



# OPENVPN IP/DNS MONITORING SOFTWARE

## OpenVPN WatchDog V3.0 User Guide

### ABOUT OPENVPN WATCH DOG V3.0

OpenVPN Watch Dog is a windows based application to securely monitor for stable encryption of internet traffic and prevent exposure of real IP address and DNS leaks thereby offering the benefits of encrypted connection to the internet with IP address anonymity and full privacy. OpenVPN Watch Dog is a program designed to monitor your OpenVPN connection and ensures that you do not blow up your anonymity when you lose your OpenVPN connection. When connected to an OpenVPN server and OpenVPN Watch Dog is enabled, you can be sure that all traffic leaving your computer is fully encrypted. When your OpenVPN crashes or is compromised, OpenVPN Watch Dog will automatically detect it, alert you of the danger and cut-off your internet access.

**Warning!:** OpenVPN is prone to IP and DNS leaks particularly in Windows. It is essential that you are aware of this and should take adequate measures to safeguard your OpenVPN connection against such security issues!

### HOW IT WORKS

Simply start the OpenVPN Watch Dog before initiating connection to your OpenVPN server. The program will automatically detect your real connection IP, OpenVPN server IP and your DNS IPs. Your real IP is stored internally when the program is started and then starts monitoring your connection IP every second after you start the OpenVPN session to make sure that your real IP is never exposed. The program ensures that all traffic leaving your computer is fully encrypted by monitoring and comparing the assigned private IP of the OpenVPN server and your local connection.

In addition, the program has the capability to lock down your OpenVPN connection. After locking down your OpenVPN connection, network traffic will only exit through your OpenVPN connection, and no other network interfaces thereby preventing DNS leaks and IP leaks through your VPN connection. In the event a security issue is detected, a barking dog sound is produced and an alert is given. In addition, the program will automatically deactivate all internet connections on your computer. To enable internet connection again, simply click the “Enable All Network Connections” button to restore the internet access.



# OPENVPN IP/DNS MONITORING SOFTWARE

## SUPPORTED OPERATING SYSTEMS

- ✓ Windows XP
- ✓ Windows Vista
- ✓ Windows 7
- ✓ Windows Server 2003
- ✓ Windows Server 2008

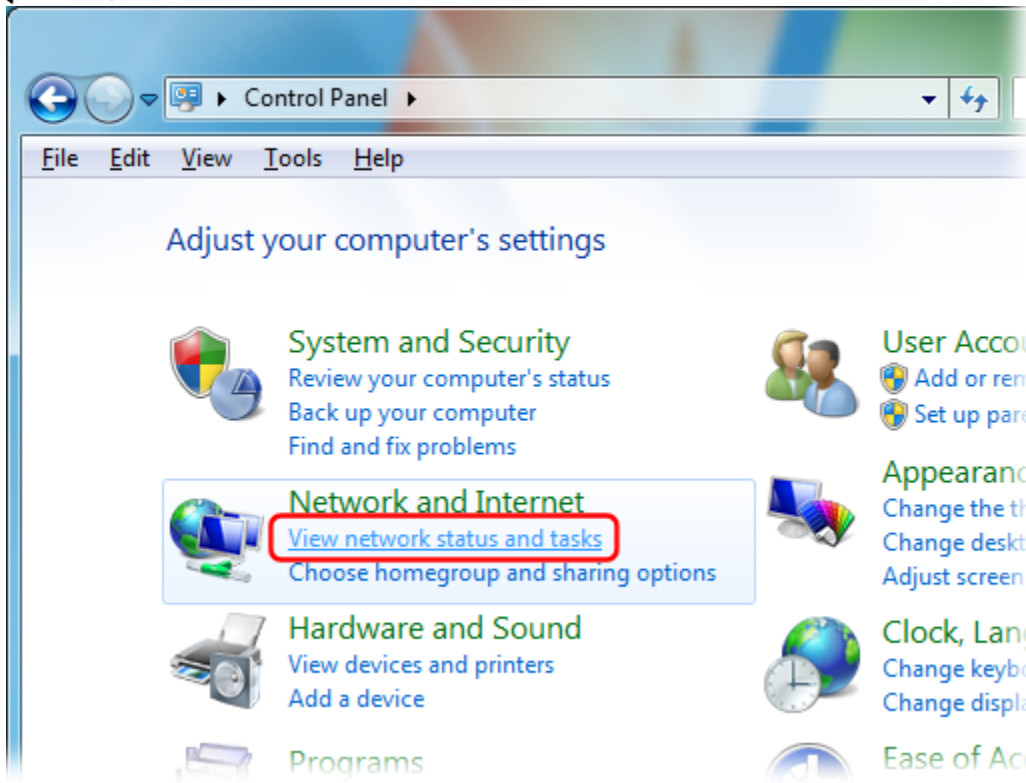
## COMPUTER LAN SETTINGS PRE-REQUISITES

To ensure that all the features of Watchdog works correctly and reliably, there are certain pre-requisites that are necessary for your computer LAN (Local Area Network) settings. These are as follows:

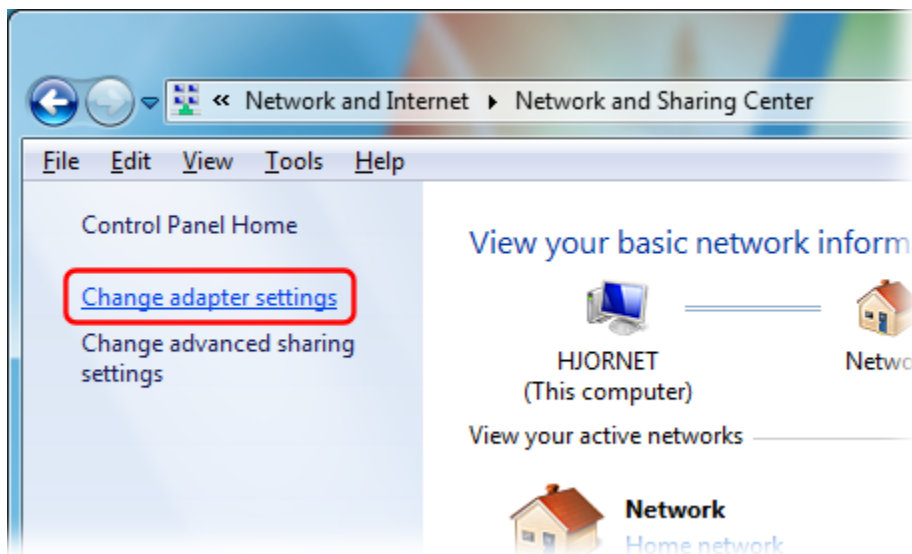
1. Ensure that your normal internet LAN adapter name is exactly named " **Local Area Connection**" and that the OpenVPN TAP adapter name is named " **Local Area Connection 2**". You can confirm the name of your LAN adapters in Windows 7 by going to Windows Control Panel then under "Network and Internet", select "View network status and tasks":



# OPENVPN IP/DNS MONITORING SOFTWARE



Click "Change adapter settings":



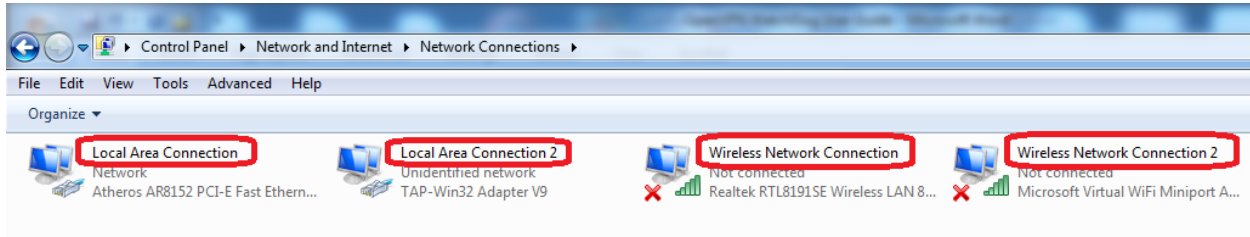
Then check the names of the Internet connection's icon as highlighted in the screenshot below. You can easily identify the active adapters by looking beneath the icons. Those with a red cross indicates that they are not active or in use. For example, as shown in the screenshot below, there



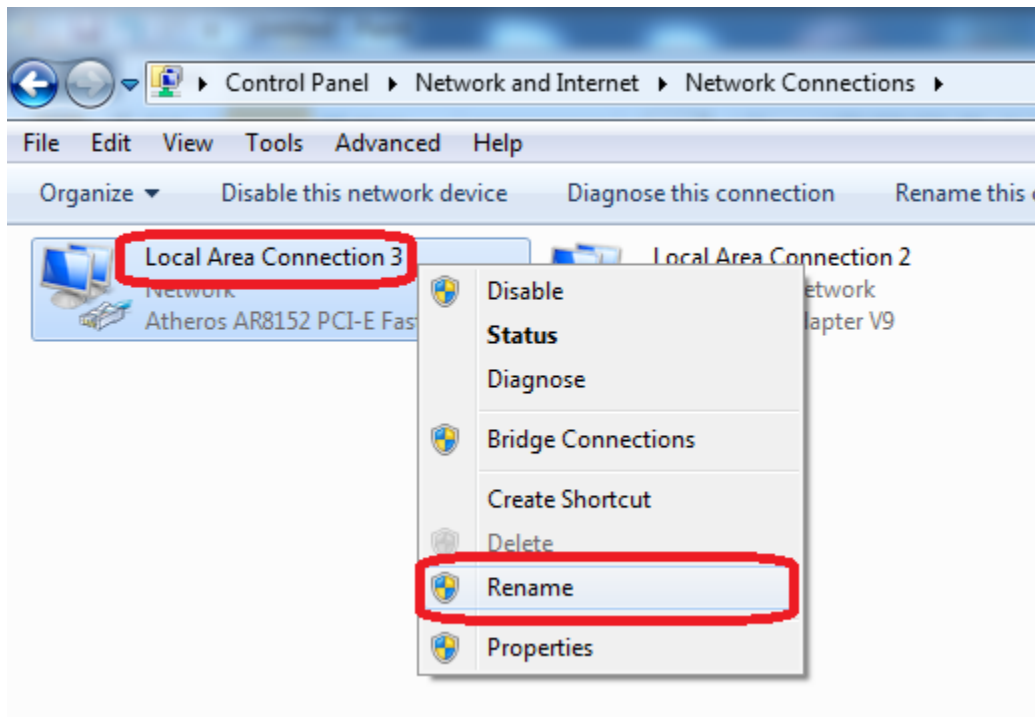
# OPENVPN IP/DNS MONITORING SOFTWARE

are 2 active network adapters; the LAN adapter for your normal internet connection and the TAP adapter for your OpenVPN connection.

