User Manual for Modified OpenVPN GUI Client

Anonyproz offers a modified/customized version of the open source OpenVPN GUI by Mathias Sundman that is fully compatible with our OpenVPN Watchdog program. However, be aware that current versions of official OpenVPN GUI clients may not work our Watchdog program. Therefore we will continue to maintain this modified version so that our Watchdog program users can continue to use the program

Using our modified version, our users can benefit from the added features which can greatly improve their OpenVPN tunneling experience.

Users can perform the following directly from the GUI:

- Connect to any server of choice
- Force all applications to connect to VPN encrypted tunnel via our OpenVPN Watchdog program
- Switch between any server with a single click
- Connect to servers in 3 different modes: Standard, Failover and Switching Connection Modes
- Automatic server failover to a redundant server upon the failure of previously active server
- Login credentials secure saving (AES 256 cipher) for automatic connection
- Switch between Google DNS, OpenDNS, Anonyproz DNS (with malware filtering support)
- Flush DNS cache and ARP (Address Resolution Protocol) easily with a single click
- Automatic connection to a default pre-selected server at GUI launch
- Automatic GUI start and connection to a default pre-selected server at system startup/boot
- Automatic server switching at a pre-determined time duration

This manual is organized in sections which describe in detail how to install and use the modified OpenVPN client for Windows. It is organized in sections as shown in the content below:

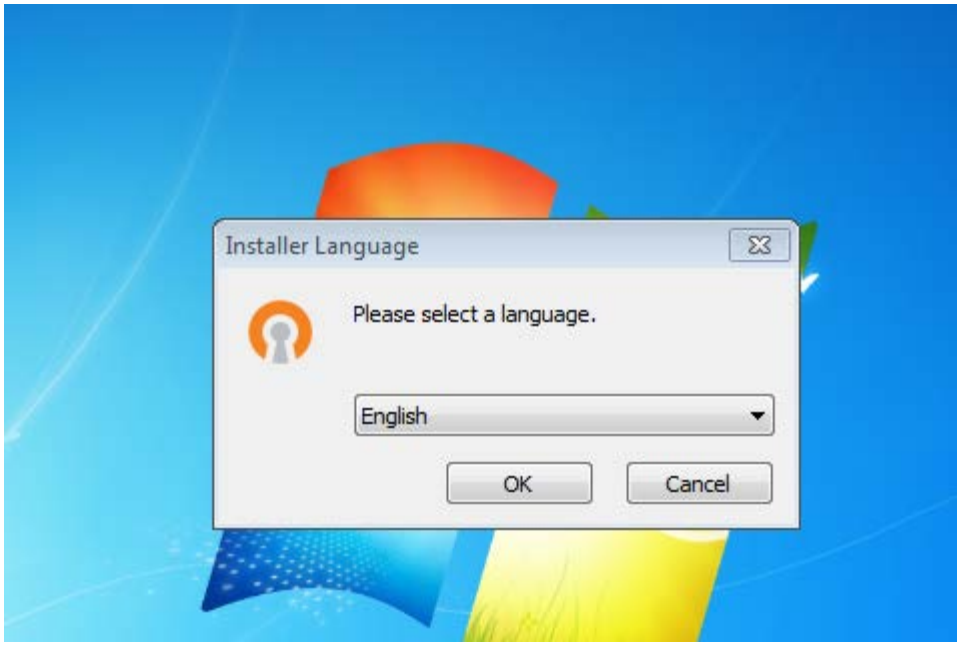
Contents

Downloading/Installing the GUI:

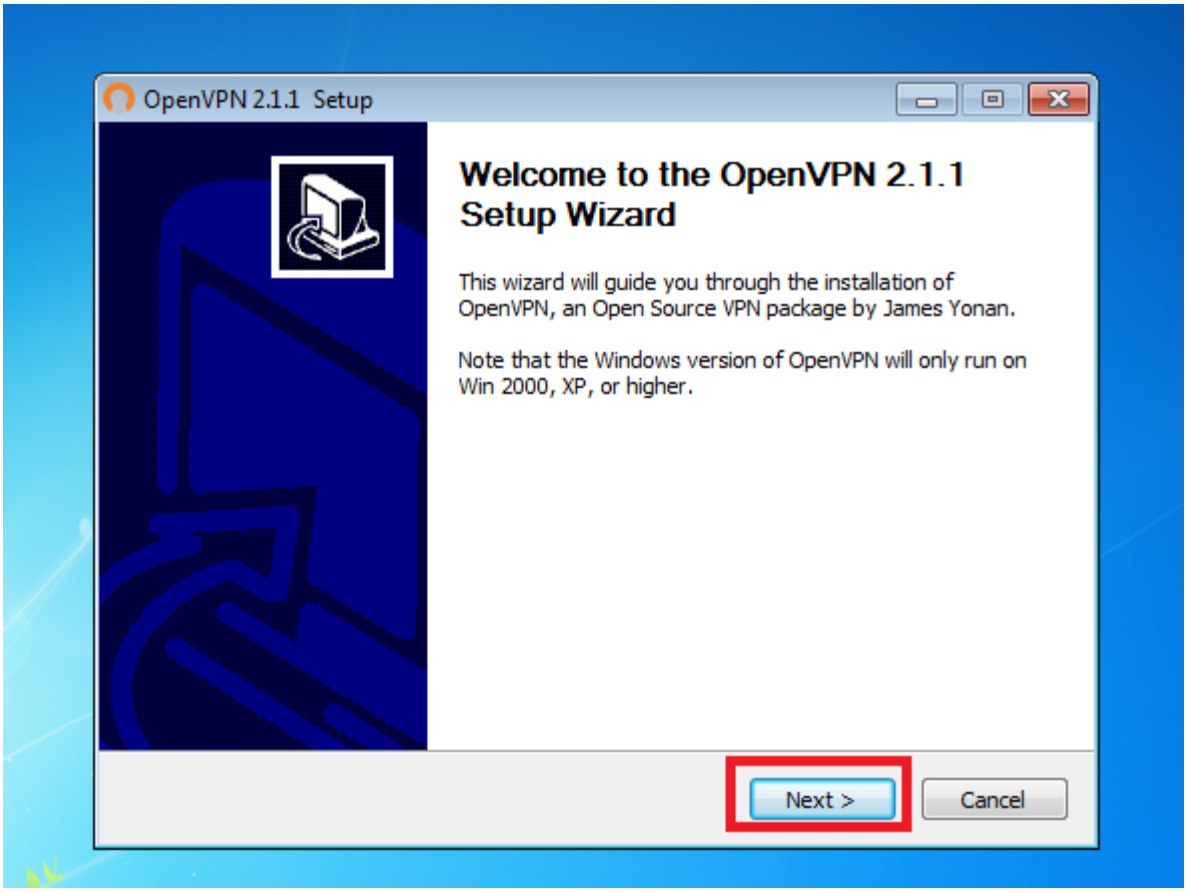
The modified OpenVPN GUI can be downloaded in the link below:

http://www.anonyproz.com/openvpnclient.exe

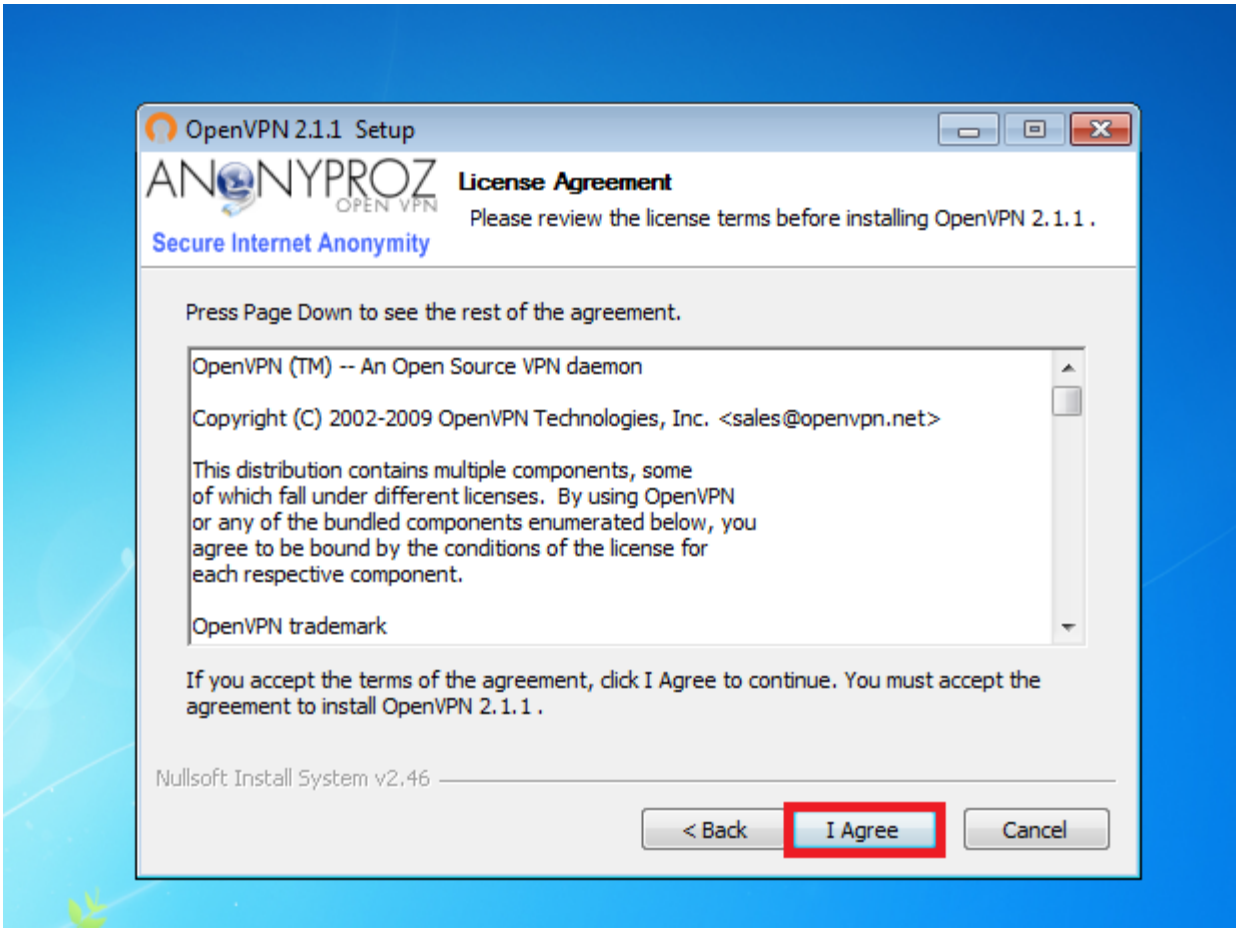
After downloading the program, proceed to run the application.



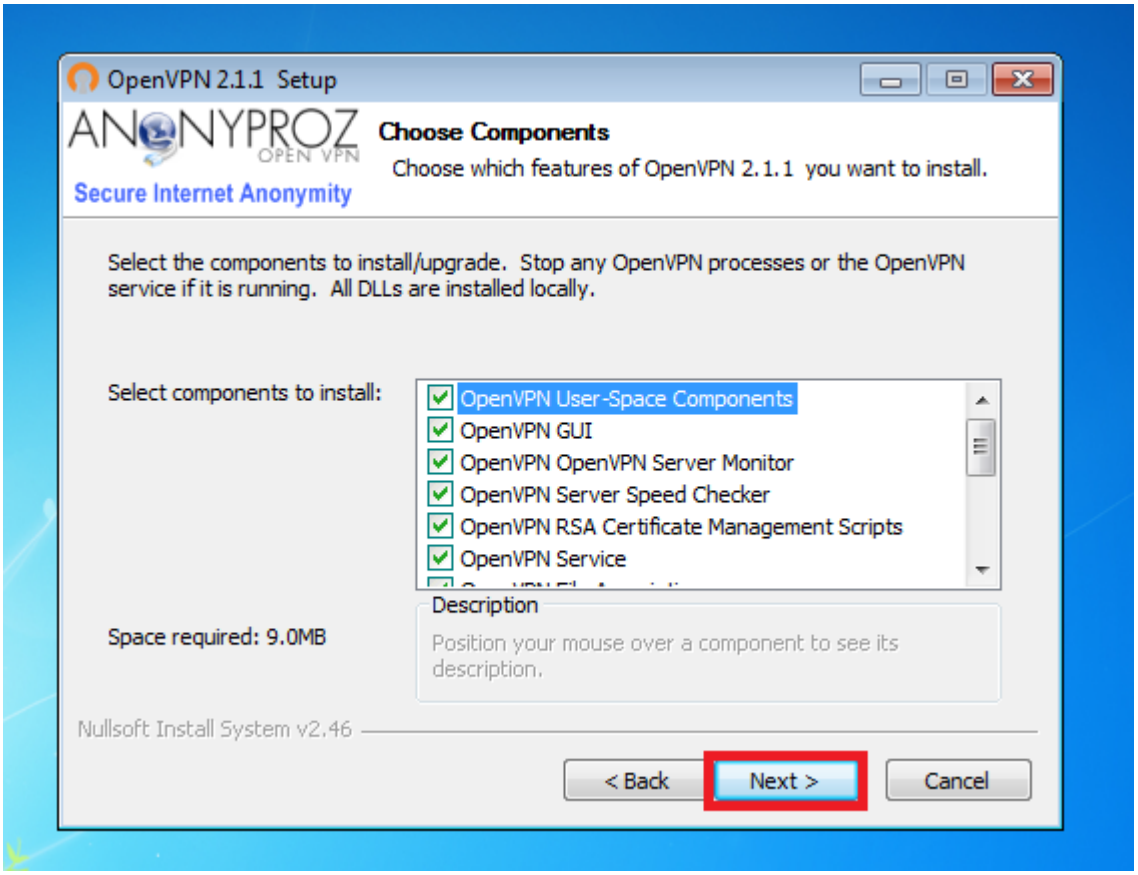
Select the preferred language for the setup and click on OK.


OpenVPN 2.1.1 Setup
Welcome to the OpenVPN 2.1.1 Setup Wizard
This wizard will guide you through the installation of OpenVPN, an Open Source VPN package by James Yonan.
Note that the Windows version of OpenVPN will only run on Win 2000, XP, or higher.
Next >
Cancel

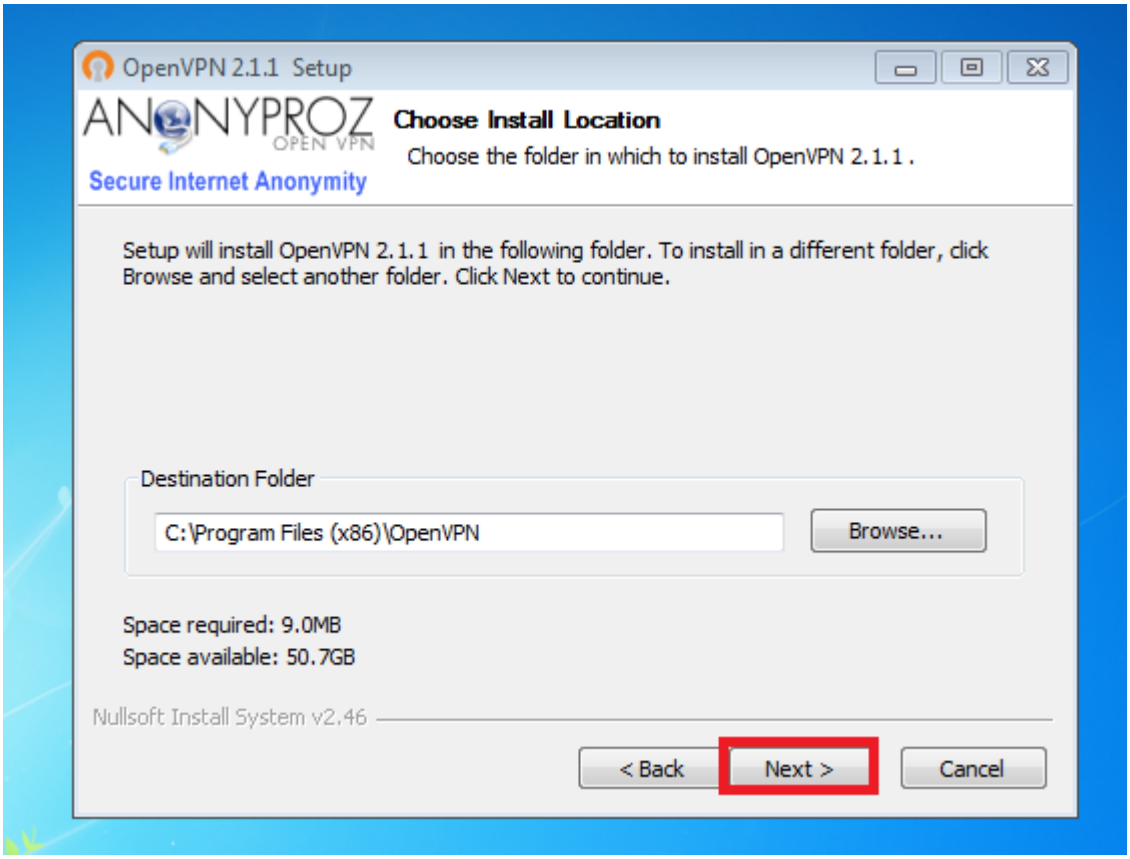
Click “Next”



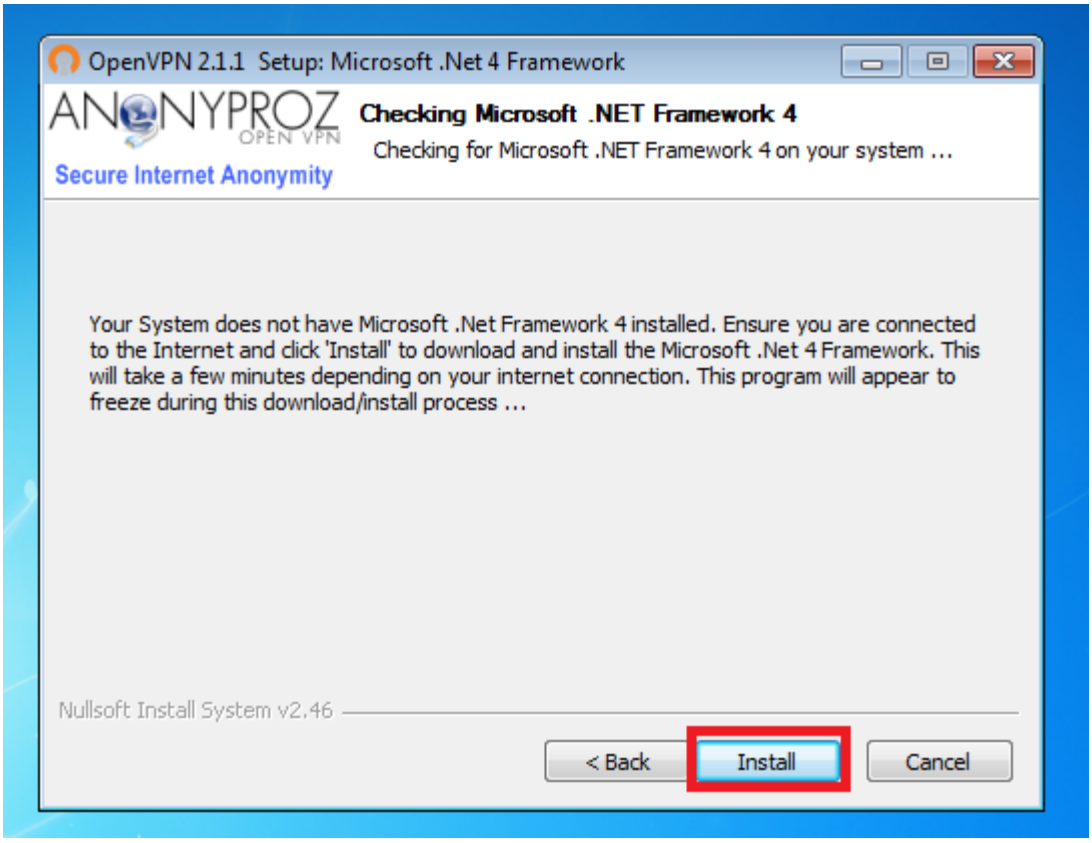
Click “I Agree” to license



Click “Next”. All the check boxes are required!



