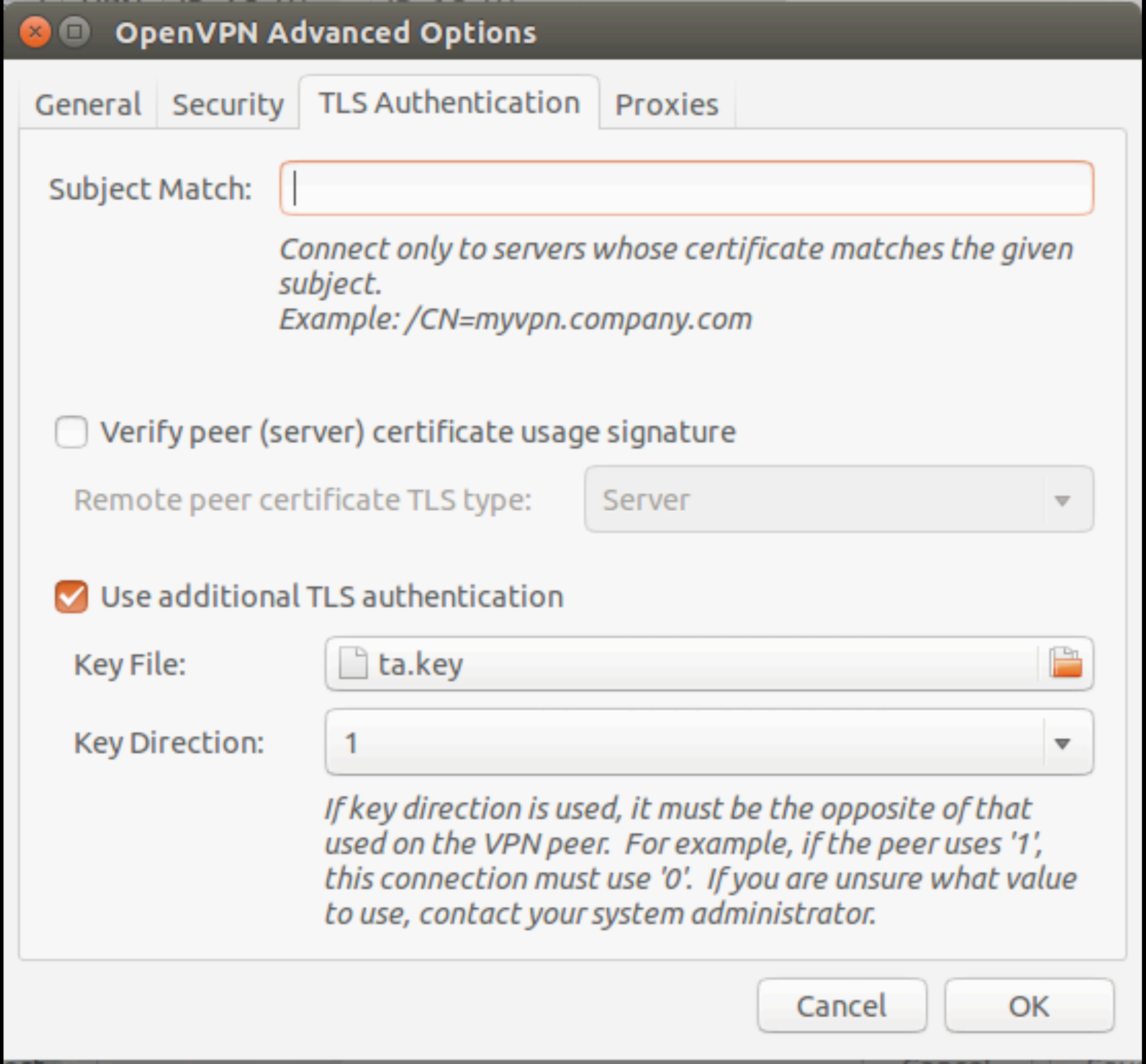
□ Restrict tunnel TCP Maximum Segment Size (MSS)

□ Randomise remote hosts



Cipher: AES-256-CBC

HMAC Authentication: SHA-384



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

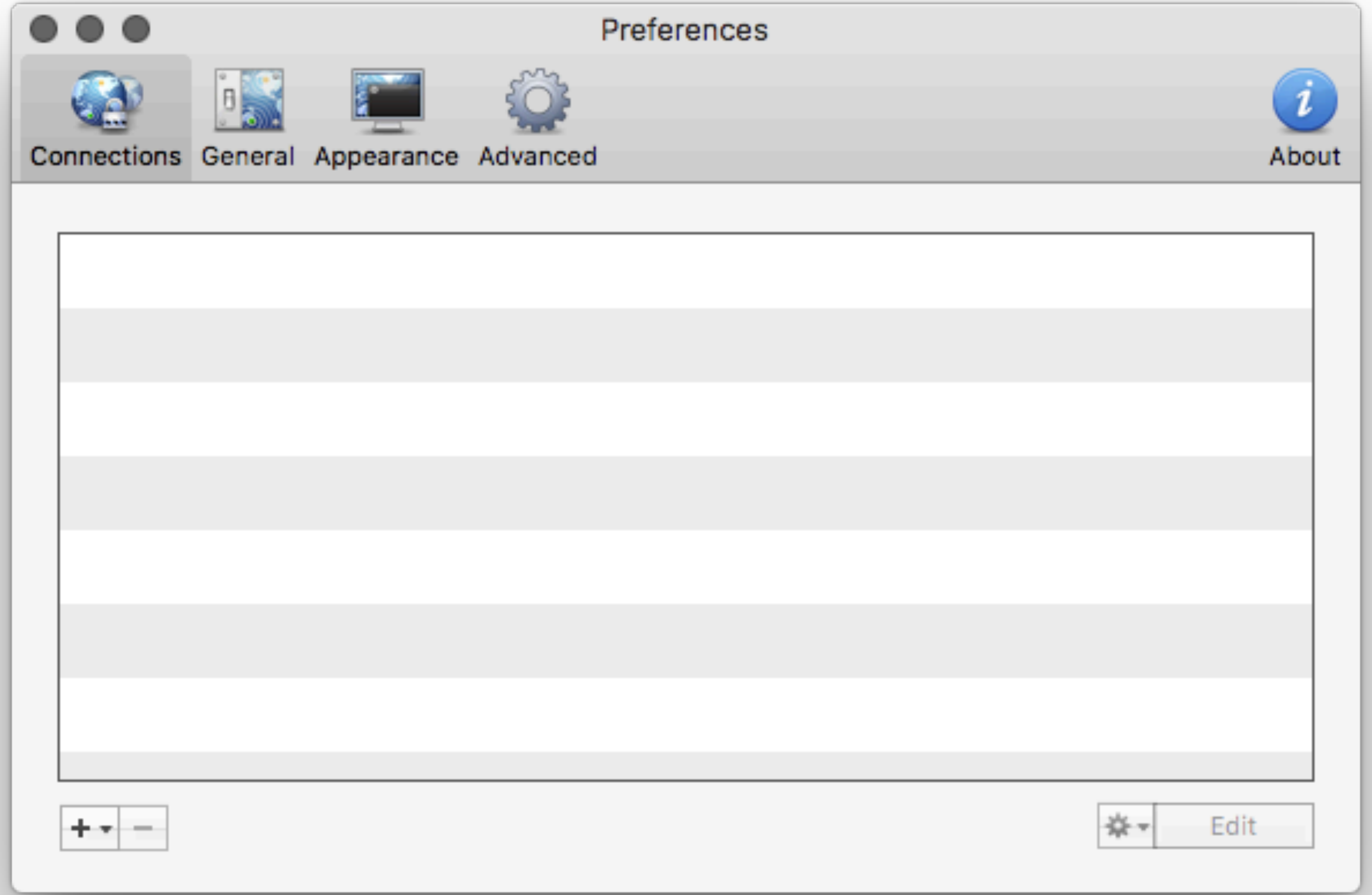
☑ Use additional TLS authentication

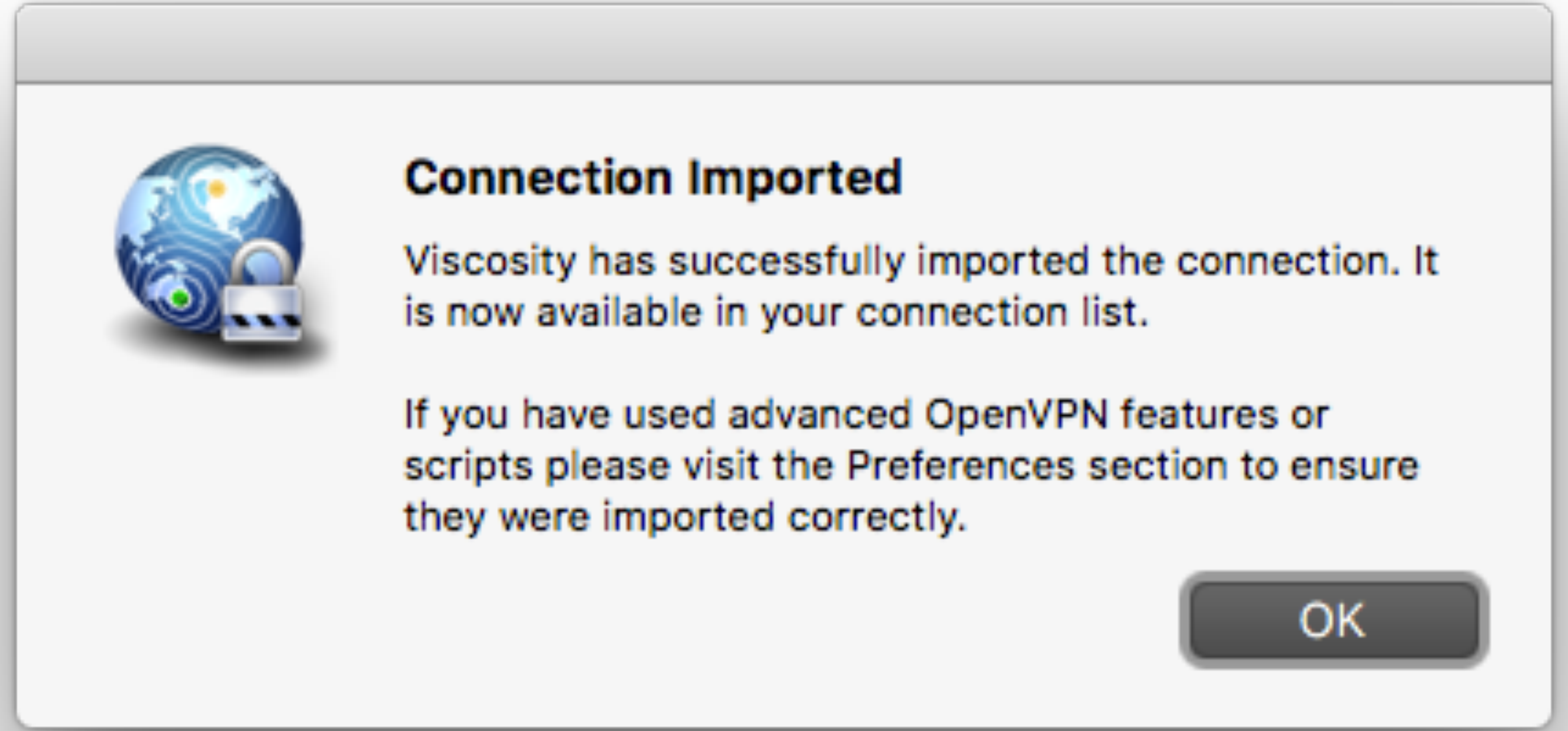
Key File: ta.key

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.

