

GDC OpenVPN Installation and Configuration Guide

Version: 20170808a

Contents

Important Notes	3
Introduction.....	4
Installing the Two Factor Auth (2FA) TOTP Client	5
FreeOTP Setup	5
Obtaining your OpenVPN config files and 2FA/TOTP code.....	7
Windows Installation of OpenVPN Client	7
Run OpenVPN GUI on Windows	8
Disconnecting from OpenVPN.....	10
Run OpenVPN via the cmd.exe.....	11
Test Connection on Windows.....	13
Troubleshooting Help for Windows	14
Mac (OS X) Installation.....	15
Disconnecting from VPN	18
Test Connection on OSX.....	18
Troubleshooting Help for Mac Os X	18
Linux (Ubuntu) Installation - Service/CLI (Recommended)	20
resolv.conf (Ubuntu <=16.04)	20
systemd-resolved (Ubuntu >=17.04 and Possibly Fedora).....	20
Linux (Ubuntu) Installation - Network Manager.....	22
Test Connection on Linux (Ubuntu).....	24
Troubleshooting Help for Linux	25
Appendix.....	27
Appendix: Editing the Host file	28
Windows 7 and Windows Vista.....	28
Mac OS X 10.6 - 10.1.8	28
Linux	28
Appendix: Setting static Metric on VPN TAP.....	29

Important Notes

- Please ensure that you are not connected to any other VPN connection (NIH VPN) while running the GDC OpenVPN. Tunnelblick will not work if another VPN client is running (e.g., 'Cisco AnyConnect Secure Mobility Client', or NIH VPN).
- Generic Linux instructions are provided in the Linux section, but exact steps on Linux may vary based on distribution. The general instructions provided are based on an Ubuntu flow.
- If you are using a Windows platform, you must run OpenVPN with install/run with admin rights every time you run OpenVPN (not just on initial installation)
- The OpenVPN configuration e-mails are sent from <support@nci-gdc.datacommons.io>.
 - Make sure this e-mail is listed as a 'safe sender'.
 - If the enrollment e-mails are not received, check your spam folder, or with your e-mail administrator.
- If there is a connectivity issue, make sure UDP traffic to port 1194 is allowed through your firewall to gdc-ovpn.datacommons.io.
- Going forward we have 1 unified VPN service that can connect to the different GDC build Environments currently labeled as : **dev, dev-2, qa, nightly, blue, and green**
- Instead of a consistent password, we will be using two factor authentication token combined with a certificate included in your ovpn config file. You will need to install a TOTP capable 2FA application on a mobile device as described below. Once configured, this APP will generate a new 6 digit token every 30 seconds and will be used in place of the password.

Introduction

The purpose of this document is to provide instructions on how to install and configure OpenVPN to connect to the Genomic Data Commons (GDC) internal environment. Once connected, the following GDC resources can be accessed.

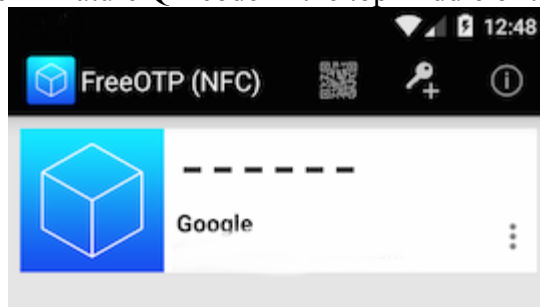
- GDC Web Site: <https://gdc.cancer.gov> - Provides access to information on GDC and associated resources including User's Guides.
- GDC Data Portal: <https://portal.gdc.cancer.gov> - Allows users to search and download cancer data sets.
- GDC API: <https://api.gdc.cancer.gov> – Provides a REST-based programmatic interface for accessing GDC data sets.
- **Consul Services: Any environment specific consul service that resolves to a Virtual Machine IP (172.21.0.0/18)**
- All future GDC websites of the form https://*.gdc.cancer.gov will be allowed

Installing the Two Factor Auth (2FA) TOTP Client

- ANDROID
 - (Recommended) FreeOTP – <https://play.google.com/store/apps/details?id=org.fedorahosted.freeotp>
 - Google Authenticator – <https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>
 - Google Authenticator may ask you to tie it to a Google Account, you can safely skip past this if you desire
- iPhone
 - (Recommended) FreeOTP – <https://itunes.apple.com/us/app/freeotp-authenticator>
 - Google Authenticator – <https://itunes.apple.com/us/app/google-authenticator>
 - Google Authenticator may ask you to tie it to a Google Account, you can safely skip past this if you desire

FreeOTP Setup

- Obtain the link to your 2FA TOTP QR Code as described below in “Obtaining your OpenVPN config files and 2FA/TOTP code”
- Open FreeOTP
- Tap the miniature QR code in the top middle of the app.



- It will open a QR scanner, showing a live stream from your camera with a white square overlaid.
- Using the on screen display, place the QRCode into the center of the square
- When aligned properly, the QR scanner will close and return you to the main screen.

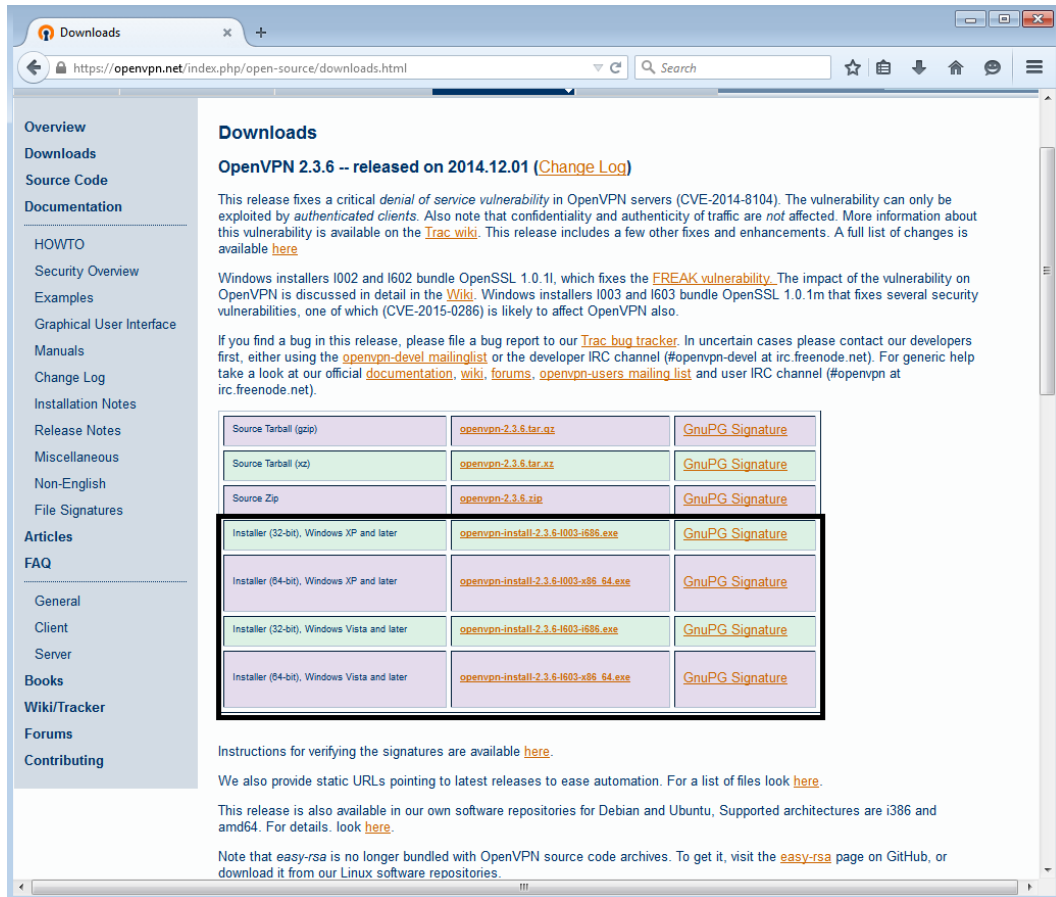
Obtaining your OpenVPN config files and 2FA/TOTP code.

