

OpenVPN GUI

CERT.hr-PUBDOC-2019-7-384

Sadržaj

1	UVOD	3
2	INSTALACIJA ALATA OPENVPN GUI	5
3	KORIŠTENJE ALATA OPENVPN GUI	17
4	ZAKLJUČAK	27

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

Internet omogućava računalima na različitim krajevima svijeta da međusobno komuniciraju – no, ta komunikacija nije sama po sebi izrazito sigurna. Uzmimo za primjer osobu koja sjedi u ugostiteljskom objektu ili nekom drugom javnom prostoru i koristi svoj pametni telefon za pregledavanje web stranica. Pretpostavimo da je telefon spojen na Wi-Fi mrežu kafića. Tada njegovi podaci prvo putuju tom Wi-Fi mrežom, pa zatim kroz usmjerivač (engl. *router*) tog javnog prostora, pa kroz opremu pružatelja mrežnih usluga, i tako dalje kroz niz drugih uređaja, dok ne stignu na svoje odredište.

Na svakom dijelu tog puta, ti mrežni paketi nisu nikako zaštićeni. Bilo koji uređaj kojim oni prolaze može gledati te čak i izmijeniti njihov sadržaj. Neki dijelovi puta tih mrežnih paketa su posebno rizični. Primjerice, Wi-Fi mreže kafića ili dućana su često nedovoljno zaštićene i omogućavaju napadačima koji se nalaze u blizini da prisluškuju ili čak mijenjaju mrežni promet spojenih korisnika.

Tehnologija virtualnih privatnih mreža, poznatija pod skraćenicom VPN (od engl. *Virtual Private Network*), omogućava sigurno povezivanje dva računala preko nesigurne, javne mreže (primjerice preko interneta). Kada se dva računala priključena na internet povežu putem VPN-a, to je efektivno kao da su sada ta dva računala spojena jednim sigurnim mrežnim kabelom, privatnim jer ga nitko drugi ne koristi.

VPN tehnologija ima niz različitih primjena. Zaposlenici često koriste VPN tehnologiju kako bi se spojili na mrežu svog ureda kada rade od doma ili su kod klijenta ili na putu. VPN tehnologijom je moguće i na siguran način povezati lokalne mreže dvije fizički udaljene podružnice iste tvrtke.

Između ostaloga, VPN tehnologija omogućava korisnicima da se zaštite od zlonamjernih ili nesigurnih Wi-Fi mreža i sličnih opasnih okolina. Korisnik spojen na opasnu Wi-Fi mrežu može VPN tehnologijom napraviti siguran mrežni tunel između svog uređaja i nekog drugog udaljenog uređaja na internetu. Time će korisnik zaštititi svoj mrežni promet na cijelom putu od svog uređaja do odredišta VPN veze, tj. zaštititi će mrežni promet od opasnosti nezaštićene Wi-Fi mreže ili od slične nesigurne okoline.

Upravo zbog ove primjene, pojavio se niz tvrtki koje korisnicima pružaju uslugu pristupa internetu putem VPN veze. Drugim riječima, te tvrtke svojim korisnicima pružaju sve što im je potrebno da svoje (korisničke) uređaje spoje na tvrtkine uređaje putem VPN-a, i na taj način usmjeravaju mrežni promet svog uređaja preko te VPN veze. U ovom kontekstu, korisnikov uređaj nazivamo VPN klijentom, dok uređaj tvrtke nazivamo VPN poslužiteljem. Time u konačnici korisnici mogu štiti svoj mrežni promet prilikom spajanja na opasne Wi-Fi mreže i slične okoline. Znači, korisnikovi podaci će biti sigurni dok putuju od korisničkog računala do VPN poslužitelja. Kad izađu iz njega, pa sve do konačnog odredišta, njihova sigurnost ovisi o mrežama kroz koje dalje putuje.

Sigurnost podataka na cijelom putu od korisnika do računalnih resursa koje koristi je moguće osigurati tek onda ako se VPN poslužitelj nalazi u istoj lokalnoj i zaštićenoj mreži u kojoj se nalazi i računalni resurs.

Za uspostavu VPN veze potreban je program na korisničkom računalu, VPN klijent, i program na VPN poslužitelju. Postoji nekoliko popularnih komercijalnih, ali i besplatnih programa.

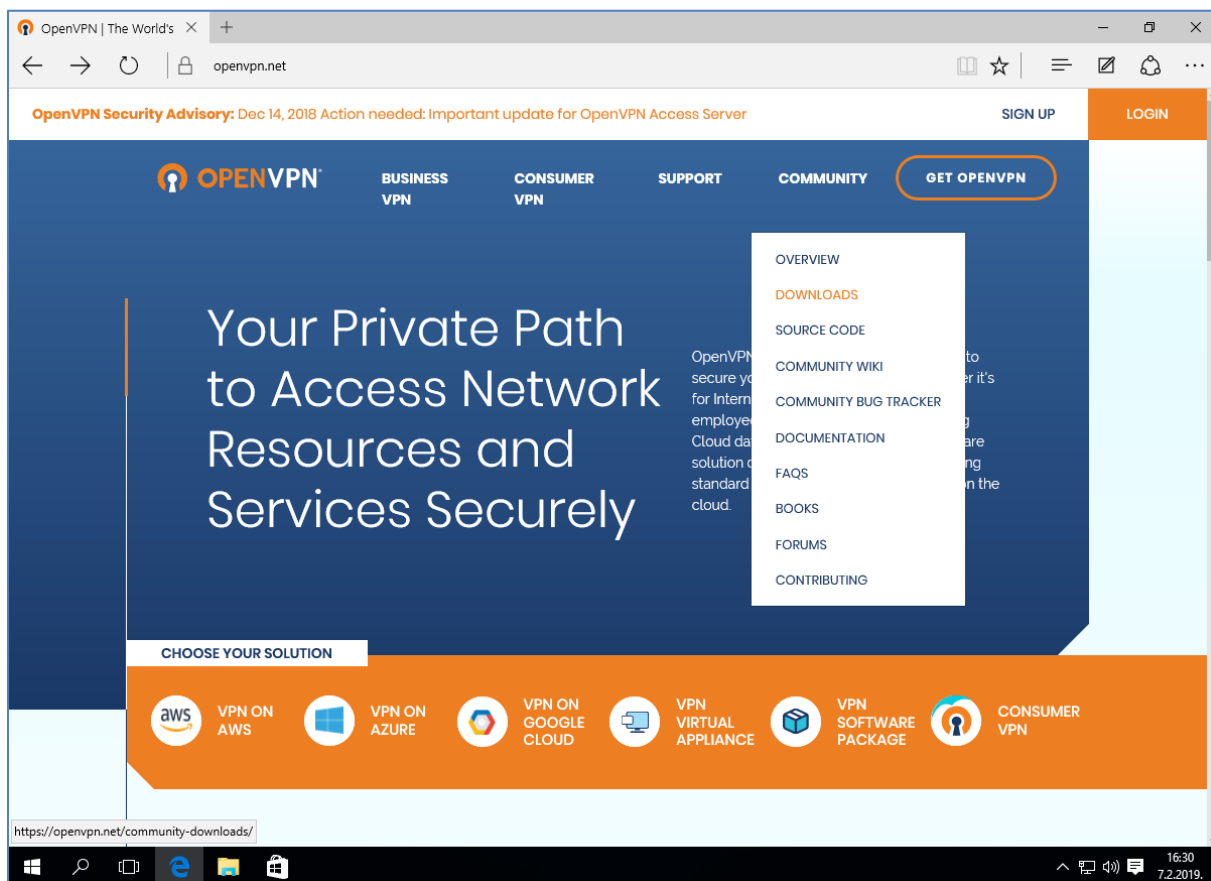
OpenVPN je široko korišteni skup slobodnog softvera (engl. *free and open source software*) koji uključuje sve što je potrebno za uspostavljanje VPN veze između dva računala. Jedan dio tog skupa softvera je i OpenVPN GUI za operacijski sustav Microsoft Windows. OpenVPN GUI je alat koji korisnici instaliraju na svoje računalo (VPN klijent) kako bi mogli uspostaviti VPN vezu s nekim VPN poslužiteljem. Ovaj dokument opisuje instalaciju i osnovno korištenje softvera OpenVPN GUI.

2 Instalacija alata OpenVPN GUI

OpenVPN GUI je klijent za uspostavu VPN veze korisnikovog računala i nekog VPN poslužitelja. Taj poslužitelj može negdje postaviti sam korisnik ili njegova organizacija, ali je moguće koristiti i javne, komercijalne ili besplatne VPN poslužitelje.

Alat je dostupan na [službenim web stranicama projekta OpenVPN](#).

1. Potrebno je odabrati padajući izbornik **Community** i kategoriju **Downloads**.



2. Preusmjereni smo na web stranicu za preuzimanja na kojoj odaberemo instalaciju namijenjenu operacijskom sustavu Microsoft Windows: "Windows installer (NSIS)". Time započinje preuzimanje instalacijske datoteke.

The screenshot shows the OpenVPN Community Downloads page. At the top, there is a navigation bar with links for BUSINESS VPN, CONSUMER VPN, SUPPORT, and COMMUNITY, along with a 'GET OPENVPN' button. A security advisory banner is visible at the top left. The main content area features a table of download links for various file formats, each with a corresponding GnuPG signature link and a download button.