OpenVPN Watchdog requires that the name of the normal connection LAN adapter be “ Local Area Connection” while the OpenVPN connection adapter name be “ Local Area Connection 2”



If the names of the adapters are not same as explained above, simply right click on the adapters and change the names accordingly.

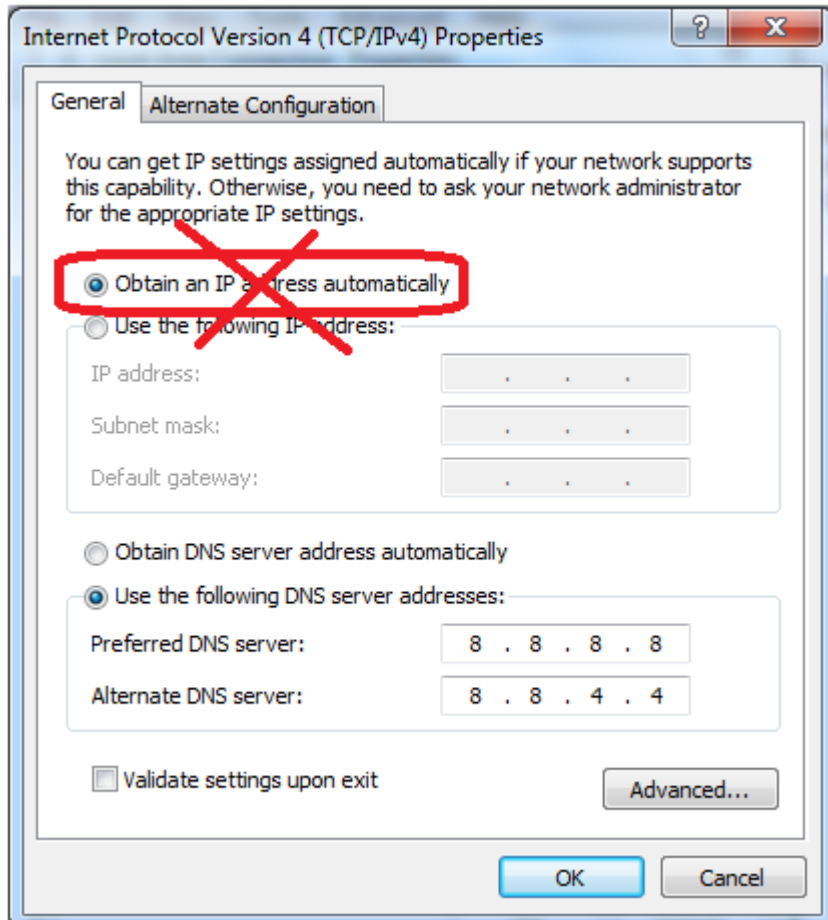


2. Ensure that DHCP is disabled for your LAN network settings for the “Lock OpenVPN Connection” feature of the Watchdog to function. If your LAN adapter DHCP is enabled, the Lock Down OpenVPN connection feature will not work! Hence you must ensure that a valid



## OPENVPN IP/DNS MONITORING SOFTWARE

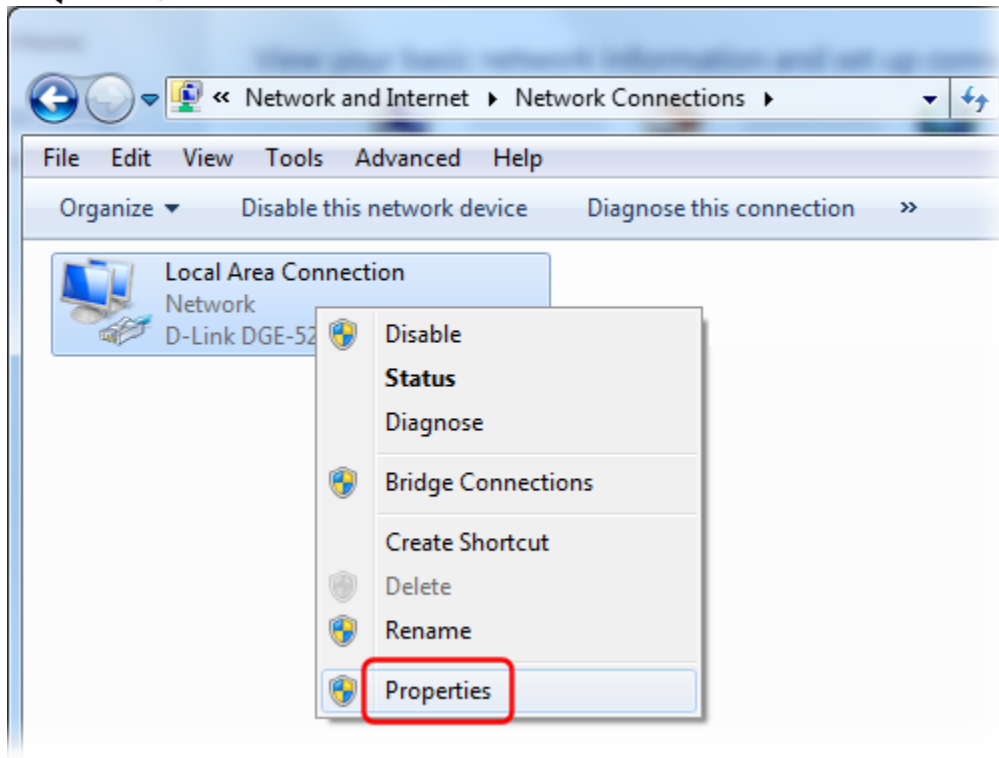
IP, subnet mask, default gateway and DNS servers is configured for your LAN network settings for the “Lock OpenVPN Connection” feature of the Watchdog to function.



You can confirm your LAN adapter settings by Right-clicking on your Internet connection's icon and select "Properties":



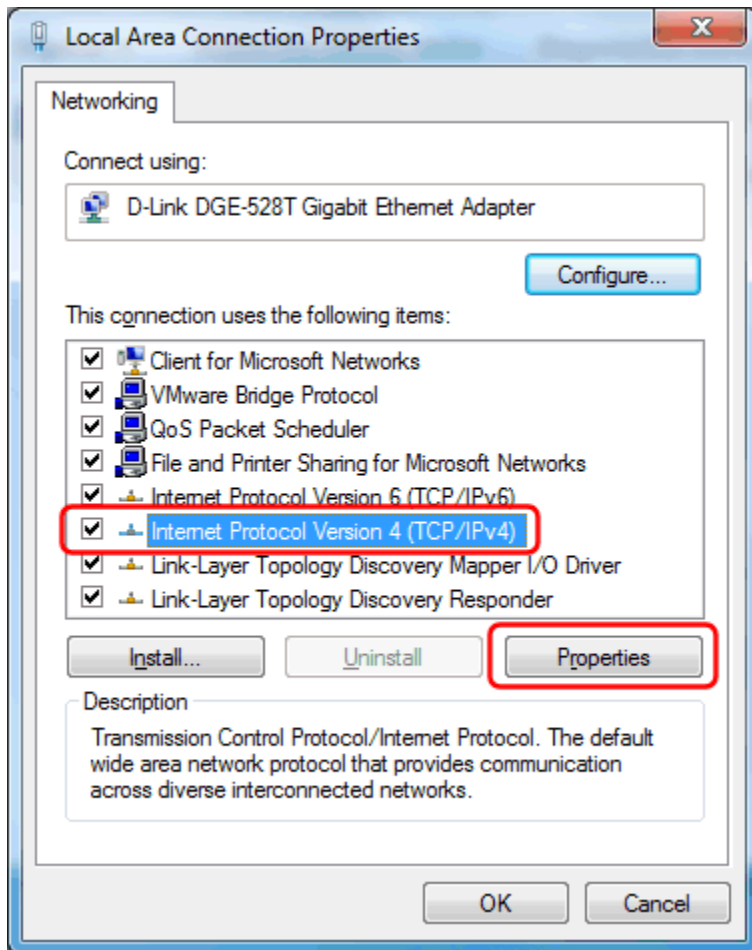
# OPENVPN IP/DNS MONITORING SOFTWARE



Select the "Internet Protocol Version 4 (TCP/IPv4)" item, and click the "Properties" button:



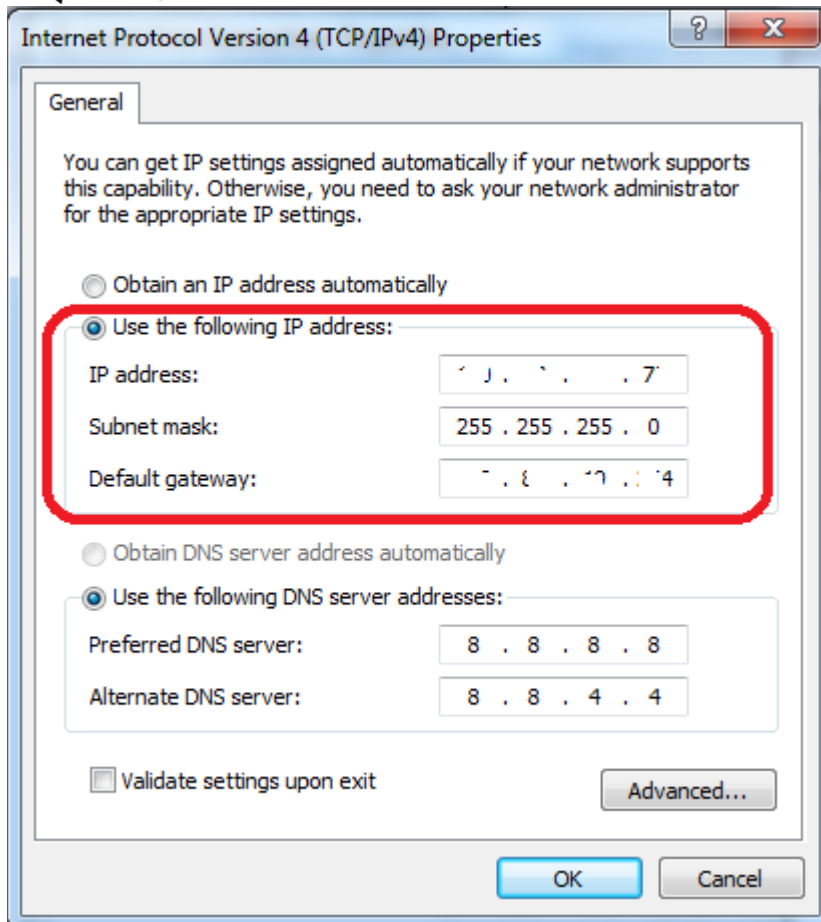
# OPENVPN IP/DNS MONITORING SOFTWARE



It should be similar to the screenshot shown below:



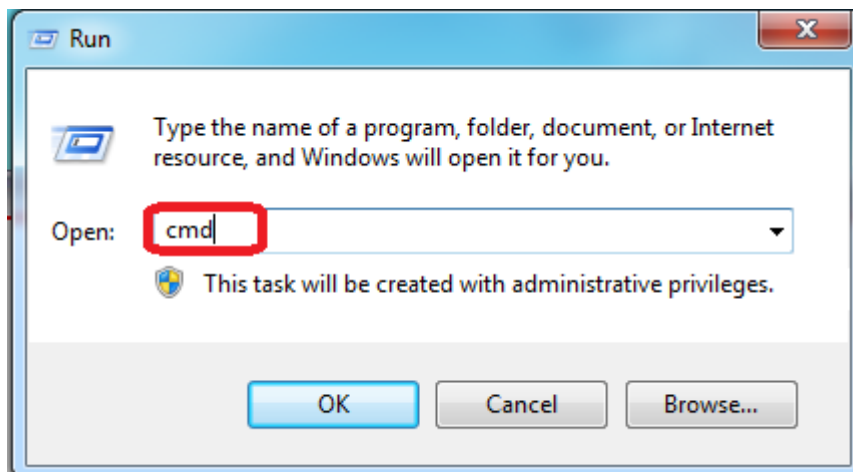
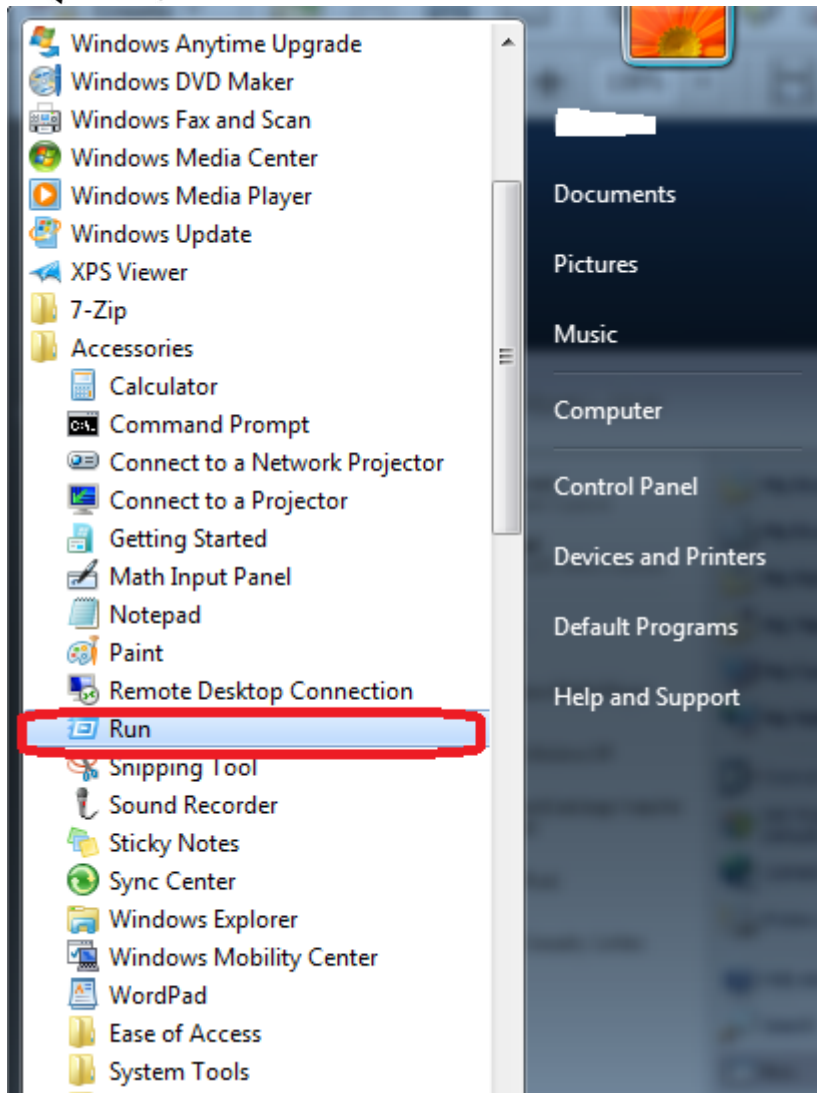
# OPENVPN IP/DNS MONITORING SOFTWARE



To confirm if DHCP has been disabled, go to command prompt. This can be done by selecting Run from the Start Menu and entering cmd.exe or starting the command prompt application, typically located in the Accessories folder within Programs on your Start Menu, as shown below:



# OPENVPN IP/DNS MONITORING SOFTWARE







# OPENVPN IP/DNS MONITORING SOFTWARE

## HOW TO INSTALL ON WINDOWS

This how to will help guide you through the installation process of the OpenVPN Watch Dog.

### Step 1: Launching the application

Launch the msi installer for the OpenVPN Watch Dog and click next:

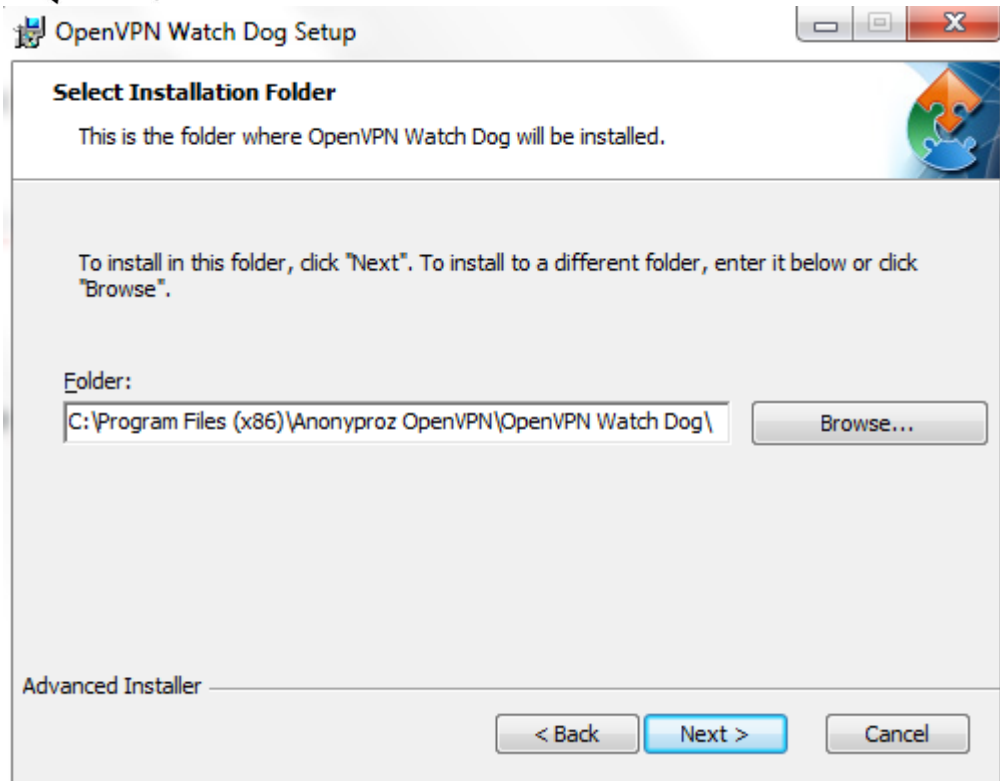


### Step 2: Installation settings

Leave the default location to install the program files for the program and click Next:

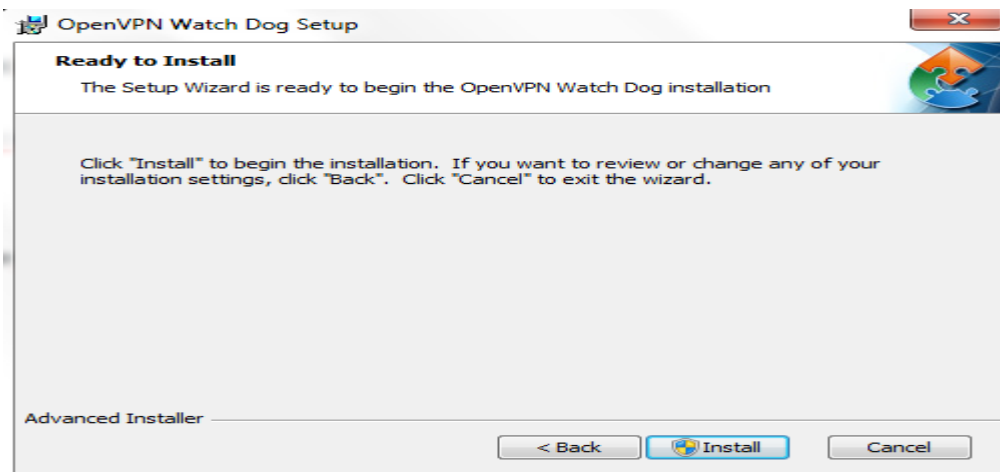


# OPENVPN IP/DNS MONITORING SOFTWARE



### Step 3: Program Installation

You are now ready to install the program, click Install to proceed:

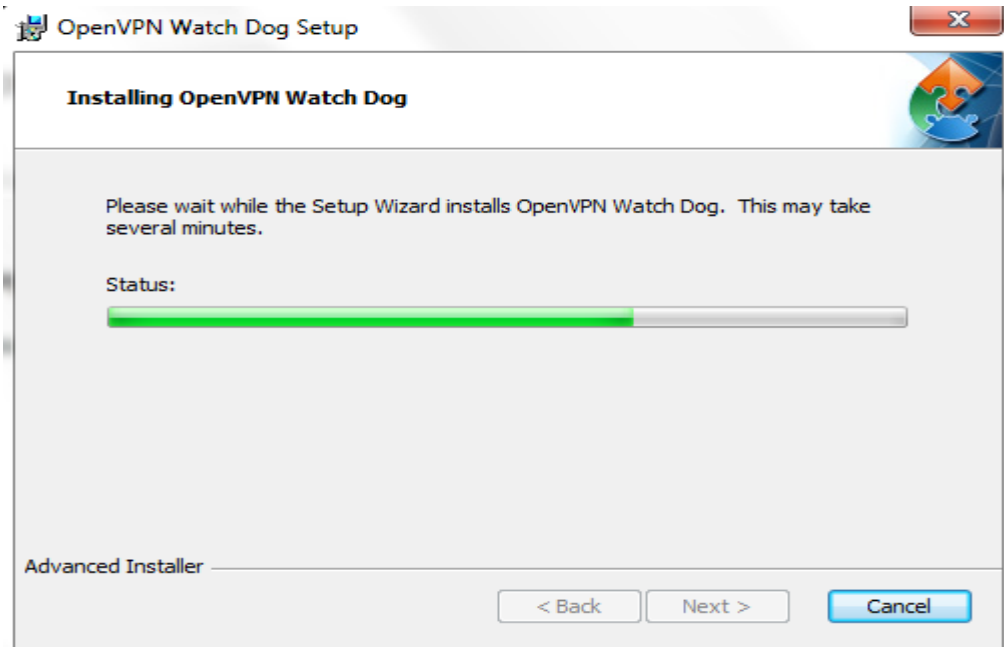




# OPENVPN IP/DNS MONITORING SOFTWARE

## Step 4: Installation Progress

Please wait while the program Installs:

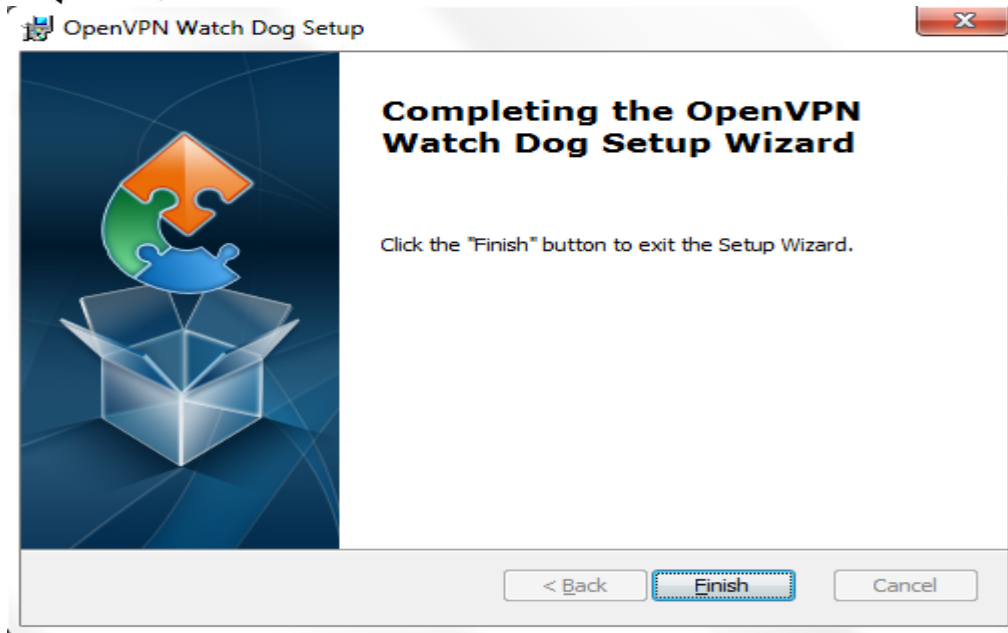


## Step 5: Installation Completion

The program is now installed; click Finish to complete the installation:



# OPENVPN IP/DNS MONITORING SOFTWARE

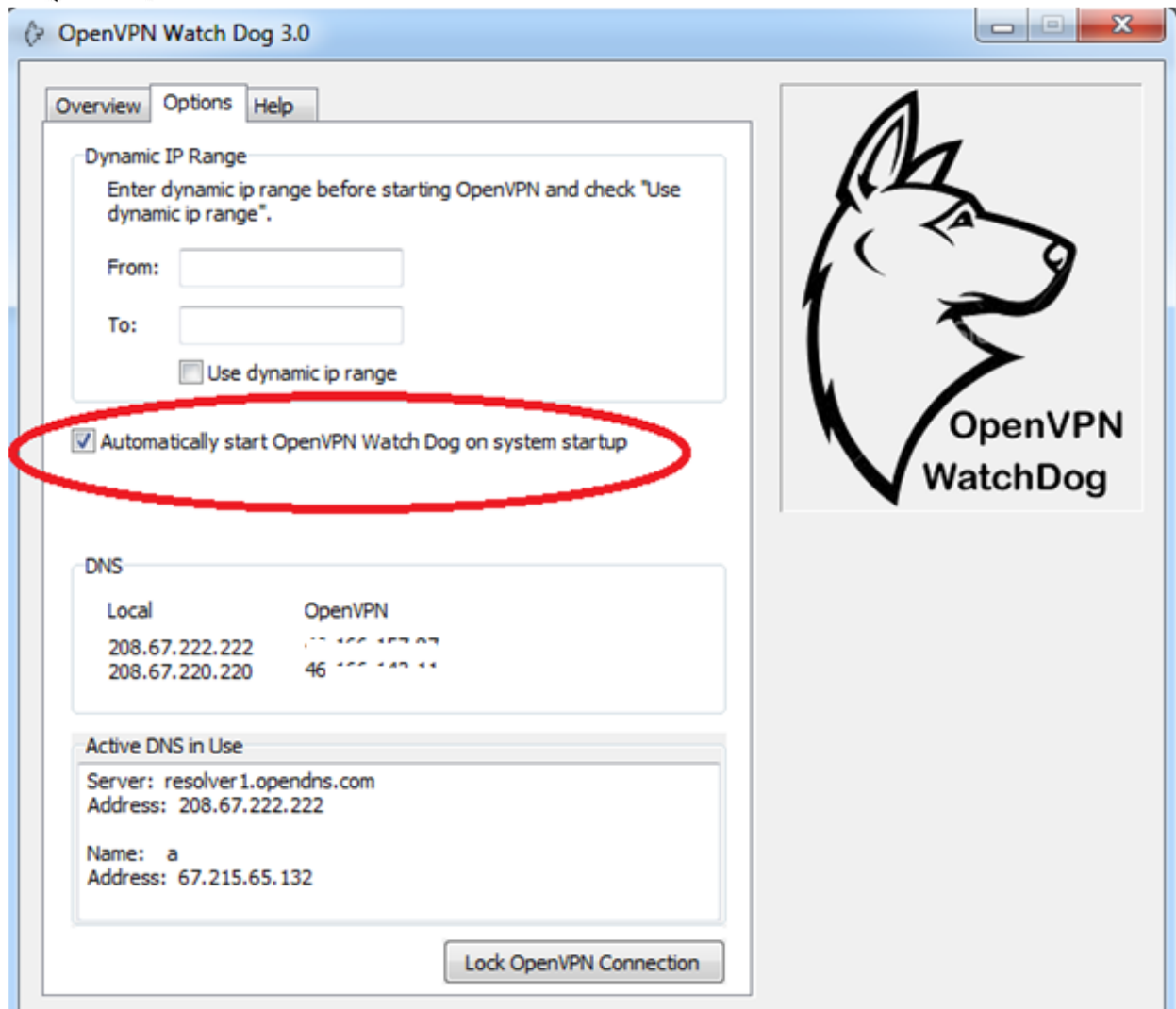


## Step 6: Enabling Program Auto Start at System Startup

OpenVPN Watch Dog has auto start feature and can be configured to automatically start at Windows startup to ensure that you do not forget to start the program before connecting to your OpenVPN server. To configure the program to start automatically on system startup, tick the "Automatically start OpenVPN Watch Dog on system startup" box under the "Options" tab.