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

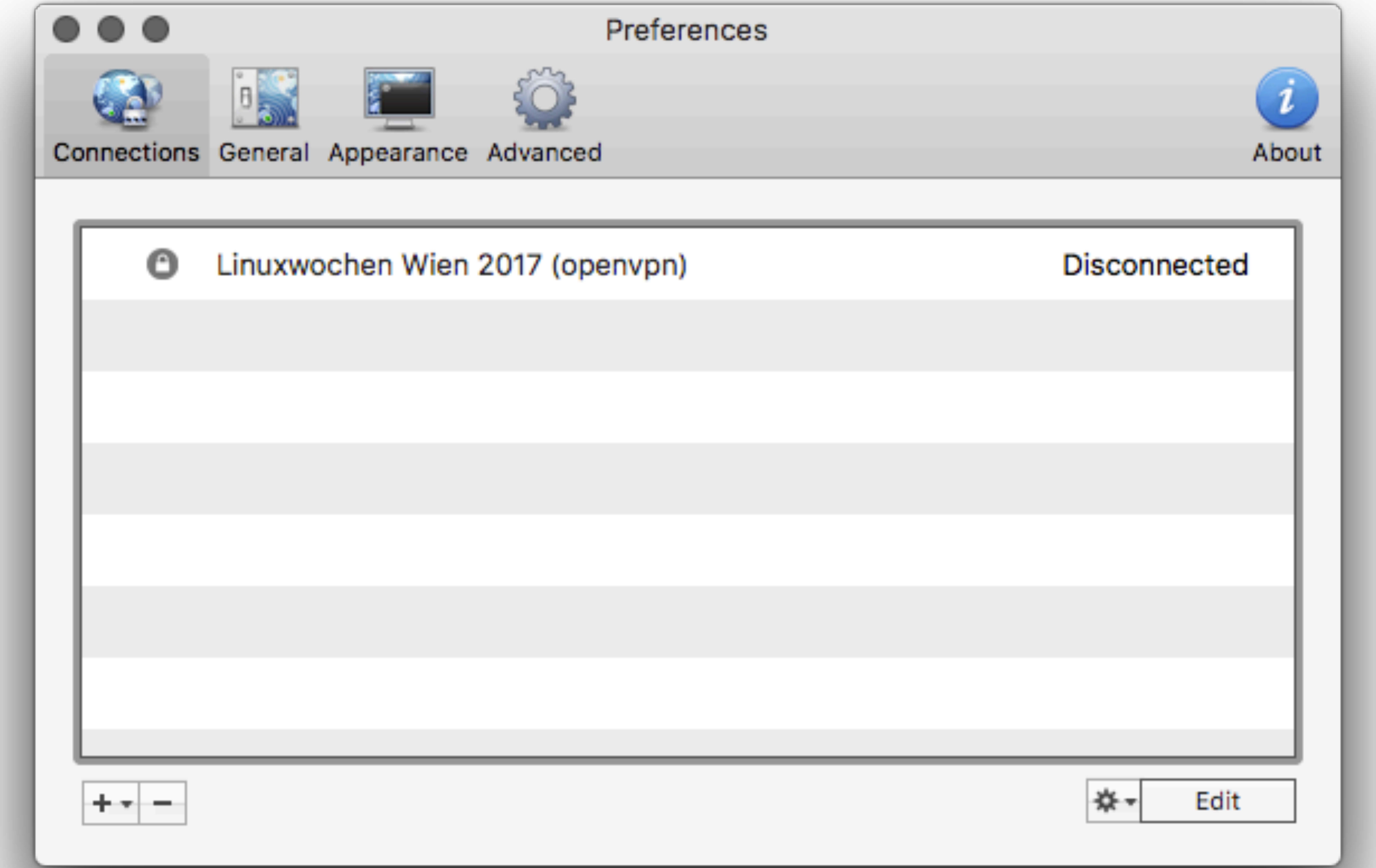

Preferences
Connections
General
Appearance
Advanced
About
+
−
Edit



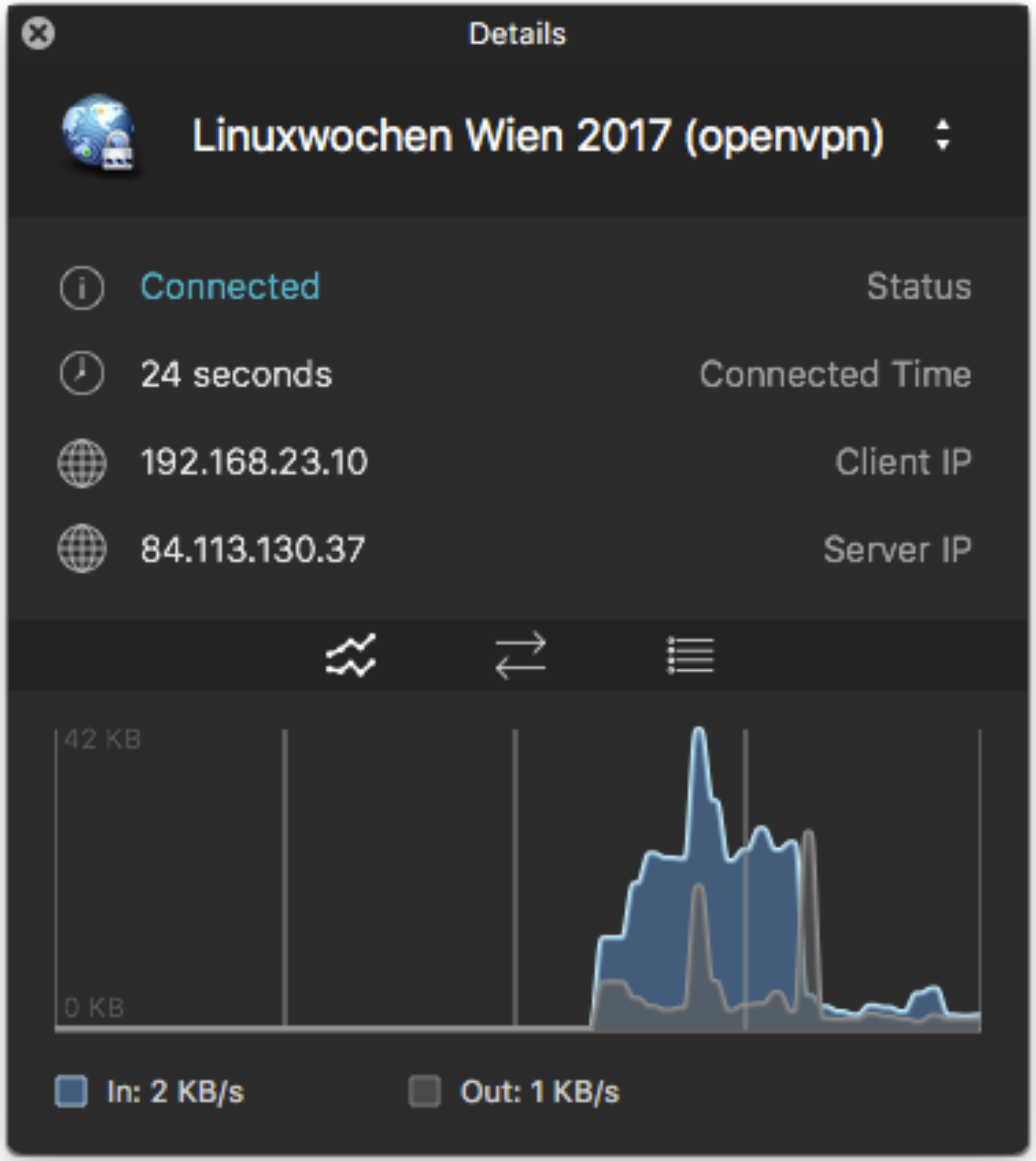
Connection Imported

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.



Linuxwochen Wien 2017 (openvpn) Disconnected



Details

Linuxwochen Wien 2017 (openvpn)