In order to use OpenVPN to connect to the GDC environment, you will need to utilize configuration files and a username/password as outlined in other sections in this guide. This information will be sent in an email from support@nci-gdc.datacommons.io . It will contain the following two things:

- GDC VPN Configuration Files: This email contains your configuration files. They will be packaged as a zip file attachment to the email.
- URL to the QR Code: A url to a svg file that you will scan later with the preferred 2FA/TOTP application. This URL is only valid for 48 hours, and should NOT be shared with anyone NOR pasted into sites/applications such as slack.

Windows Installation of OpenVPN Client

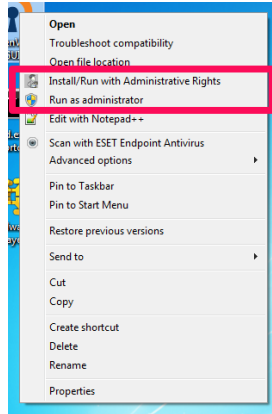
- On Windows, the official client installer and instructions can be downloaded from:
<https://openvpn.net/index.php/open-source/downloads.html>
- First, determine whether you are running Windows in 32-bit or 64-bit:
 - To **find** out if your computer is running a **32-bit or 64-bit** version of **Windows** in **Windows 7** or **Windows Vista**, do the following: Open System by clicking the Start button , right-clicking Computer, and then clicking Properties. Under System, you can view the system type.
- Windows 10 users: Please see "Setting static Metric on VPN TAP" in the appendix after you successfully install the OpenVPN client.
- Depending on your Windows OS and PC, download:
 - Installer (32-bit), Windows XP
 - Installer (64-bit), Windows XP
 - Installer (32-bit), Windows Vista and later (includes Windows 7, 8, & 10)
 - Installer (64-bit), Windows Vista and later (includes Windows 7, 8, & 10)



- The user will need to enter administrative credentials in order to install software on workstation.
 - If you are unable to obtain administrative credentials, you may need to contact your system administrator.
- Download and unzip the zip file containing your OpenVPN configuration files that was provided by the GDC Team.
 - The file should be named: "USERNAME-gdc-vpn.ovpn"

Run OpenVPN GUI on Windows

- Once installed right click the openvpn icon, and depending on your setup, select "Install/Run with Administrator Rights" or "Run as administrator".



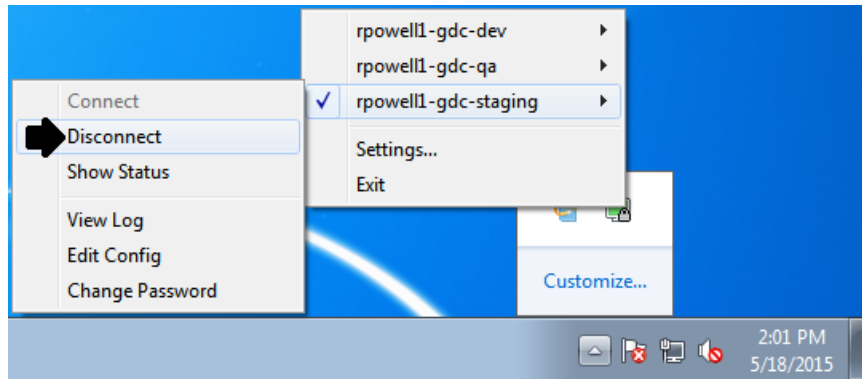
- Depending on your security settings you may receive a “registry” error. If so skip to “Running OpenVPN from cmd.exe ”
- Copy the USERNAME-gdc-vpn.ovpn to “C:\Program Files\OpenVPN\config”
- Check System Tray for the OpenVPN icon. Depending on your windows setup, the icon may be “hidden”. If so, expand the System Tray in the bottom right by clicking the up arrow.



- Right Click the System Tray icon. The copied configuration files should show up at the top of the top of the menu. Mouse over to USERNAME-gdc-. Click “Connect” from the available options.
- Where it says “Username” enter the environment you wish to connect to. Examples: dev,dev-2,qa,nightly,blue,green
- Where it says “Password” enter the 2FA/TOTP token from your phone app.
- You are connected to OpenVPN.

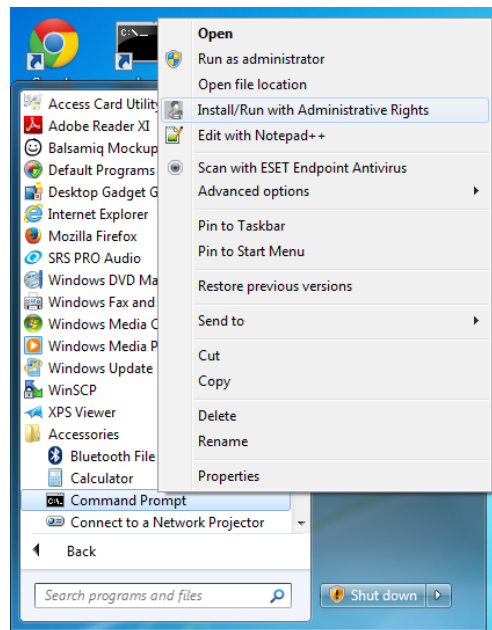
Disconnecting from OpenVPN

- To disconnect from the VPN, right click the system tray icon, select the environment, and click "Disconnect"