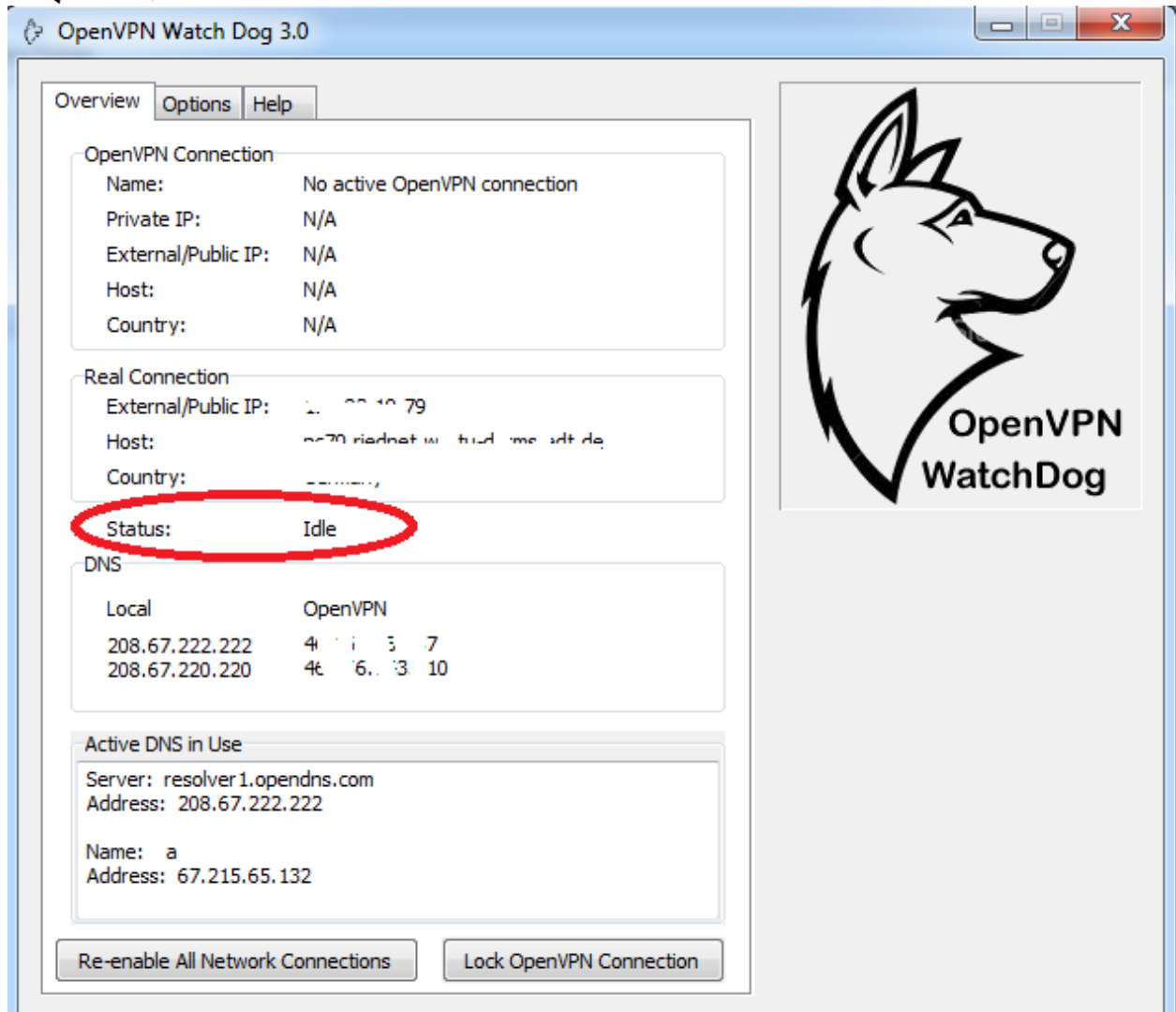
# OPENVPN IP/DNS MONITORING SOFTWARE



Hence at system startup, the program automatically starts and you can access the program GUI and start monitoring your OpenVPN connection by double clicking on the desktop icon or start menu icon. The GUI shown below with "idle" status will appear indicating that OpenVPN Watch Dog is waiting for OpenVPN connection. The program automatically detects your real IP and the information is displayed on the GUI.



# OPENVPN IP/DNS MONITORING SOFTWARE



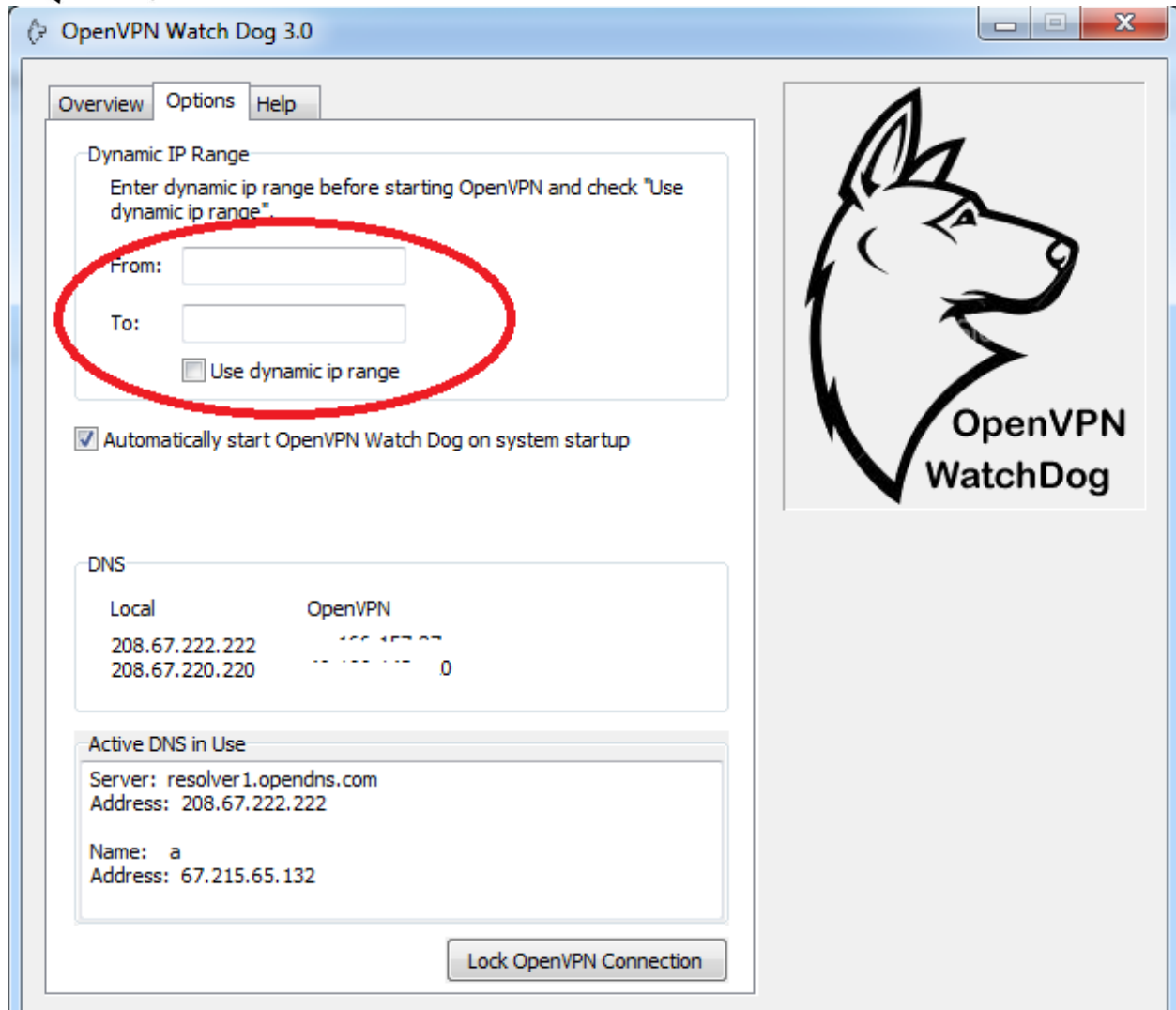
On the system tray applet, a yellow icon indicating an idle state for the program will appear in the lower-right corner of the screen as shown below:



Optionally, if you have a network connection that has dynamic IP and your real IP changes often, you can input the dynamic IP ranges under the “options” tab. If you do not know the dynamic IP ranges, you can request it from your ISP.



# OPENVPN IP/DNS MONITORING SOFTWARE



## Step 7: Connection to OpenVPN Server

Start your OpenVPN connection. As soon as a successful authentication is made to the OpenVPN server, the status of the OpenVPN Watch Dog changes to "Watching" and the yellow icon changes to green. The program also detects the connection details of the OpenVPN server such as public and private IPs, host etc. and begins to monitor the OpenVPN connection.

The following details are automatically detected and displayed on the GUI:

- **OpenVPN Connection Name:** This is the OpenVPN adapter name

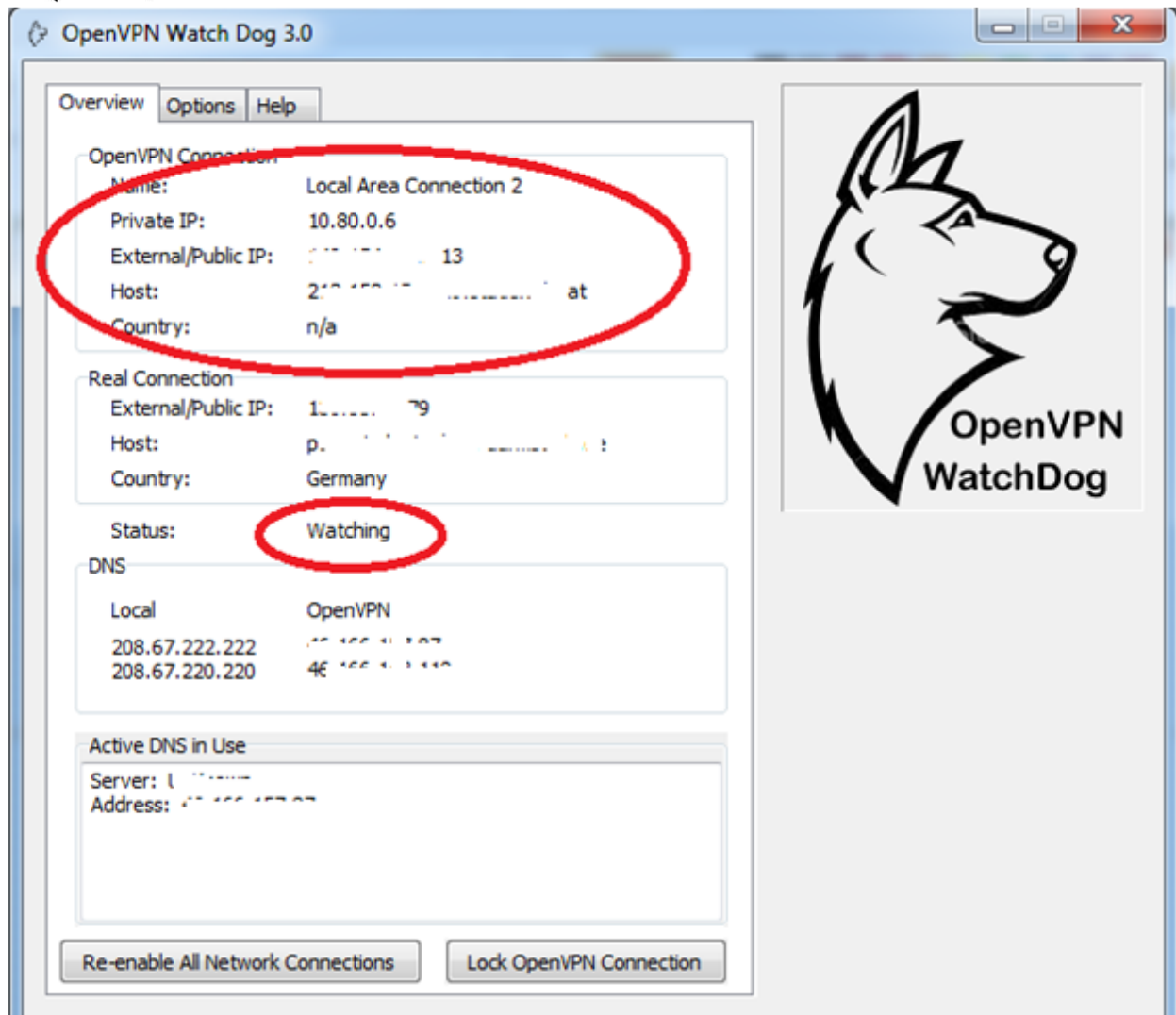


# OPENVPN IP/DNS MONITORING SOFTWARE

- **OpenVPN Connection Private IP:** This is the private IP which is automatically pushed to the client upon connection to the VPN server.
- **OpenVPN Connection External/Public IP:** This is the public IP of the VPN server which should replace your real IP when connected to the VPN server
- **OpenVPN Connection Host:** This is the hostname of the VPN server IP
- **OpenVPN Connection Country:** This is the VPN server IP location
- **Real Connection External/Public IP:** This is your real IP as assigned to you by your ISP
- **Real Connection Host:** This is the hostname of your real IP
- **Real Connection Country:** This is your real IP location



# OPENVPN IP/DNS MONITORING SOFTWARE



## Step 8: Locking Down OpenVPN Connection & Clearing DNS Resolver Cache

OpenVPN Watchdog has a unique feature to lock down your OpenVPN connection after connecting to the server. After locking down your OpenVPN connection, network traffic will only exit through your OpenVPN connection, and no other network interfaces thereby preventing DNS leaks and IP leaks through your VPN connection. This is particularly useful in preventing all forms of DNS leaks including Transparent DNS proxies which allow ISPs to intercept all DNS lookup requests and transparently proxy the results thereby effectively forcing you to use their DNS service for all DNS lookups. Even if you have changed your DNS settings to an open DNS



## **OPENVPN IP/DNS MONITORING SOFTWARE**

service such as Google, Comodo or OpenDNS, some ISPs are still able to intercept your DNS queries using this technology (Transparent DNS proxy)

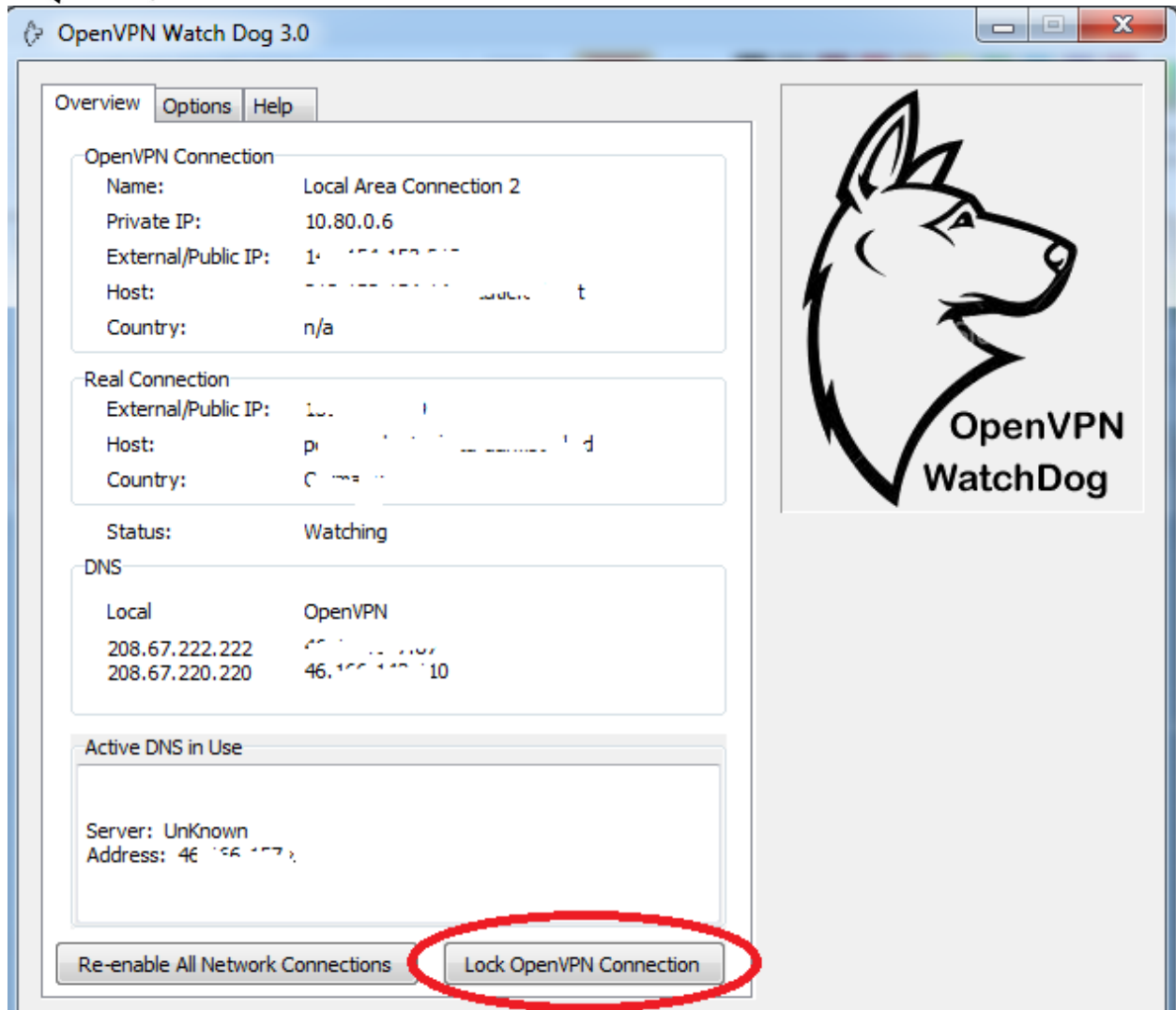
In addition to preventing DNS leaks, the OpenVPN Connection Lock Down feature also effectively fixes DNS cache poisoning which is a filtering method commonly used by ISPs to block access to certain sites. Note that in order to help speed up Web browsing, Windows comes with a local cache containing any DNS addresses that have been looked up recently. Once an URL has been resolved by an Internet name server into a numerical IP, the information is stored locally. Anytime your browser requests an URL, Windows first looks in the local cache to see if it is there before querying the external name server used by your ISP. If it finds the resolved URL locally it uses that IP.

However, this DNS cache can be poisoned by ISPs for sites such as Youtube, Facebook, Twitter etc when you attempt to visit these restricted sites before connecting to the VPN. Sometimes even after connecting to the OpenVPN server, you will still be unable to access these sites for at least 5 minutes which is the default time for retaining a negative DNS query response in the DNS resolver cache. In other words, once a negative response is received you will not be able to connect to the site for at least five more minutes.

Thus in order to avoid this 5 minutes delay nuisance, you can use the Watchdog OpenVPN Connection Lock button to effectively clear the DNS resolver cache to remove any corrupted or poisoned DNS entries in your existing resolver cache before connecting to the VPN.