Connected Status

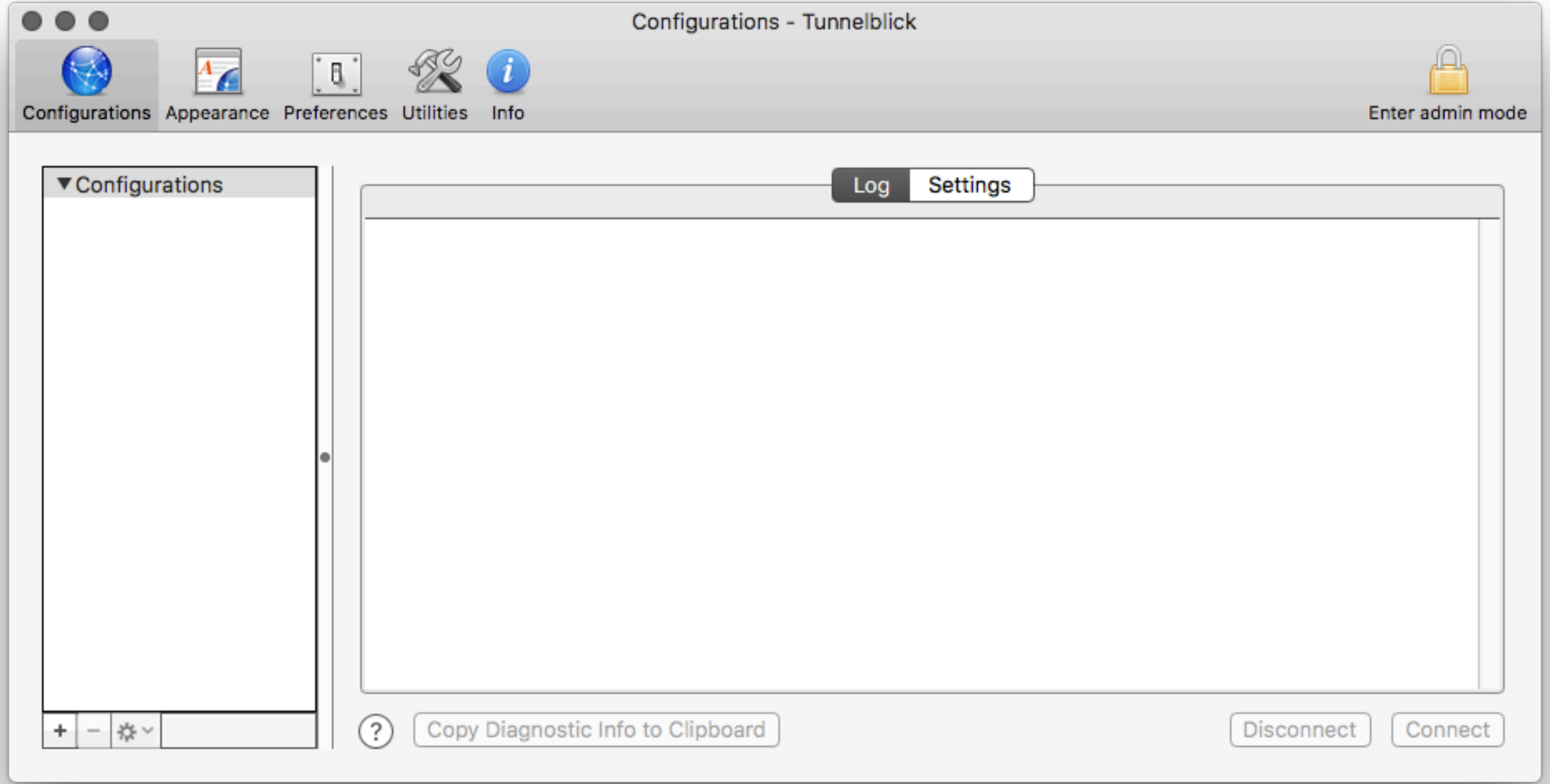
24 seconds Connected Time

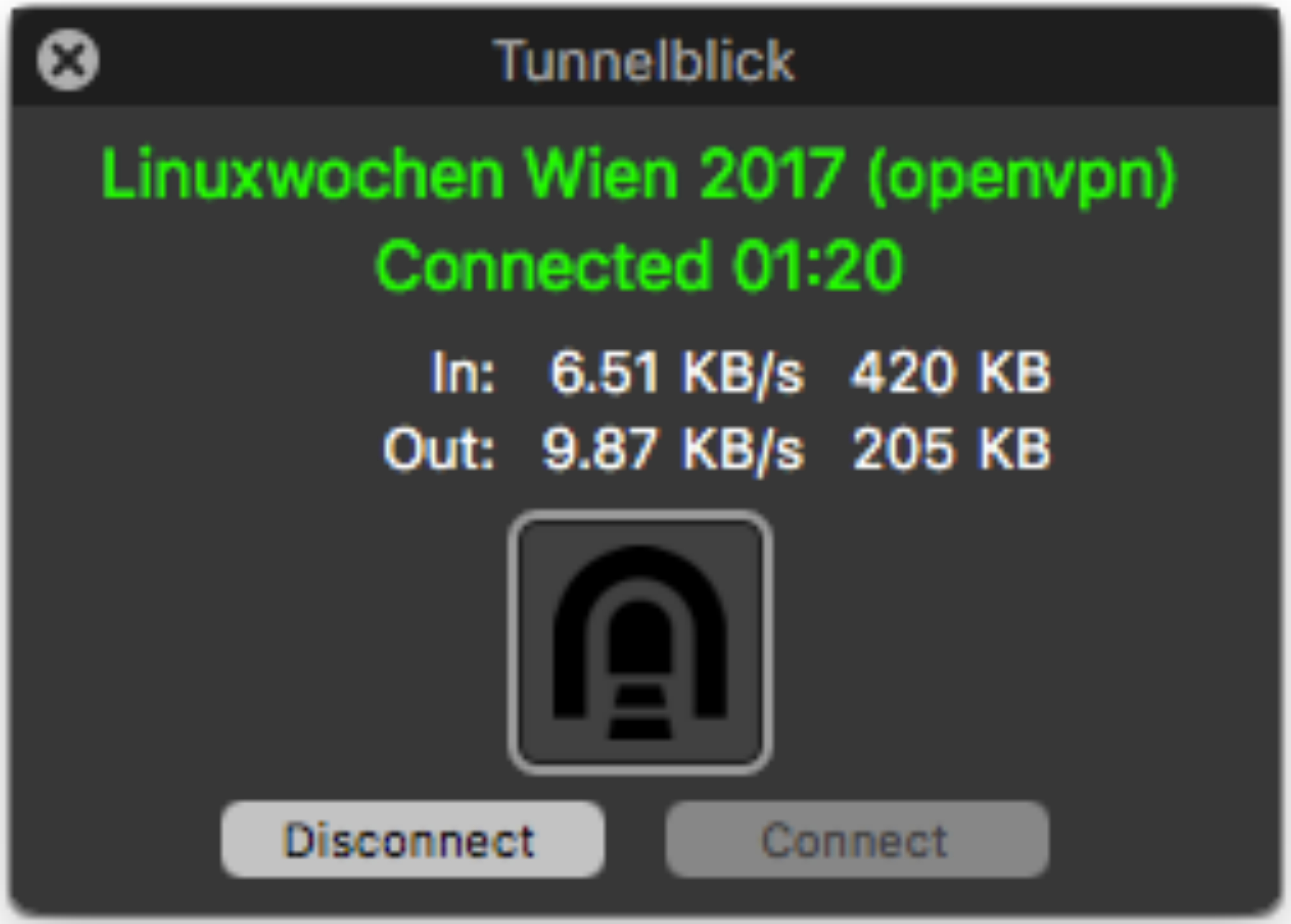
192.168.23.10 Client IP

84.113.130.37 Server IP

🟦 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



Linuxwochen Wien 2017 (openvpn)