Leave the default location and click “install”

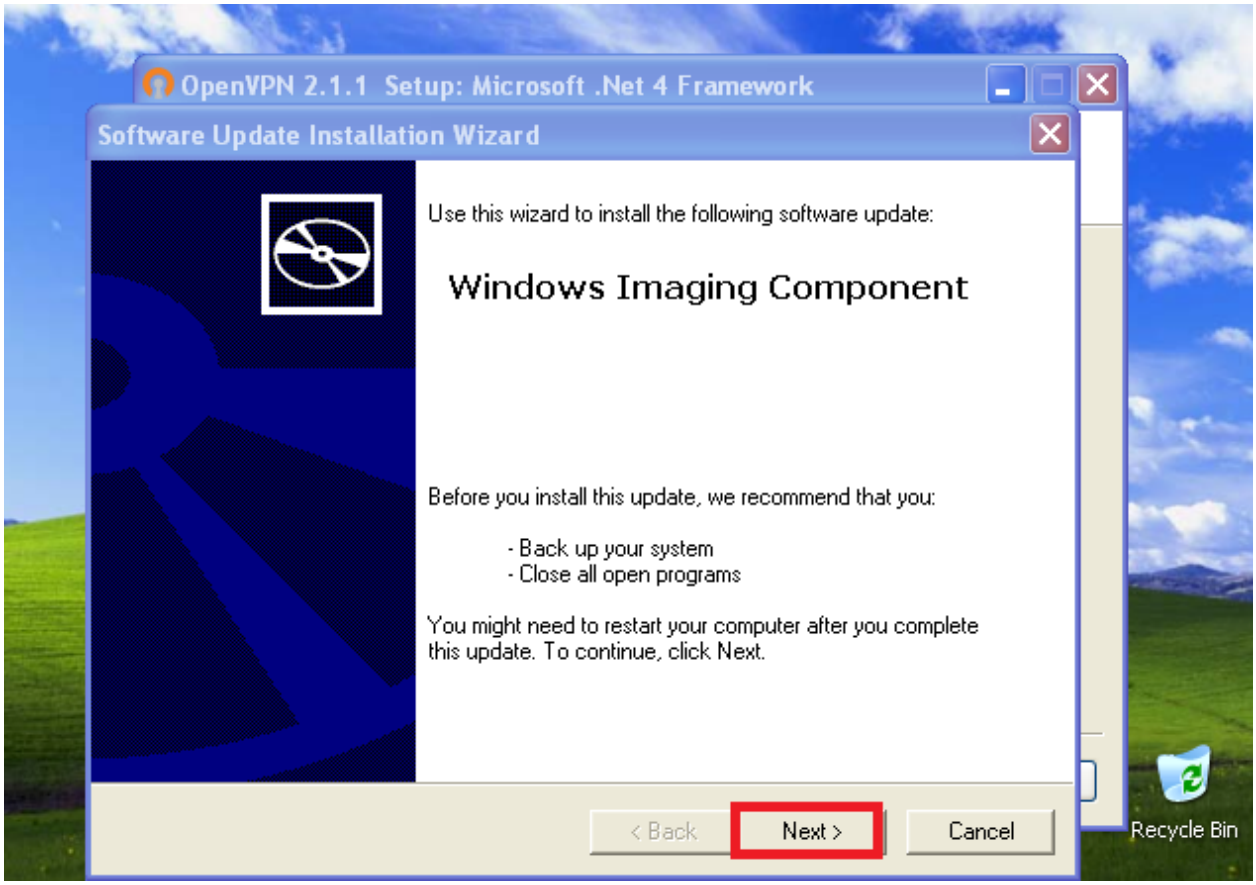


Some features of the GUI requires the Microsoft .NET Framework 4 to function. If you do not have .NET framework installed on your computer, the setup wizard will detect it and will be downloaded and installed automatically. Click on Install to proceed.

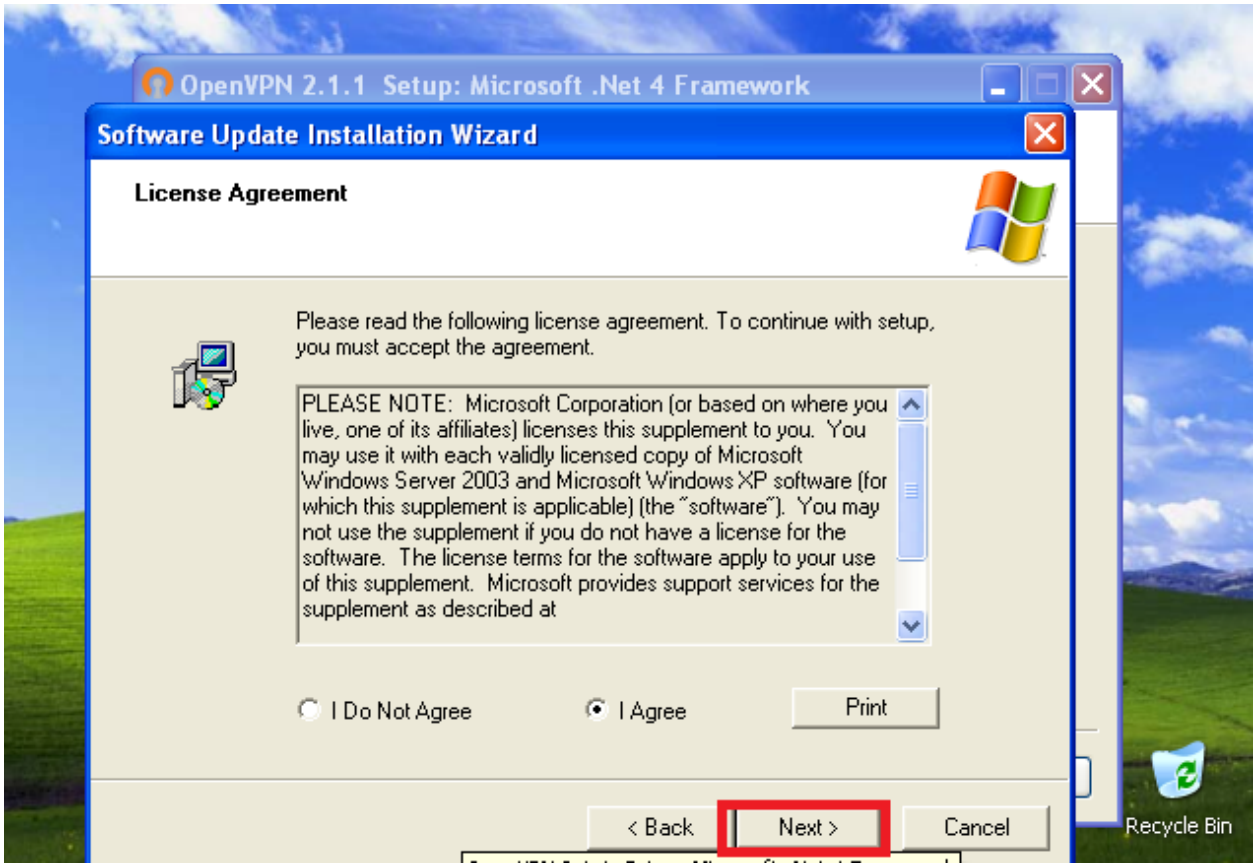
If installing on Windows XP, 2 other dependencies are required:

- Windows Imaging Component
- Windows Installer 3

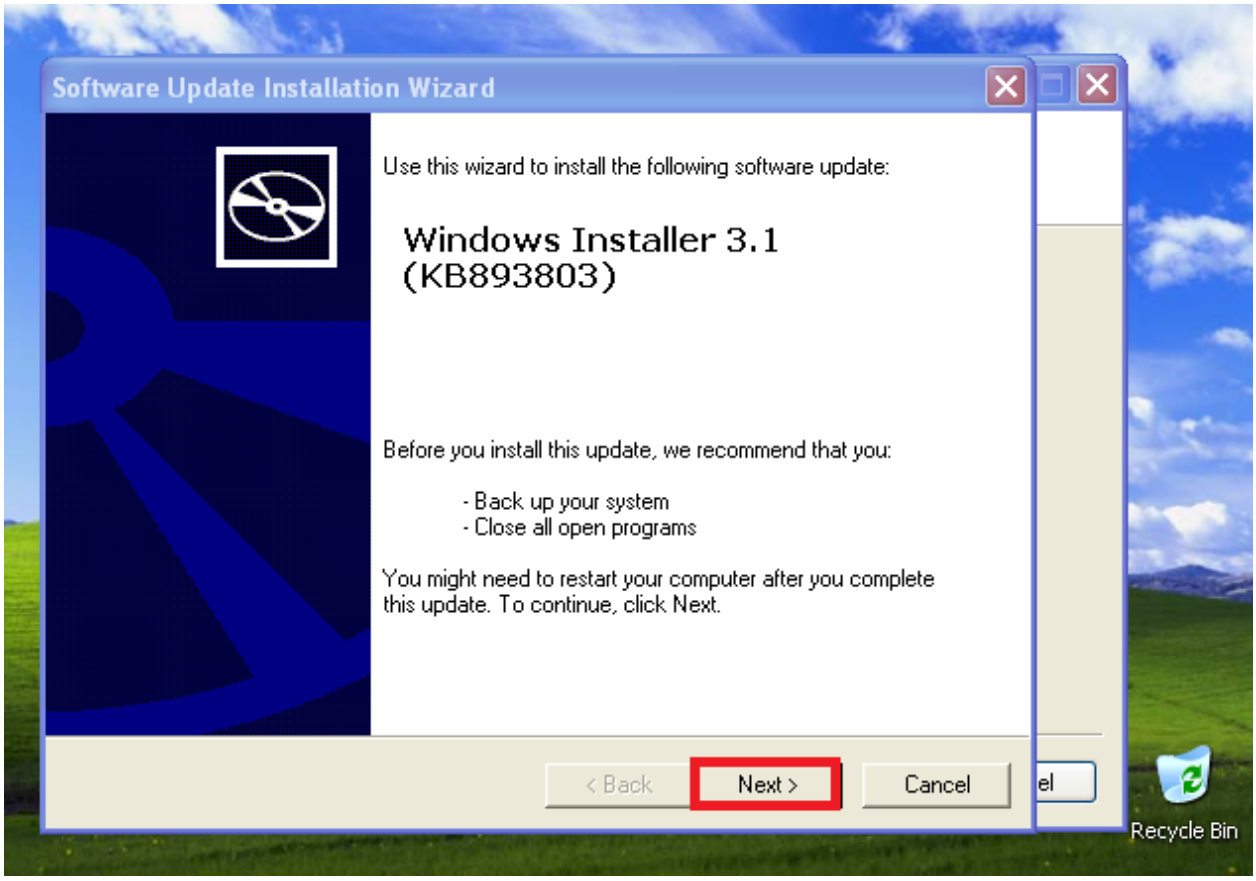
These dependencies will be automatically detected if not already installed and will be downloaded from Microsoft website and the install wizards will be started:

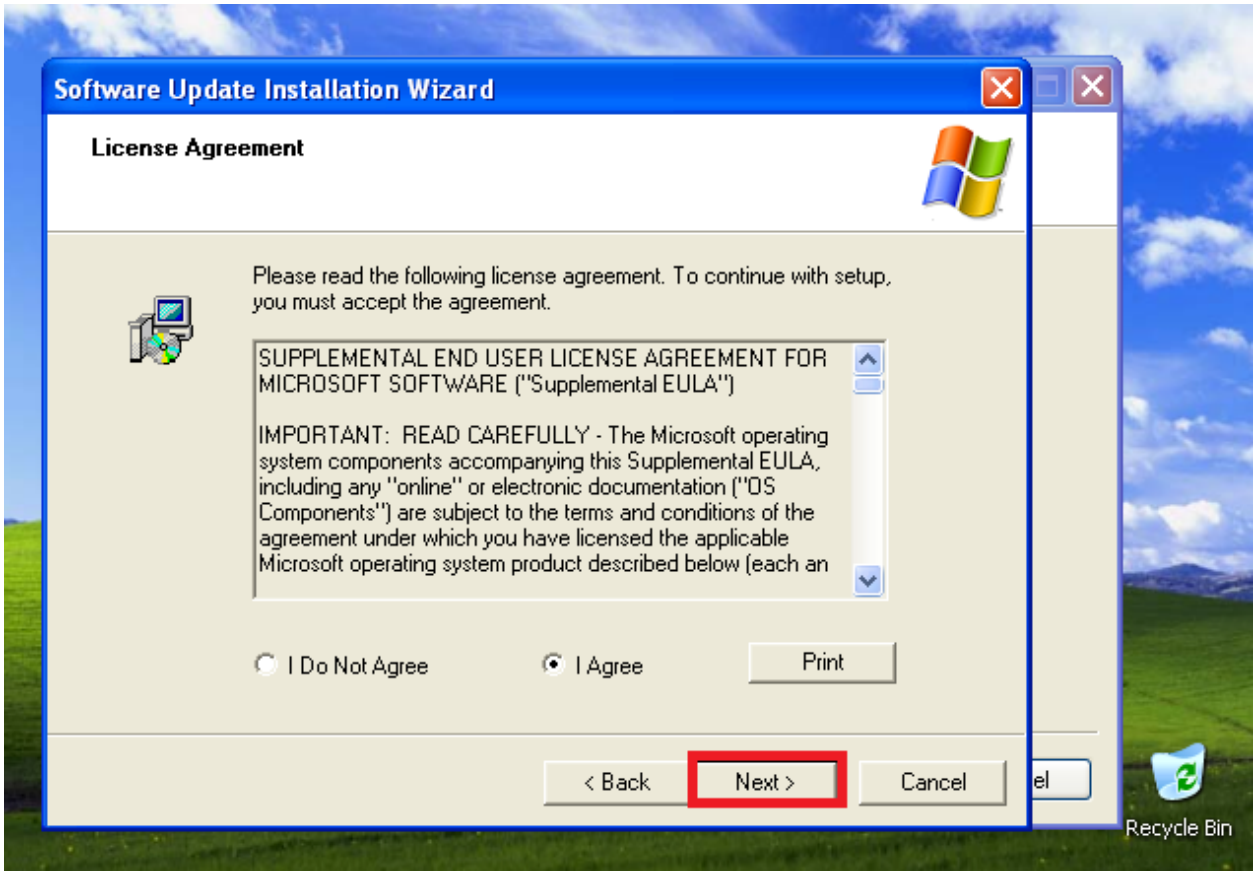


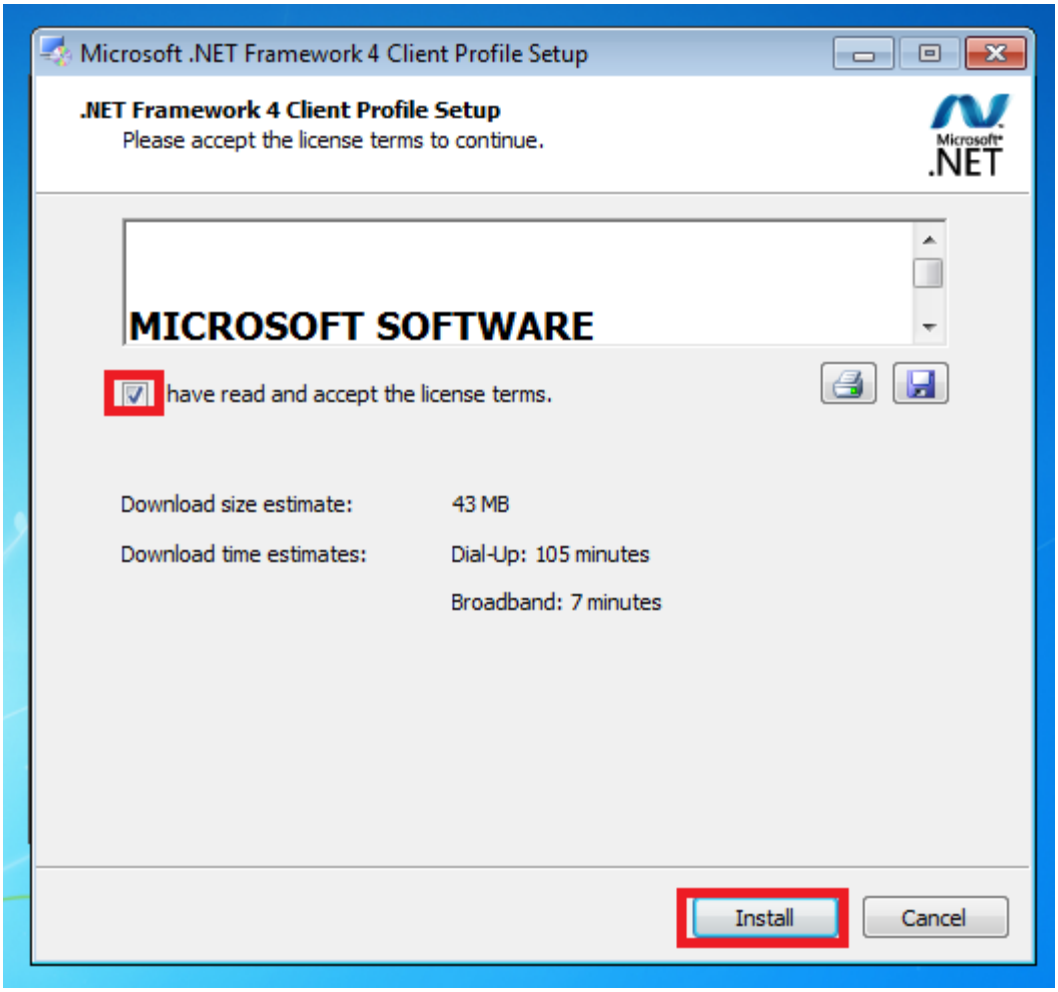
Click on Next



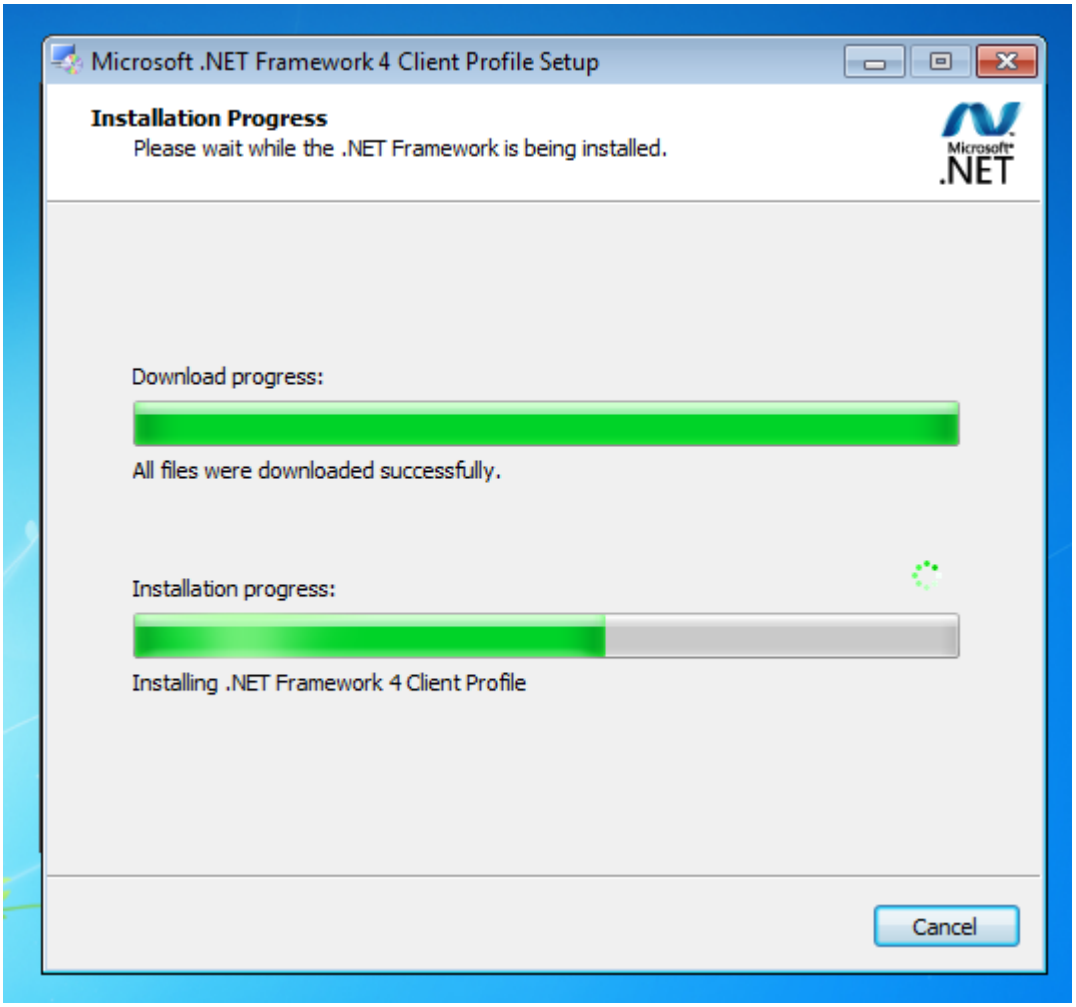
Accept the license and click on Next to begin the installation. At the end of the setup, the Windows Imaging Component setup will begin. Follow the same procedure to begin the installation.

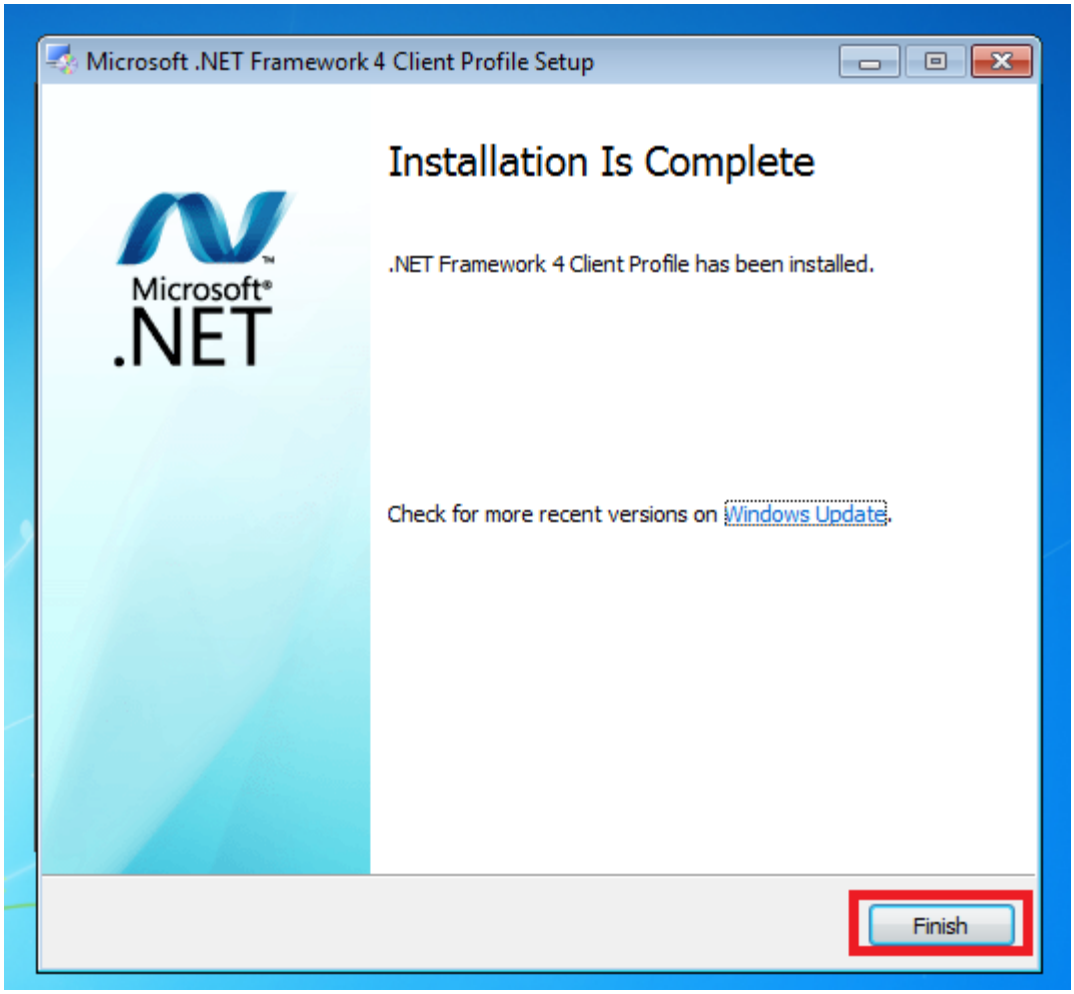

Software Update Installation Wizard
Use this wizard to install the following software update:
Windows Installer 3.1 (KB893803)
Before you install this update, we recommend that you:
- Back up your system
- Close all open programs
You might need to restart your computer after you complete this update. To continue, click Next.
< Back
Next >
Cancel
Recycle Bin


Software Update Installation Wizard
License Agreement
Please read the following license agreement. To continue with setup, you must accept the agreement.
SUPPLEMENTAL END USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE ("Supplemental EULA")
IMPORTANT: READ CAREFULLY - The Microsoft operating system components accompanying this Supplemental EULA, including any "online" or electronic documentation ("OS Components") are subject to the terms and conditions of the agreement under which you have licensed the applicable Microsoft operating system product described below (each an
I Do Not Agree
I Agree
Print
< Back
Next >
Cancel
Recycle Bin

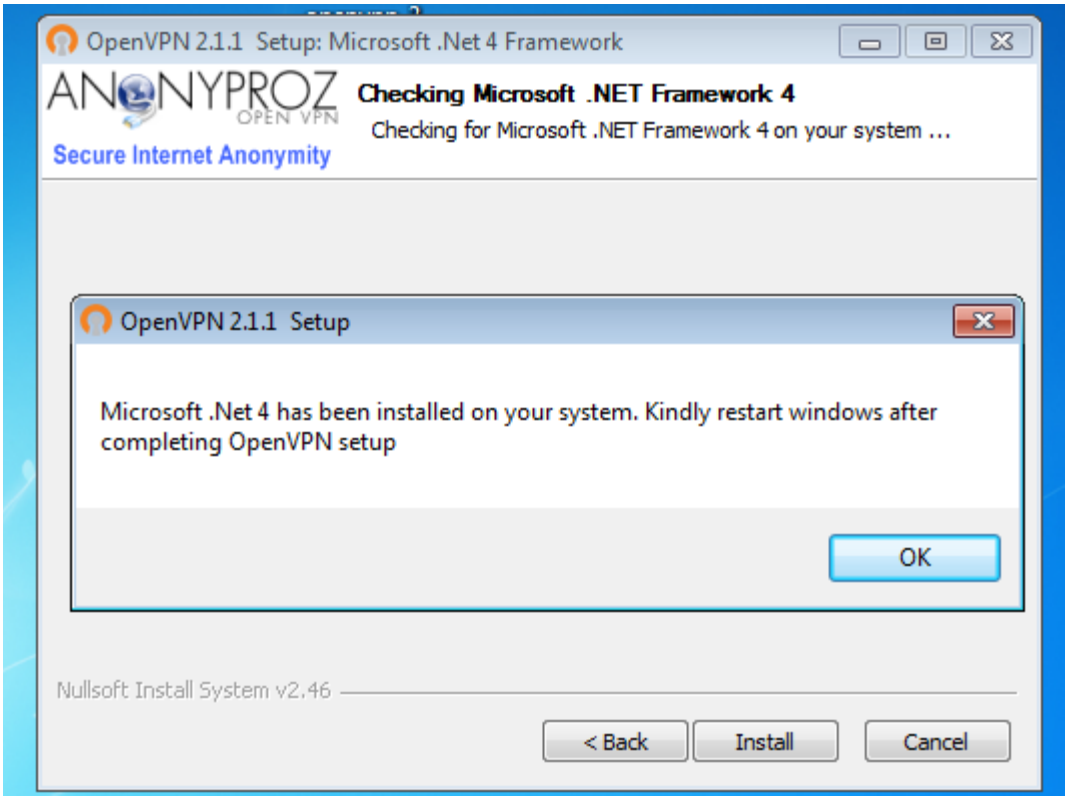


Accept the license and install on Install.

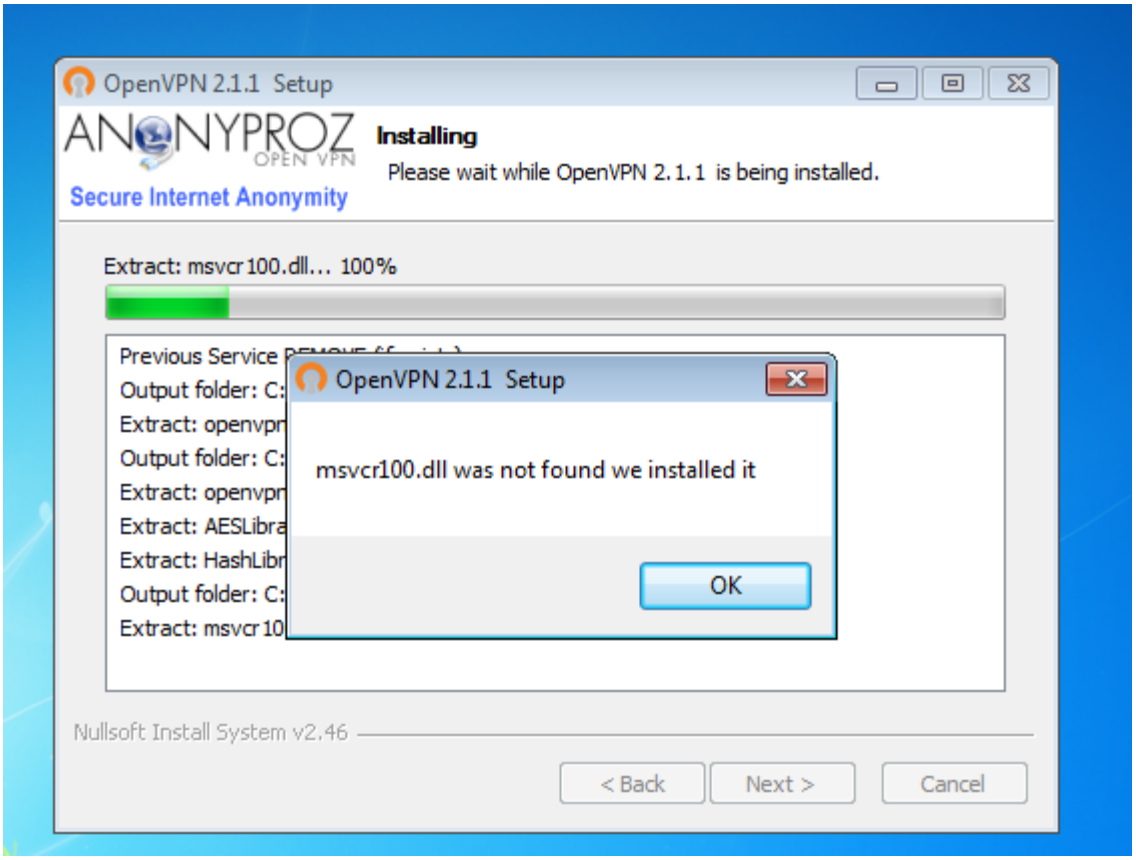

Microsoft .NET Framework 4 Client Profile Setup
Installation Progress
Please wait while the .NET Framework is being installed.
Microsoft .NET
Download progress:
All files were downloaded successfully.
Installation progress:
Installing .NET Framework 4 Client Profile
Cancel



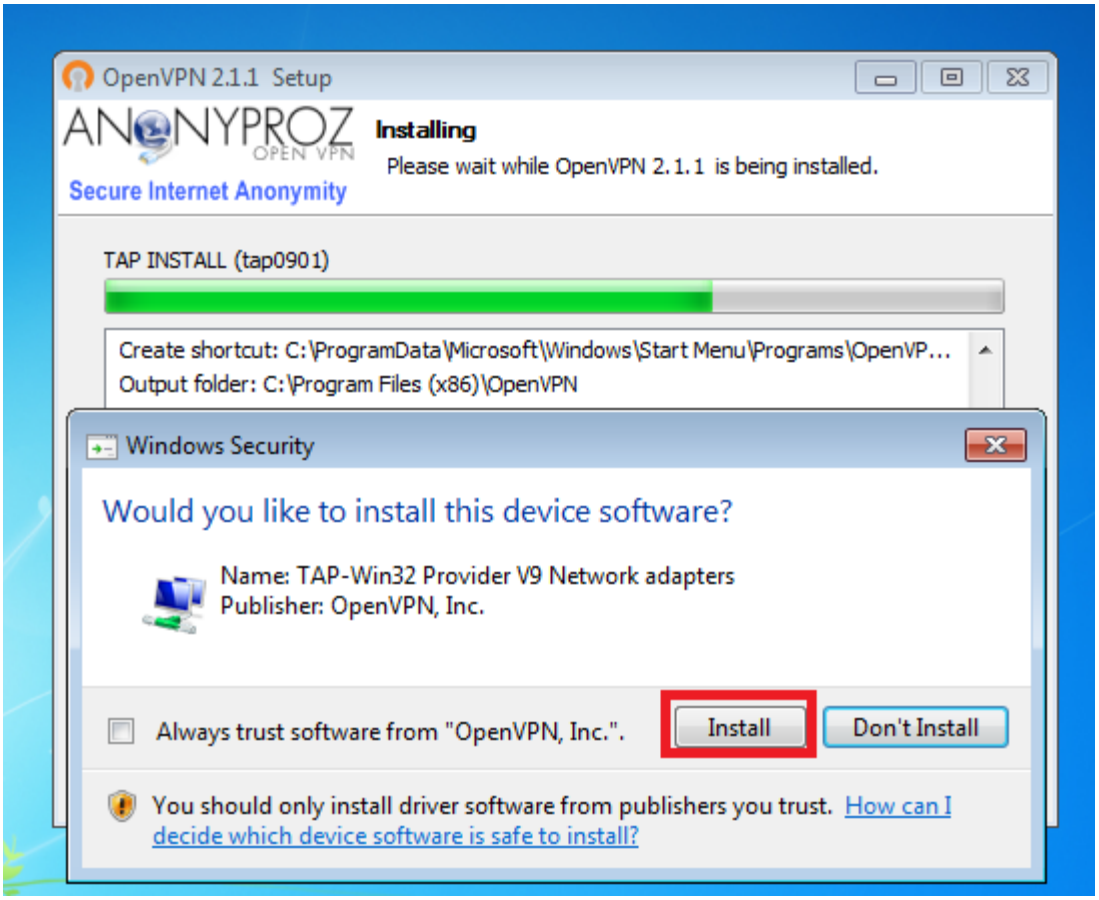
Click on Finish to complete the .NET framework installation.