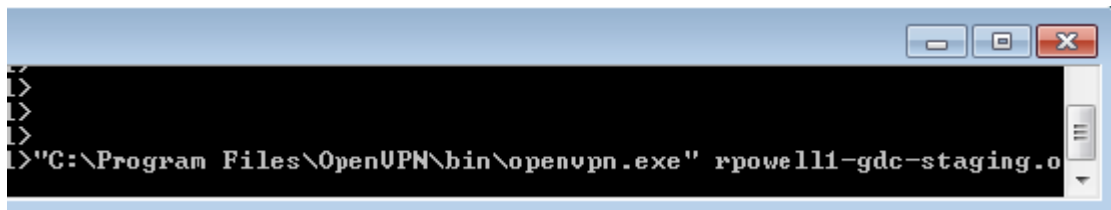


Run OpenVPN via the cmd.exe

- Click the "Start Menu",
- Click "All Programs"
- Click "Accessories"
- Right Click "Command Prompt"
- Click select "Install/Run with Administrator Rights" or "Run as administrator"



- Enter in Administrative account password for your workstation.
- Type ***"C:\Program Files\OpenVPN\bin\openvpn.exe" "C:\Program Files\OpenVPN\config\<filename>.ovpn"*** (see example below)



- Select 'enter/return' and the VPN client will attempt to connect.
 - Note, there will be a fair amount of unimportant text that will scroll up your screen.

- When prompted for a username and password, add the environment and 2FA/TOTP token as described above in the GUI section.

```

C:\[rpowell@gdc-staging.ovpn] OpenVPN 2.3.6 F4:EXIT F1:USR1 F2:USR2 F3:HUP
Mon May 18 10:11:16 2015 us=462169 cf_max = 0
Mon May 18 10:11:16 2015 us=462169 cf_per = 0
Mon May 18 10:11:16 2015 us=462169 max_clients = 1024
Mon May 18 10:11:16 2015 us=462169 max_routes_per_client = 256
Mon May 18 10:11:16 2015 us=462169 auth_user_pass_verify_script = '[UNDEF]'
Mon May 18 10:11:16 2015 us=462169 auth_user_pass_verify_script_via_file = DISABLED
Mon May 18 10:11:16 2015 us=462169 client = ENABLED
Mon May 18 10:11:16 2015 us=462169 pull = ENABLED
Mon May 18 10:11:16 2015 us=462169 auth_user_pass_file = 'stdin'
Mon May 18 10:11:16 2015 us=462169 show_net_up = DISABLED
Mon May 18 10:11:16 2015 us=462169 route_method = 0
Mon May 18 10:11:16 2015 us=462169 ip_win32_defined = DISABLED
Mon May 18 10:11:16 2015 us=462169 ip_win32_type = 3
Mon May 18 10:11:16 2015 us=462169 dhcp_masq_offset = 0
Mon May 18 10:11:16 2015 us=462169 dhcp_lease_time = 31536000
Mon May 18 10:11:16 2015 us=462169 tap_sleep = 0
Mon May 18 10:11:16 2015 us=462169 dhcp_options = DISABLED
Mon May 18 10:11:16 2015 us=462169 dhcp_renew = DISABLED
Mon May 18 10:11:16 2015 us=462169 dhcp_pre_release = DISABLED
Mon May 18 10:11:16 2015 us=462169 dhcp_release = DISABLED
Mon May 18 10:11:16 2015 us=462169 domain = '[UNDEF]'
Mon May 18 10:11:16 2015 us=462169 netbios_scope = '[UNDEF]'
Mon May 18 10:11:16 2015 us=462169 netbios_node_type = 0
Mon May 18 10:11:16 2015 us=462169 disable_nbt = DISABLED
OpenVPN 2.3.6 x86_64-w64-mingw32 [SSL [OpenSSL]] [LZO] [PKCS11]
library versions: OpenSSL 1.0.1m 19 Mar 2015, LZO 2.08
Enter Auth Username:rpowell11
Enter Auth Password:
  
```

- Connected:

```

C:\[rpowell@gdc-staging.ovpn] OpenVPN 2.3.6 F4:EXIT F1:USR1 F2:USR2 F3:HUP
8B6819467BFF> [DHCP-serv: 192.168.123.9, lease-time: 31536000]
Mon May 18 12:12:46 2015 us=375838 DHCP option string: 0f096e6f 76616c6f 63616c0
6 04ac1100 b5
Mon May 18 12:12:46 2015 us=375838 Successful ARP Flush on interface [18] <EDCC9
C2B-4F5A-4F30-AFC7-8B6819467BFF>
Mon May 18 12:12:51 2015 us=633047 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/
d=up
Mon May 18 12:12:51 2015 us=633047 C:\Windows\system32\route.exe ADD 172.17.0.0
MASK 255.255.192.0 192.168.123.9
Mon May 18 12:12:51 2015 us=633047 ROUTE: route addition failed using CreateIpFo
rwardEntry: The object already exists. [status=5010 if_index=18]
Mon May 18 12:12:51 2015 us=633047 Route addition via IPAPI failed [adaptive]
Mon May 18 12:12:51 2015 us=633047 Route addition fallback to route.exe
Mon May 18 12:12:51 2015 us=633047 env_block: add PATH=C:\Windows\System32;C:\WI
NDOWS;C:\WINDOWS\System32\Wbem
Mon May 18 12:12:51 2015 us=664247 C:\Windows\system32\route.exe ADD 192.168.123
.1 MASK 255.255.255.255 192.168.123.9
Mon May 18 12:12:51 2015 us=664247 ROUTE: route addition failed using CreateIpFo
rwardEntry: The object already exists. [status=5010 if_index=18]
Mon May 18 12:12:51 2015 us=664247 Route addition via IPAPI failed [adaptive]
Mon May 18 12:12:51 2015 us=664247 Route addition fallback to route.exe
Mon May 18 12:12:51 2015 us=664247 env_block: add PATH=C:\Windows\System32;C:\WI
NDOWS;C:\WINDOWS\System32\Wbem
Mon May 18 12:12:51 2015 us=679847 Initialization Sequence Completed
  