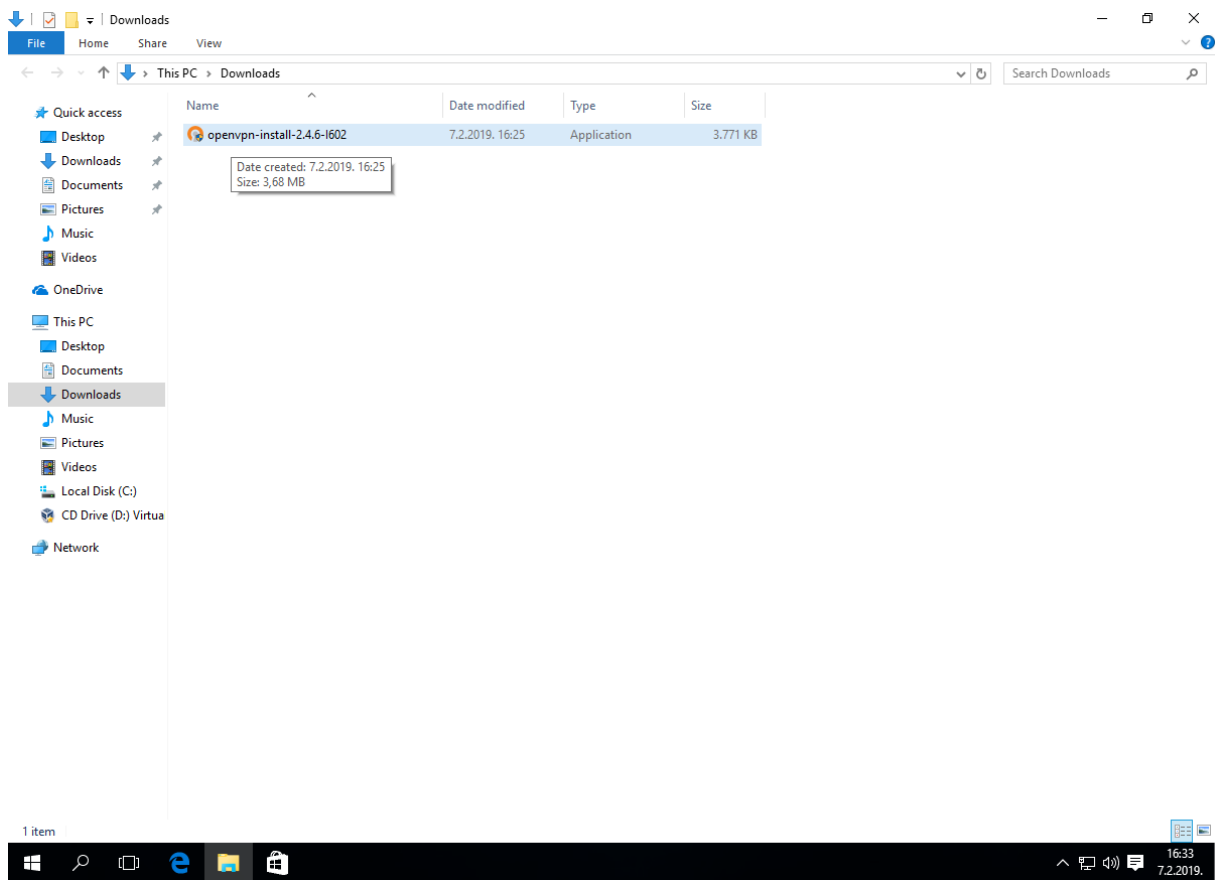
SOURCE TARBALL (GZIP)	GnuPG Signature	openvpn-2.4.6.tar.gz
SOURCE TARBALL (XZ)	GnuPG Signature	openvpn-2.4.6.tar.xz
SOURCE ZIP	GnuPG Signature	openvpn-2.4.6.zip
WINDOWS INSTALLER (NSIS)	GnuPG Signature	openvpn-install-2.4.6-i602.exe

NOTE: the GPG key used to sign the release files has been changed since OpenVPN 2.4.0. Instructions for verifying the signatures, as well as the new GPG public key are available [here](#).

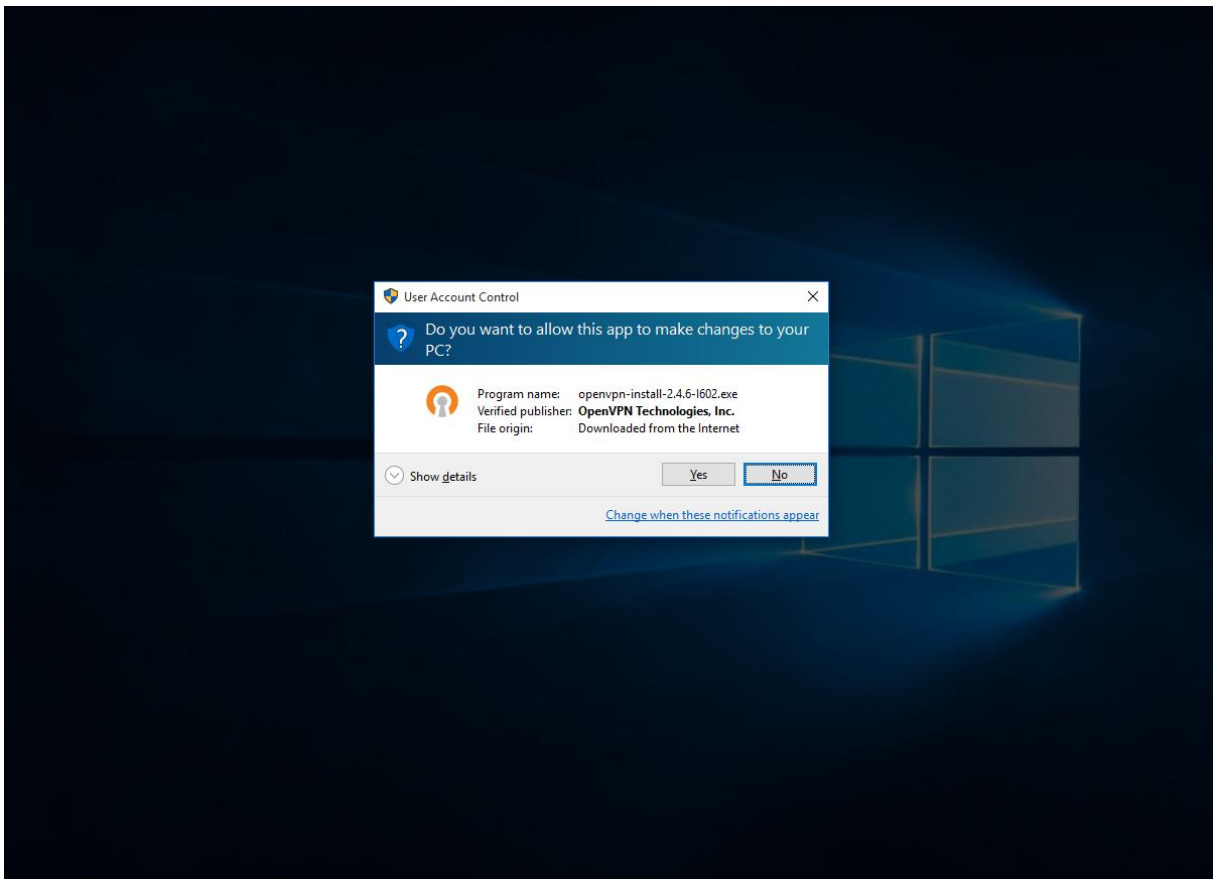
We also provide static URLs pointing to latest releases to ease automation. For a list of files look [here](#).

<https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.6-i602.exe> es for Debian and Ubuntu. Supported architectures are i386 and amd64. For details, look [here](#).

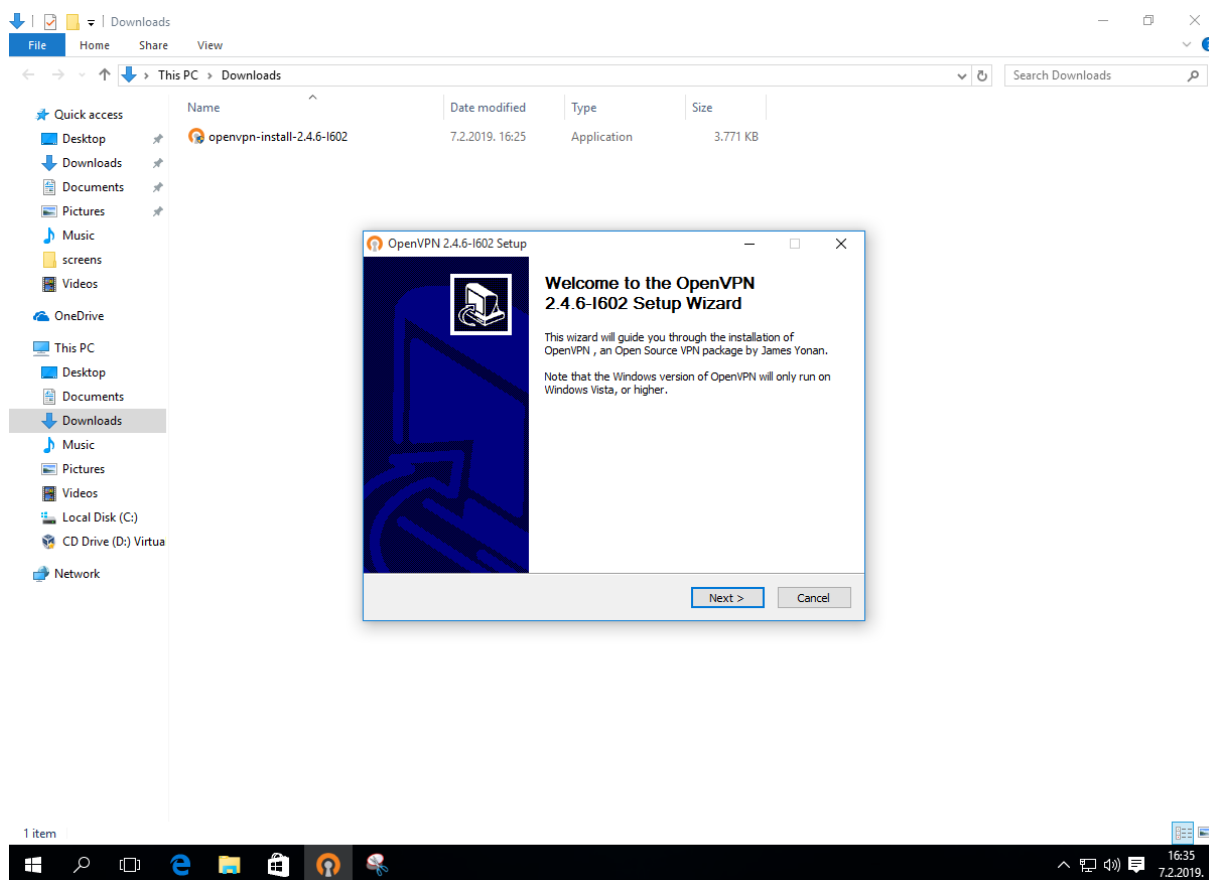
3. Nakon što je dovršeno preuzimanje, instalacijski paket je spremljen na zadanu (engl. *default*) lokaciju web preglednika, obično „C:\Users*korisnik*\Downloads\“.