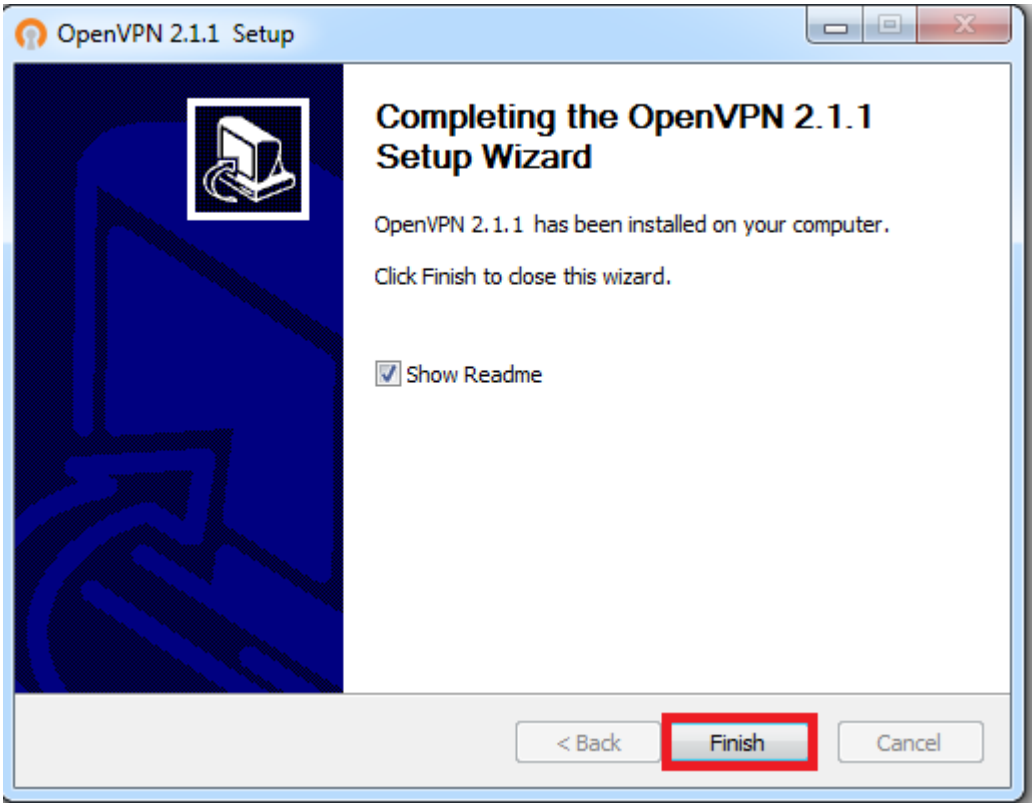
Important: While running the OpenVPN client installer, all required dependencies setup should be allowed to complete before continuing with the OpenVPN client installer as shown below. After completing the OpenVPN client setup, you should reboot your computer.



The GUI setup will continue and additional dependencies will be installed. Click OK to install the dependencies.



Click Install when prompted for the TAP adapter installation.



Leave the "Show Readme" checkbox checked and click on "Finish" to finish the setup. The GUI user guide document will automatically open on your computer. Please make sure you read this guide in order to familiarize yourself with the GUI.

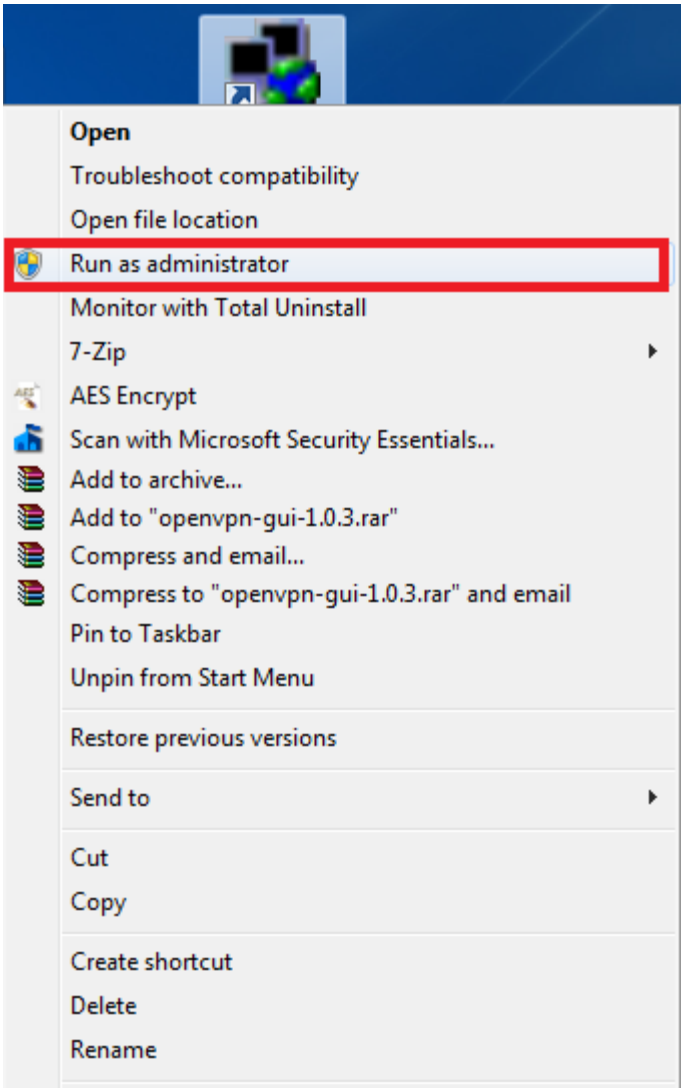
Important: After installing the GUI, you must restart your computer to save the system changes.

After completing the setup and rebooting your computer, you will now see the OpenVPN GUI icon in your desktop. The OpenVPN Client requires a configuration file and key/certificate files. You should obtain these and save them to \Program Files\OpenVPN\config. As default, you will find free OpenVPN config files from www.freeopenvpn.org that you can use as a quick start. Simply head to the site and get a password. Please ensure that you verify the config files prior to connecting to the servers.

Disclaimer: We are not in any way affiliated with www.freeopenvpn.org. All questions related to their services must be addressed to them directly.

To start it, simply double click on the icon and the GUI icon will become visible in your taskbar as shown below

Important: For Windows 7/Vista users, you must run the GUI as “Administrator”. To run the GUI as Administrator, simply right click on the GUI desktop icon and click on “Run as administrator” as shown below:



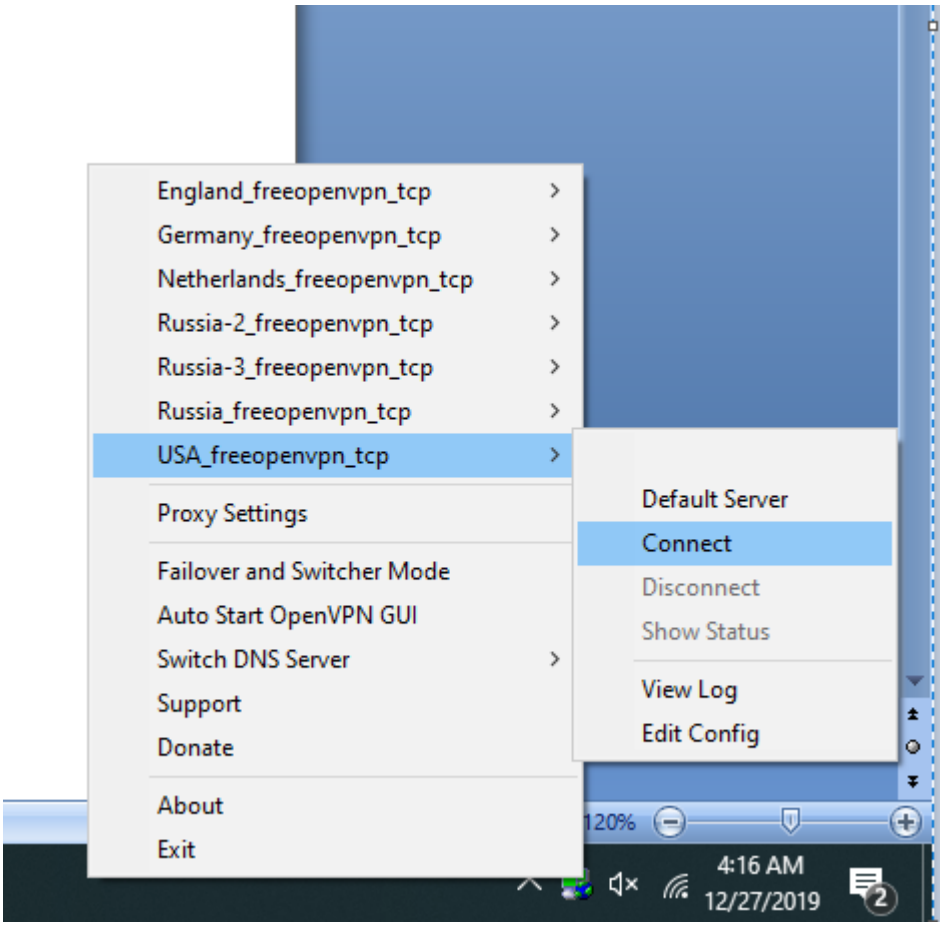
Connection Modes

Three modes of connection to OpenVPN servers are possible with the GUI as follows:

- Standard Single Server Connection Mode
- Failover Connection Mode
- Switching Connection Mode

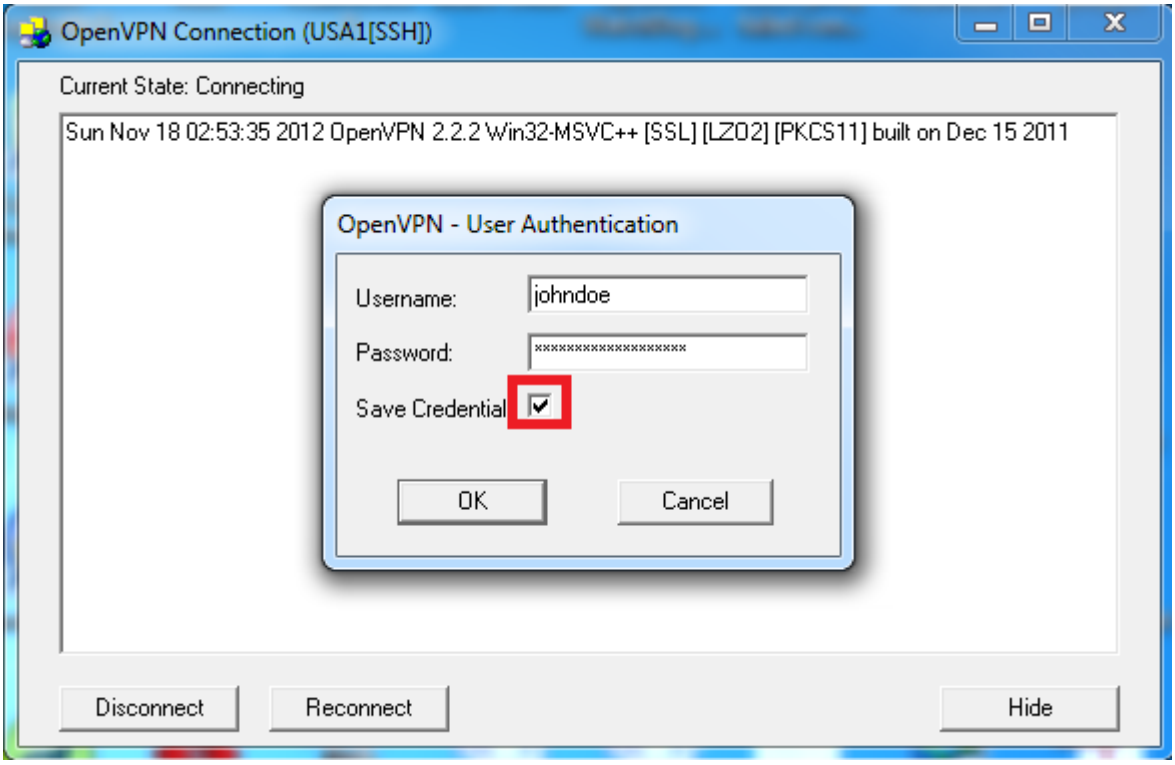
The 3 modes of connections are explained as follows:

Standard Single Server Connection: In the Standard Single Connection mode, users can connect to any single server of choice by simply right clicking on the GUI icon and navigating to the server name and clicking on “Connect” as illustrated in the screenshot below:

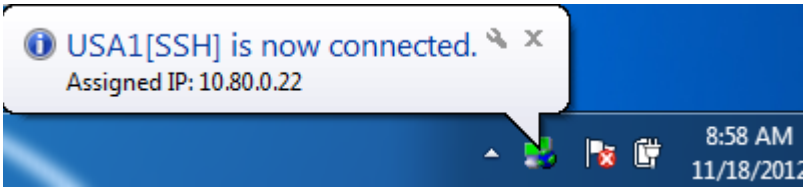


If your OpenVPN server config file is setup to use username/password authentication, you will be prompted for your username and password which will be passed on to the server over the secure TLS channel. If the credentials are correct, you will be authenticated and connected to the server. When

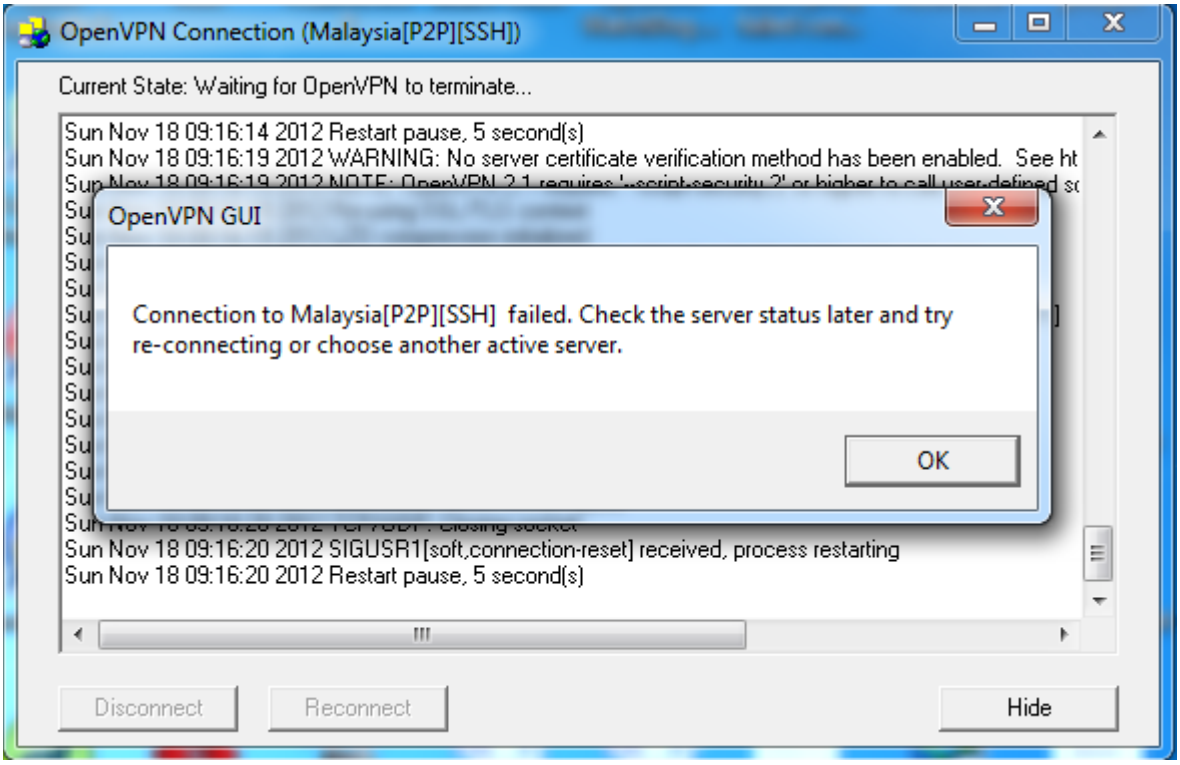
authenticating to the server, make sure you tick the “Save Credentials” checkbox in order to securely save your login credentials on your system so that you don’t have to enter your login each time you connect to your servers.