```

- Not connected

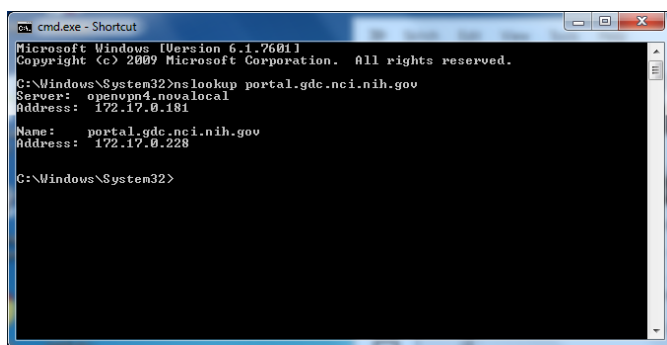
```
Administrator: Command Prompt
oud.org
Mon May 18 12:11:56 2015 us=49149 VERIFY OK: nsCertType=SERUER
Mon May 18 12:11:56 2015 us=49149 VERIFY OK: depth=0, C=US, ST=IL, L=Chicago, O=
CDIS, OU=GDC, CN=gdc-ovpn-staging.opensciencedatacloud.org, name=GDC-OpenVPN, em
ailAddress=admin@opensciencedatacloud.org
Mon May 18 12:11:56 2015 us=251950 Data Channel Encrypt: Cipher 'AES-256-CBC' in
itialized with 256 bit key
Mon May 18 12:11:56 2015 us=267550 Data Channel Encrypt: Using 160 bit message h
ash 'SHA1' for HMAC authentication
Mon May 18 12:11:56 2015 us=267550 Data Channel Decrypt: Cipher 'AES-256-CBC' in
itialized with 256 bit key
Mon May 18 12:11:56 2015 us=267550 Data Channel Decrypt: Using 160 bit message h
ash 'SHA1' for HMAC authentication
Mon May 18 12:11:56 2015 us=267550 Control Channel: TLSv1, cipher TLSv1/SSLv3 DH
E-RSA-AES256-SHA, 4096 bit RSA
Mon May 18 12:11:56 2015 us=267550 [gdc-ovpn-staging.opensciencedatacloud.org] P
eer Connection Initiated with [AF_INET]192.170.230.208:1194
Mon May 18 12:11:58 2015 us=513954 SENT CONTROL [gdc-ovpn-staging.opensciencedat
acloud.org]: 'PUSH_REQUEST' (status=1)
Mon May 18 12:11:58 2015 us=513954 AUTH: Received control message: AUTH_FAILED
Mon May 18 12:11:58 2015 us=513954 TCP/UDP: Closing socket
Mon May 18 12:11:58 2015 us=513954 SIGTERM[soft,auth-failure] received, process
exiting
c:\Users\vpntest\Downloads\rpowell>
```

- To close the VPN connection, simply close your "Command Prompt" window by clicking the X in the upper right corner.

```
[rpowell@gdc-staging.ovpn] OpenVPN 2.3.6 F4:EXIT F1:USR1 F2:USR2 F3:HUP
8B6819467BFF> [DHCP-serv: 192.168.123.9, lease-time: 31536000]
Mon May 18 12:12:46 2015 us=375838 DHCP option string: 0f096e6f 76616c6f 63616c
6 04ac1100 b5
Mon May 18 12:12:46 2015 us=375838 Successful ARP Flush on interface [18] <EDCC9
C2B-4F5A-4F30-AFC7-8B6819467BFF>
Mon May 18 12:12:51 2015 us=633047 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/
d=up
Mon May 18 12:12:51 2015 us=633047 C:\Windows\system32\route.exe ADD 172.17.0.0
MASK 255.255.192.0 192.168.123.9
Mon May 18 12:12:51 2015 us=633047 ROUTE: route addition failed using CreateIpFo
rwardEntry: The object already exists. [status=5010 if_index=18]
Mon May 18 12:12:51 2015 us=633047 Route addition via IPAPI failed [adaptive]
Mon May 18 12:12:51 2015 us=633047 Route addition fallback to route.exe
Mon May 18 12:12:51 2015 us=633047 env_block: add PATH=C:\Windows\System32;C:\WI
NDOWS;C:\WINDOWS\System32\Wbem
Mon May 18 12:12:51 2015 us=664247 C:\Windows\system32\route.exe ADD 192.168.123
.1 MASK 255.255.255.255 192.168.123.9
Mon May 18 12:12:51 2015 us=664247 ROUTE: route addition failed using CreateIpFo
rwardEntry: The object already exists. [status=5010 if_index=18]
Mon May 18 12:12:51 2015 us=664247 Route addition via IPAPI failed [adaptive]
Mon May 18 12:12:51 2015 us=664247 Route addition fallback to route.exe
Mon May 18 12:12:51 2015 us=664247 env_block: add PATH=C:\Windows\System32;C:\WI
NDOWS;C:\WINDOWS\System32\Wbem
Mon May 18 12:12:51 2015 us=679847 Initialization Sequence Completed
```

Test Connection on Windows

- Open New Cmd Prompt Window:
 - Click the "Start Menu",
 - Click "All Programs"
 - Click "Accessories"
 - Right Click "Command Prompt"
 - Click select "Install/Run with Administrator Rights" or "Run as administrator"
- In newly opened Command prompt window:
- Type `nslookup portal.gdc.cancer.gov`



```
cmd.exe - Shortcut
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup portal.gdc.nci.nih.gov
Server: openvpn4.novalocal
Address: 172.17.0.181

Name: portal.gdc.nci.nih.gov
Address: 172.17.0.228

C:\Windows\System32>
```

- If you see an IP address beginning with 172, it means that your computer is able to successfully resolve portal.gdc.cancer.gov which is required for the portal to load.
- Note: The exact IPs address may vary, but the objective is just to ensure that your computer is using a GDC DNS server, and that your computer can resolve portal.gdc.cancer.gov using the OpenVPN server.

Troubleshooting Help for Windows

- Please ensure you are started both the OpenVPN client and the cmd prompt for nslookup check with Admin privileges.
- Please ensure you have already commented out or remove any previous redirection in your hosts file for portal.nci.nih.gov or portal.gdc.nci.nih.gov. For instructions on how to check/edit the host file, please refer to the Appendix.
- Please ensure that you are not connected to any other VPN connection (e.g. NIH VPN) while running the GDC OpenVPN.

Mac (OS X) Installation

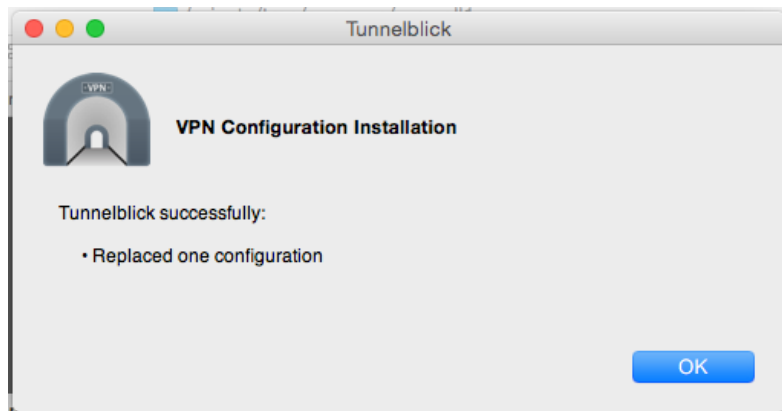
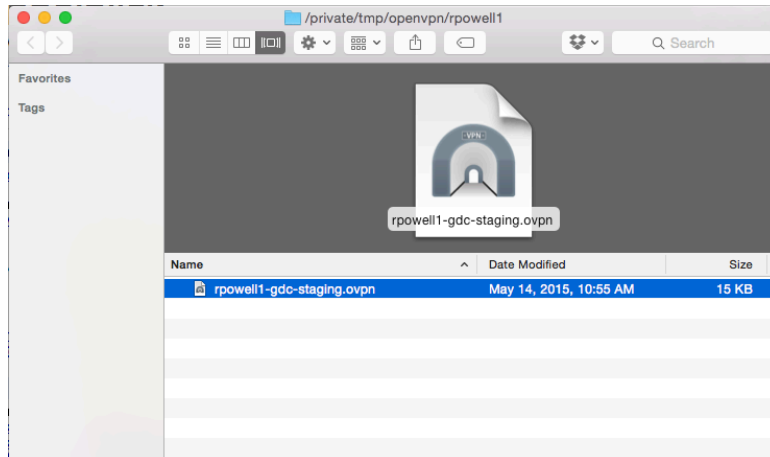
- The TunnelBlick client is our preferred method for connecting to OpenVPN on OS X and is available from:

<https://tunnelblick.net/>

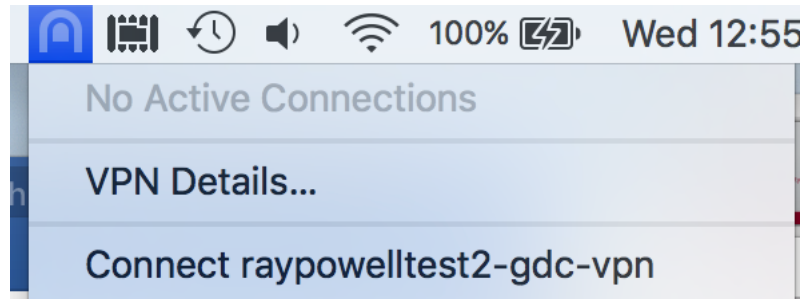


- Install the TunnelBlick software, you will be prompted for administrative credentials on your Mac to install software.
- During the installation process, you may receive two selection prompts:
 - Do you already have VPN config files? *Select Yes.*
 - Do you want to receive a warning about your IP not changing? *Select No.*
- Open TunnelBlick by going to Applications > TunnelBlick.
 - The first time you run it OSX may ask you to confirm that it is safe to run an application downloaded from the Internet. Click OK.
- Once installed, TunnelBlick registers the .ovpn file extension with the OS. Locate the configuration files and double click them. You will be asked to enter your username and password for the Mac to install software.
 - When complete it will inform you that the configuration installation was successful.
- You may need to reboot once Tunnelblick has been installed and configuration imported.
 - Otherwise DNS do not get updated and the system stick to other VPNs configured (<https://airvpn.org/topic/11665-tunnelblick-how-to-force-using-airvpn-dns-when-connected-and-routers-dns-when-disconnected/>).

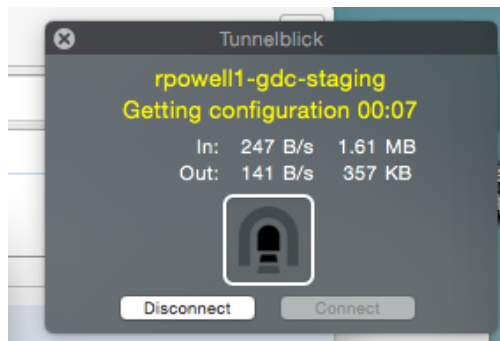
- *Note: Sometimes the Mac TunnelBlick client will hide windows in the background. If this happens, you may need to first quit TunnelBlick by right clicking the icon next to the system clock and then double click the config file again.*



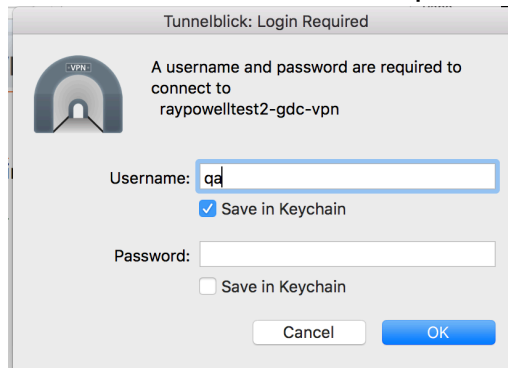
- TunnelBlick should place an icon in the upper right corner of your Menu Bar.
 - Right clicking will drop down a list of available VPN configurations. Choose "USERNAME-gdc-vpn" and click it.



- While connecting you will may see a status message similar to the image below.



- You will be prompted to enter a username and password.



- Where it says "Username" enter the environment you wish to connect to. Examples: dev,dev-2,qa,nightly,blue,green . NOTE: It is okay to click "Save in Keychain" for the username. As it will just prefill the last environment you connected to.
- Where it says "Password" enter the 2FA/TOTP token from your phone app. NOTE: Do NOT click "Save in keychain" under Password, as the 2FA/TOTP token expires after 30 seconds, and you will need to enter a new one each time you connect.
Click "OK"

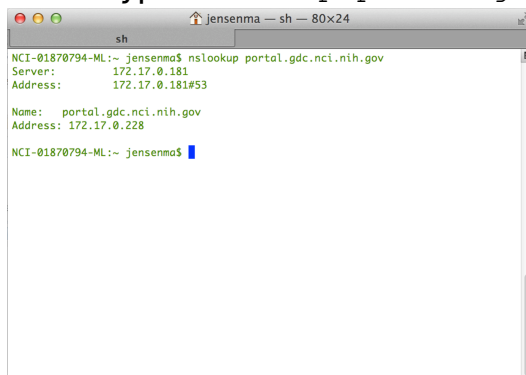
- Note: If local NIC obtained IP/DNS after tunnel has been established, it may override OpenVPN DNS.
 - This might happen if a user roams while moving from one room to another, etc.

Disconnecting from VPN

- When you wish to disconnect from the VPN, click the TunnelBlick icon in the Menu Bar then click "Disconnect USERNAME-gdc-VPN" for the active VPN connection.

Test Connection on OSX

- Open New Terminal Window:
- In newly opened Terminal window:
 - Type `nslookup portal.gdc.cancer.gov`



```

sh
jensenma — sh — 80x24
NCI-01870794-ML:~ jensenma$ nslookup portal.gdc.nci.nih.gov
Server:      172.17.0.181
Address:     172.17.0.181#53

Name:   portal.gdc.nci.nih.gov
Address: 172.17.0.228
NCI-01870794-ML:~ jensenma$

```

- If you see an IP address beginning with 172, it means that your computer is able to successfully resolve portal.gdc.cancer.gov which is required for the portal to load.

Troubleshooting Help for Mac Os X

- Please ensure you have already commented out or remove any previous redirection in your hosts file for portal.gdc.cancer.gov. For instructions on how to check/edit the host file, please refer to the Appendix.

- Please ensure that you are not connected to any other VPN connection (e.g. NIH VPN) while running the GDC OpenVPN.