Connected 01:20

```
 In:  6.51 KB/s  420 KB
Out:  9.87 KB/s  205 KB
```

```
/etc/openvpn/server.conf
  mtu-test
```

```
lww-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 Security Audits

OSTIF & **private**internetaccess™

/ OpenVPN

Community Edition

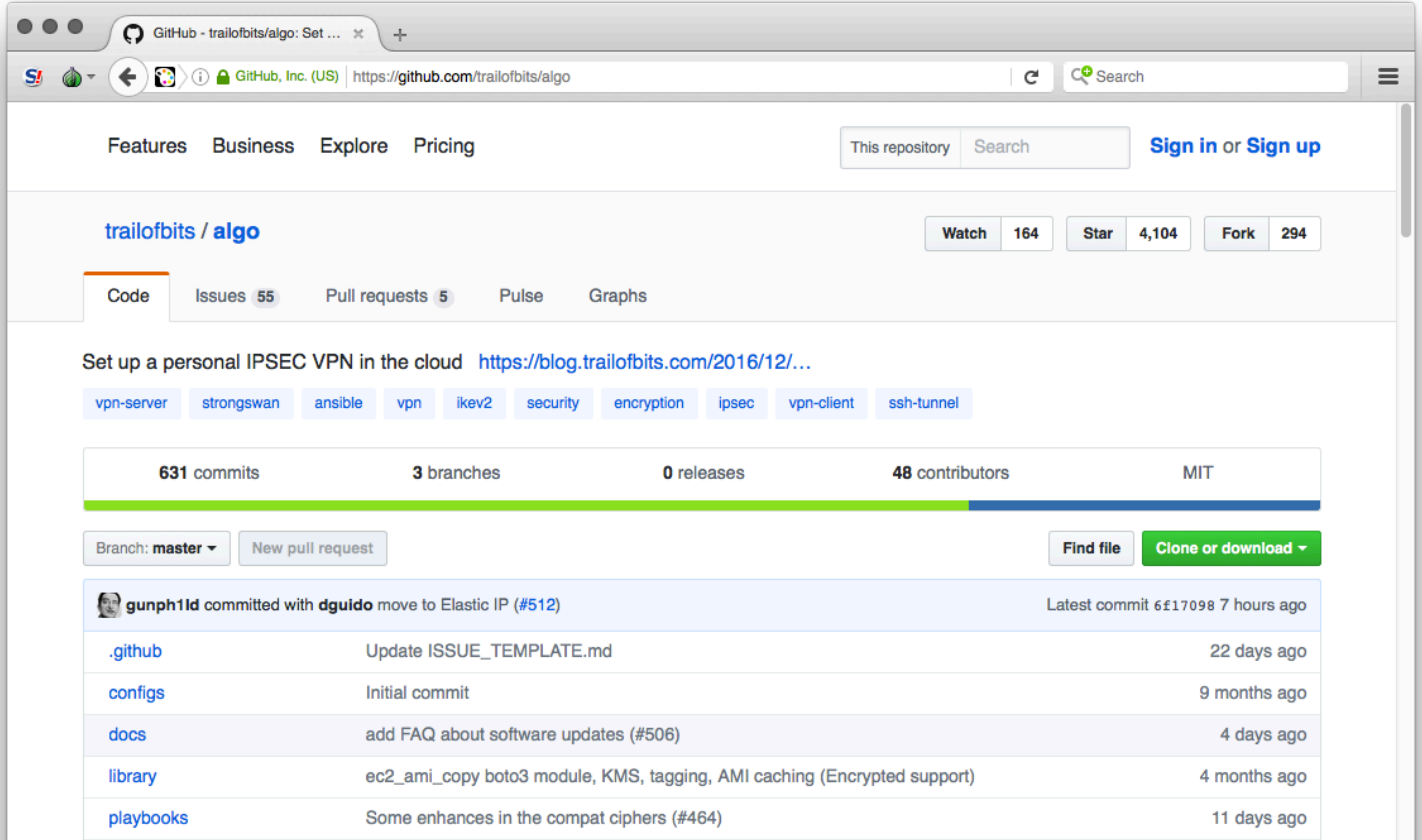
<‘(((^(((><

Die Mitte des Vortrags

Für gewisse Definitionen von „Mitte“.

IPSec, IKEv2

AlgoVPN



Set up a personal IPSEC VPN in the cloud https://blog.trailofbits.com/2016/12/...

gunph1ld committed with dguido move to Elastic IP (#512) Latest commit 6f17098 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

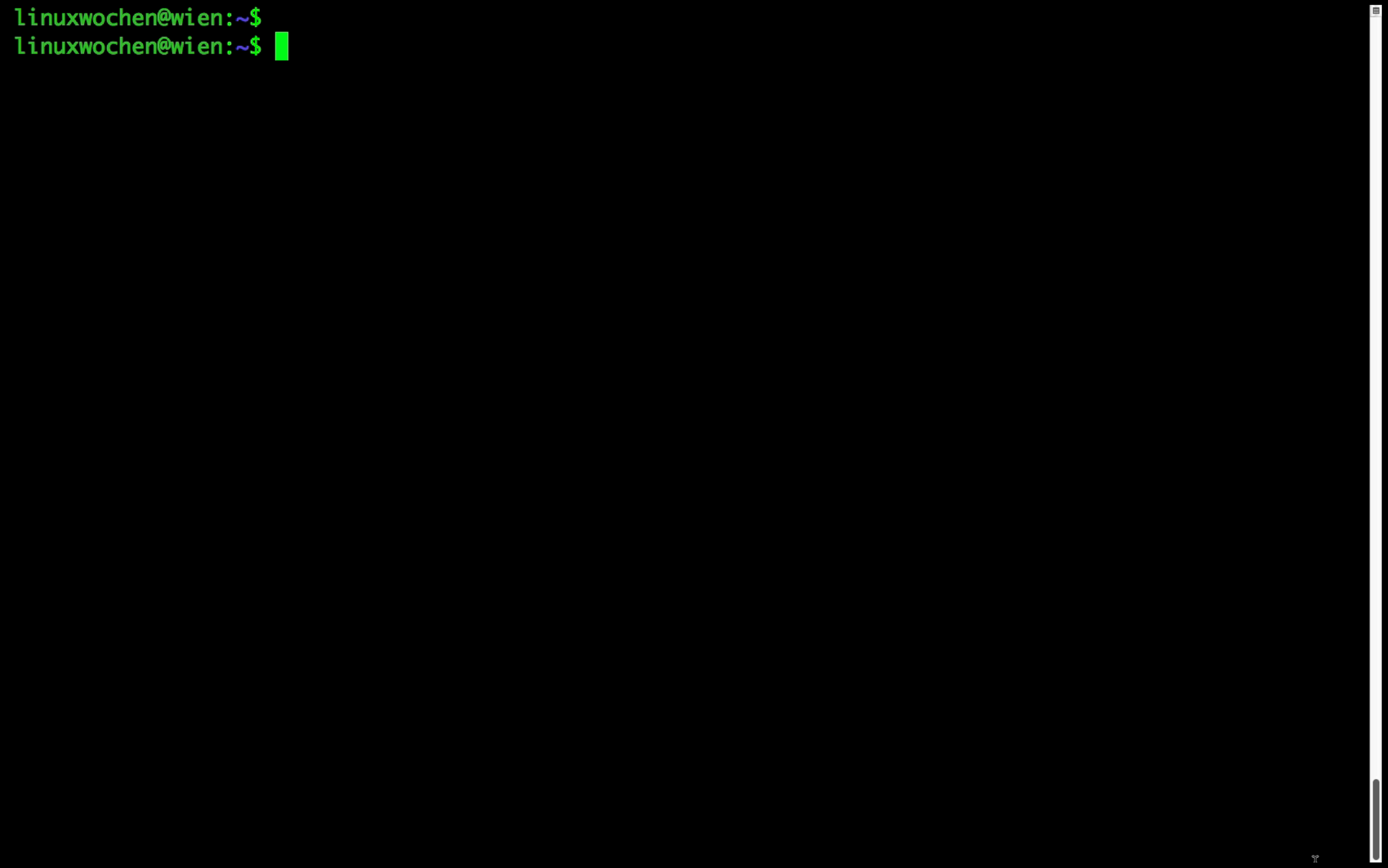
AlgoVPN

Antifeatures

ubuntu®

Ubuntu Server 16.04 LTS