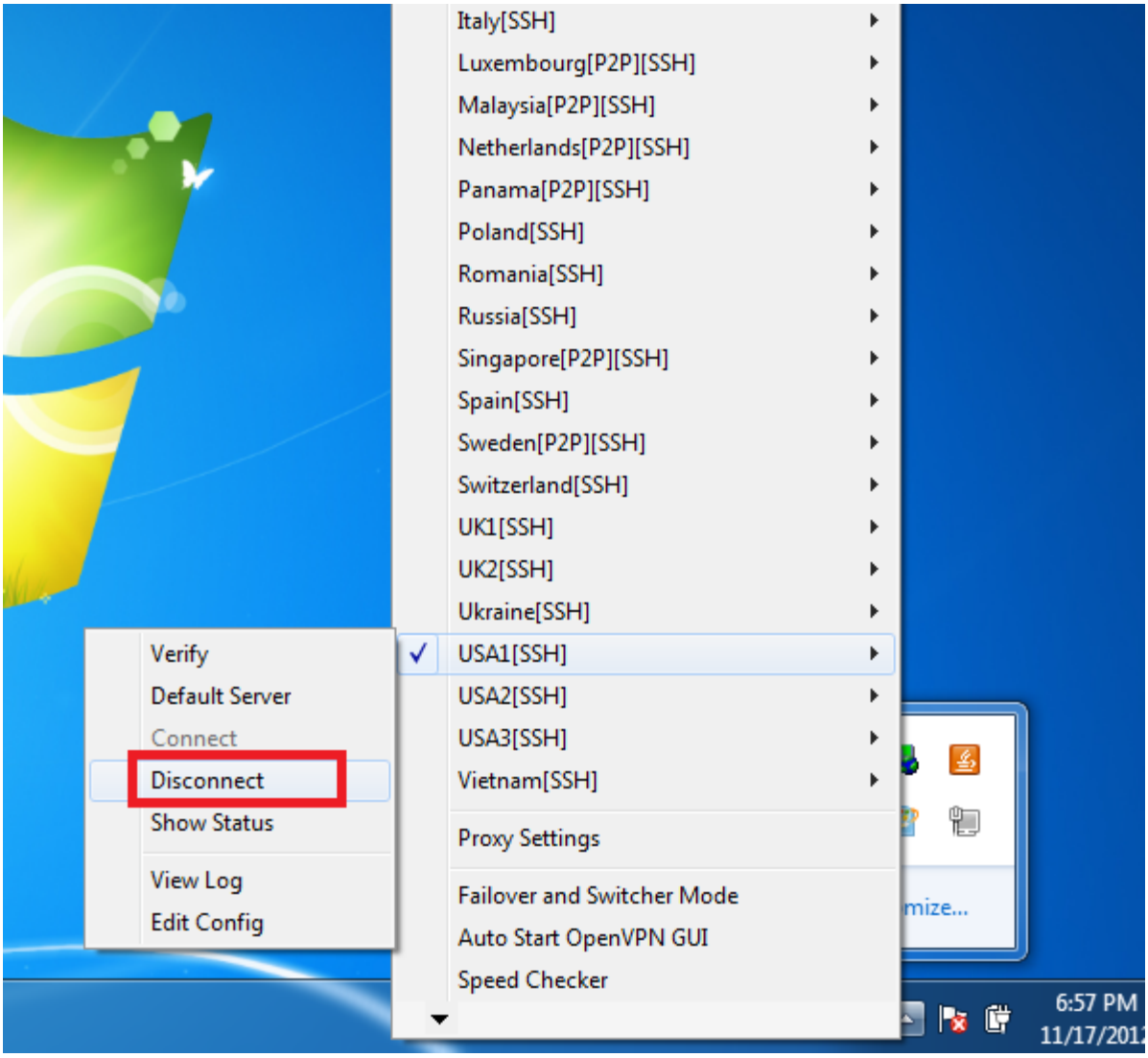
After connecting to the server, the GUI icon will change to green indicating a successful connection.



Congratulations! You are now connected to the server and all your traffic is now routed via the server securely. To disconnect from the server, simply go to the GUI and click on “Disconnect”.



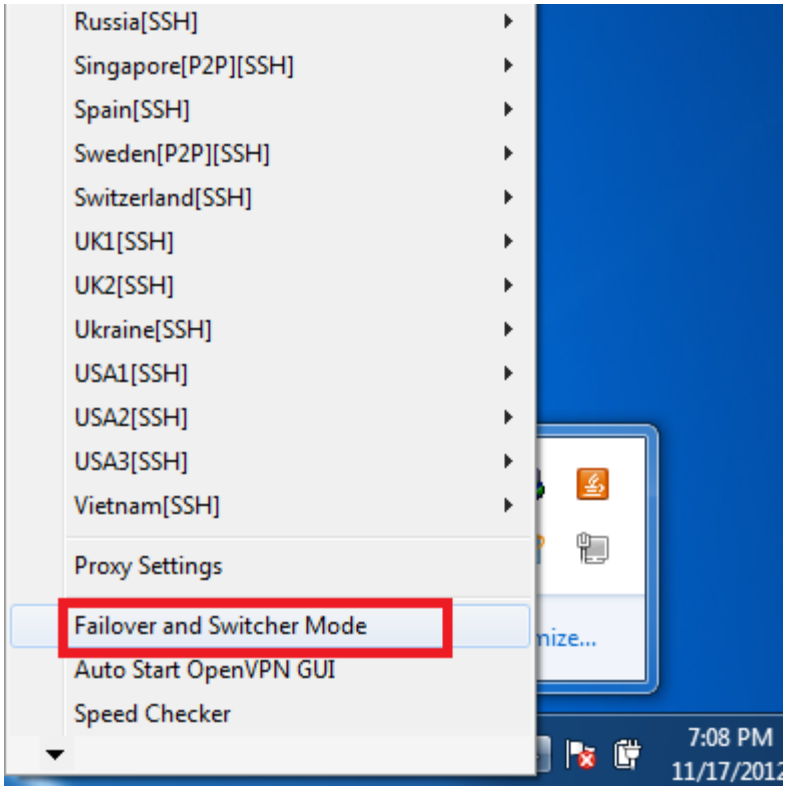
To switch from one server to another using the standard single server connection mode, simply disconnect from the former server by clicking on the “Disconnect” button and then connect to the new server. Note that you are required to disconnect from the former server before switching to the new one!



Failover Connection Mode: The GUI failover mode ensures high availability and redundancy for users by providing automatic switching to a user specified redundant server(s) upon the failure of the previously active connection. It is highly recommended to use the Failover mode when connecting to multiple servers. To use the Failover mode, take the following steps:

Step 1: Start the GUI.

Step 2: Click on the "Failover and Switcher Mode" menu as shown below:



Step 3: On the Failover/Switcher window, select the Failover mode and select your desired servers (redundant servers). You can select any number of servers as your redundant servers. After selecting your desired servers, click on "Connect" to start the connection. Please note that the order in which the servers are listed from top to bottom in the OpenVPN client main interface is order the servers will run no matter which server is ticked first.

Important:

The order in which the servers are listed from top to bottom is order the servers will run no matter which server is ticked first.

In the Failover and Switcher mode interface, the Servers will run from left to right and from top to bottom. For instance if a user selects servers in this order:

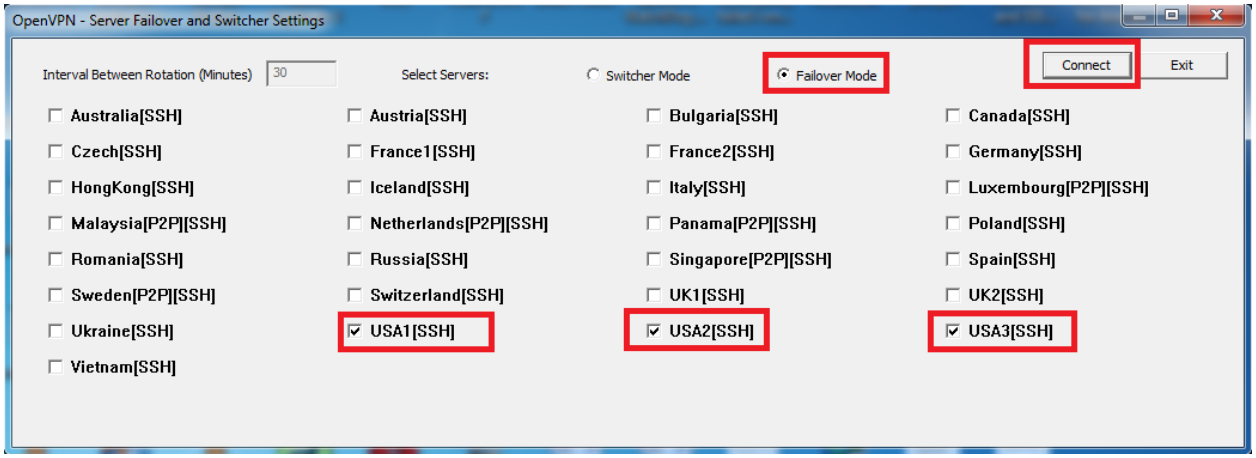
USA 3 >>>> USA 1>>>>France 1 >>>>Canada

Then the GUI will connect to the servers in this order:

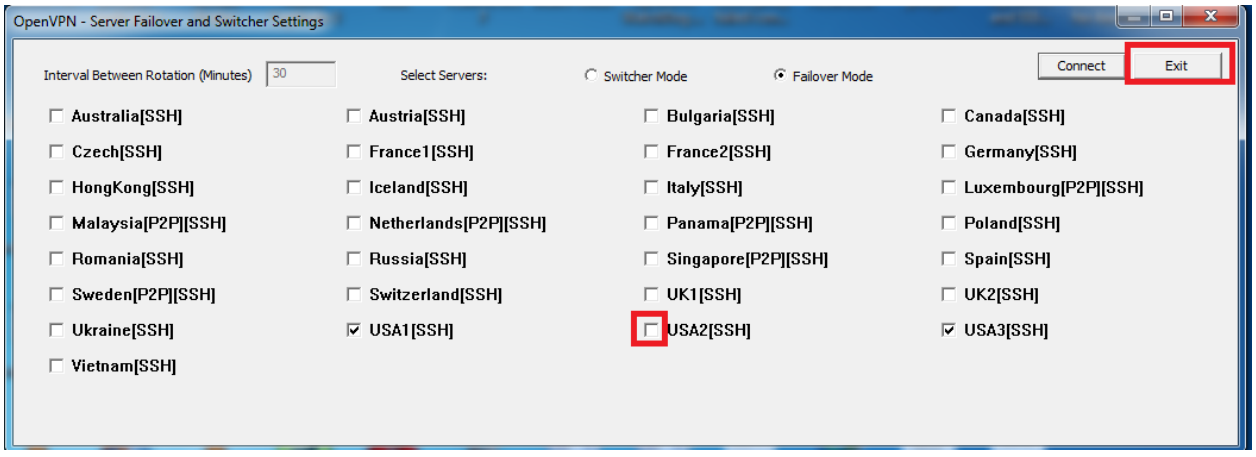
Canada >>>> France 1 >>>>USA 1 >>>> USA 3

As an illustrative example as shown in the screenshot below, we selected USA Server 1, USA server 2 and USA server 3 in this order and ticked the failover connection mode. With this configuration, the GUI

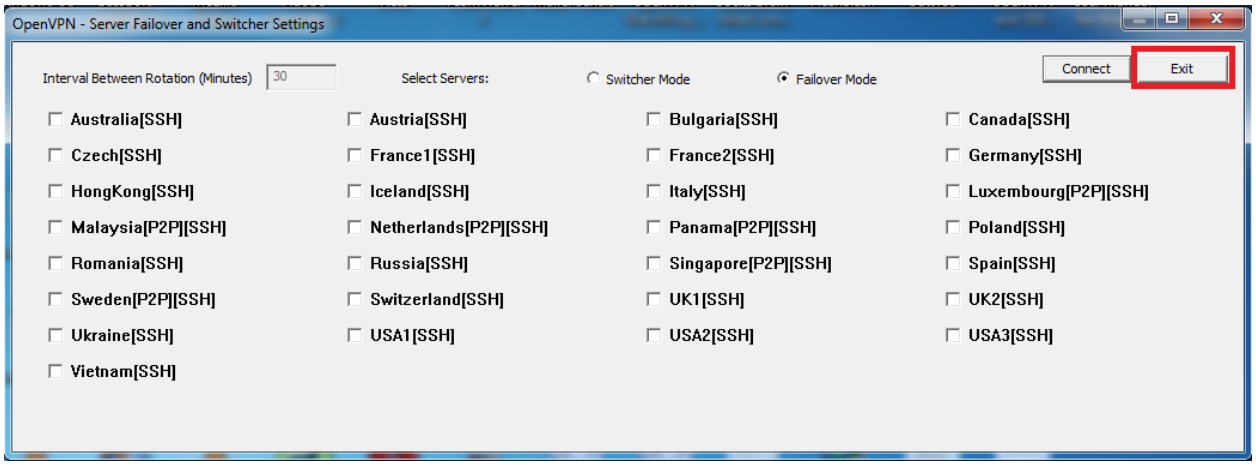
will first connect to USA server 1 and will remain connected until there is an outrage or failure in USA server 1. In the event that USA server 1 connection fails, the GUI will automatically failover or connect to USA server 2 using your saved login credentials. If also in the event that USA server 2 fails, the GUI will then failover to USA server 3 until USA server 3 fails. In the event that USA server 3 fails, the GUI will loop back to USA server 1 and will continue in this cyclic manner in order to ensure high availability and uninterrupted connection. The duration between the server switches takes approximately 30-38 seconds.



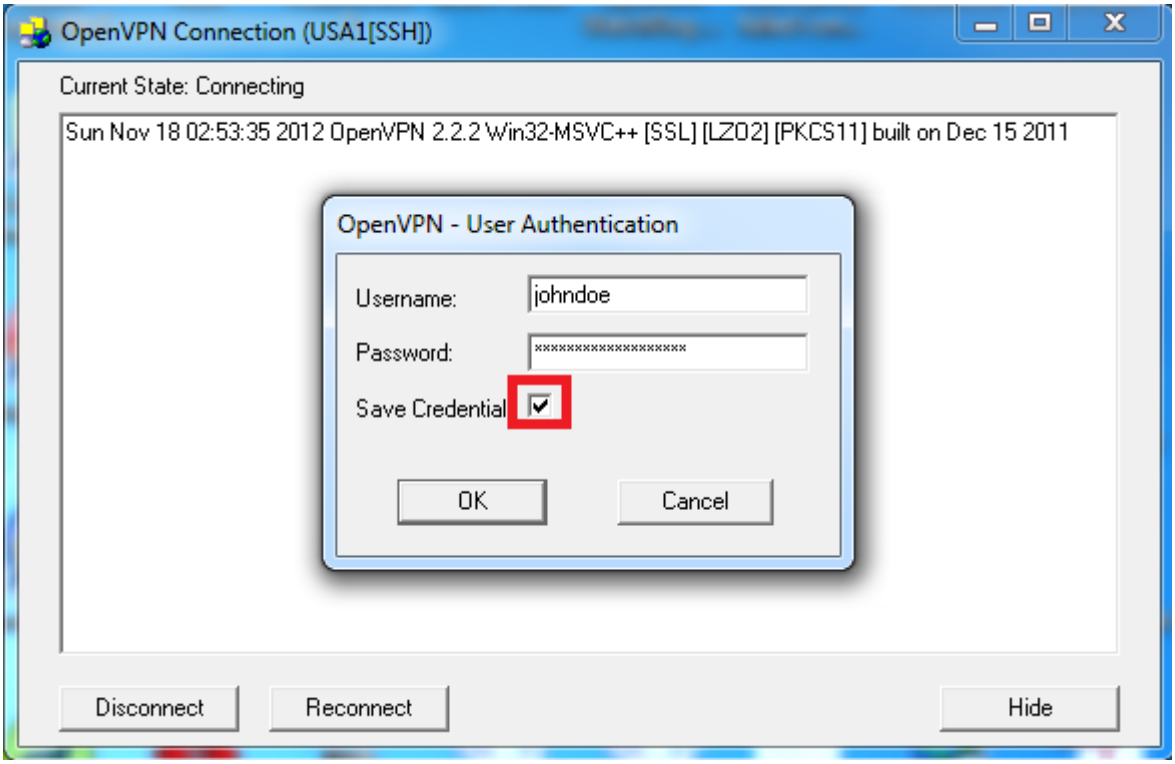
To disable or remove a particular server as a redundant server, simply untick the checkbox beside the server and click on “Exit” and the server will be removed or disabled from the failover mode of connection. Please note that you must de-select all the servers in the window if you wish to use the standard single server connection mode thereafter.