Linux (Ubuntu) Installation – Service/CLI (Recommended)

With the acceptance of Systemd handling dns resolution, Network Manager doesn't seem to handle updating your local dns correctly. Until Network Manager stabilizes we recommend starting the service directly via your init .

resolv.conf (Ubuntu <=16.04)

- Obtain and unzip your ZIP file containing the OVPN configuration files. You will want to use the file similar to example-gdc/linux/example-gdc-vpn-resolvconf.ovpn (Where “example” has been replaced with your name)

- \$unzip example.zip

```
Archive:  example.zip
  inflating: example-gdc/example-gdc-vpn.ovpn
  extracting: example-gdc/example-gdc-vpn-seperated.tgz
   creating: example-gdc/linux/
  inflating: example-gdc/linux/example-gdc-vpn-resolvconf.ovpn
  inflating: example-gdc/linux/example-gdc-vpn-systemd.ovpn
```

- Install openvpn
 - \$ sudo apt-get install -y openvpn
- Copy your config file to /etc/openvpn/gdc.conf
 - \$ sudo cp /home/ubuntu/downloads/ example-gdc/linux/example-gdc-vpn-resolvconf.ovpn /etc/openvpn/gdc.conf
- Start openvpn with @gdc systemctl command.
 - \$ sudo systemctl start openvpn@gdc
- Verify that openvpn has modified your /etc/resolv.conf file. It should look similar to the following. The values may be different, as long as the first DNS server begins with 172.21.x.y you are working properly.
 - \$ sudo cat /etc/resolv.conf

```
#Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 172.21.40.77
nameserver 127.0.0.1
Search gdc.cancer.gov
```

- You should now be connected to the VPN!

systemd-resolved (Ubuntu >=17.04 and Possibly Fedora)

- Obtain and unzip your ZIP file containing the OVPN configuration files. You will want to use the file similar to example-gdc/linux/example-gdc-vpn-systemd.ovpn (Where “example” has been replaced with your name)
 - \$unzip example.zip

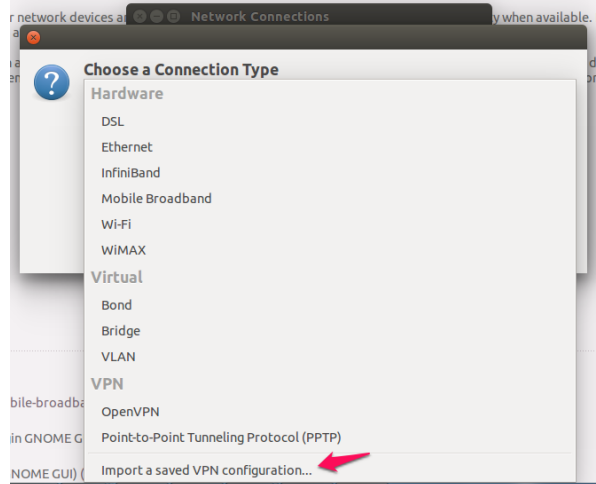
```
Archive:  example.zip
  inflating: example-gdc/example-gdc-vpn.ovpn
  extracting: example-gdc/example-gdc-vpn-seperated.tgz
    creating: example-gdc/linux/
  inflating: example-gdc/linux/example-gdc-vpn-resolvconf.ovpn
  inflating: example-gdc/linux/example-gdc-vpn-systemd.ovpn
```

- Install openvpn
 - `$ sudo apt-get install -y openvpn`
- Copy your config file to `/etc/openvpn/gdc.conf`
 - `$ sudo cp /home/ubuntu/downloads/ example-gdc/linux/example-gdc-vpn-systemd.ovpn /etc/openvpn/gdc.conf`
- Check the status of systemd-resolve:
 - `$ sudo systemd-resolved --status | grep "DNS Servers"`
 - DNS Servers: 128.135.249.50
- Start openvpn with `@gdc`
 - `$ sudo systemctl start openvpn@gdc`
- Verify that openvpn has modified your dns servers. The values may be different, as long as the first DNS server begins with 172.21.x.y you are working properly.
 - `$ sudo systemd-resolved --status | grep "DNS Servers"`
 - DNS Servers: 172.21.40.77
 - Servers: 128.135.249.50
- You should now be connected to the VPN!

Linux (Ubuntu) Installation – Network Manager

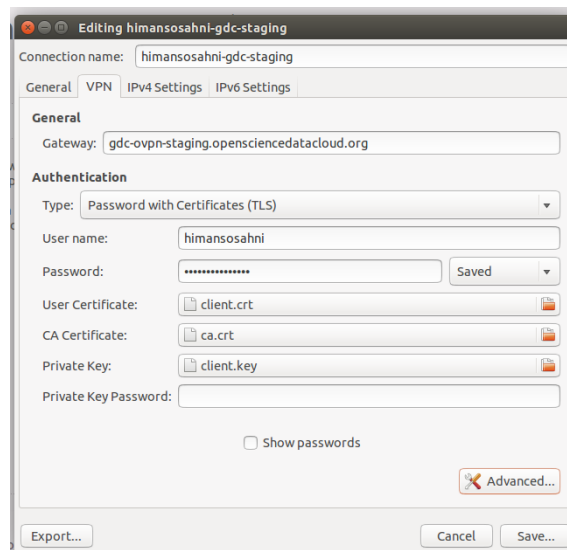
- Network Manager has been acting irregularly on some newer installations and so we do not recommend unless you are capable of trouble shooting issues on your own.
- Installation on Linux will vary by distribution, but most popular repositories have OpenVPN available for download. These generic steps are taken from the context of an Ubuntu flow.
 - For more detailed and specific instructions for using OpenVPN on Linux, please see: <https://openvpn.net/index.php/open-source/documentation/howto.html>
- Download and install the following packages from your repository of choice:
 - On Ubuntu:

```
apt-get install network-manager network-manager-openvpn  
network-manager-openvpn-gnome
```
- The included .ovpn file does not work natively on Ubuntu. To work, un-tar “username-gdc-vpn-seperated.tgz” to the following:
 -
 - *username-gdc-vpn/client.key*
 - *username-gdc-vpn/johndoe-gdc-vpn.ovpn*
 - *username-gdc-vpn/client.crt*
 - *username-gdc-vpn/ta.key*
 - *username-gdc-vpn/ca.crt*
 - You can now add this VPN configuration as a VPN connection in the Desktop GUI:
 - Choose connection Type:



- Click the network manager icon in the top menu bar and select "Edit Connections..."
- In the Network Connections box click "Add".
- On the dropdown menu, under VPN, click "Import a saved VPN configuration..." and click create.
- Select the ovpn file modified above.