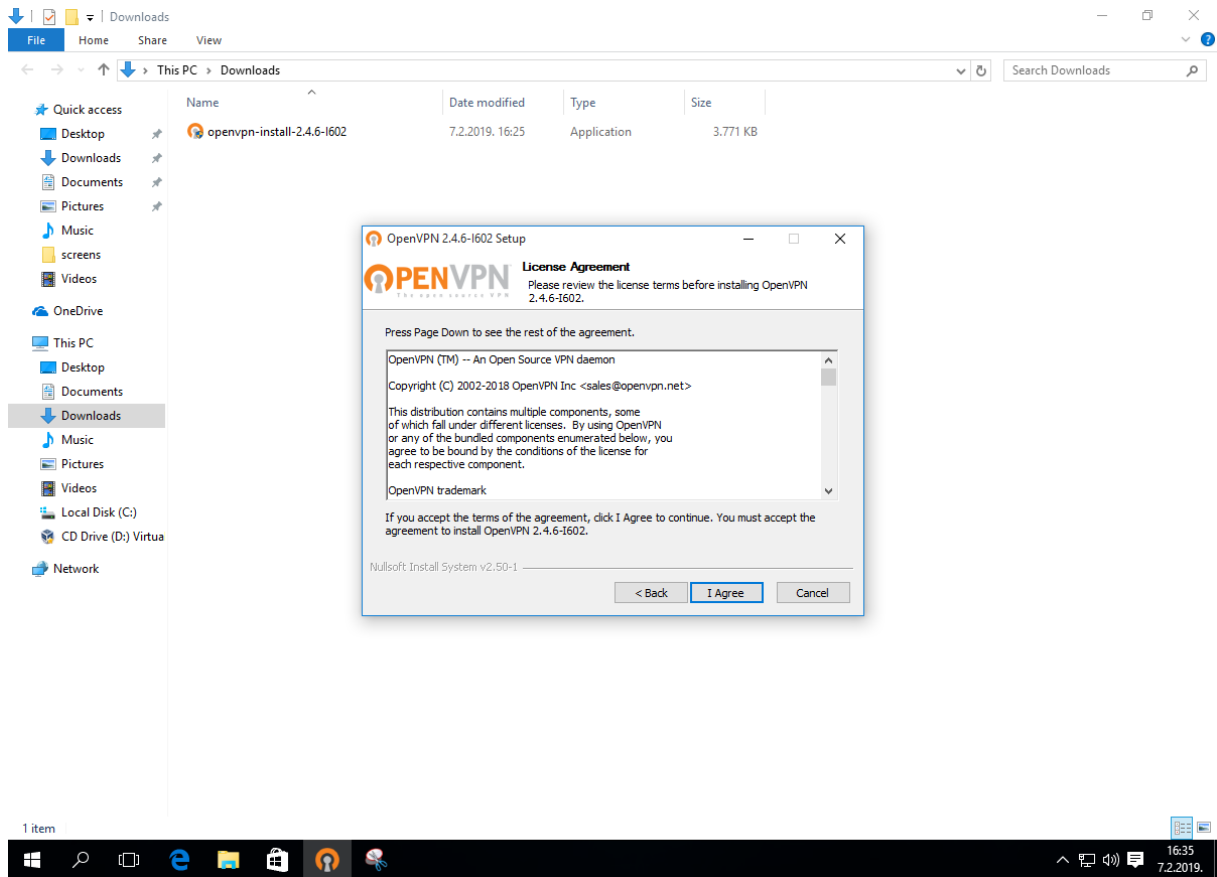
4. Potrebno je pokrenuti preuzetu datoteku (u ovom slučaju *openvpn-install-2.4.6-1602.exe*). Time smo započeli instalaciju alata. Ako se pojavi upozorenje prikazano na sljedećoj slici, potrebno je odabrati **Yes**.



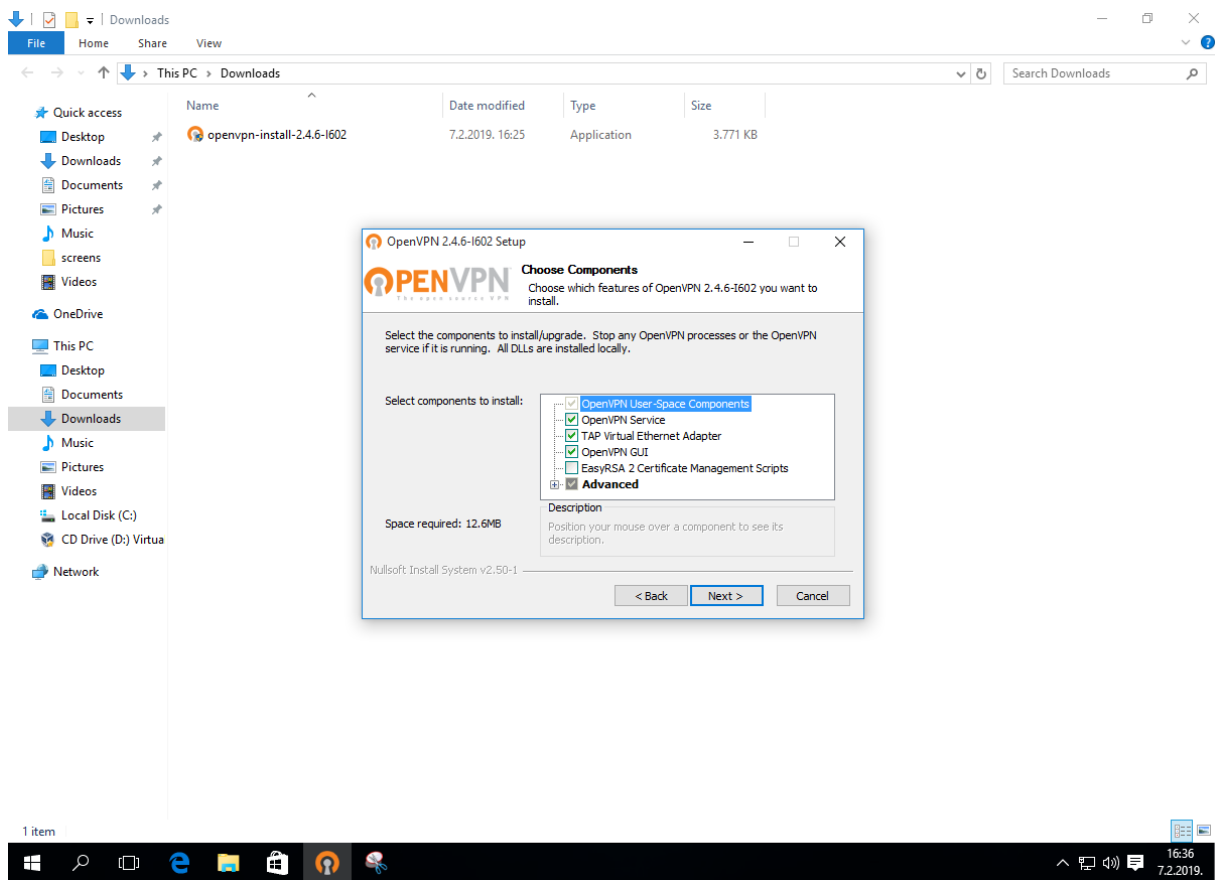
5. Zatim se prikazuje početni zaslone instalacije na kojemu je potrebno odabrati **Next**.



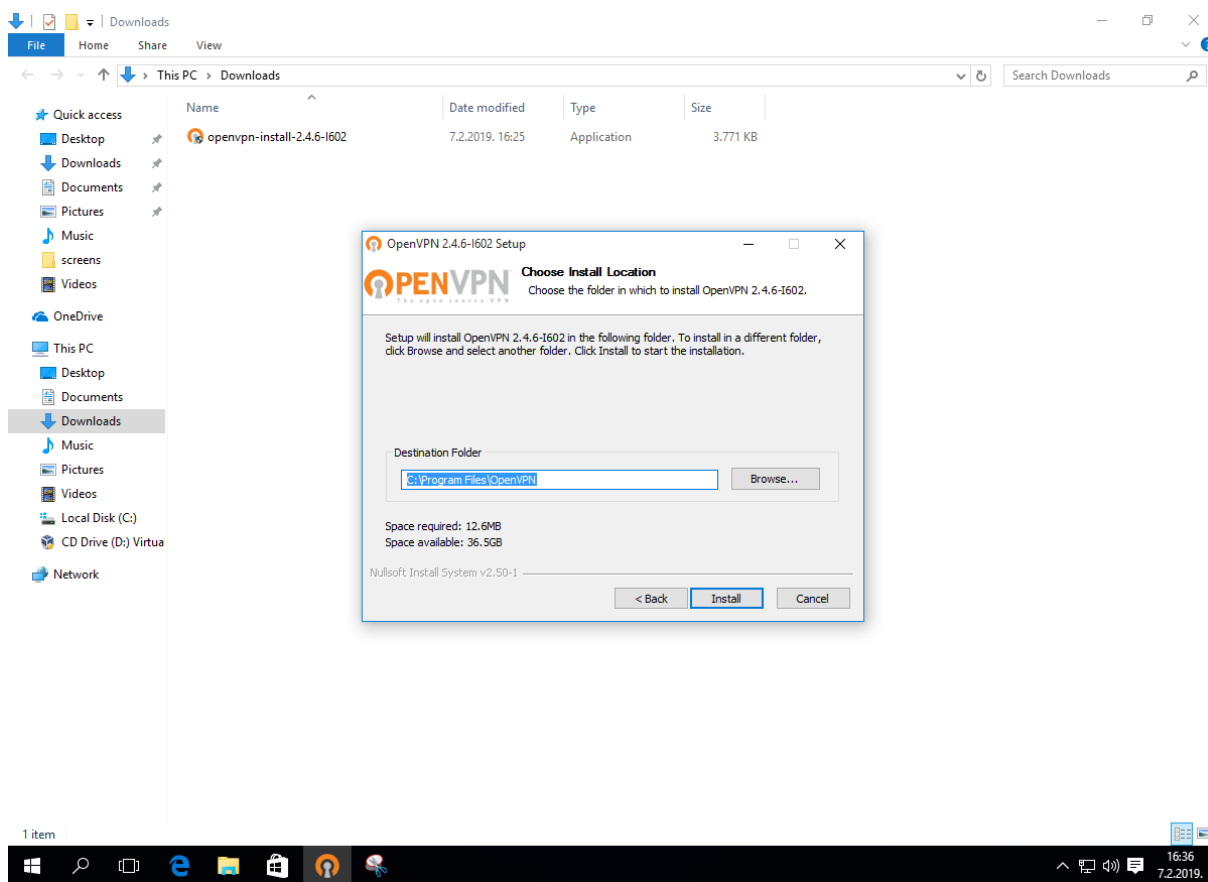
6. Zatim, nakon što pročitamo i složimo se s uvjetima korištenja, potrebno je odabrati **Next**.