# OPENVPN IP/DNS MONITORING SOFTWARE



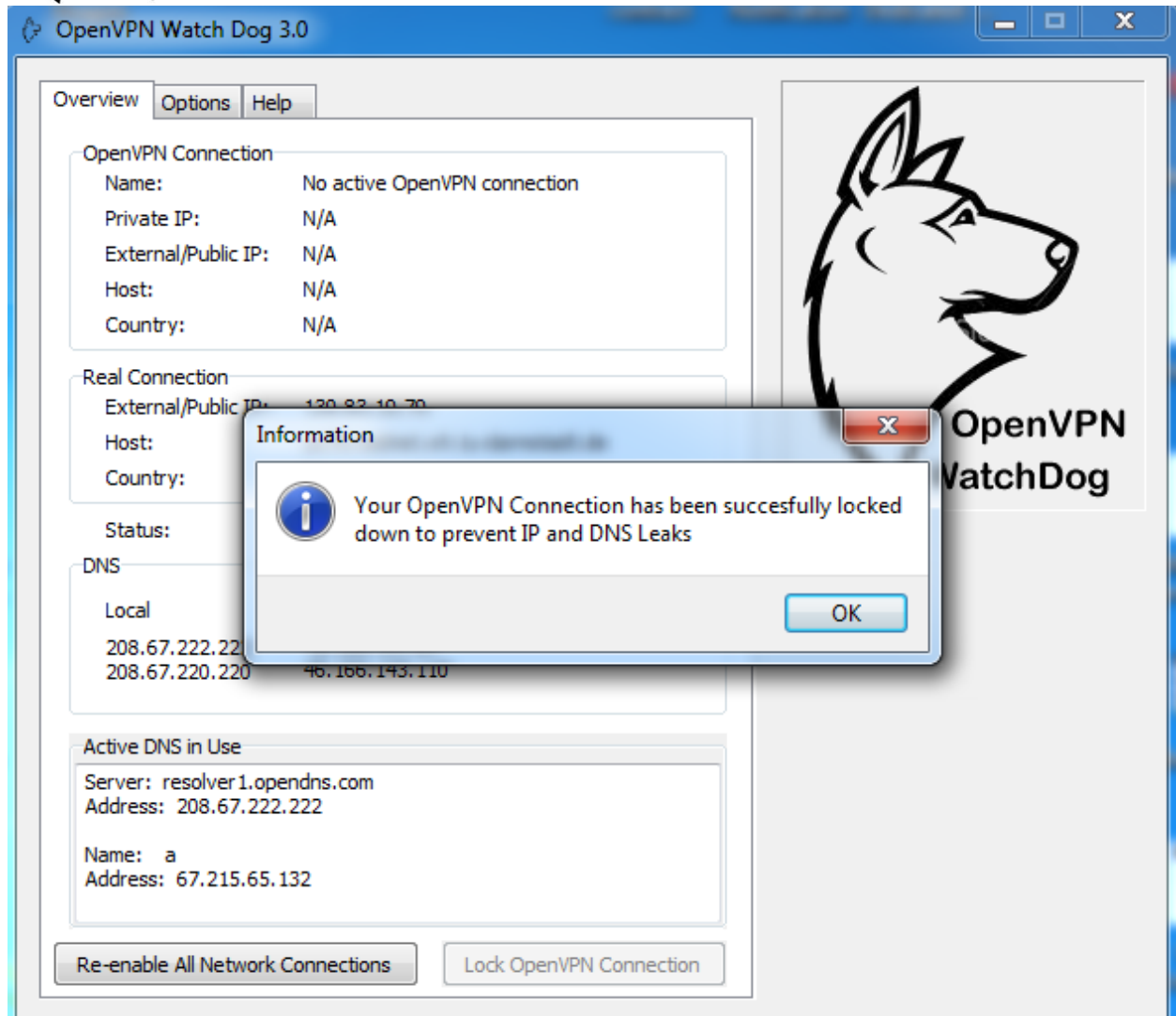
To lock down your OpenVPN connection, simply click on the “Lock OpenVPN Connection” button as shown above.

**Important:** Make sure you are connected to the OpenVPN before you click on the “Lock OpenVPN Connection” button.

After pressing the button, your internet will be automatically disconnected and connected again. This brief internet disconnection and re-connection indicates that the OpenVPN connection has been locked.



# OPENVPN IP/DNS MONITORING SOFTWARE






**Note :** For Vista and Windows 7 users, User Access Control (UAC) must be disabled before the Lock down process can be completed. To disable UAC, perform the following steps below:

1. Go to Start Menu -> Control Panel -> User Accounts and Family Safety -> User Account.
2. Click on User Account Control settings link.



# OPENVPN IP/DNS MONITORING SOFTWARE

## Make changes to your user account

- Create a password for your account
- Change your picture
-  Change your account name
-  Change your account type
  
-  Manage another account
- Change User Account Control settings



- Slide the slider bar to the lowest value (towards Never Notify), with description showing Never notify me.

## Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.  
[Tell me more about User Account Control settings](#)

Always notify



Never notify

**Never notify me when:**

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

 Not recommended but can be selected if you use programs that are not certified for Windows 7 because they do not support User Account Control

- Click OK to make the change effective.
- Restart the computer to turn off User Access Control.

## Automatic Monitoring for DNS Leaks

OpenVPN Watchdog offers the capability to monitor your DNS information in real time. Your DNS information configured on your network adapters are automatically read and displayed in the program GUI. Both your Local Area Connection (Local) and OpenVPN adapter DNS IPs are automatically detected and displayed in the program GUI. In addition, the program will





## **OPENVPN IP/DNS MONITORING SOFTWARE**

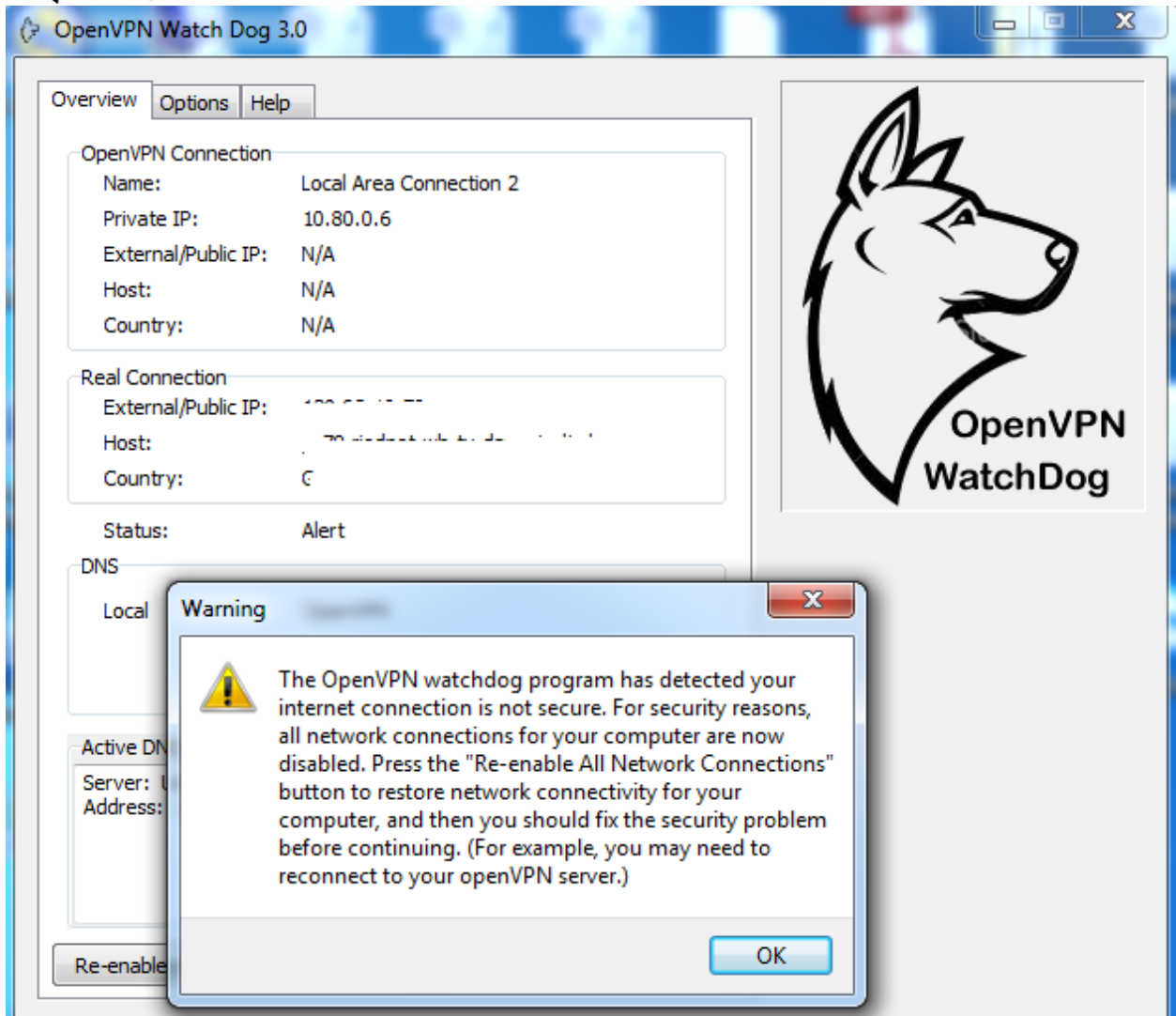
- **Local DNS:** This corresponds to the DNS settings that has been configured on your Local Area Connection or Wireless Area Connection in your computer network adapter
- **OpenVPN DNS:** This corresponds to the DNS server that was automatically pushed to you by the OpenVPN server. The OpenVPN DNS can be a private DNS or a public DNS such as OpenDNS, Google DNS, Comodo etc. You can confirm the OpenVPN DNS IPs from your VPN service provider.
- **Active DNS in Use:** This is the real-time DNS which is used in resolving websites at any point in time. Before connecting to the OpenVPN server, the Active DNS IP in Use will tally with one of your Local DNS IPs as displayed on the program GUI. When connected to the OpenVPN server, the Active DNS IP in Use should tally with one of your OpenVPN DNS IPs as displayed on the program GUI. If this is not so, then you have DNS Leaks. The Active DNS in Use data is automatically refreshed once every 10 seconds.

### **Automatic Internet Connection Shut-down**

During your OpenVPN connection session, in the event that a problem is detected by the program a barking dog alert and visual alerts are produced. The alerts are triggered when either the program detects that unencrypted traffic is leaving your computer, your real IP is being exposed or your DNS is leaking. As a security measure, your internet access is automatically disabled when such alerts are triggered and you need to re-enable the internet access by clicking on the “Re-enable All Network Connections” button. At this point, you should be aware that your OpenVPN connection is no longer secure and appropriate steps should be taken to fix the issue.