AlgoVPN
Server Installation



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

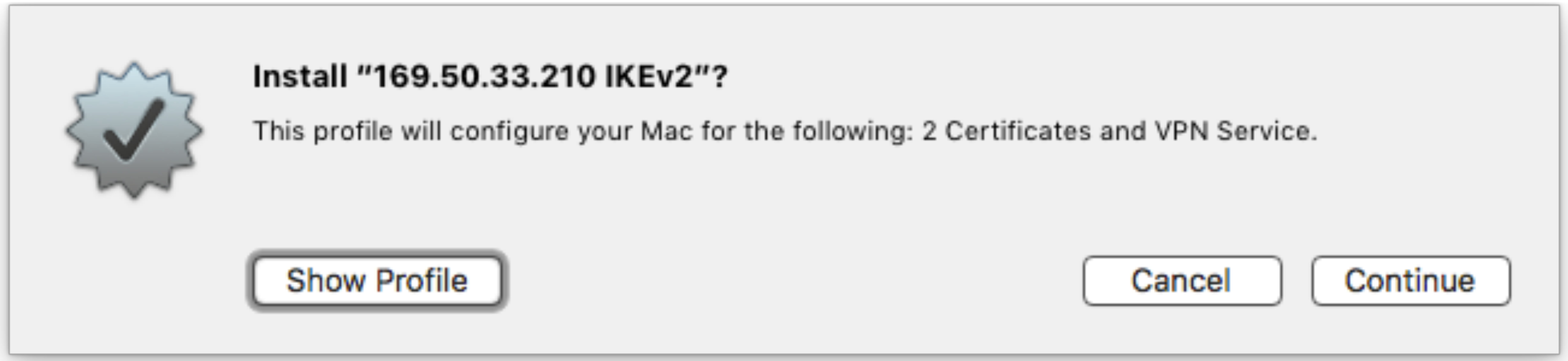
IPSec, IKEv2 Clients

10

Client Installation

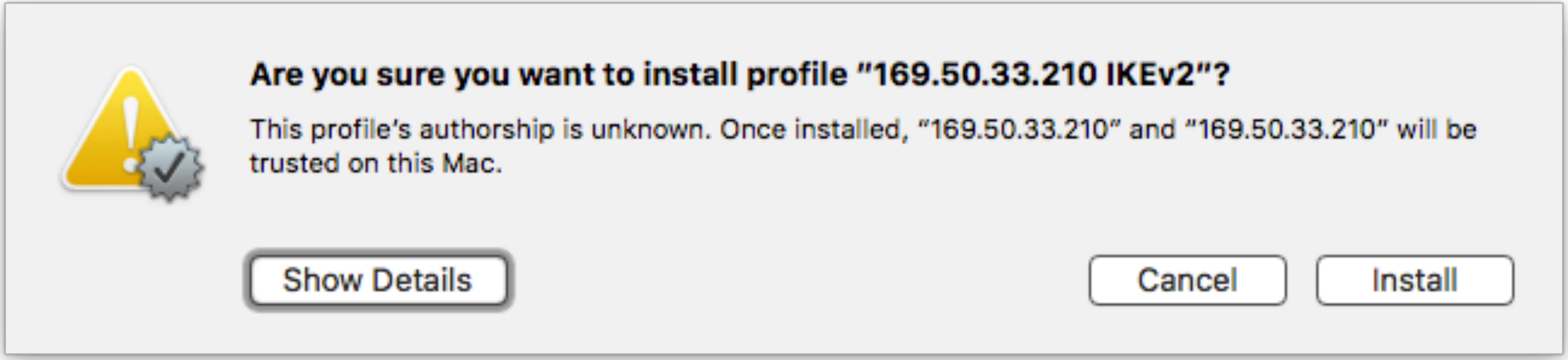
macOS

Linuxwochen.mobileconfig



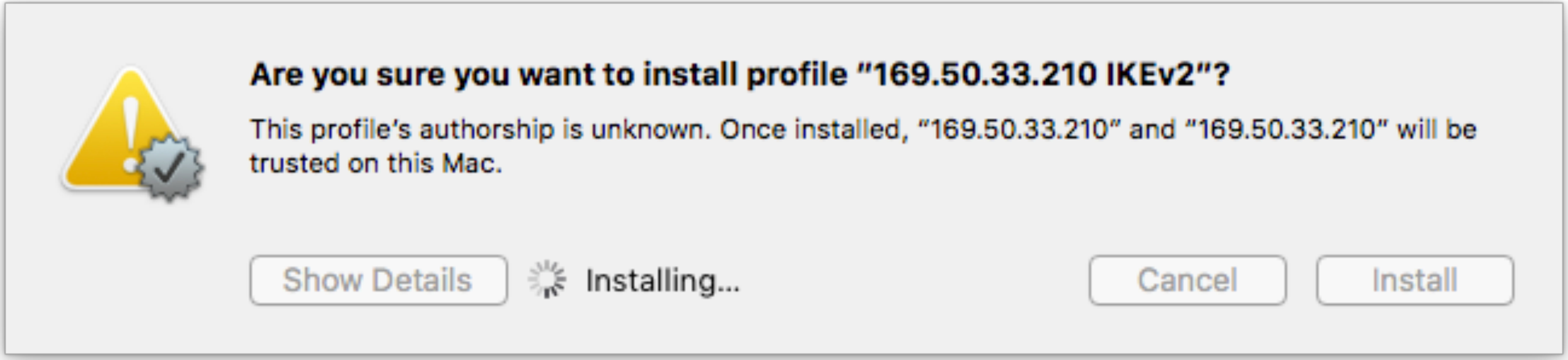
Install “169.50.33.210 IKEv2”?

This profile will configure your Mac for the following: 2 Certificates and VPN Service.



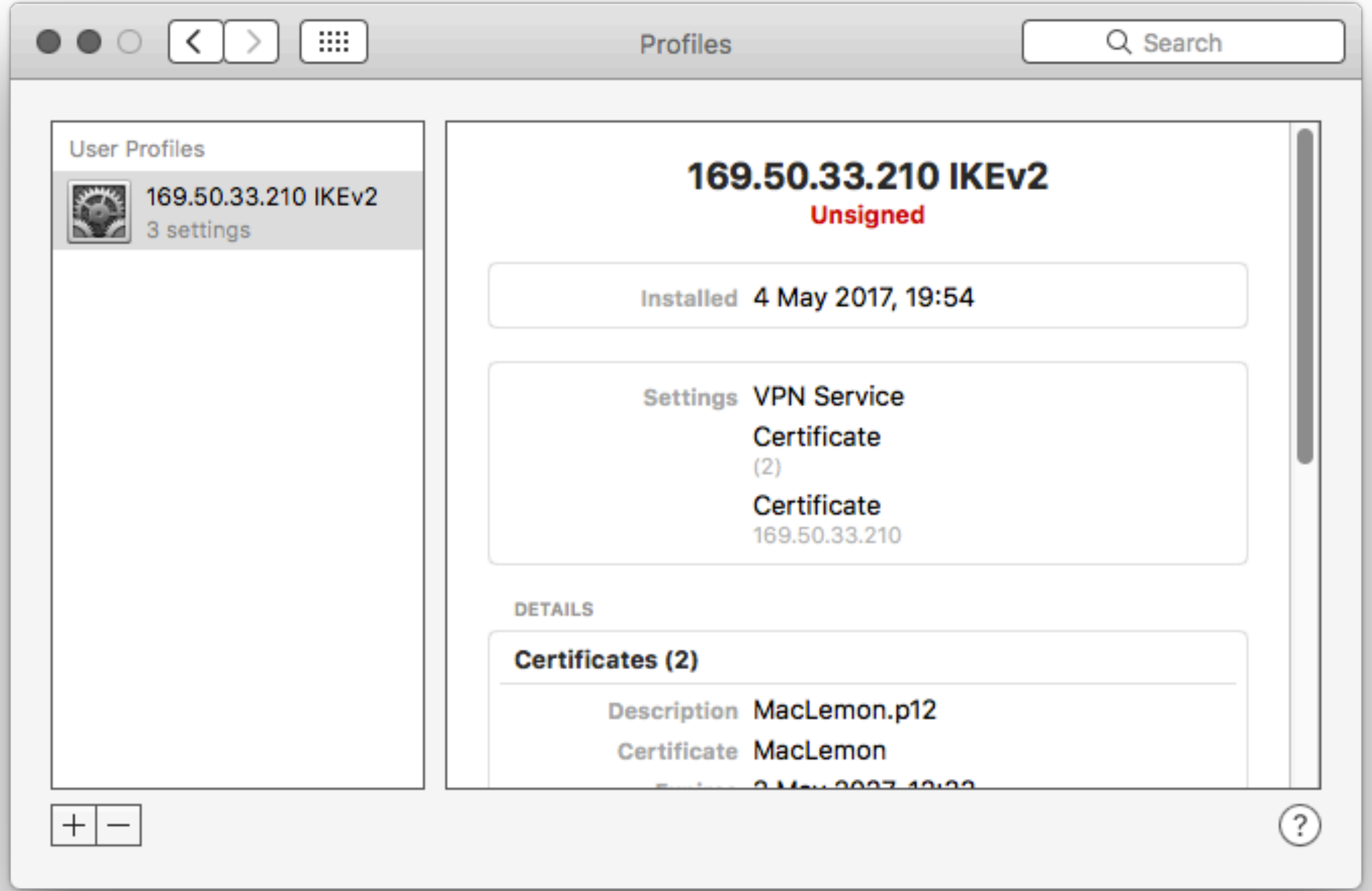
Are you sure you want to install profile "169.50.33.210 IKEv2"?

This profile's authorship is unknown. Once installed, "169.50.33.210" and "169.50.33.210" will be trusted on this Mac.



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.