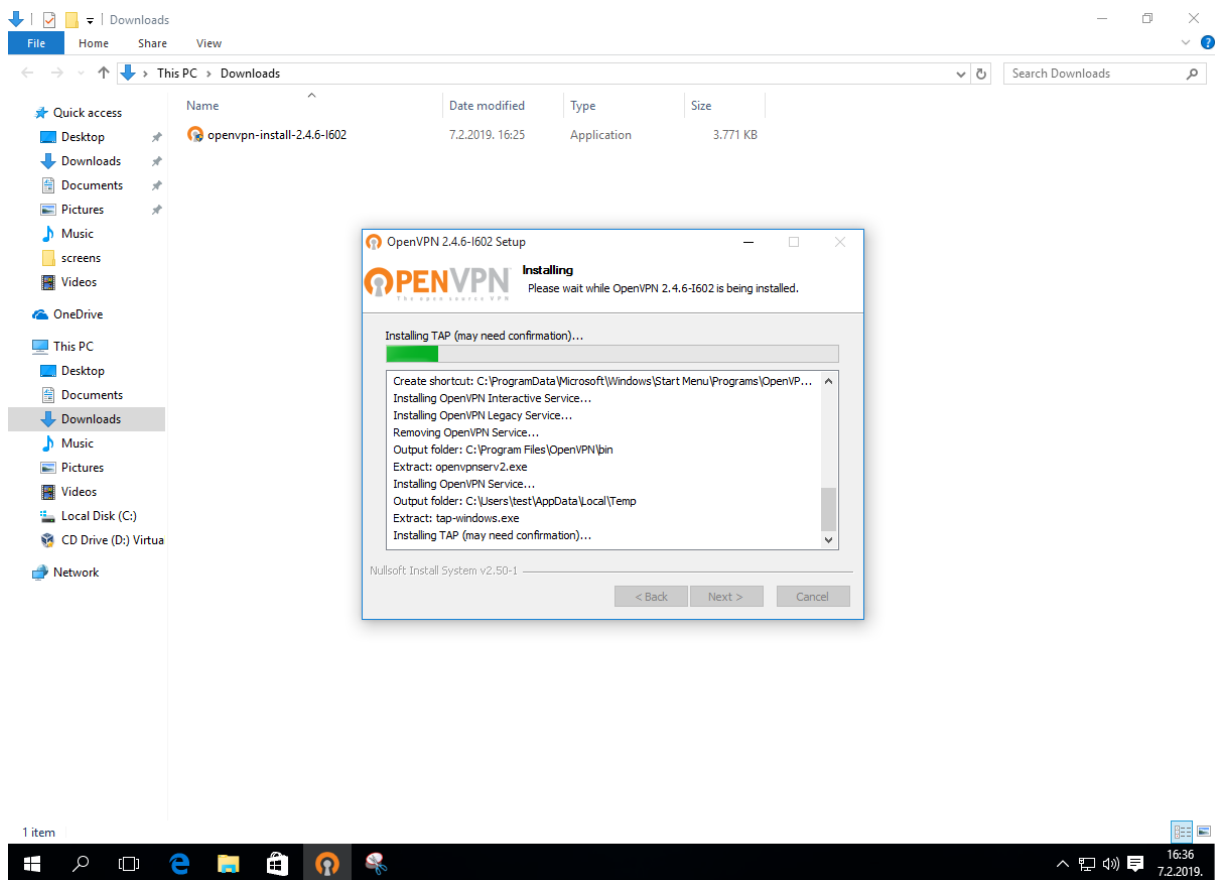
7. U sljedećem koraku se biraju komponente koje će biti instalirane, preporuka je ostaviti kako je zadano (engl. *default*) i odabrati **Next**.



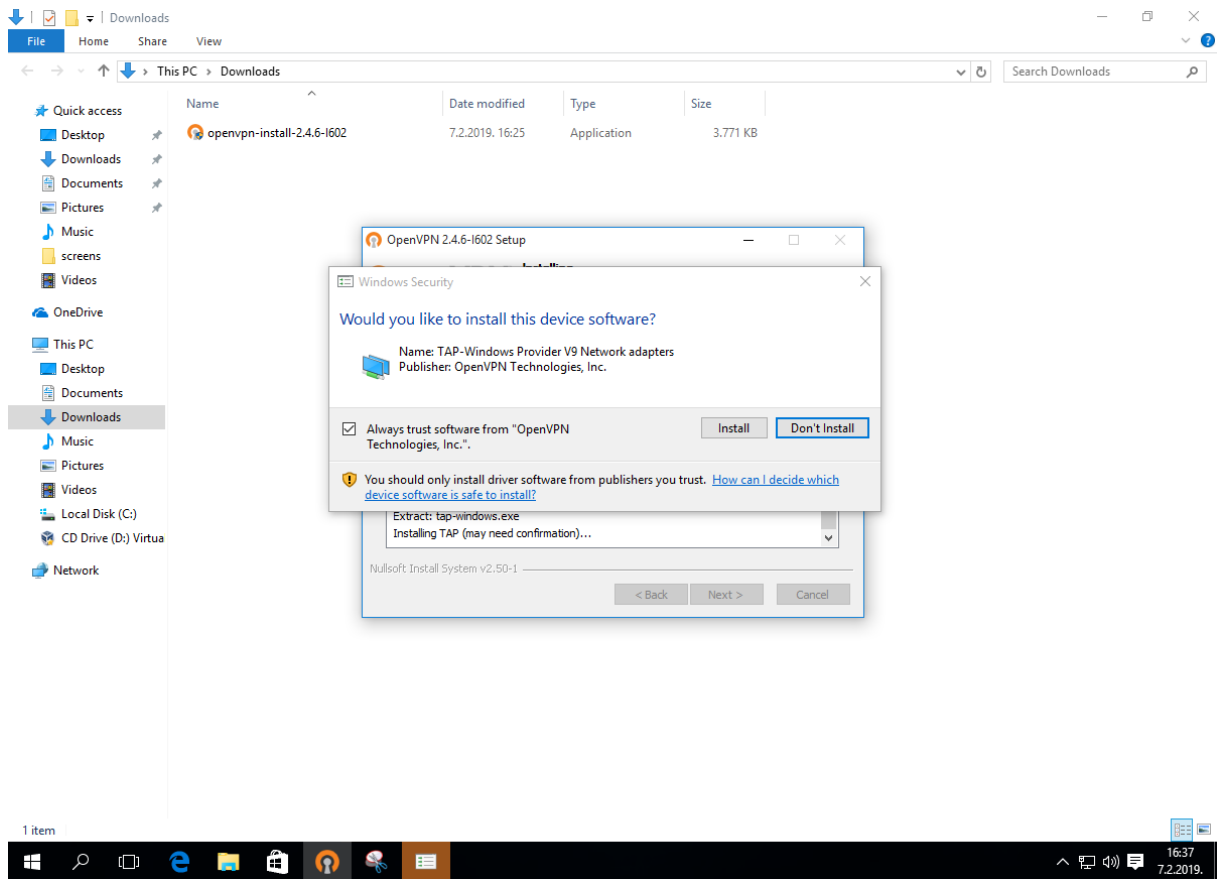
8. Zatim se bira lokacija na disku gdje će alat biti instaliran.



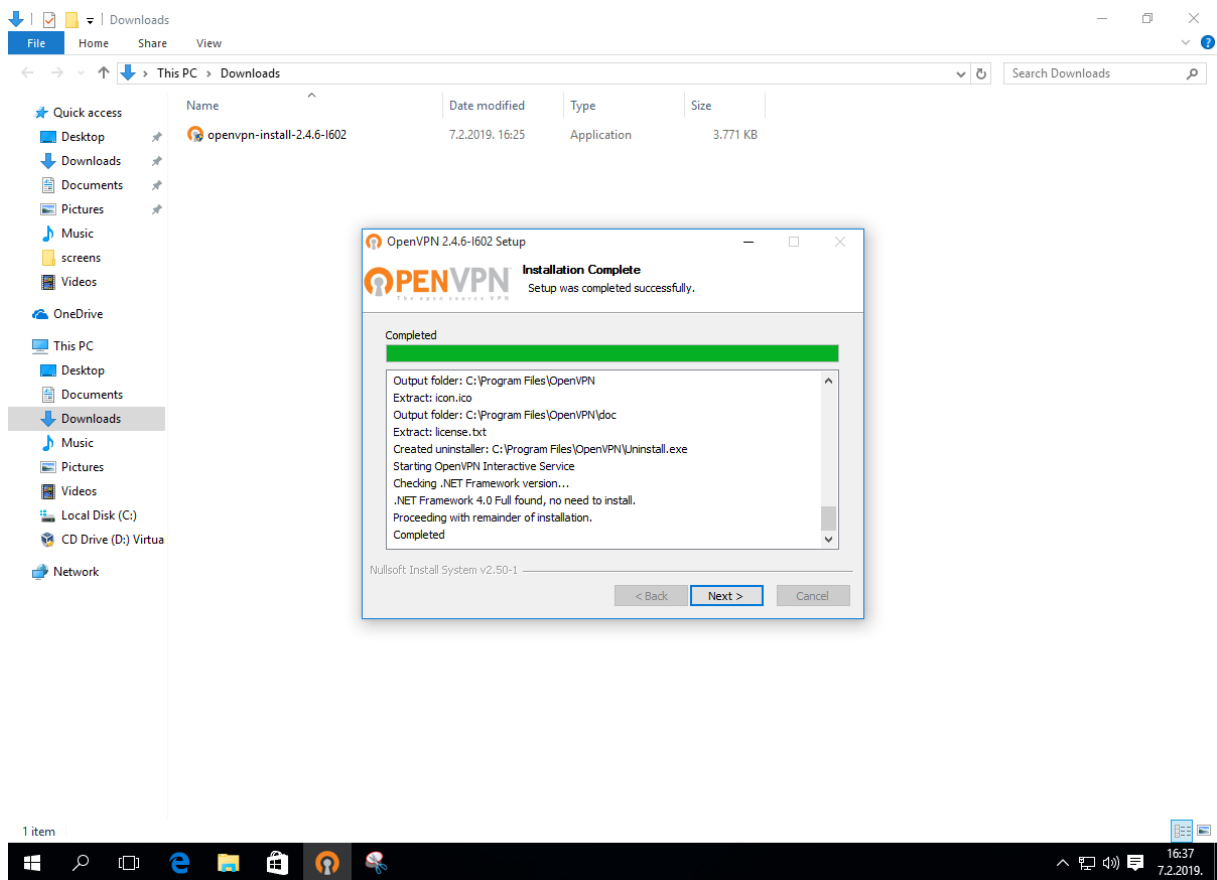
9. Sljedeći korak prikazuje kako napreduje instalacija.