# OPENVPN IP/DNS MONITORING SOFTWARE



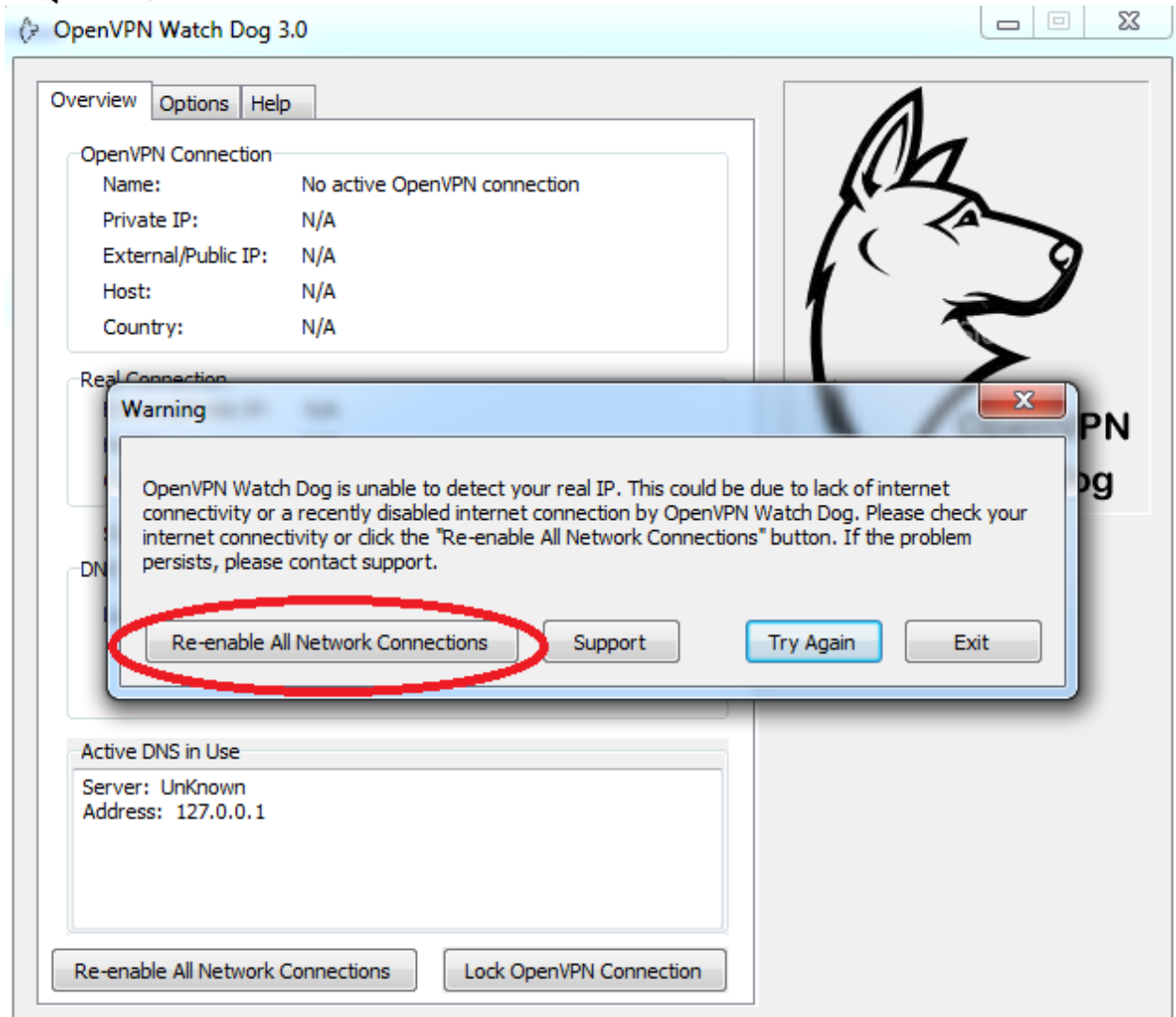
On the system tray applet, a red icon indicating an alert state for the program will appear in the lower-right corner of the screen as shown below:



When alerts are triggered, it is important that you click on the “Re-enable All Network Connections” button to restore your internet access before closing the program. However, should you close the program in panic before clicking this button; you can still do this by starting the program again and clicking the “Re-enable All Network Connections” button.



# OPENVPN IP/DNS MONITORING SOFTWARE

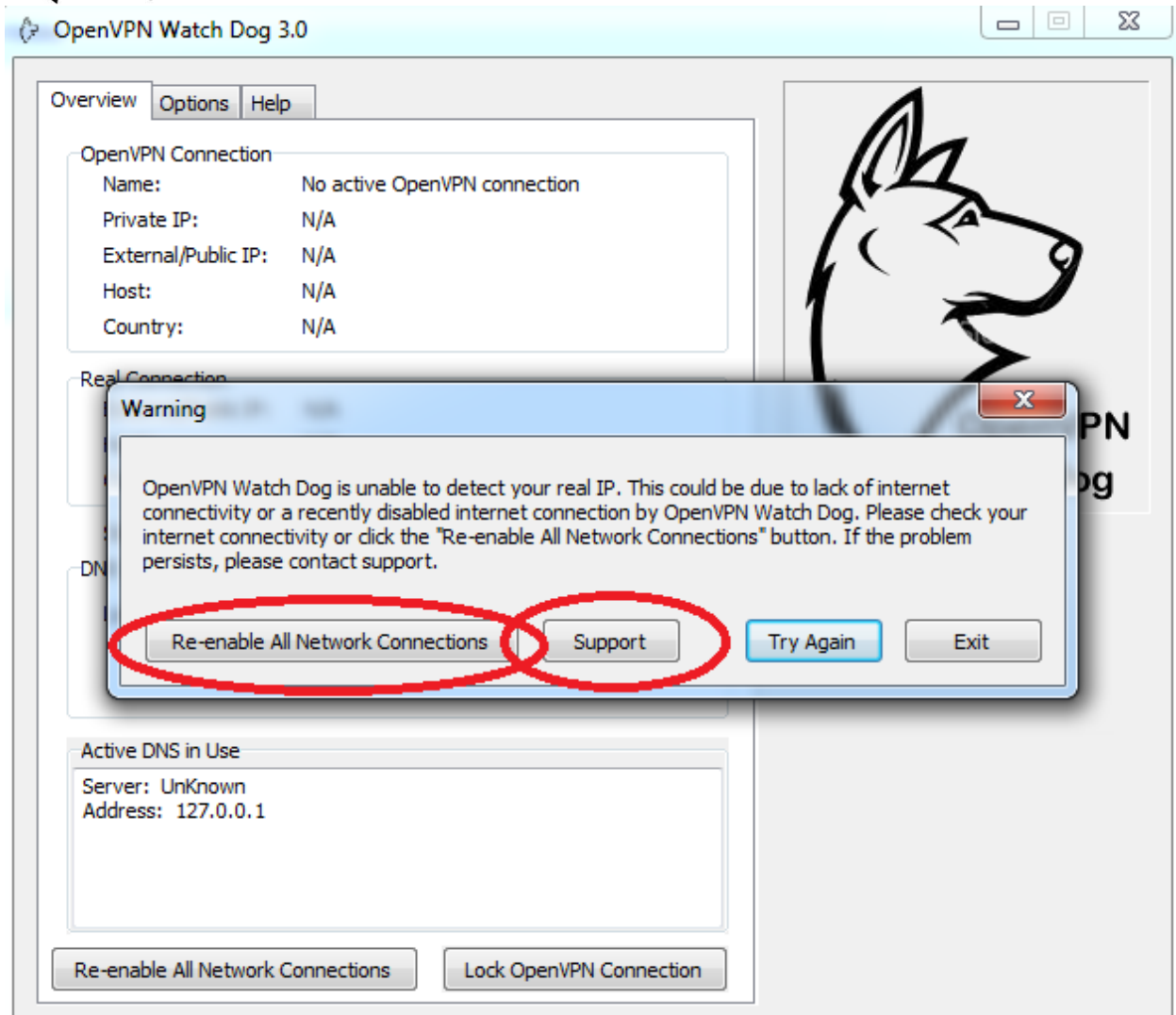


## Troubleshooting and Contacting Support:

The OpenVPN Watch Dog uses private GeoIP servers to determine your real and OpenVPN IP information. If the program is unable to determine the IP parameters, it might be due to server issues. Should you experience this, you can submit a trouble ticket using the contact button as shown below:



# OPENVPN IP/DNS MONITORING SOFTWARE



## Things to Keep in Mind:

1. OpenVPN Watchdog is secure and will not breach your security. It does not transfer any data from your system nor log any information from your computer.
2. OpenVPN Watchdog is designed to automatically cut-off your internet when it detects that your OpenVPN connection is no longer secure such as when your IP or DNS is leaking. To re-enable your internet, simply re-start the watchdog program and click on “Re-enable All Network Connections”
3. OpenVPN Watchdog will make an outbound secure connection to our secure GeoIP server which is used in determining the location of your OpenVPN server IP and real connection IP



## **OPENVPN IP/DNS MONITORING SOFTWARE**

4. OpenVPN Watchdog uses GeoIP (IP to Location) database which may not be 100% accurate. Thus you may see a different country being reported for the actual country to which the IP belongs while using the program. Due to the nature of geo-location technology and other factors beyond our control, we cannot guarantee any specific future accuracy level.
5. When detecting your active DNS in use, the program may sometimes display the DNS info with this error message “DNS Request Timed Out”. This error does not impact the functionality of the program. This error message is triggered when the remote DNS server fails to respond on time during the query.
6. OpenVPN Watchdog will perform best when you have a very stable internet connection. If your ISP internet connection is very shaky or unstable, you will get constant disconnections and Dog barkings which might be annoying.

For more details, please visit our website. If you have any issues or questions regarding the application, you can send us a support ticket at our support center:

<https://www.anonyproz.com/supportsuite/>

Anonyproz.com|Openvpnchecker.com