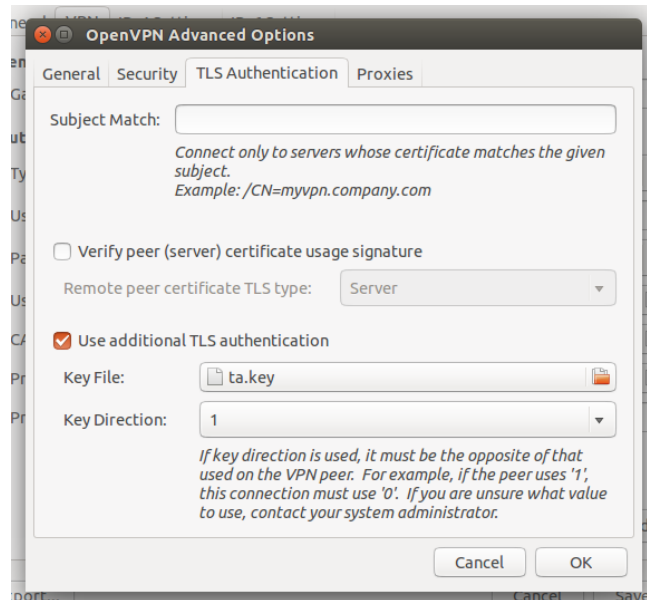
Edit OVPN file settings:



- Ensure "Password with Certificates (TLS)" is selected as the Type underneath "Authentication."
- Enter your username and password provided for the environment chosen.
- For *User Certificate* choose *client.crt* from above.
- For *CA Certificate* choose *ca.crt* from above.

- For *Private Key* choose *client.key* from above.
- Click on the *Advanced* button.

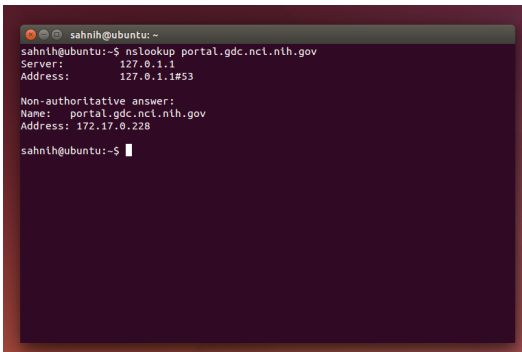
Under Advanced Settings:



- Click on the *TLS Authentication* tab.
- Check the “Use Additional TLS authentication” box
- Choose *ta.key* from above for *Key File*
- Choose *1* for the *Key Direction*
- Select *OK*
- Select *Save*
- The VPN connection will now be added to your network manager connections list and can be selected.

Test Connection on Linux (Ubuntu)

- Open New Terminal Window:
- In newly opened Terminal window:
- Type `nslookup portal.gdc.cancer.gov`

A terminal window with a dark background and light text. The prompt is 'sahnth@ubuntu:~'. The command entered is 'nslookup portal.gdc.nci.nih.gov'. The output shows 'Server: 127.0.1.1' and 'Address: 127.0.1.1#53'. Below that, it says 'Non-authoritative answer:', 'Name: portal.gdc.nci.nih.gov', and 'Address: 172.17.0.228'. The prompt returns to 'sahnth@ubuntu:~\$'.

- If you see an IP address starting with 172, it means that your computer is able to successfully resolve portal.gdc.cancer.gov which is required for the portal to load.
- Note: The exact IP address may vary, but the objective is just to ensure that your computer is using a GDC DNS server, and that your computer can resolve portal.gdc.cancer.gov using the OpenVPN server.

Troubleshooting Help for Linux

- Please ensure that you do not have any duplicate resources in Google authenticator prior to taking a screenshot. Google Authenticator will silently fail to add the new secret. IE if you have user@bionimbus-pdc.opensciencedatacloud.org and take picture of a qr for user@bionimbus-pdc.opensciencedatacloud.org it will keep your old one. Please delete your old secret prior to taking a picture of the new secret.
- FreeOTP for iPhones seems to be a bit buggy when adding a secret manually. If you can't seem to add your secret please verify the following:
 - Issuer, ID, and Secret are all filled in.
 - The format of your secret matches the format specified (ie sha1,sha256,md5, etc)
 - Click back and forth between issuer and ID and see if the add button becomes available.
- Please ensure you have already commented out or remove any previous redirection in your hosts file for portal.nci.nih.gov or portal.gdc.nci.nih.gov. For instructions on how to check/edit the host file, please refer to the Appendix.
- Please ensure that you are not connected to any other VPN connection (e.g. NIH VPN) while running the GDC OpenVPN.

Appendix

Appendix: Editing the Host file

Windows 7 and Windows Vista

1. For Click **Start** -> **All Programs** -> **Accessories**.
2. Right click Notepad and select **Run/Install with administrative rights**.
3. Click **Continue** on the "Windows needs your permission" UAC window.
4. When Notepad opens Click **File** -> **Open**.
5. In the filename field type:
C:\Windows\System32\Drivers\etc\hosts
6. Click **Open**.
7. Make the necessary changes to the hosts file.
8. Click **File** -> **Save** to save your changes.

Mac OS X 10.6 - 10.1.8

1. Open **Applications** > **Utilities** > **Terminal**.
2. Open the hosts file by typing the following in the Terminal window:

```
sudo nano /private/etc/hosts
```

3. Type your user password when prompted.
4. Make the necessary changes to the hosts file.
5. Save the hosts file by pressing **Control+x** and answering **y**.
6. Make your changes take effect by flushing the DNS cache with the following command:

```
dscacheutil -flushcache
```

7. New mappings should now take effect.

Linux

1. Open a terminal window.
2. Open the hosts file in a text editor (you can substitute any text editor):

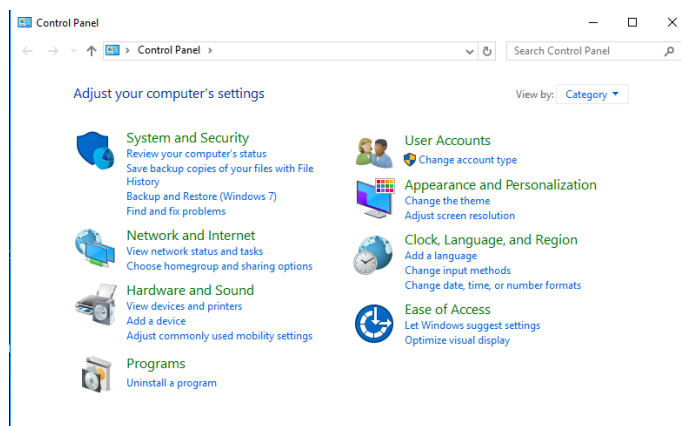
```
sudo nano /etc/hosts
```

3. Enter your password.
4. Make the necessary changes to the hosts file.
5. Press **control-X** (hold control and hit X), then answer **y** when asked if you want to save your changes.