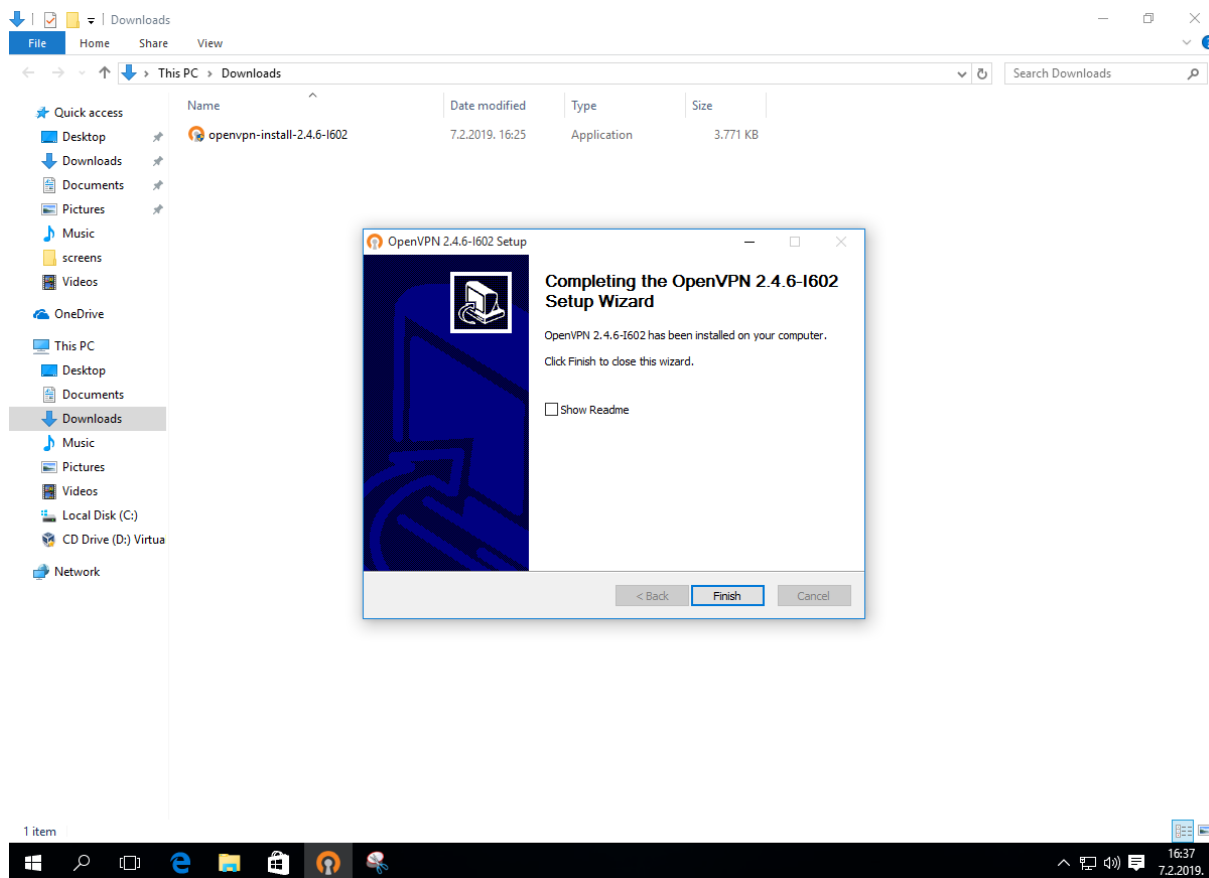
10. Tijekom instalacije može se pojaviti skočni prozor (engl. *pop-up window*) koji traži dozvolu za instalaciju odgovarajućih upravljačkih programa. Treba dozvoliti pritiskom na **Install**.



11. Sljedeća slika prikazuje uspješan završetak instalacije nakon čega je potrebno kliknuti **Next**.

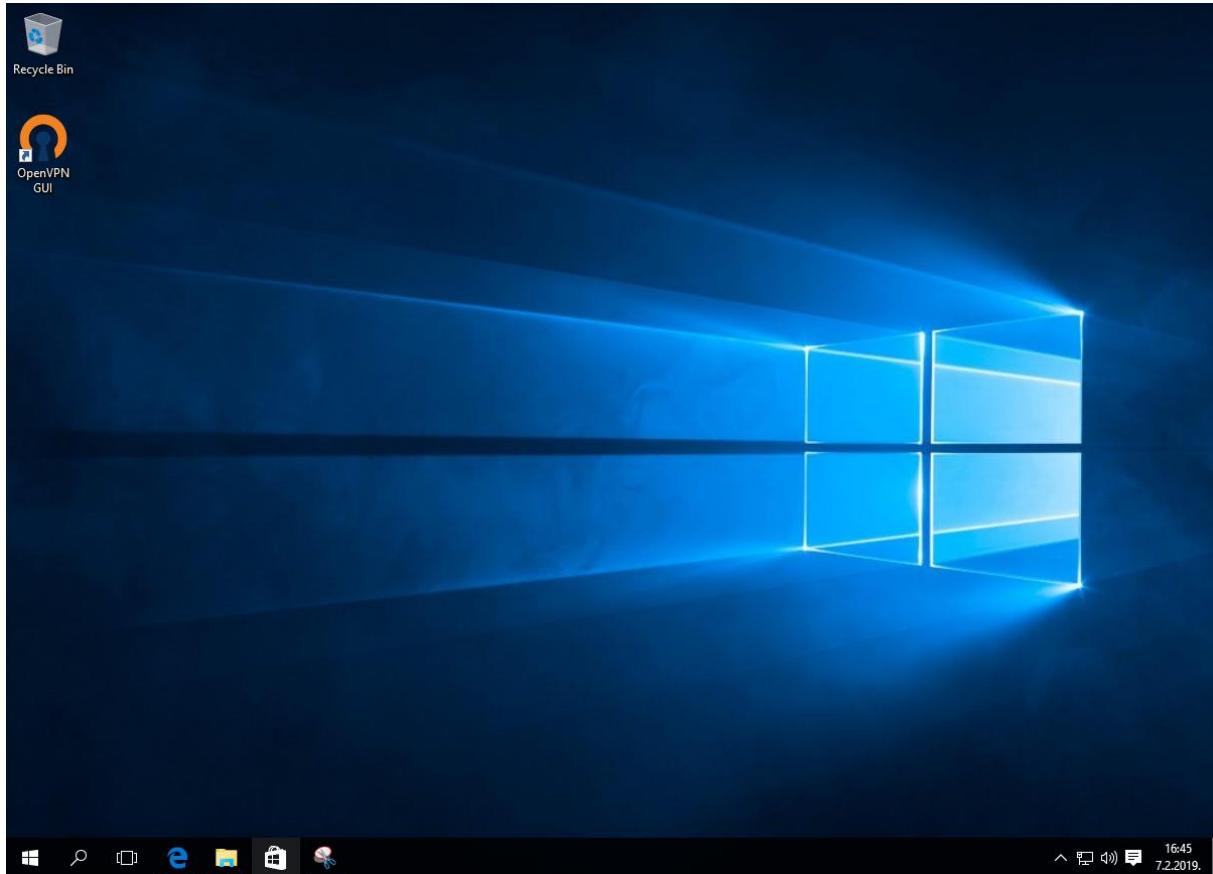


12. Posljednji prozor instalacije prikazuje kako je alat uspješno instaliran na računalo, za završetak je potrebno kliknuti **Finish**.

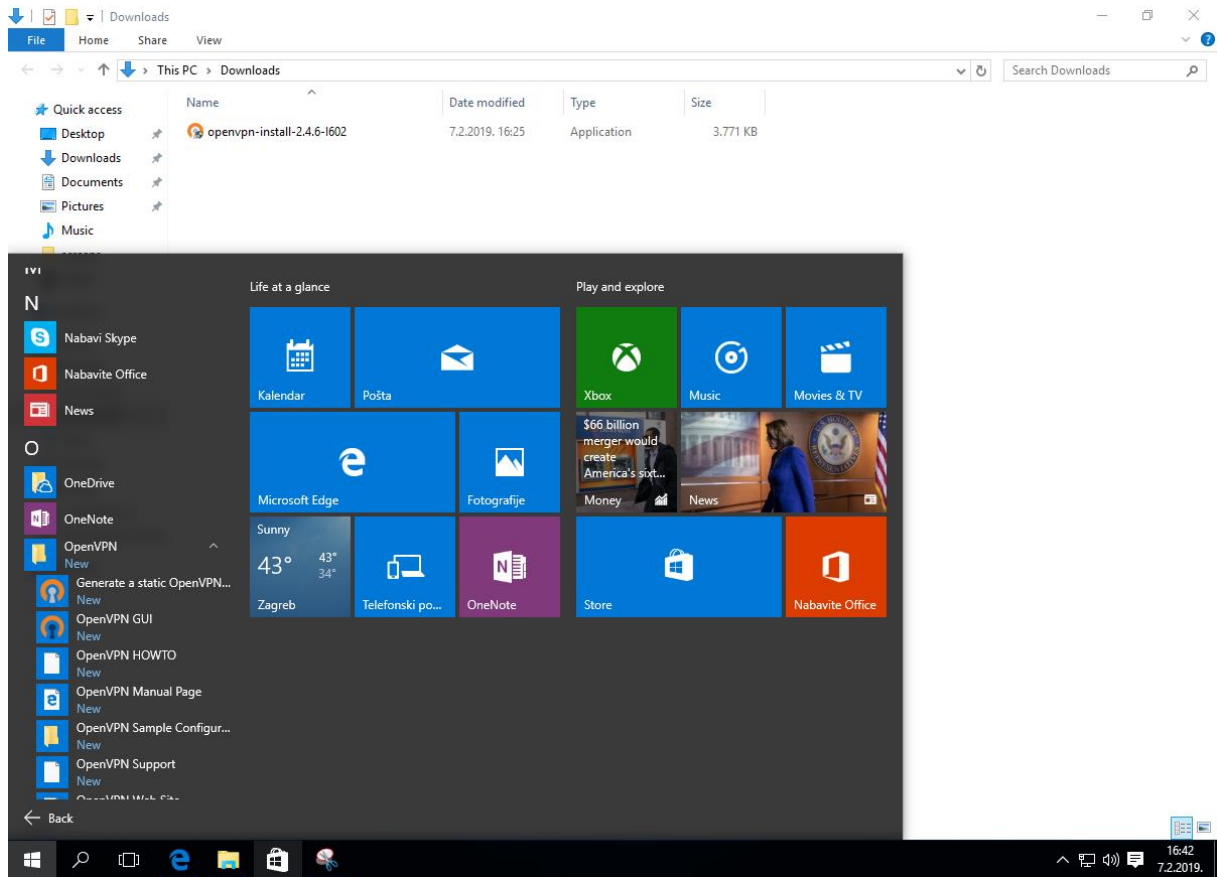


3 Korištenje alata OpenVPN GUI

1. Nakon uspješne instalacije, na radnoj površini (engl. *desktop*) će se pojaviti prečac (engl. *shortcut*) nazvan *OpenVPN GUI*.