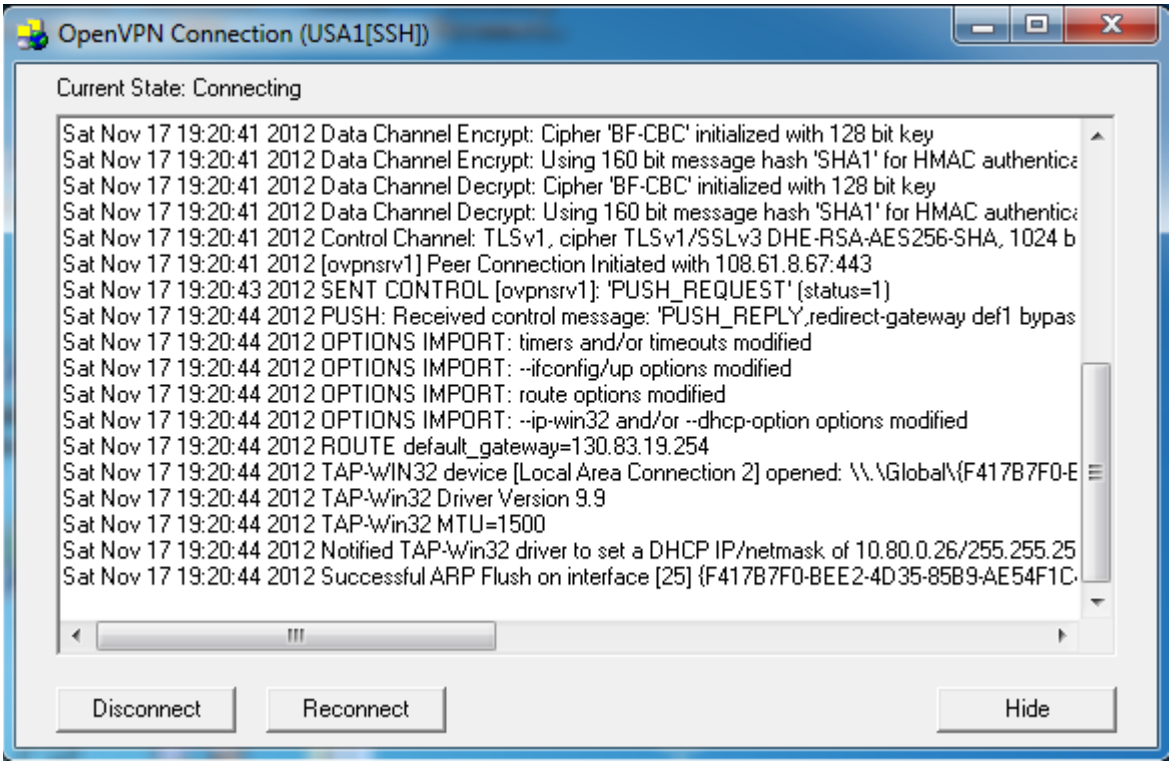


To discard the failover mode, simply unselect ALL selected servers and click on “Exit”



If it is your first time of authenticating to your servers, the login prompt window will appear as shown below. Please enter your correct username and password and make sure you tick the “Save Credentials” checkbox before clicking on OK. Your login credentials is only saved securely on your computer after successfully connecting to a server.





If you wish to terminate the failover mode and disconnect from your current active connected server while running the GUI in the failover mode, simply navigate to the current connected server and click on "Disconnect".

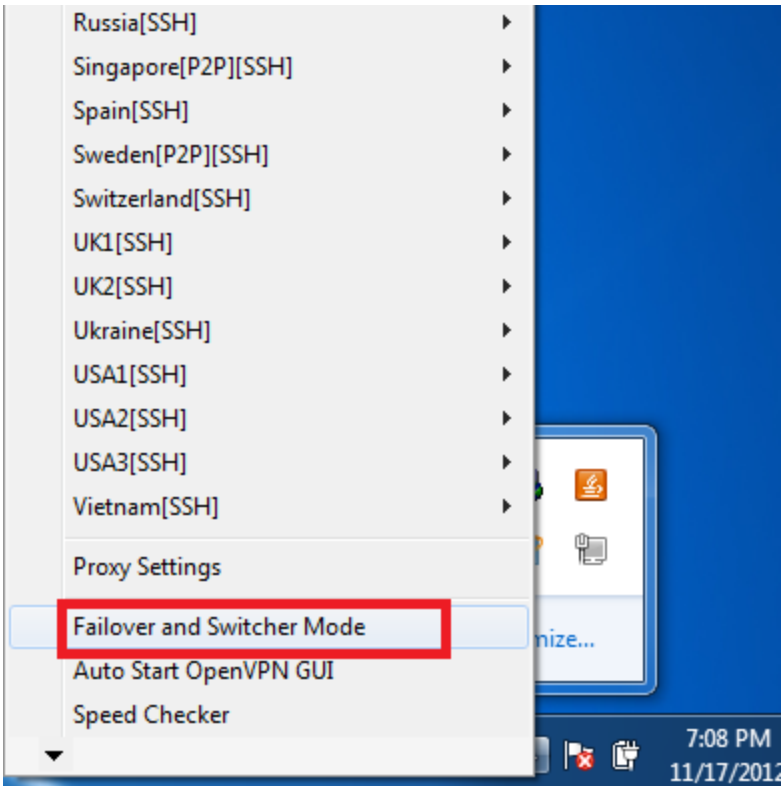
Switching Connection Mode: Instead of connecting to a single server one at a time each time the GUI is launched, you may want to connect and switch between multiple pre-selected server locations for increased anonymity. The GUI offers you the ability to connect to multiple pre-selected server locations at set time intervals thereby changing your IP address during each server switching. In addition to the increased anonymity benefits, by switching between multiple OpenVPN servers at scheduled time interval, certain Deep Packet Inspection or Firewalls can be bypassed.

As most DPI devices tend to block encrypted traffic which are characterized by very high encrypted traffic volume to a single destination or server, it is recommended that excessive and prolonged connections to a single OpenVPN server be avoided. In addition, most DPI tend to block VPN connections not by IP or port, but by simply cutting off any connection that sends too much data to a single location or server.

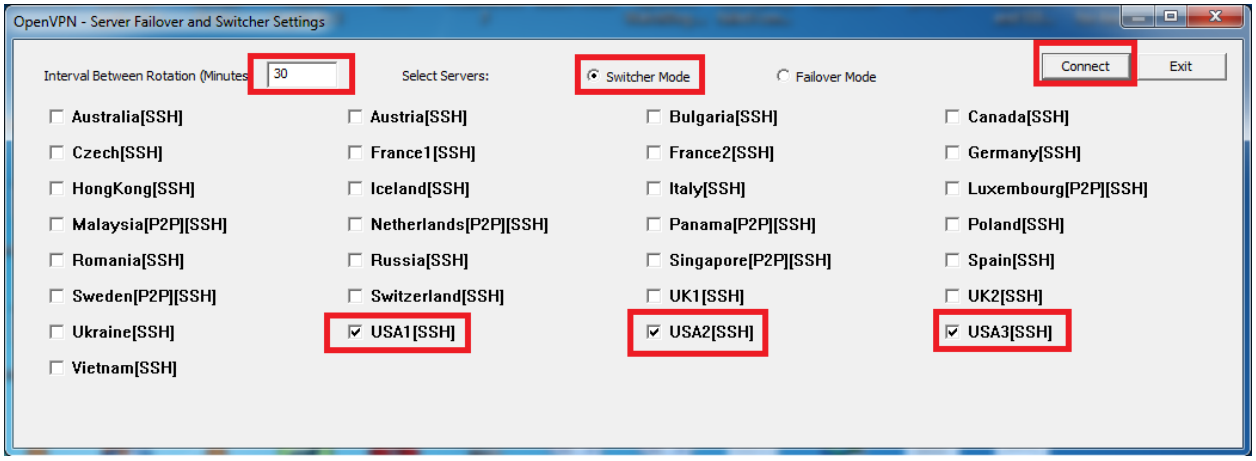
The following steps show how to run the GUI in switching connection mode:

Step 1: Start the GUI

Step 2: Navigate to the "Failover and Switcher Mode" menu



Step 3: Click on the "Failover and Switcher Mode"menu and you will be presented a window to select the servers you wish to switch between.Enter a desired time interval in minutes between each rotation and then finally click on "Connect". Note that the server switching connections will be made in that order in which they are ticked in the server switcher settings window.



Step 4: After clicking on Connect button, the GUI will automatically connect to the first server selected in the queue and will automatically re-connect to the next server on queue after the set time interval

has elapsed. After connecting to the last server selected on the switching queue, the GUI will connect to the first server again and continue this in a cyclic manner.

If a particular server in the queue cannot be connected due to server outrage, the server will be bypassed and you will be connected to the next server in queue.

As soon as a new connection is made to a new server, you should see a connection notification message pop up on the taskbar. A sample is shown below

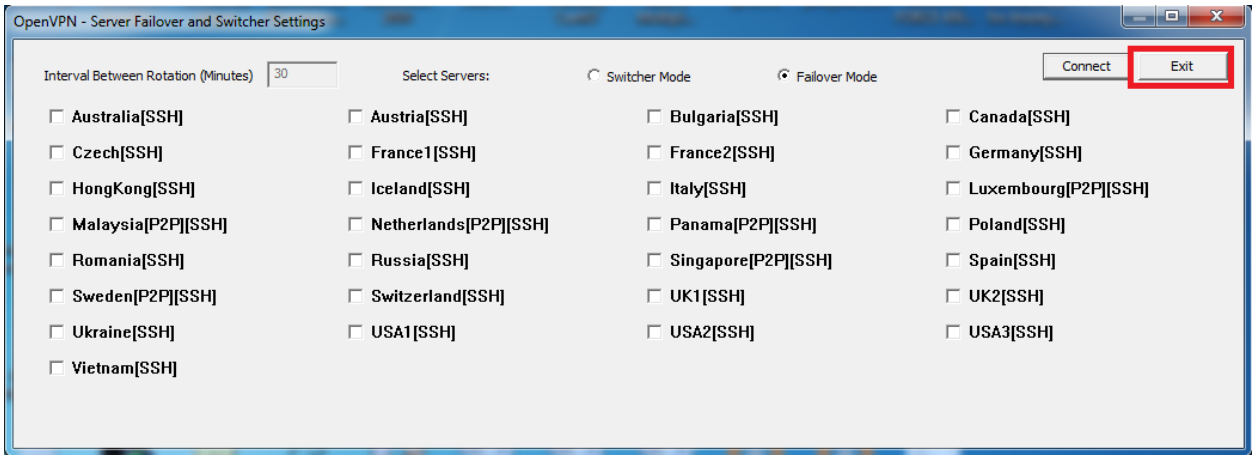
Note: While the GUI is switching from one server to another, you will be unable to connect to the internet. This is done to safeguard your connection and ensure that your real IP do not leak while the GUI is switching servers. The server switching duration normally takes just few seconds to complete.

Step 5: To disconnect the connection, simply locate the current active servers that in the queue by looking for the right mark before the server or by hovering your mouse over the GUI taskbar icon. Then click on “Disconnect” to disconnect from the VPN server.

Note: If a default server is enabled in the GUI, you must disable the default server before running the GUI in Switcher or Failover modes. Otherwise, the failover or switcher modes of connection cannot be started.

Switching from Failover or Switcher Connection Modes to Standard Single Server Connection Mode

If you wish to switch to the standard single server connection mode after exiting from the failover mode then go to the failover and switcher mode window and un-tick or un-select all selected servers and finally click on the “Exit” button. After this, you can then connect to any server in the standard single server connection mode.



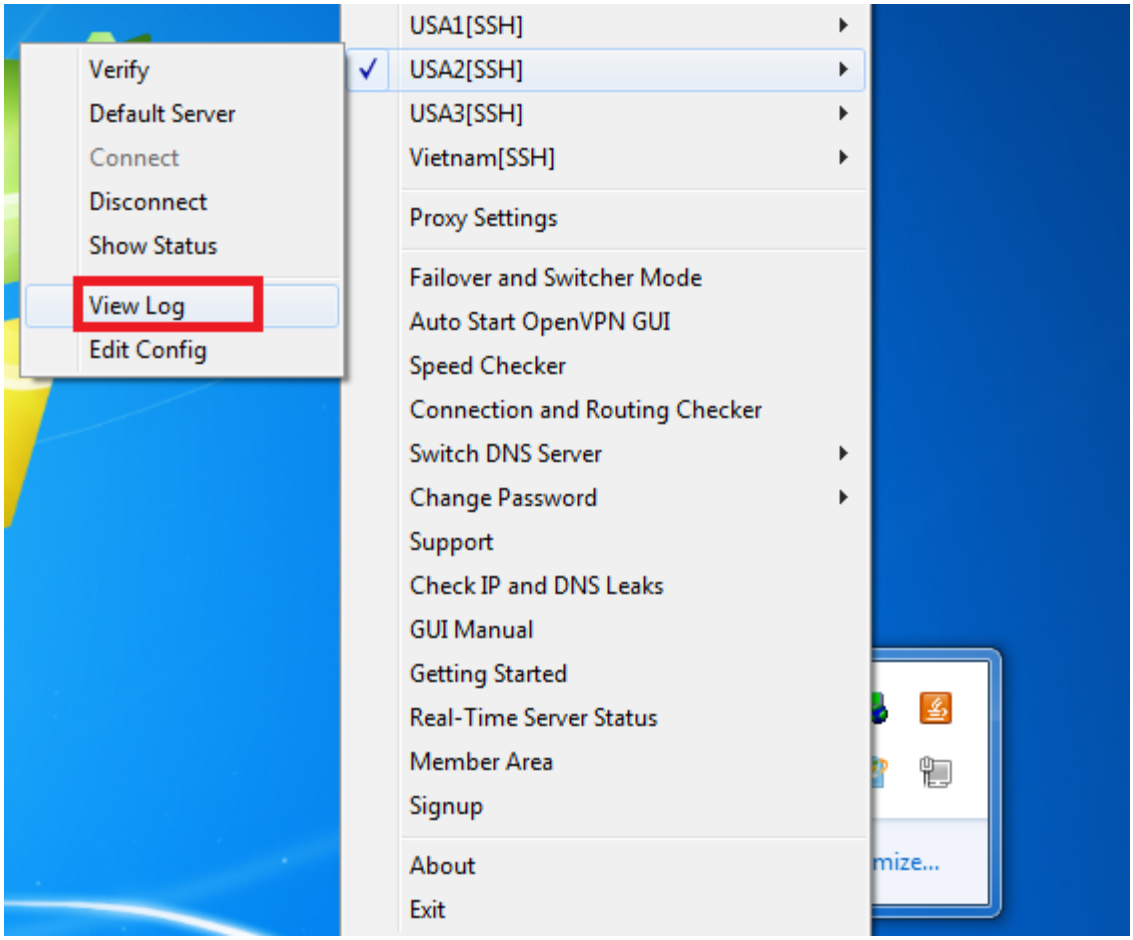
Viewing Connection Logs:

If you are unable to connect to any server which could be due to wrong login credentials, server outrage or ISP OpenVPN protocol blocking, you can view the logs which can aid you or your OpenVPN server provider to troubleshoot.

The OpenVPN log contains all information regarding an OpenVPN connection, including extra connection details about your connection, warning messages, and error messages. If you are unable to connect, or your VPN connection drops out, you should be able to find the reason contained in the OpenVPN log.

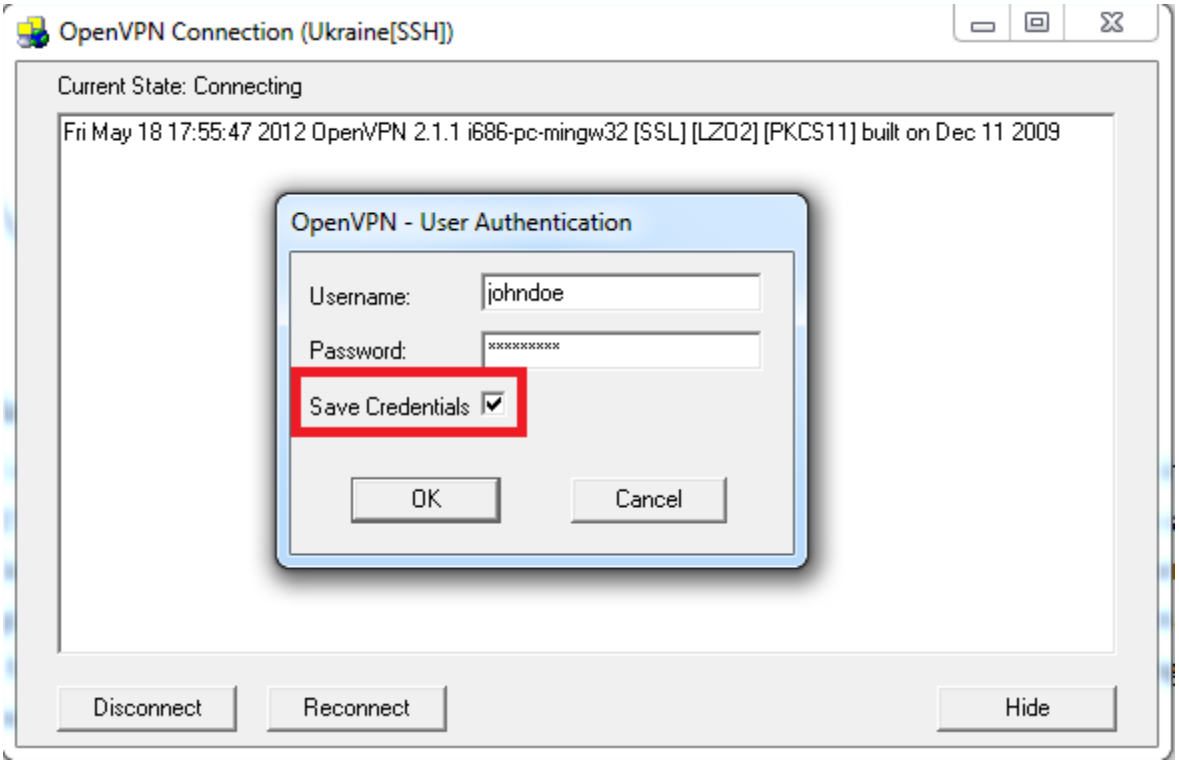
You can view the OpenVPN Log from the OpenVPN client for Windows by following the following steps:

1. Right click on the OpenVPN icon on the taskbar on your system
2. Move the mouse to the server which is having the connection issue and then click on “View Log”