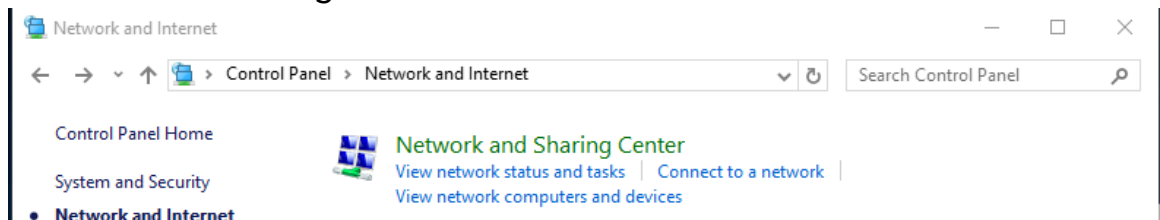
Appendix: Setting static Metric on VPN TAP

Windows 10 changed how windows networking handles multiple connections. This prevents DNS from resolving properly over the VPN. The below steps will adjust your VPN connections "metric" to be below the default value and allow DNS to resume working.

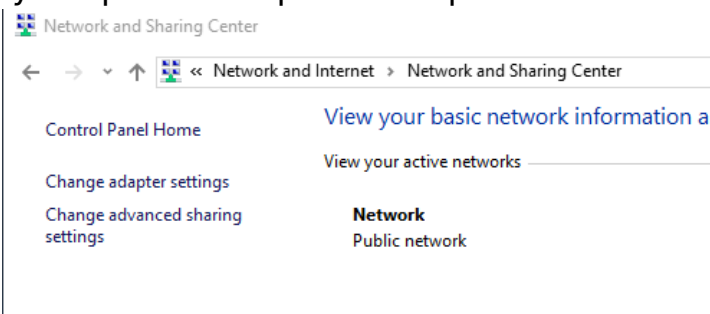
1. Make sure the OpenVPN client has been installed. If it asked for you to reboot, then please reboot before proceeding.
2. Go to Control Panel
3. Select "Network and Internet"



4. Select "Network and Sharing Center"

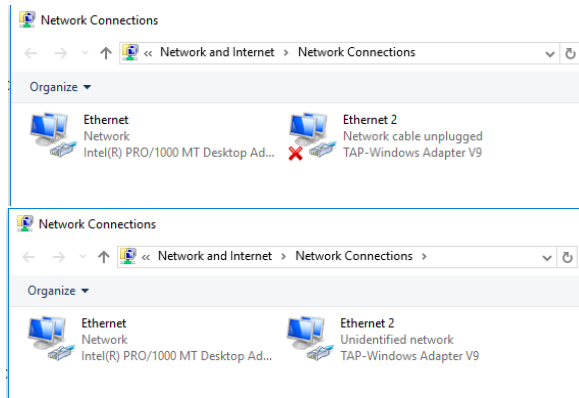


5. Select ,on the left, "Change Adapter Settings" . This will open a new window showing all your network "adapters" on the computer. Including physical ports and OpenVPN "taps".

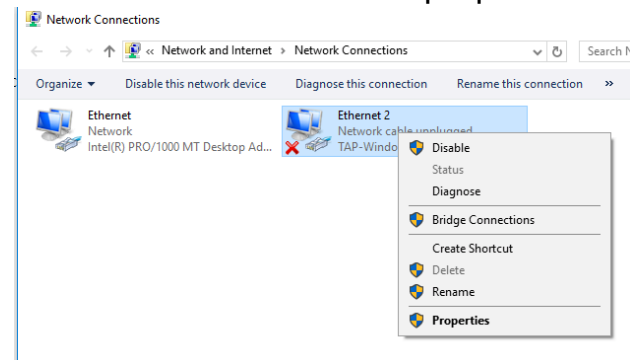


6. The new window will look similar to the picture below. However the number and names of the adapters will be different on every computer.

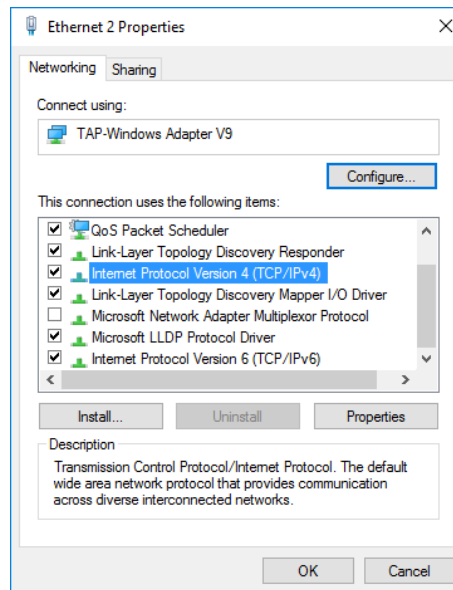
If you are not currently connected to the VPN the “VPN TAP” will have a red X under the icon. Locate the “TAP” interface for OpenVPN.



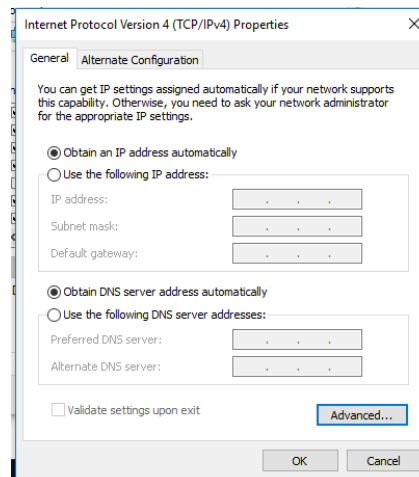
7. Right click the “TAP” interface and select properties



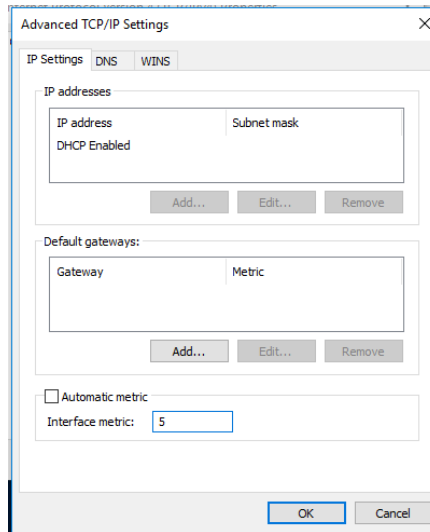
8. Under “This connection uses the following items:” you will have some options. Each computer will look slightly different. Scroll down and find the “Internet Protocol Version 4 (TCP/IPv4)” or similar. Do not select the “IPv6” item. Select “Internet Protocol Version 4 (TCP/IPv4)” and then click “Properties”.



9. On the new window click "Advanced" in the bottom right.



10. On this last window will be a check box next to "Automatic Metric". Uncheck that box. Then in the "Interface metric:" box, enter the value "5" (minus the quotes).



11. Click "OK" and "CLOSE" until you have closed all the windows we opened above. Your VPN TAP interface will now be given higher priority by Windows 10. Allowing DNS to work properly.