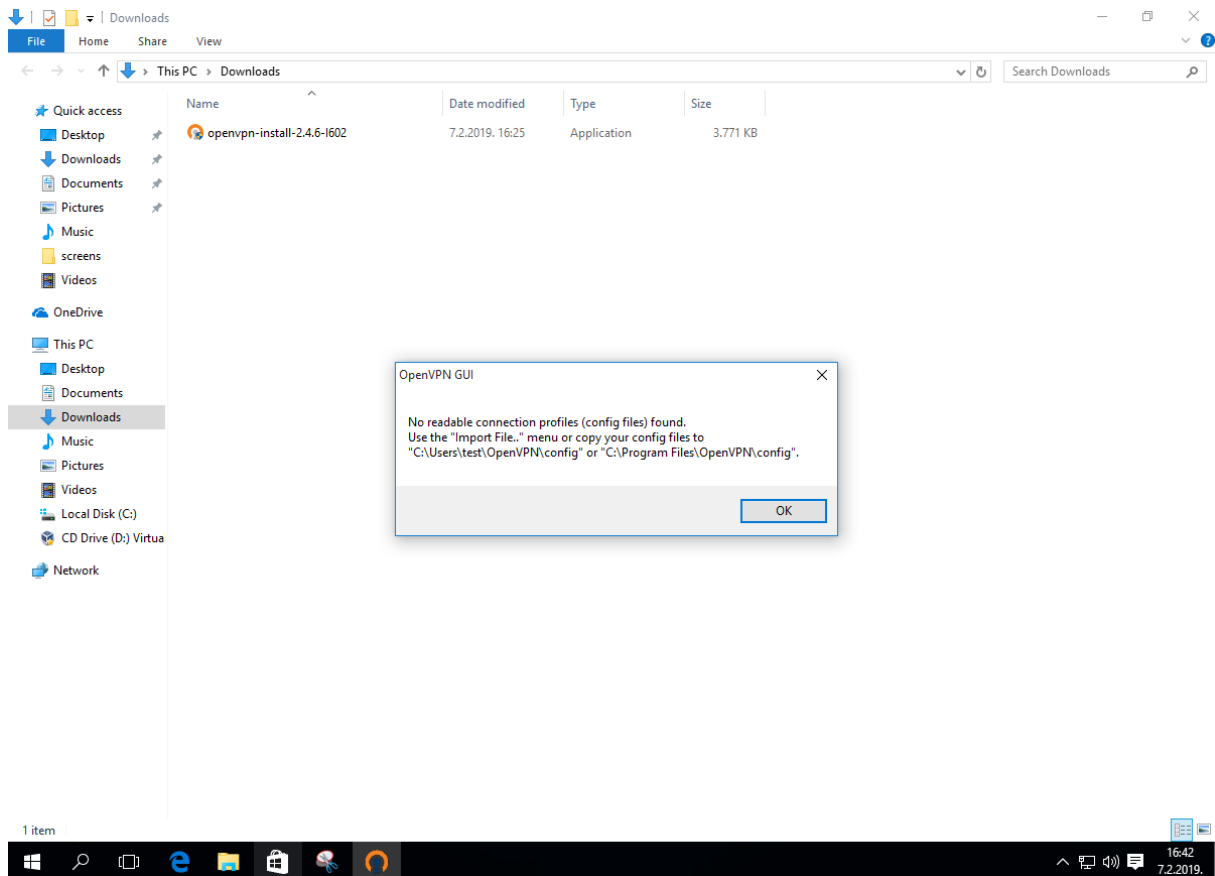


2. Alternativno, OpenVPN GUI može se pokrenuti otvaranjem izbornika Start i odabirom OpenVPN GUI ikone unutar direktorija OpenVPN.

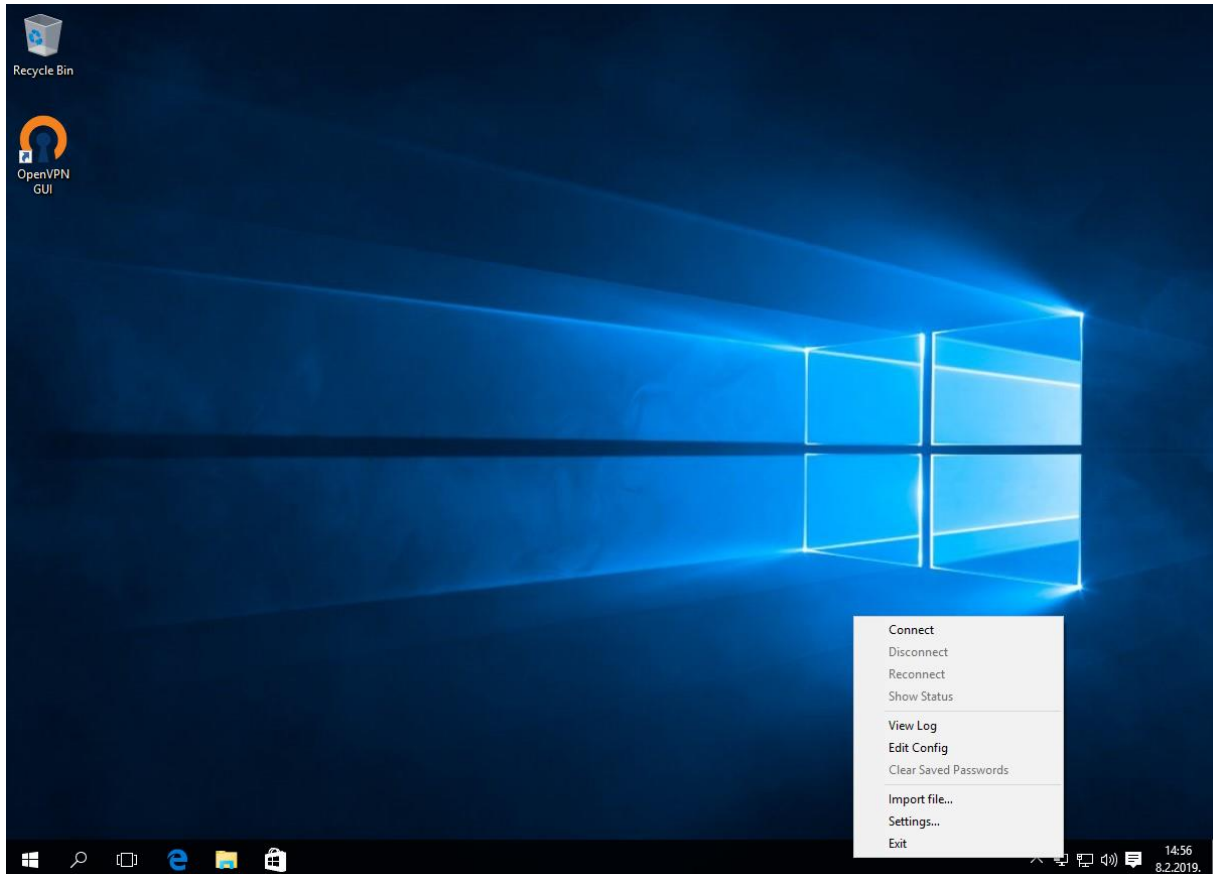


3. Kako bi OpenVPN mogao raditi, potrebna mu je odgovarajuća konfiguracijska datoteka. U slučaju kada korisnik plaća VPN uslugu, tada će tvrtka (pružatelj VPN usluga) korisniku dati odgovarajuću konfiguracijsku datoteku, obično putem svoje web stranice.

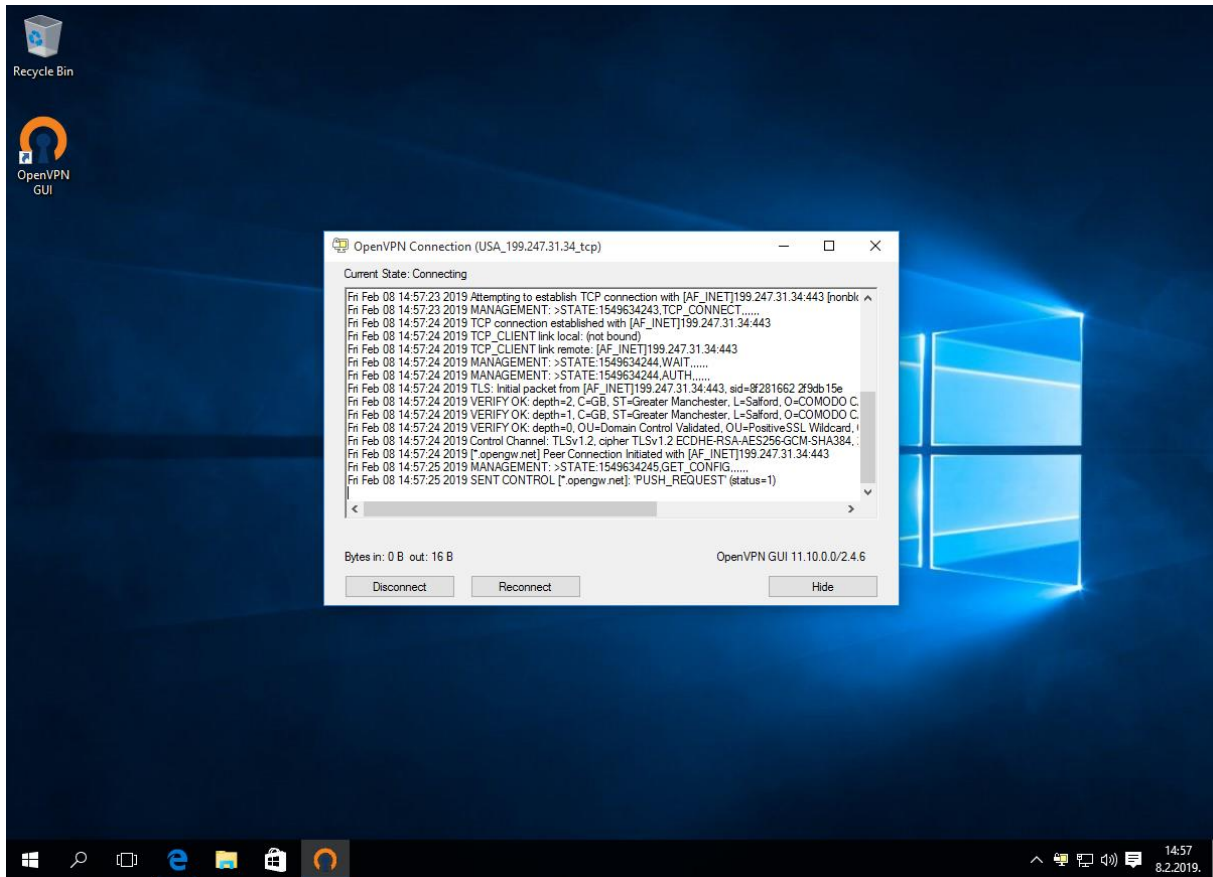
Ako se konfiguracijska datoteka ne nalazi na mjestu na kojem ju OpenVPN GUI očekuje, program ne može ispravno raditi i pojavljuje se skočni prozor (engl. *popup window*). Skočni prozor navodi na koju je lokaciju potrebno pohraniti konfiguracijsku datoteku. Alternativno, moguće je uvesti konfiguracijsku datoteku (pohraniti ju na odgovarajuću lokaciju) klikom na **Import file...** u izborniku prikazanom na slici u sljedećem koraku.