User Profiles

169.50.33.210 IKEv2
3 settings

169.50.33.210 IKEv2

Unsigned

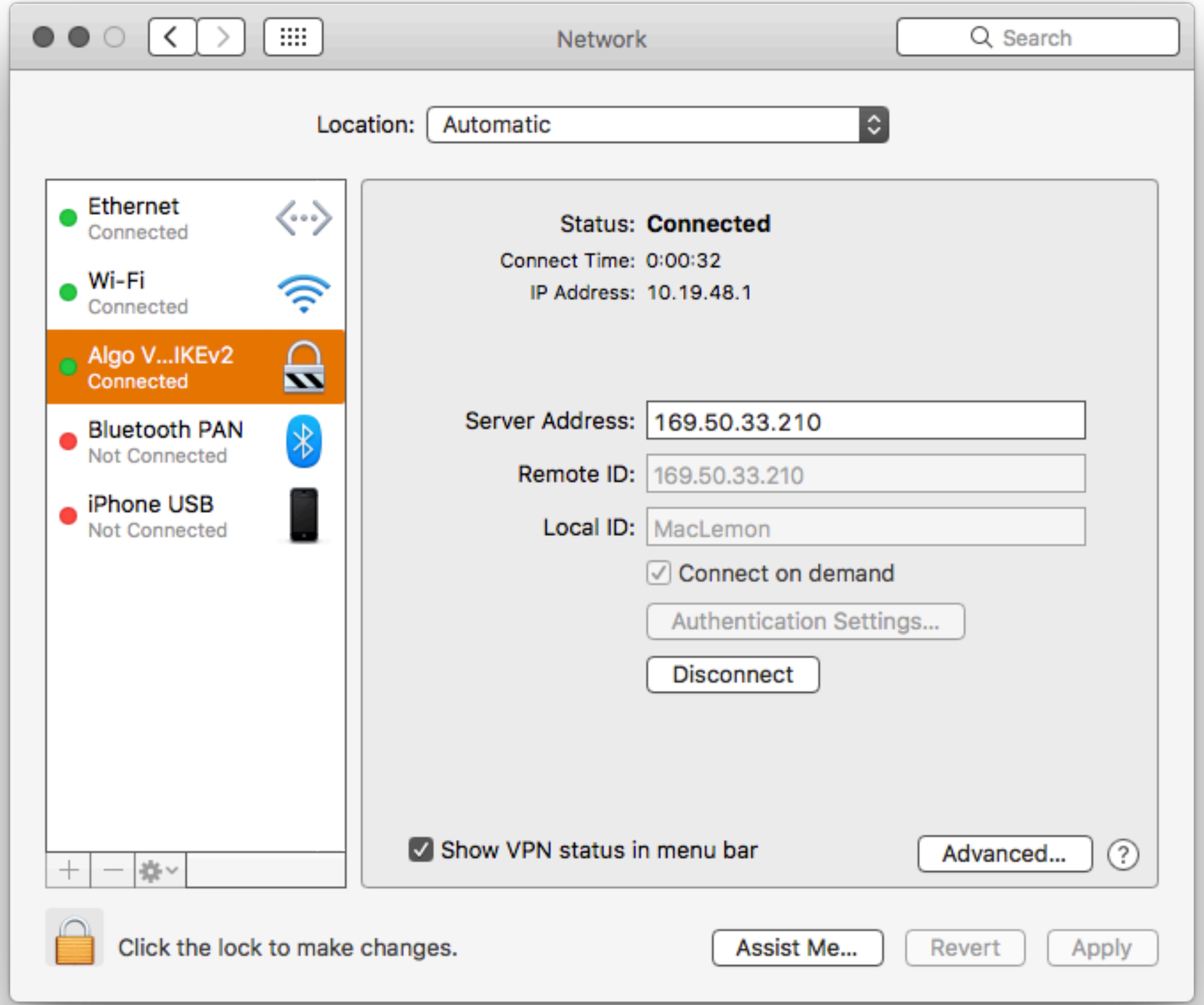
Installed 4 May 2017, 19:54

Settings VPN Service
Certificate
(2)
Certificate
169.50.33.210

DETAILS

Certificates (2)

Description MacLemon.p12
Certificate MacLemon



Network

Location: Automatic

Ethernet
Connected

Wi-Fi
Connected

Algo V...IKEv2
Connected

Bluetooth PAN
Not Connected

iPhone USB
Not Connected

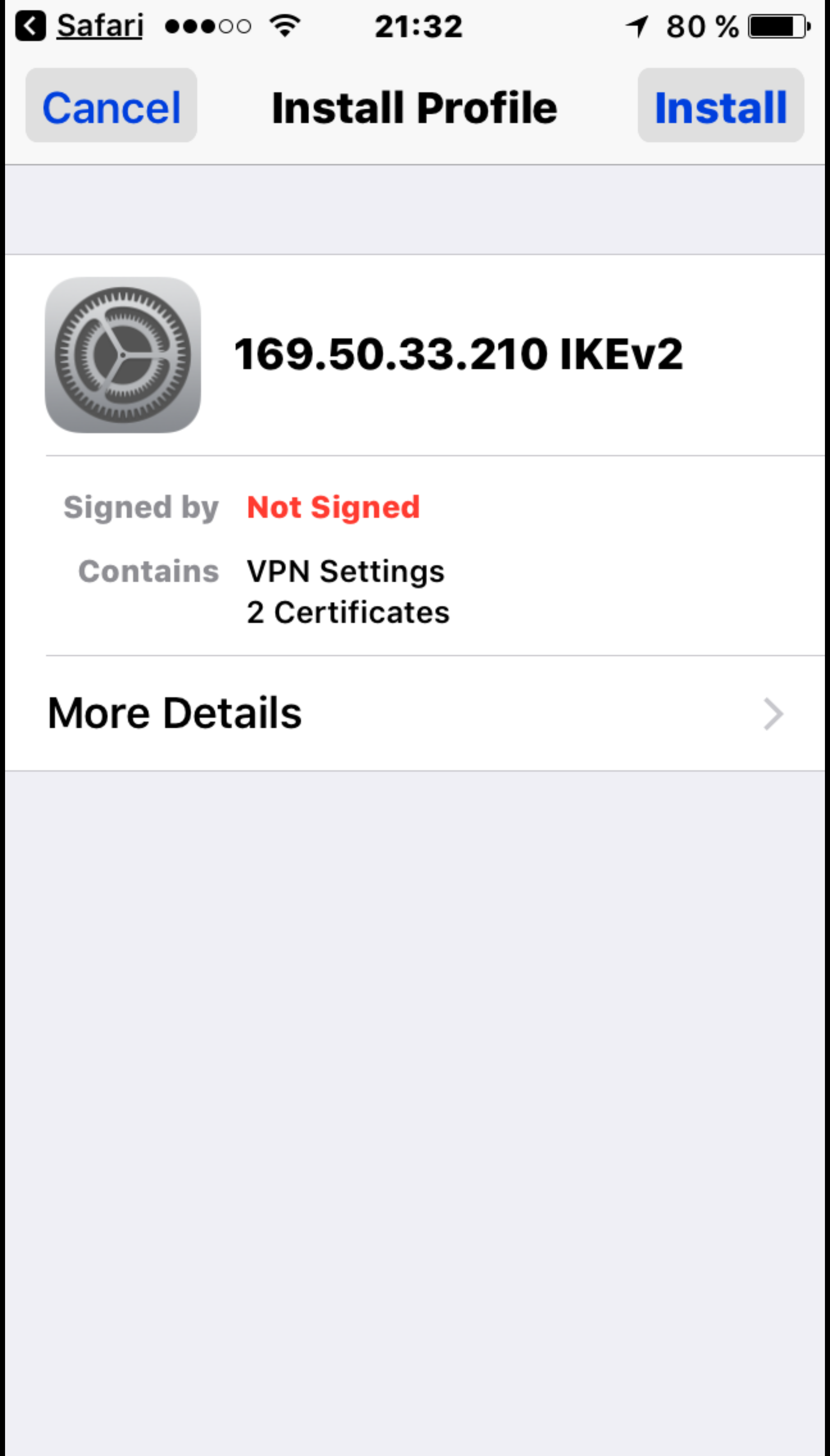
Status: **Connected**
Connect Time: 0:00:32
IP Address: 10.19.48.1

Server Address: 169.50.33.210
Remote ID: 169.50.33.210
Local ID: MacLemon
☑ Connect on demand

☑ Show VPN status in menu bar

Click the lock to make changes.