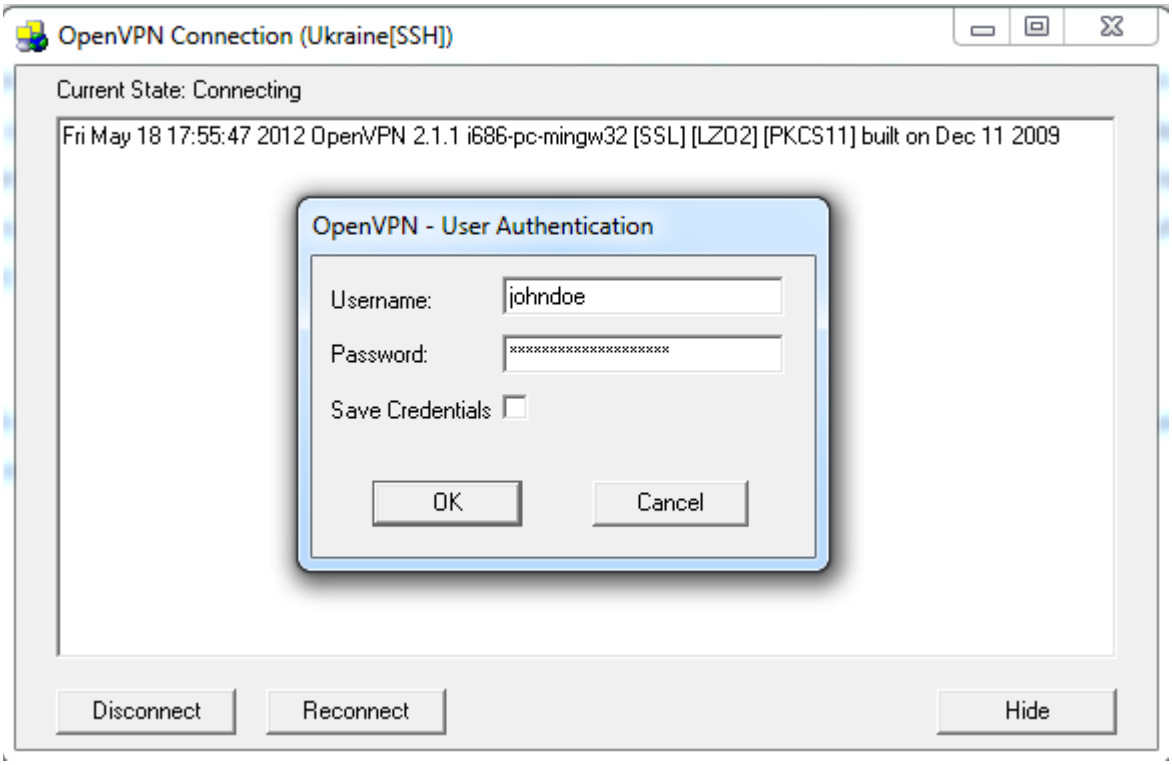
Saving Login Credentials:

The GUI includes an optional feature to enable you save your login credentials securely in an encrypted form (AES 256 cipher) on your computer when authenticating to the OpenVPN server. To save your login credentials, simply click on the “Save” check box on the authentication window as shown below. Once your login is saved securely, the GUI will then use this saved login to connect automatically to the servers for subsequent connections thereby saving you the stress of typing your username and password manually each time you wish to connect to the server.



In addition, using the encrypted saved login credentials for automatic connections can prevent the possibility of a keylogger (hardware and software that's designed to secretly record your keystrokes) or spyware program to steal or capture your login. Once the login is saved, it is encrypted using strong AES 256 ciphers on your system and you do not have to manually enter your login anymore when you wish to connect to the VPN server. Note that your login credentials are only saved securely on your computer after successfully connecting to a server.

If you wish to delete previously saved login credentials, just uncheck the check box and click OK as shown below and the login credentials will be erased securely from your computer when you connect to the server. Thereafter you can proceed to login to the server with the new login credentials while ticking the "Save Credentials" checkbox.



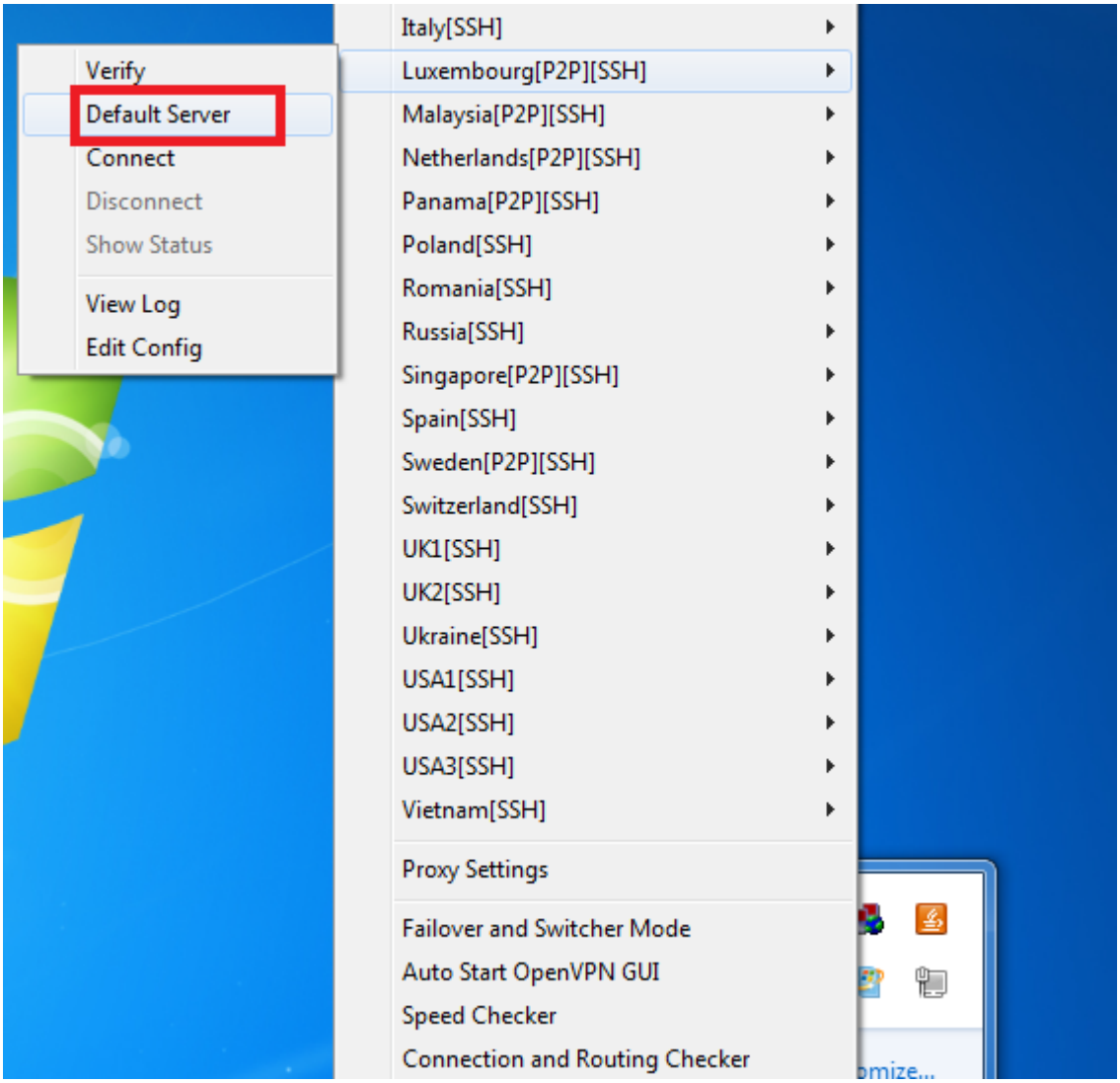
Automatic Connection at GUI launch

The GUI allows you to select a specific server of your choice as a default server or select multiple servers which will be rotated and make the GUI automatically connect to the server(s) using your saved login credentials whenever the GUI is launched or restarted. The following explains how each mode of operation is carried out.

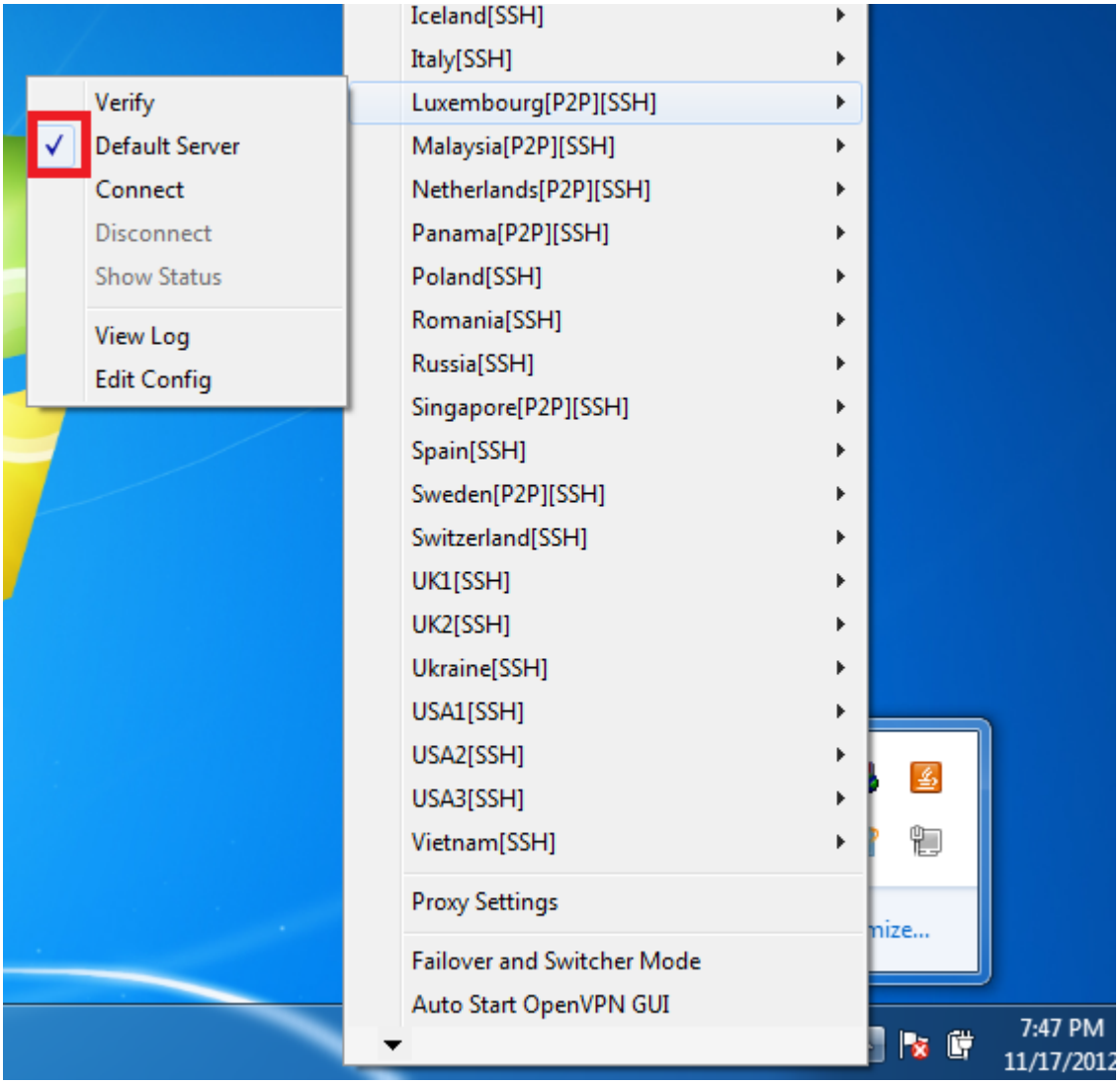
Connecting to a Single Default Server at GUI launch:

To make the GUI automatically connect to a single default server of your choice whenever it is launched, take the following steps:

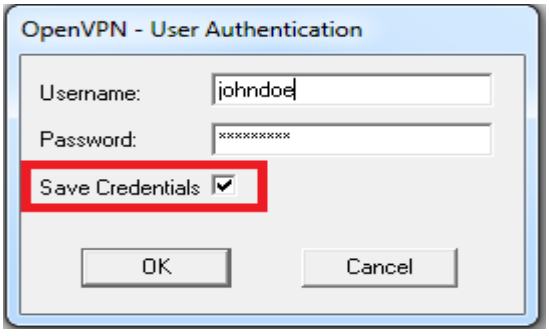
1. Start the GUI
2. Navigate to your desired server which you intend to set as your default server and click on "Default Server". An example is shown below for Luxembourg server.



3. After clicking on the “Default Server”, confirm that the server has been made the default server by looking for a right mark ✓ before the “Default Server” button as shown below

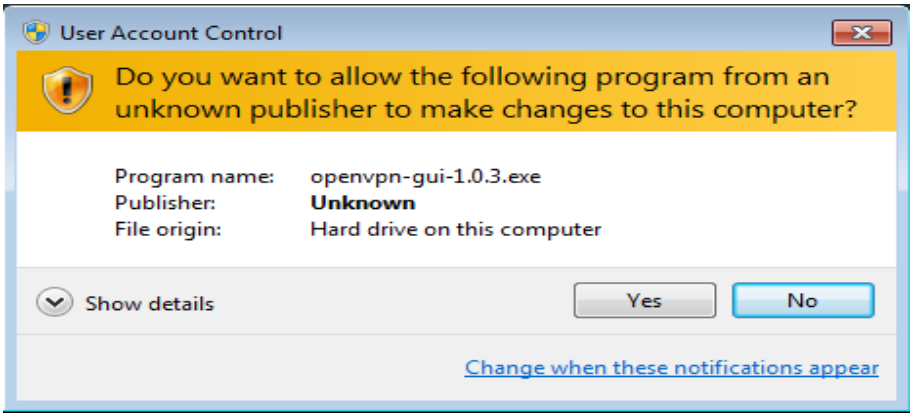


4. For the automatic connection to work, your login credentials must be saved previously on your computer. To save your login credentials securely on your computer, click the “Save Credentials “checkbox before you connect to any server.



5. When next you launch the GUI, the GUI will automatically select the default server and will connect to the server without any input or action from you.

Note: You must disable User Access Control (UAC) on your system if you intend to make the GUI auto start and connect to a default server at system boot time unattended. If UAC is not disabled, you will get security prompts as shown below:



In Windows 7/Vista, you can easily disable/enable UAC from the command Line by running the following commands:

Disable UAC

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f

Enable UAC

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 1 /f

After you enable or disable UAC, you will have to reboot your computer for the changes to take effect.

Note: Please note that the above commands are single line commands. Enter the commands in a single line.

Changing the Default Server

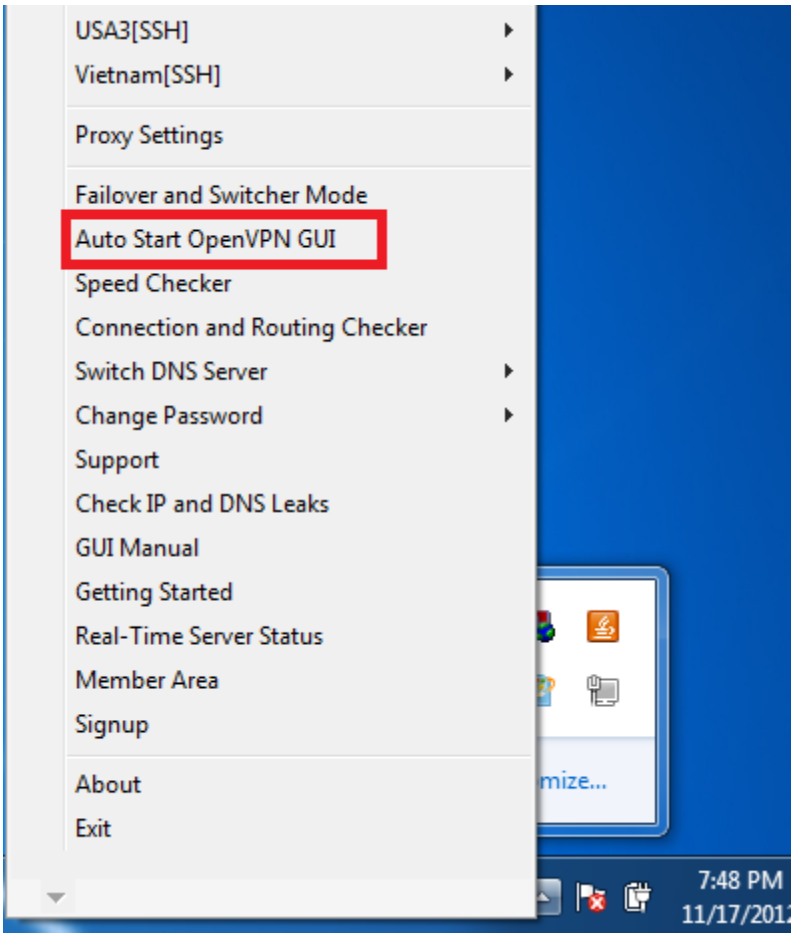
To disable the current active default server and select a new default server, simply go to the current default and click on the “Default Server” button to deselect/de-activate the server as the default server.

Thereafter, you can select a new server as your default server by clicking on the “Default Server” button for the new server. As soon as the server has been deselected as the current active server, the right mark will be removed.