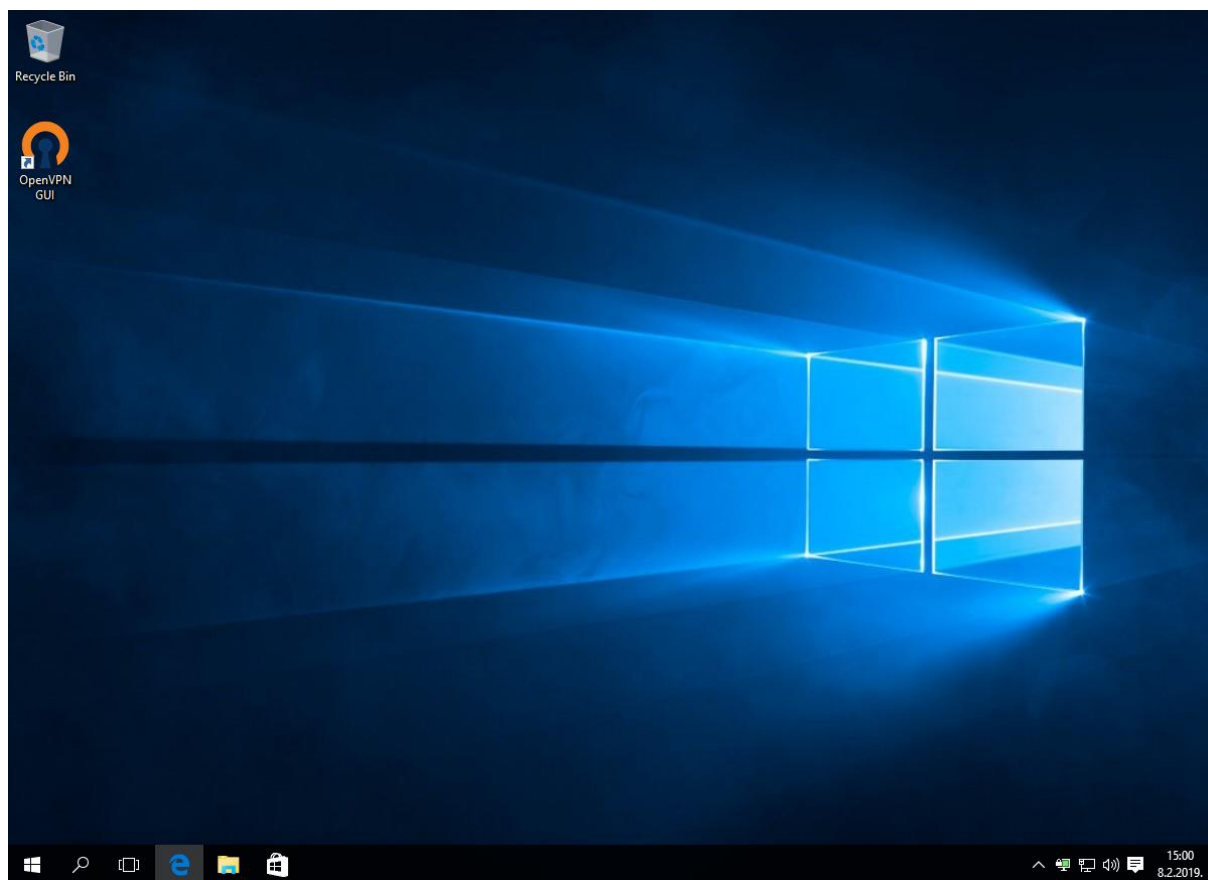
4. Nakon što je OpenVPN GUI pokrenut, pojavljuje se njegova ikona u programskoj traci. Pritiskom desne tipke miša na ikonu OpenVPN GUI-a otvara se izbornik koji između ostaloga uključuje i stavku **Import file...** za uvoz konfiguracijske datoteke. Jednom kada je konfiguracijska datoteka pohranjena na pravom mjestu, za uspostavljanje VPN veze treba u izborniku odabrati **Connect**.



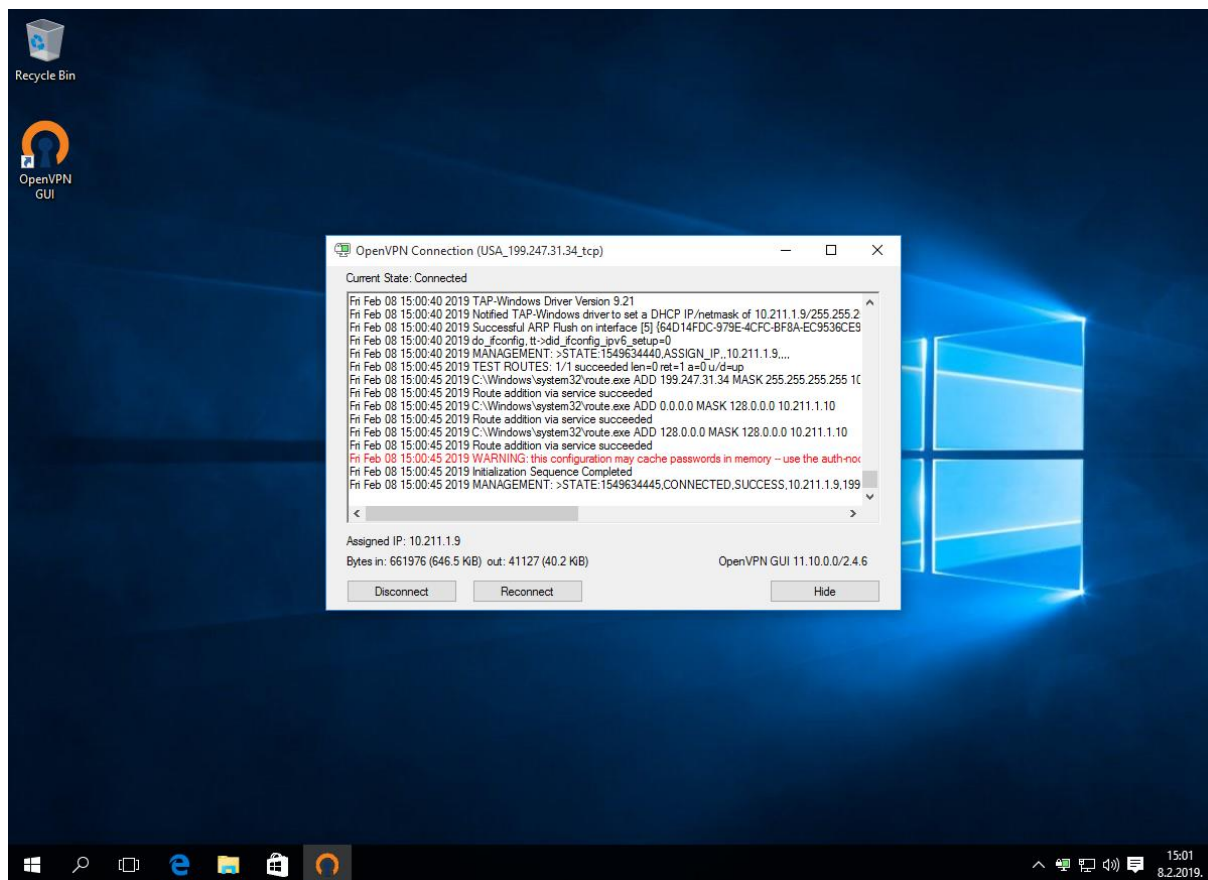
5. Nakon klika na **Connect**, prikazuje se sučelje u kojemu je prikazan napredak uspostave VPN veze odnosno prikaz trenutnog stanja veze.



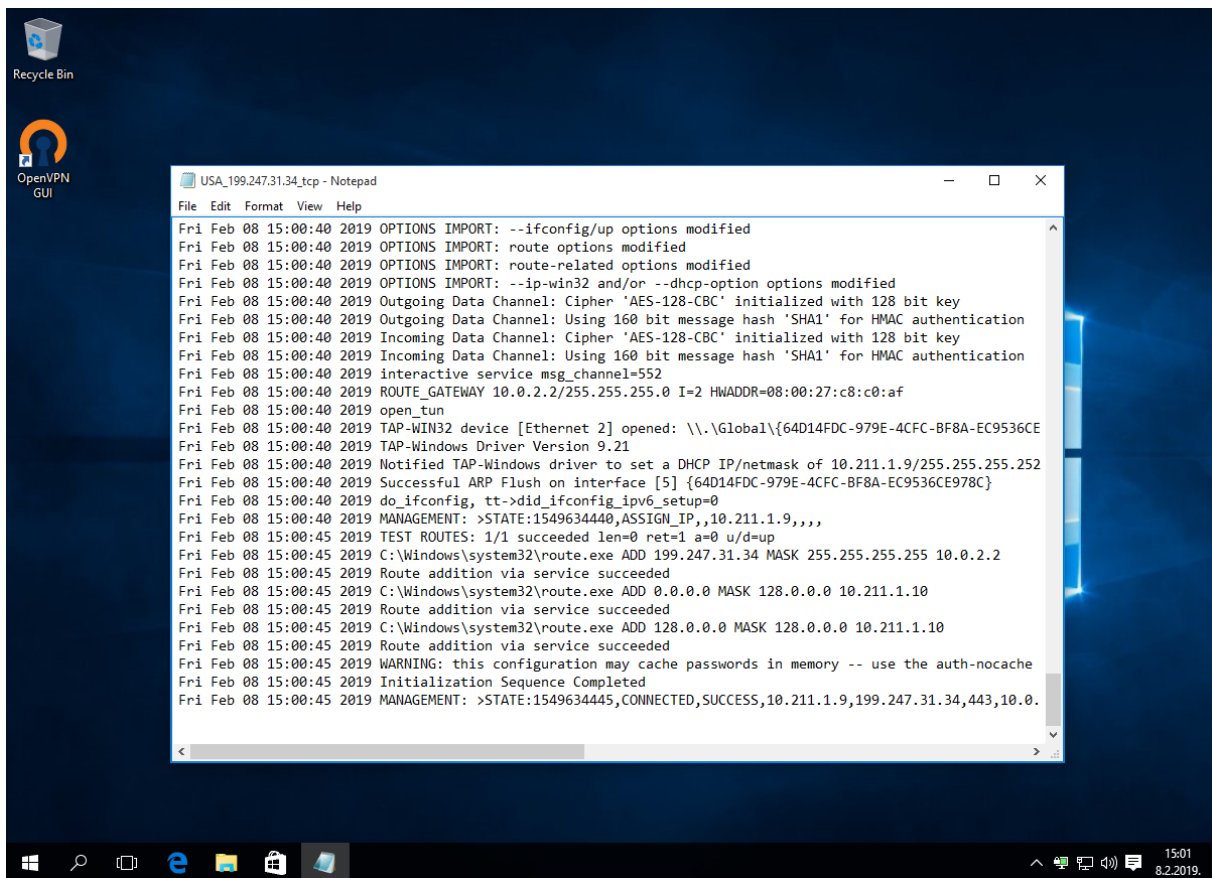
6. Nakon uspješnog uspostavljanja veze, OpenVPN GUI ikona u programskoj traci (eng. *task bar*) mijenja boju iz prozirne u zelenu.