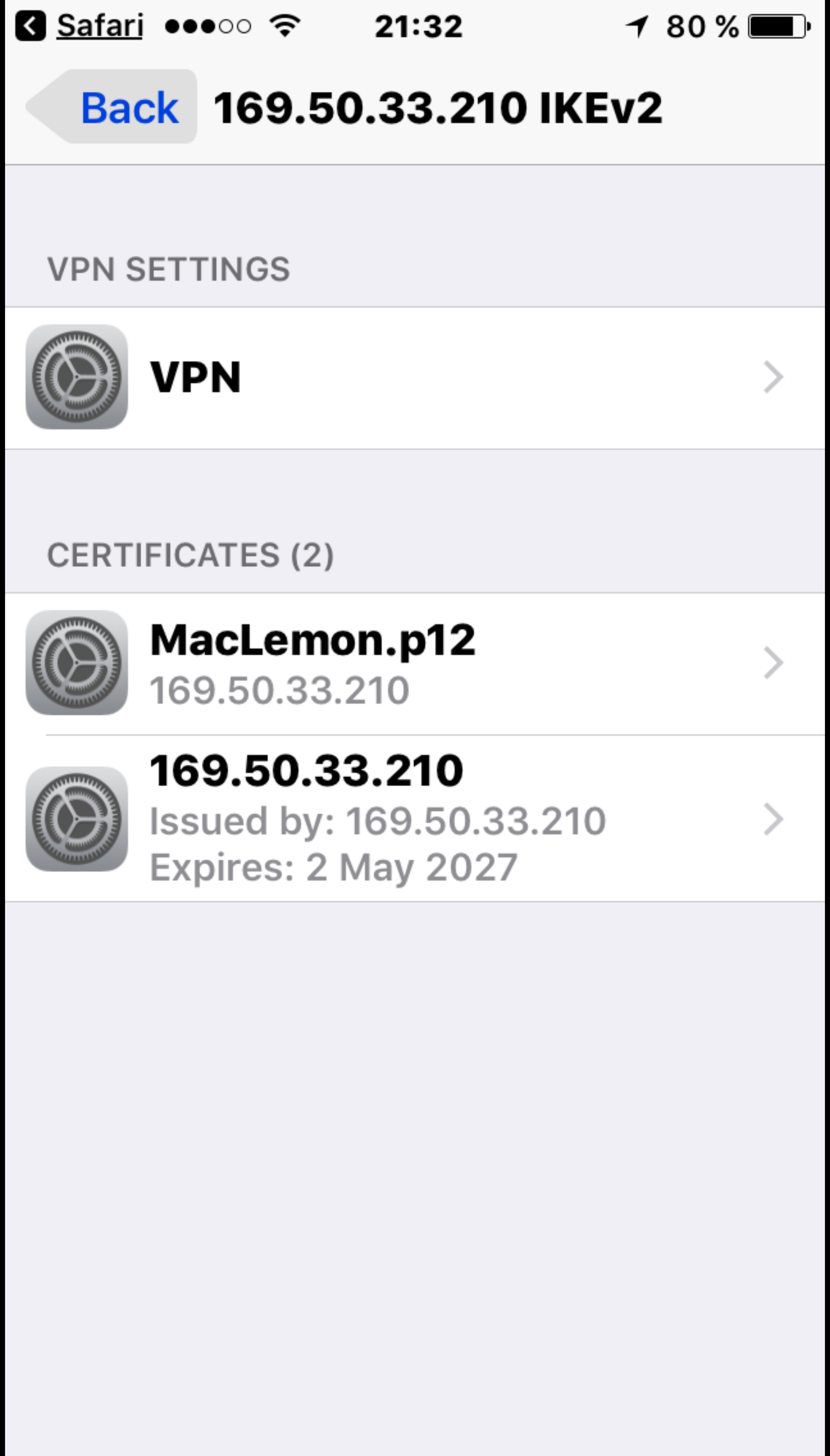
iOS



169.50.33.210 IKEv2

Signed by Not Signed

Contains VPN Settings
2 Certificates



169.50.33.210 IKEv2

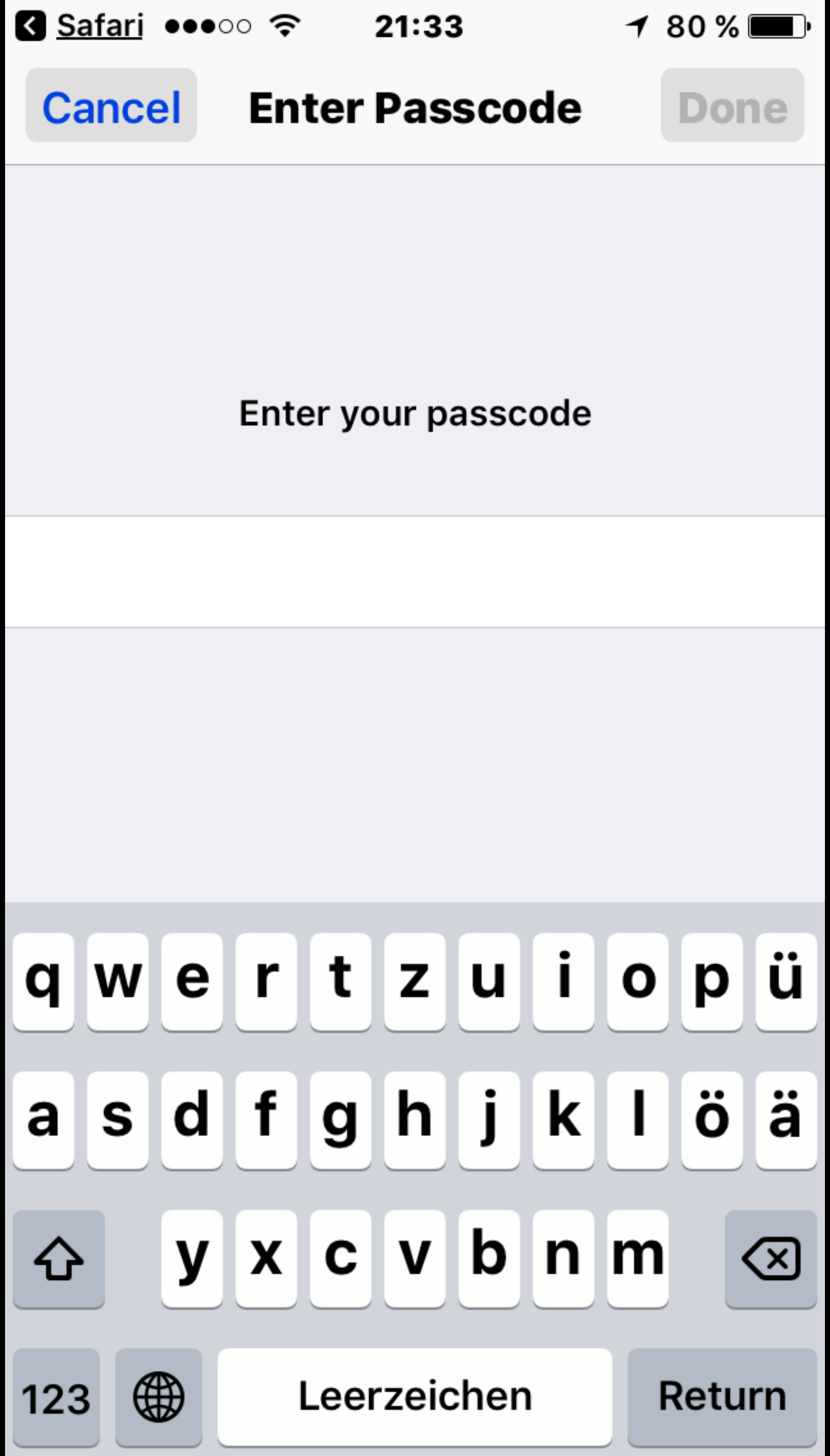
VPN SETTINGS

VPN

CERTIFICATES (2)

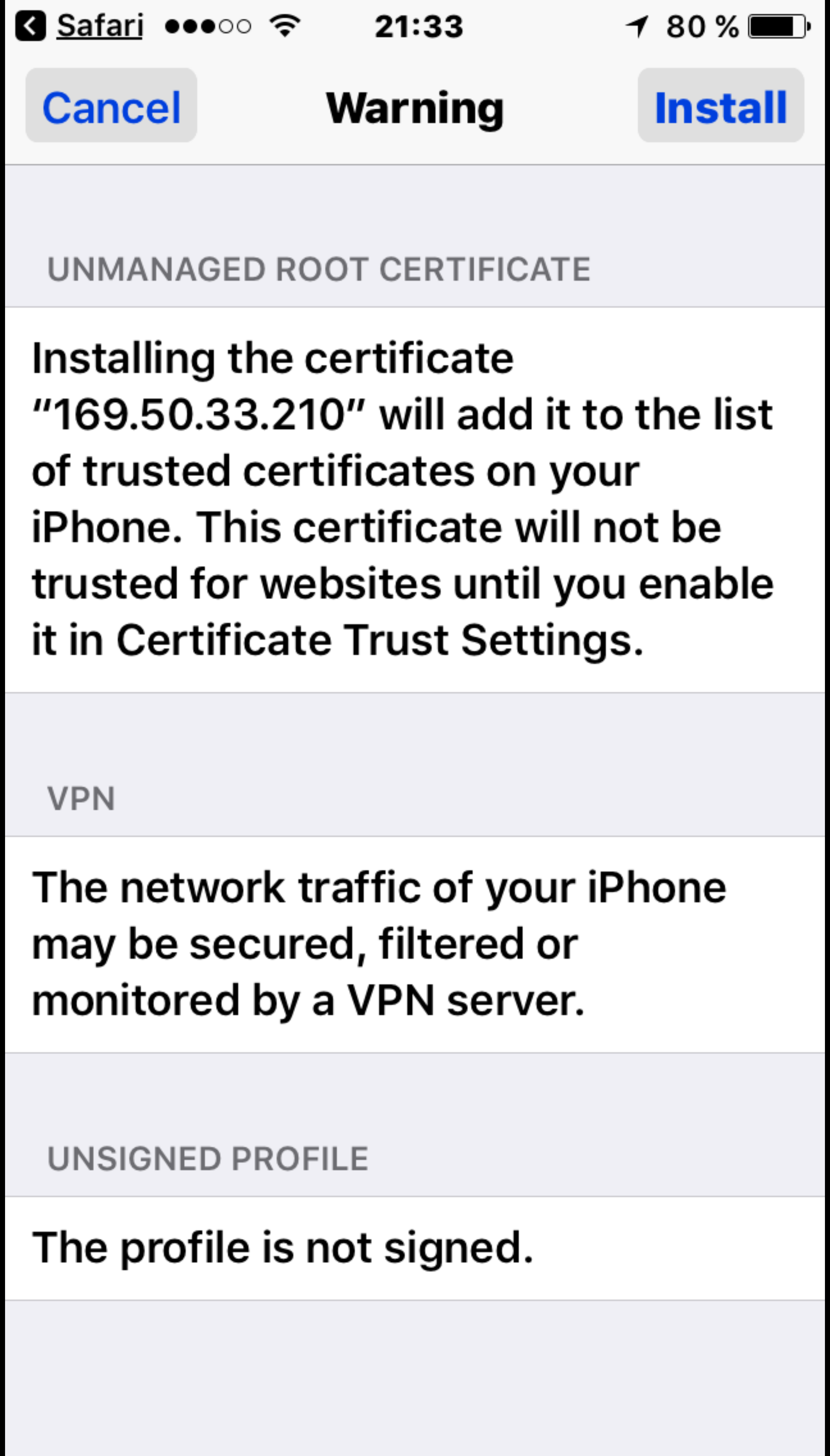
MacLemon.p12
169.50.33.210

169.50.33.210
Issued by: 169.50.33.210
Expires: 2 May 2027



Enter Passcode

Enter your passcode



UNMANAGED ROOT CERTIFICATE

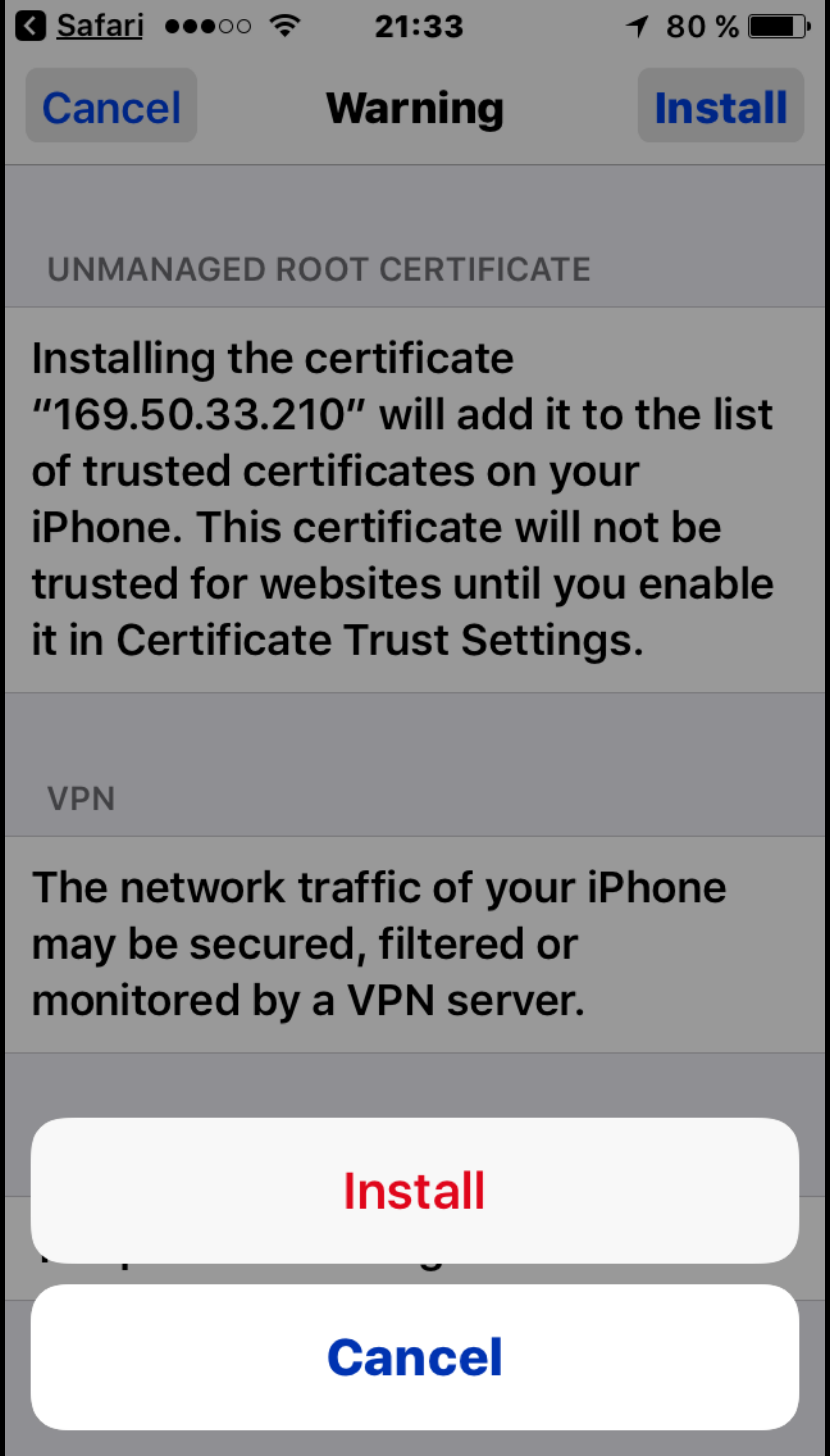
Installing the certificate “169.50.33.210” will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.

VPN

The network traffic of your iPhone may be secured, filtered or monitored by a VPN server.

UNSIGNED PROFILE

The profile is not signed.