7. Ako želimo vidjeti stanje trenutne veze, treba u izborniku (koji se otvara pritiskom desne tipke miša na ikonu OpenVPN GUI-a u programskoj traci) odabrati **Show Status**.

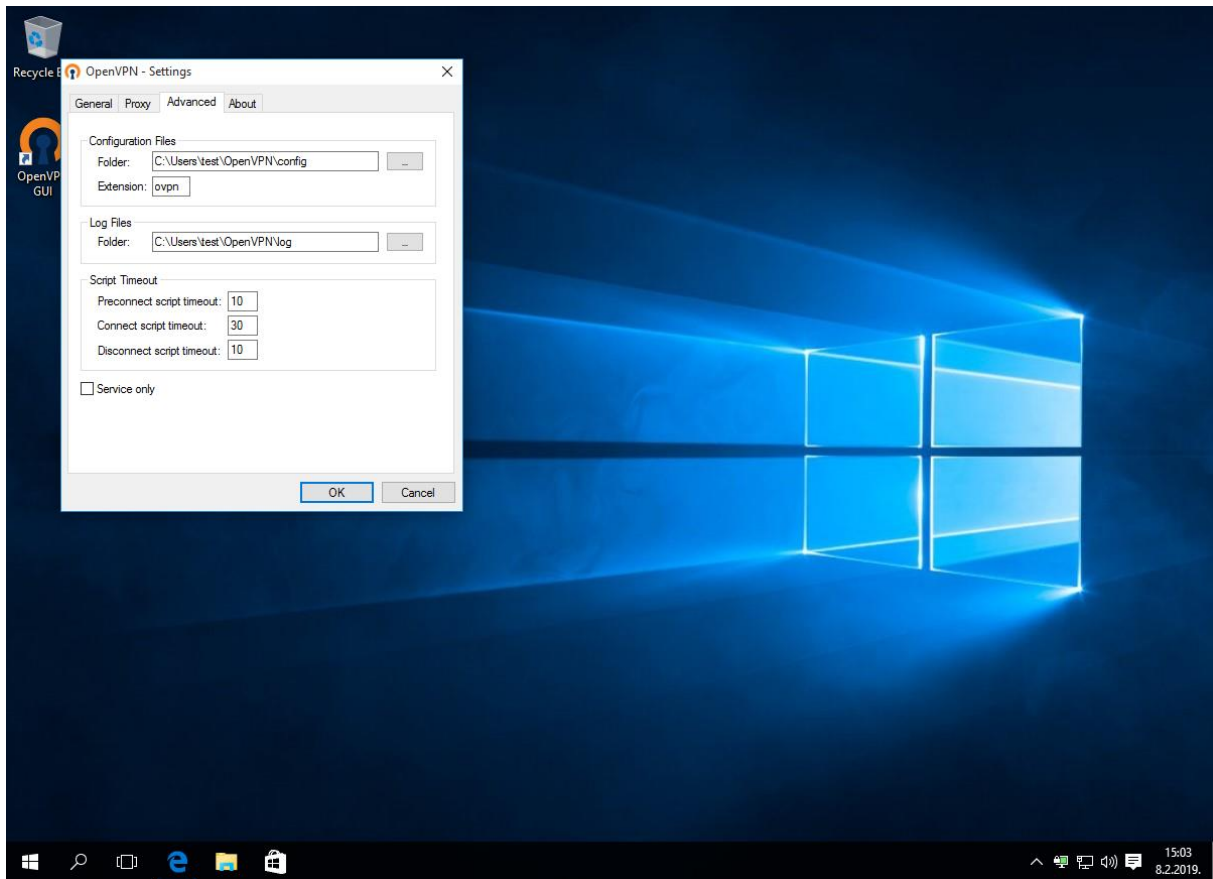


8. Ako želimo vidjeti dnevnik (engl. *log*) trenutne veze, u izborniku treba odabrati **View Log**.



```
USA_199.247.31.34_tcp - Notepad
File Edit Format View Help
Fri Feb 08 15:00:40 2019 OPTIONS IMPORT: --ifconfig/up options modified
Fri Feb 08 15:00:40 2019 OPTIONS IMPORT: route options modified
Fri Feb 08 15:00:40 2019 OPTIONS IMPORT: route-related options modified
Fri Feb 08 15:00:40 2019 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Fri Feb 08 15:00:40 2019 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
Fri Feb 08 15:00:40 2019 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Feb 08 15:00:40 2019 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
Fri Feb 08 15:00:40 2019 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Feb 08 15:00:40 2019 interactive service msg_channel=552
Fri Feb 08 15:00:40 2019 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 I=2 HWADDR=08:00:27:c8:c0:af
Fri Feb 08 15:00:40 2019 open_tun
Fri Feb 08 15:00:40 2019 TAP-WIN32 device [Ethernet 2] opened: \\.\Global\{64D14FDC-979E-4CFC-BF8A-EC9536CE
Fri Feb 08 15:00:40 2019 TAP-Windows Driver Version 9.21
Fri Feb 08 15:00:40 2019 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.211.1.9/255.255.252.252
Fri Feb 08 15:00:40 2019 Successful ARP Flush on interface [5] {64D14FDC-979E-4CFC-BF8A-EC9536CE978C}
Fri Feb 08 15:00:40 2019 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Fri Feb 08 15:00:40 2019 MANAGEMENT: >STATE:1549634440,ASSIGN_IP,,10.211.1.9,,,
Fri Feb 08 15:00:45 2019 TEST ROUTES: 1/1 succeeded len=0 ret=1 a=0 u/d=up
Fri Feb 08 15:00:45 2019 C:\Windows\system32\route.exe ADD 199.247.31.34 MASK 255.255.255.255 10.0.2.2
Fri Feb 08 15:00:45 2019 Route addition via service succeeded
Fri Feb 08 15:00:45 2019 C:\Windows\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.211.1.10
Fri Feb 08 15:00:45 2019 Route addition via service succeeded
Fri Feb 08 15:00:45 2019 C:\Windows\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.211.1.10
Fri Feb 08 15:00:45 2019 Route addition via service succeeded
Fri Feb 08 15:00:45 2019 WARNING: this configuration may cache passwords in memory -- use the auth-nocache
Fri Feb 08 15:00:45 2019 Initialization Sequence Completed
Fri Feb 08 15:00:45 2019 MANAGEMENT: >STATE:1549634445,CONNECTED,SUCCESS,10.211.1.9,199.247.31.34,443,10.0.
```


9. Ako želimo promijeniti postavke, u izborniku je potrebno odabrati **Settings**. Postavke je preporučljivo ostaviti na zadanim (engl. *default*) vrijednostima. U postavkama je, u kartici **Advanced**, vidljiva lokacija pohrane datoteka dnevnika (engl. *log files*).



10. Otvaranjem bilo kojeg servisa koji prikazuje našu trenutnu IP adresu, moguće je potvrditi da smo sada na internet spojeni putem VPN veze. Naime, naša uobičajena, fizička adresa bit će promijenjena u novu IP adresu koju je dodijelio pružatelj VPN usluge. To može imati i posljedicu promjene prividne lokacije korisnika (određene na temelju IP adrese) – na niže prikazanom primjeru, web stranica navodi kako je korisnikova lokacija u Amsterdamu, dok je korisnik zapravo bio u Zagrebu.

What is my IP address? x +

What is my IP address?

https://www.iplocation.net/find-ip-address

Your IP Address is **199.247.31.34**.
[Hide IP with VPN](#)

This is the public IP address of your computer. If your computer is behind a router or used a proxy server to view this page, the IP address shown is your router or proxy server.

Do you want to find an IP address of your network printer? Please read [How to find an IP of a printer](#) to find ways to obtain an IP number of your network printer.

Do you want to find IP Addresses of private network? Please read [How to find IP addresses of computing devices on the private network?](#)

AdChoices [Locate Address](#) [IP Location](#) [PC or Computer](#)

IP Address Details

IP Address	199.247.31.34 [Hide this IP with VPN]
IP Location	Amsterdam, Noord-Holland (NL) [Details]
Host Name	199.247.31.34.vultr.com
Proxy	199.247.31.34, 198.143.34.220
Device Type	PC
OS	Windows 10
Browser	Chrome
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.96 Safari/537.36

SEARCH OUR WEBSITE

Google Custom Search

IP TOOLS

- [TOOL: Trace Email Source](#)
- [TOOL: Verify Email Address](#)
- [TOOL: Proxy Check](#)
- [TOOL: Subnet Calculator](#)

ADVERTISEMENT

DOMAIN TOOLS

- [TOOL: Who is Hosting a Website](#)
- [TOOL: Alexa Traffic Rank Checker](#)
- [TOOL: Domain Age Checker](#)
- [TOOL: Reverse DNS Lookup](#)
- [TOOL: HTTP Server Header Check](#)

POPULAR ARTICLES

Čekanje predmemorije...

15:07
8.2.2019.

4 Zaključak

Za korisnike koji se često spajaju na nove, potencijalno nesigurne mreže – primjerice za korisnike koji puno putuju – spajanje na internet putem pouzdane VPN usluge je jedna od ključnih mjera zaštite. Po pitanju softvera za ostvarivanje tog cilja, OpenVPN je bez sumnje jedan od najboljih izbora. OpenVPN je ujedno slobodan (eng. *free and open source*) i siguran softver te mnogi pružatelji VPN usluga podržavaju njegovo korištenje.

Napredni korisnici ne moraju nužno plaćati VPN uslugu, već mogu samostalno konfigurirati i postaviti vlastiti VPN poslužitelj, primjerice na nekom svojem računalu ili na iznajmljenom virtualnom poslužitelju (eng. *virtual private server*).

Nedavno se, kao jedan ozbiljan konkurent OpenVPN-u, pojavio Wireguard. Ukratko, cilj Wireguarda je pružiti sve što pruža i OpenVPN, samo uz još bolje performanse, višu razinu sigurnosti i jednostavnije iskustvo korištenja za krajnjeg korisnika. Za sada, Wireguard je još u relativno ranom stadiju razvoja, no s vremenom, mogao bi preuzeti ulogu OpenVPN-a kao vodećeg skupa slobodnog softvera za uspostavljanje VPN veza.