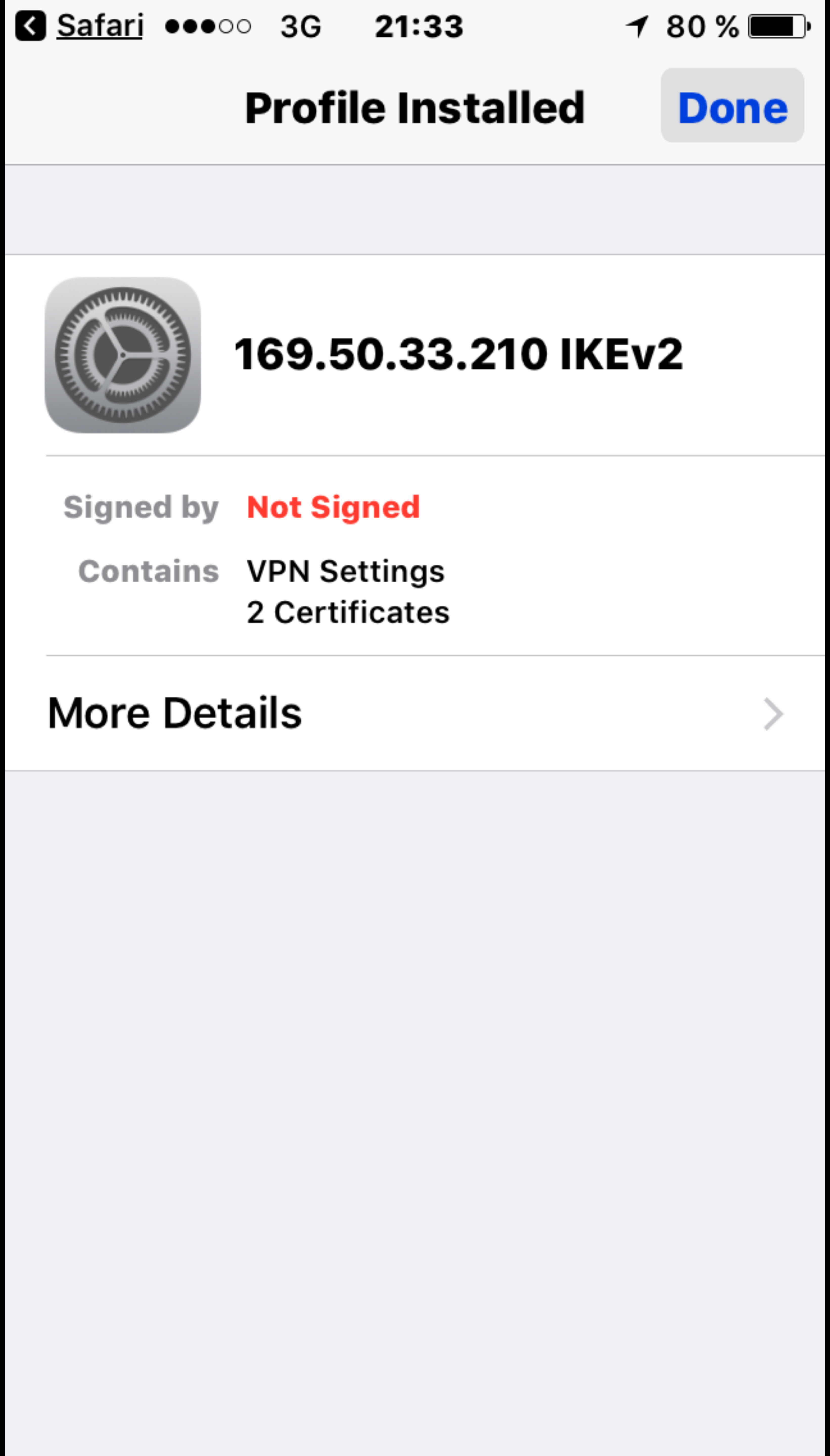


UNMANAGED ROOT CERTIFICATE

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.

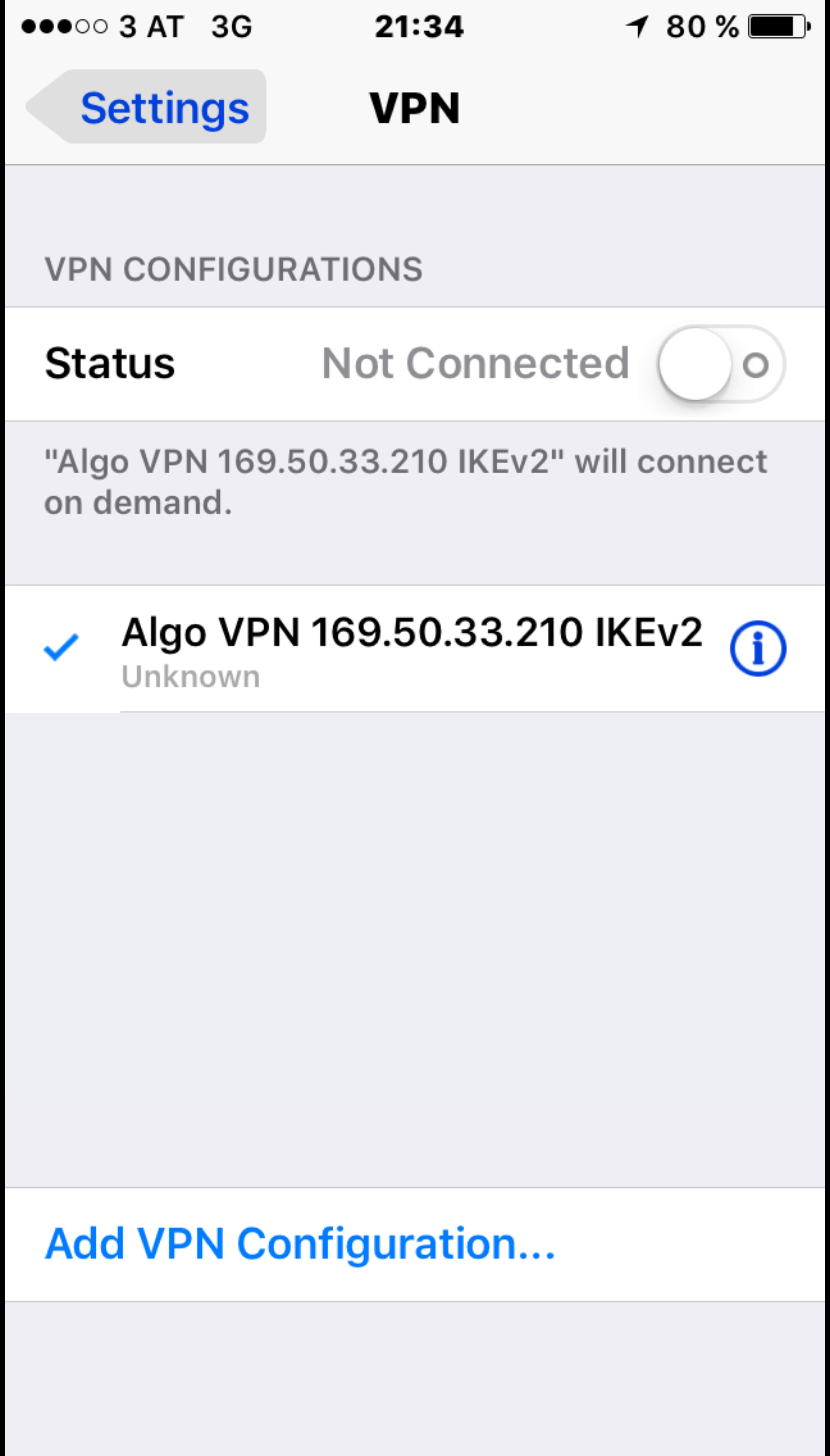


Profile Installed

169.50.33.210 IKEv2

Signed by Not Signed

Contains VPN Settings
2 Certificates



●●●○○ 3 AT 3G 21:34 80 %

Settings VPN

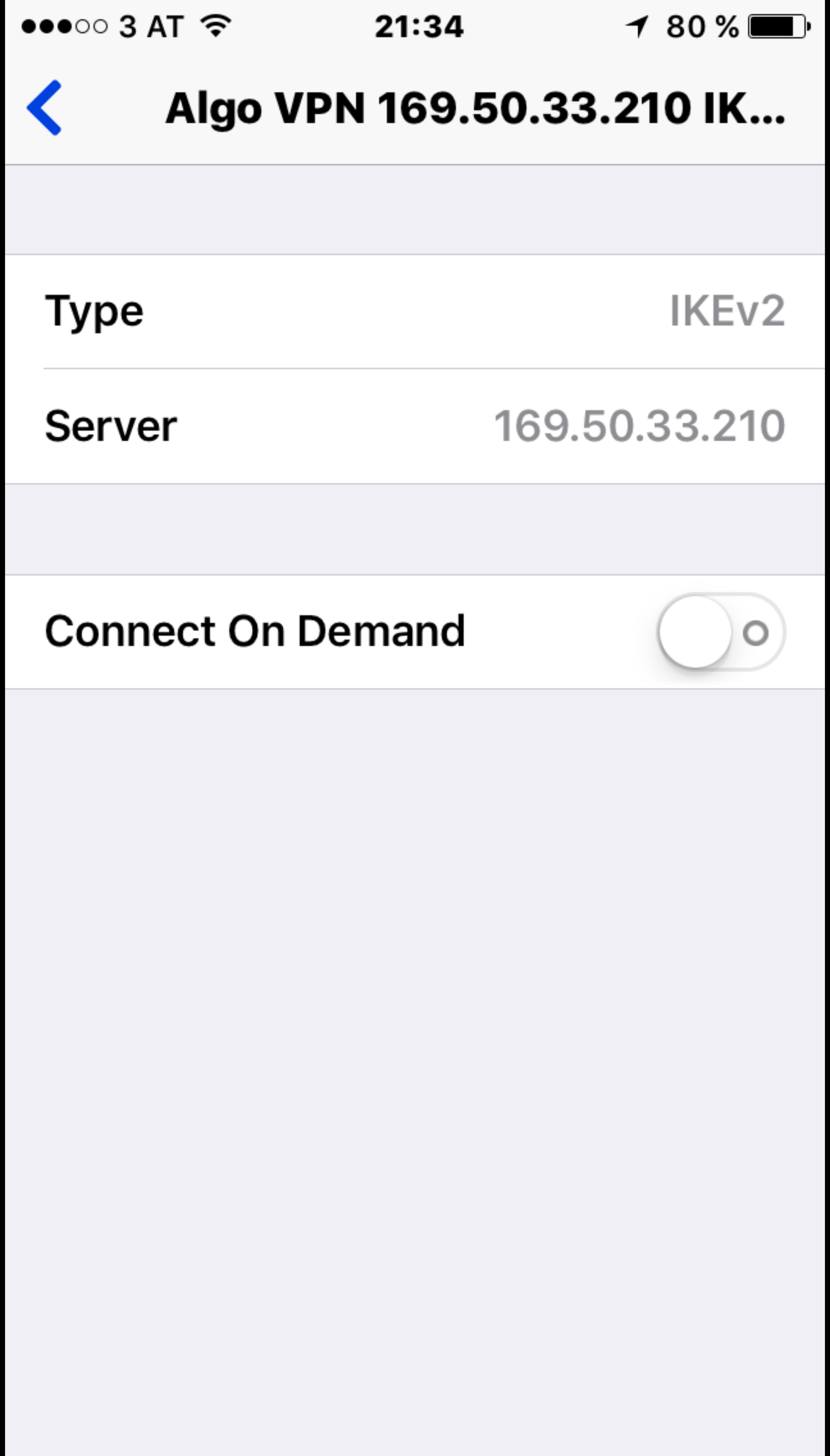
VPN CONFIGURATIONS

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...

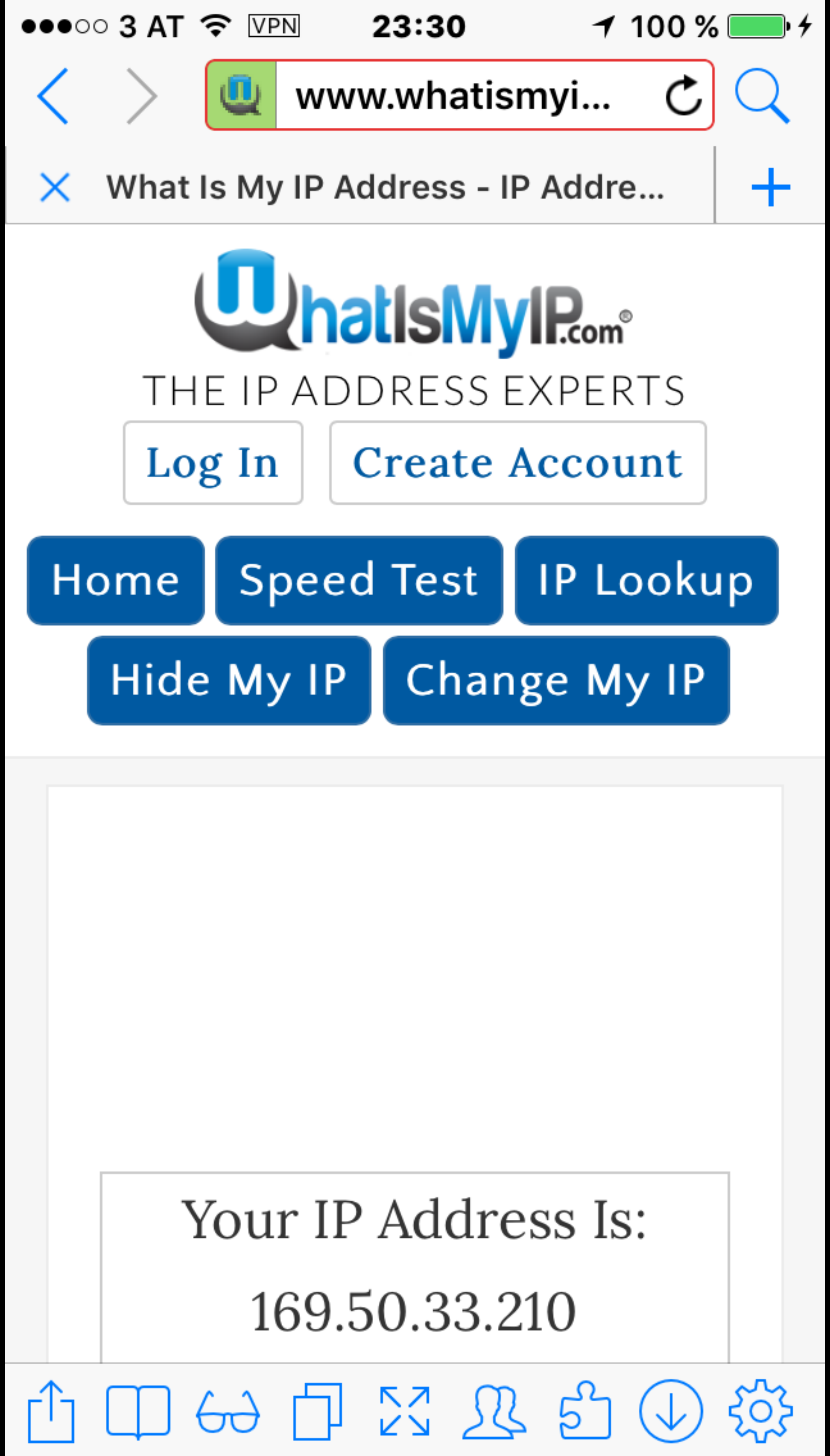


Algo VPN 169.50.33.210 IK...

Type IKEv2

Server 169.50.33.210

Connect On Demand ○



Your IP Address Is:

169.50.33.210

/Algo VPN

Andere VPN Lösungen

SSH Layer 2 VPN

SSHuttle

SSH -D

DynamicForward

#lww17

@leyrer

@MacLemon

Danke