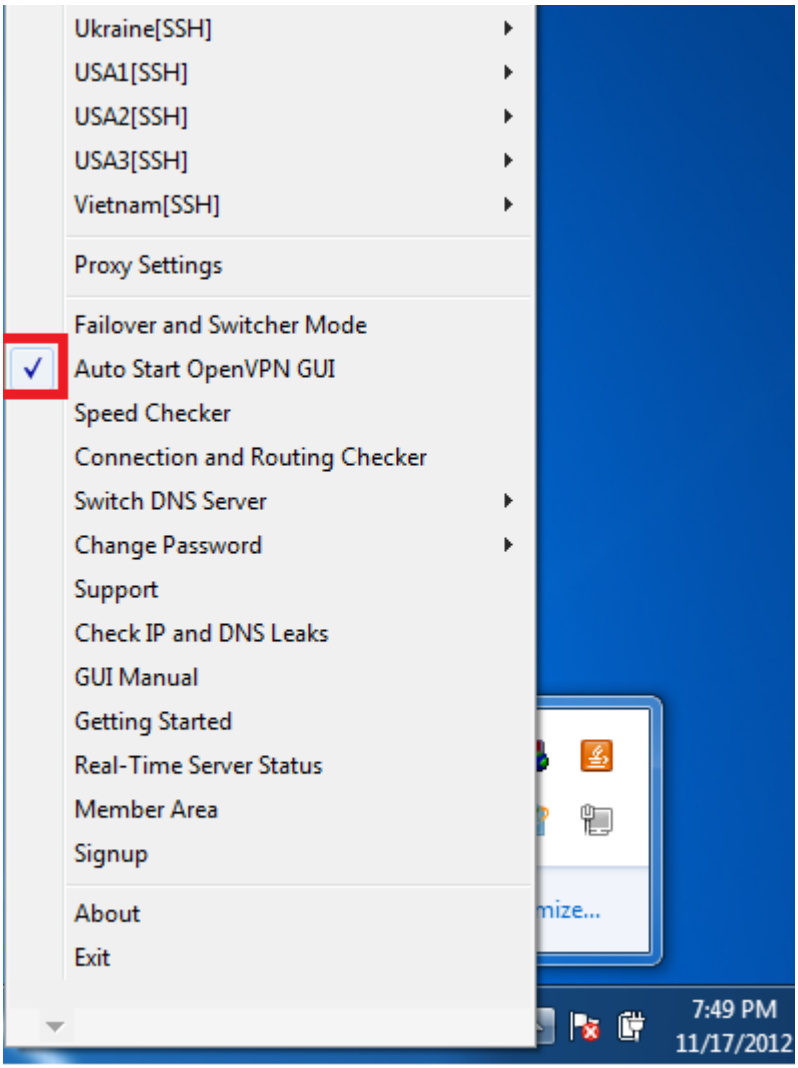
Automatic GUI Start and Connection at System Startup

Sometimes it can be useful to have the GUI automatically startup and connect to a server at system boot time. For example, supposing you wish to run the GUI on unattended systems or servers and you require that certain applications or programs access the internet securely via OpenVPN connection at all times, you can install the GUI on the unattended systems and setup the GUI to automatically start and connect to the VPN server(s) at boot time or during system restarts; all in unattended mode. When the GUI automatically launch at system boot time, it can be made to connect to either a default single server or multiple switching servers.

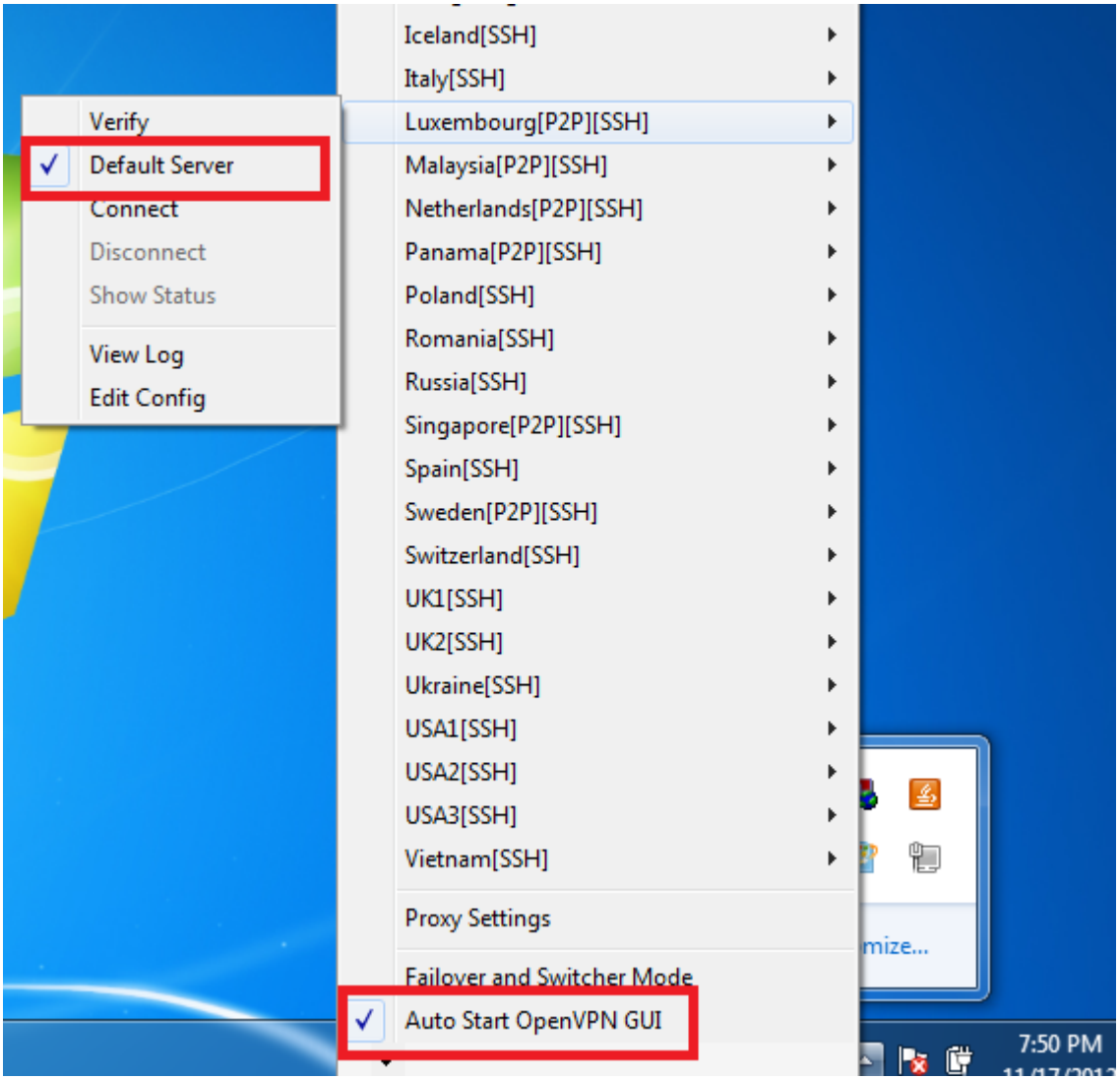
To configure the GUI to automatically connect to a pre-selected default server or multiple rotating servers configured in the automatic server switcher settings window at system boot, click on the “Auto Start OpenVPN GUI” menu to activate it as shown below



Once activated, the right mark sign will appear beside the menu as shown below.



Note: Make sure that the right marks are present in the “Default Server” and the “Auto Start OpenVPN GUI” menus for the automatic connection to the default server at system boot time to be active! For example, in the sample screenshot shown below, the GUI will automatically connect to the Luxembourg server when the system restarts or boots up.

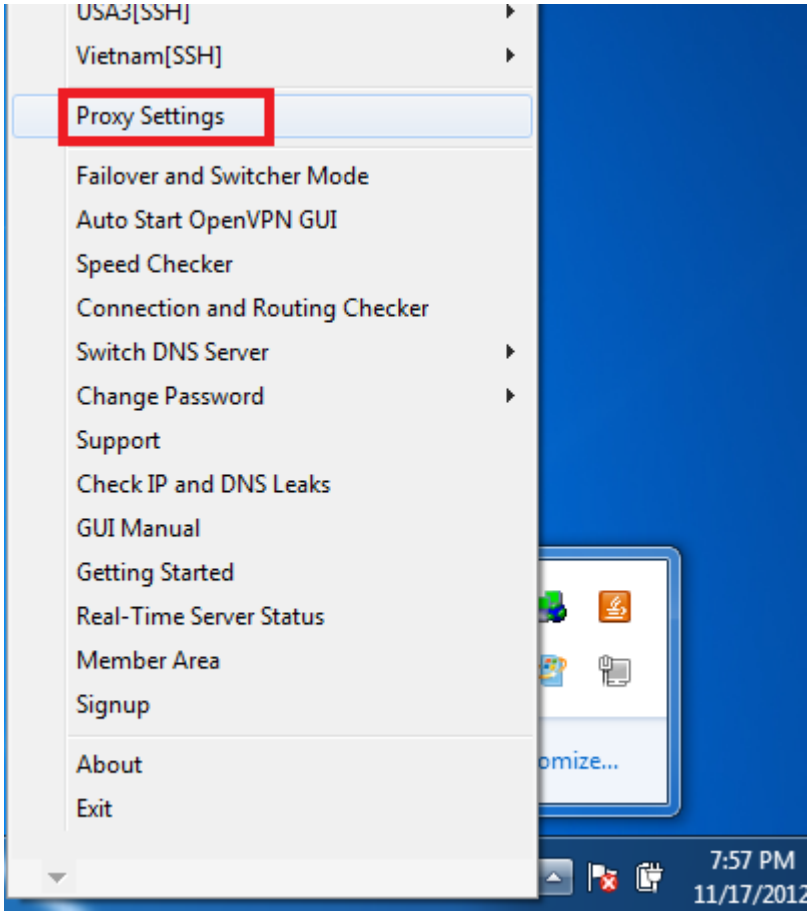


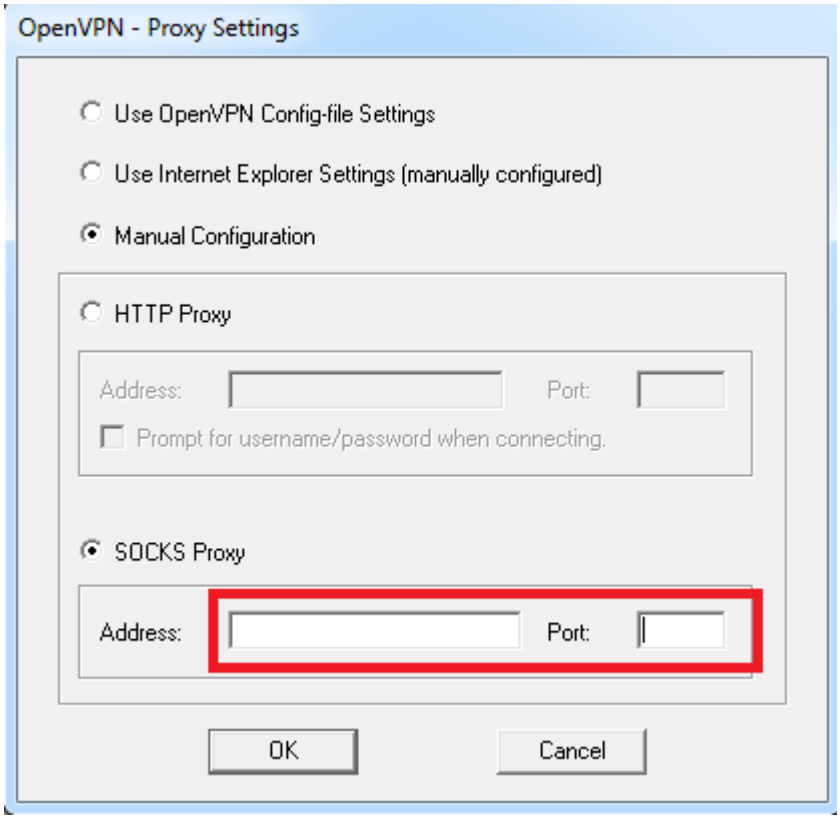
Once activated, the GUI will automatically start and connect to the default server.

To de-activate the GUI Auto start, simply click on the menu again and the automatic start of the GUI will be disabled. Once disabled, the right mark sign beside the menu will no longer be visible indicating that the Auto start has been disabled.

Proxy Setting:

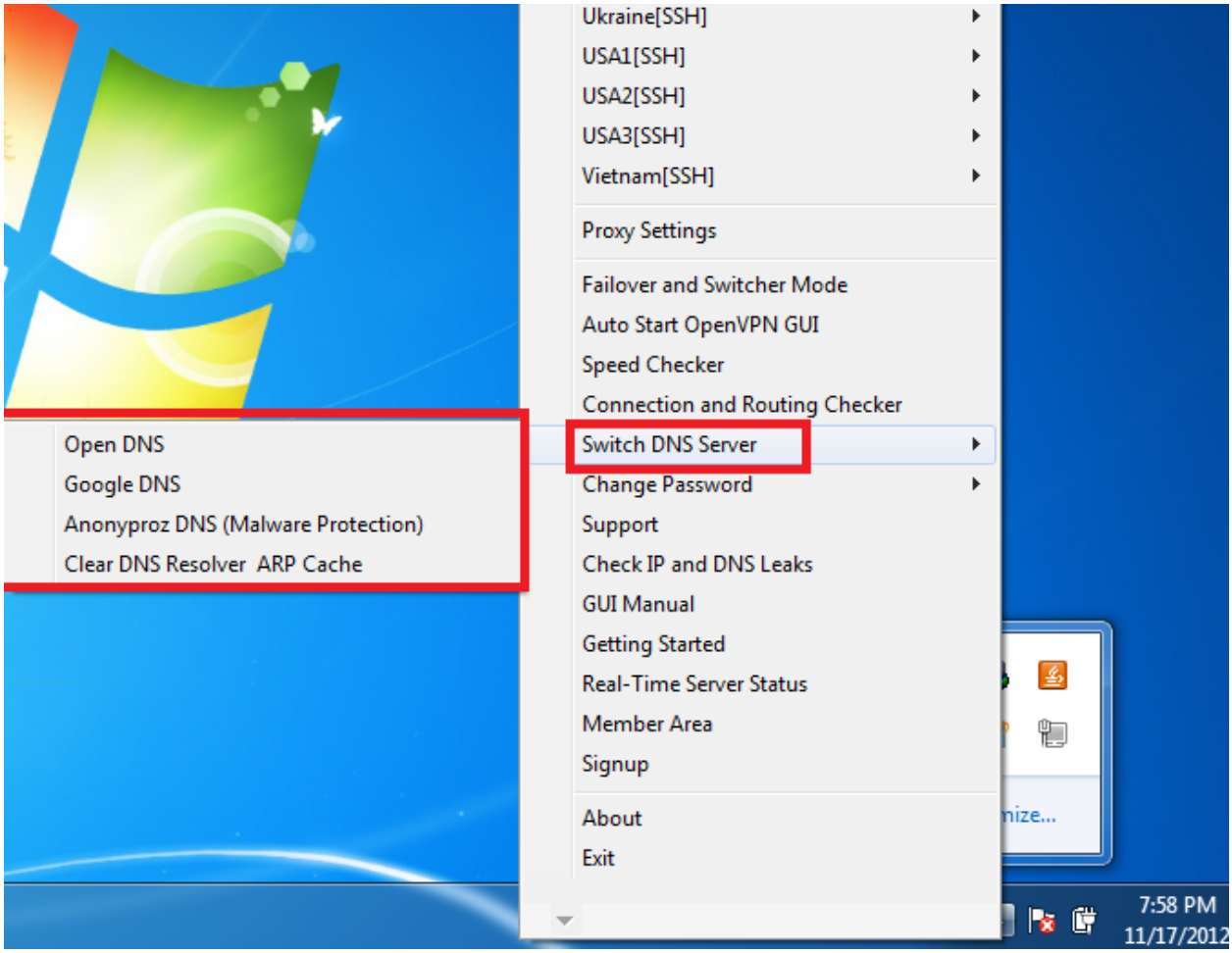
OpenVPN supports connections via proxy servers. HTTP and SOCKS proxies are currently supported. SSH Socks 5 proxy is also supported. To connect to any of the server via a proxy, simply click on the "Proxy Settings" menu and configure the proxy settings.


USA3[SSH]
Vietnam[SSH]
Proxy Settings
Failover and Switcher Mode
Auto Start OpenVPN GUI
Speed Checker
Connection and Routing Checker
Switch DNS Server
Change Password
Support
Check IP and DNS Leaks
GUI Manual
Getting Started
Real-Time Server Status
Member Area
Signup
About
Exit
omize...
7:57 PM
11/17/2012



Switching DNS Server:

Anonyproz offers subscribers the ability to switch the DNS used for resolving websites when connected to our OpenVPN servers using the OpenVPN client GUI. Using the GUI, you can easily switch between Google DNS, OpenDNS or our private malware domain filtering enabled DNS servers. Switching between these DNS servers only requires a single click when connected to the VPN. Your connection will not be disconnected when you switch between DNS servers.



Note that OpenDNS and Google DNS are public DNS servers which offer large scale caching system and offers fast DNS look ups using a technology known as "anycast routing" to direct all DNS queries to the closest DNS server to you. Thus, by using OpenDNS or Google DNS, your browsing experience can be improved significantly and websites are more likely to be resolved faster.

By offering users the option to switch between our private DNS, Google DNS and OpenDNS, users can then utilize any of the DNS which offers them the best browsing experience and speed.

Please note that when using one of these free public DNS servers (Google DNS and OpenDNS), all DNS queries will originate from the server IP and not your personal IP hence your privacy is assured. To learn more about Google DNS and OpenDNS, please go to the links below:

OpenDNS: http://www.opendns.com/

Google DNS: https://developers.google.com/speed/public-dns/

The table below summarizes the main differences between Google DNS, OpenDNS and our private DNS servers:

DNS Server	Malware Domain Filtering	Redirection (Advertising)	Logging
OpenDNS	YES	YES	YES
Google DNS	NO	NO	YES
Anonyproz DNS	YES	NO	NO

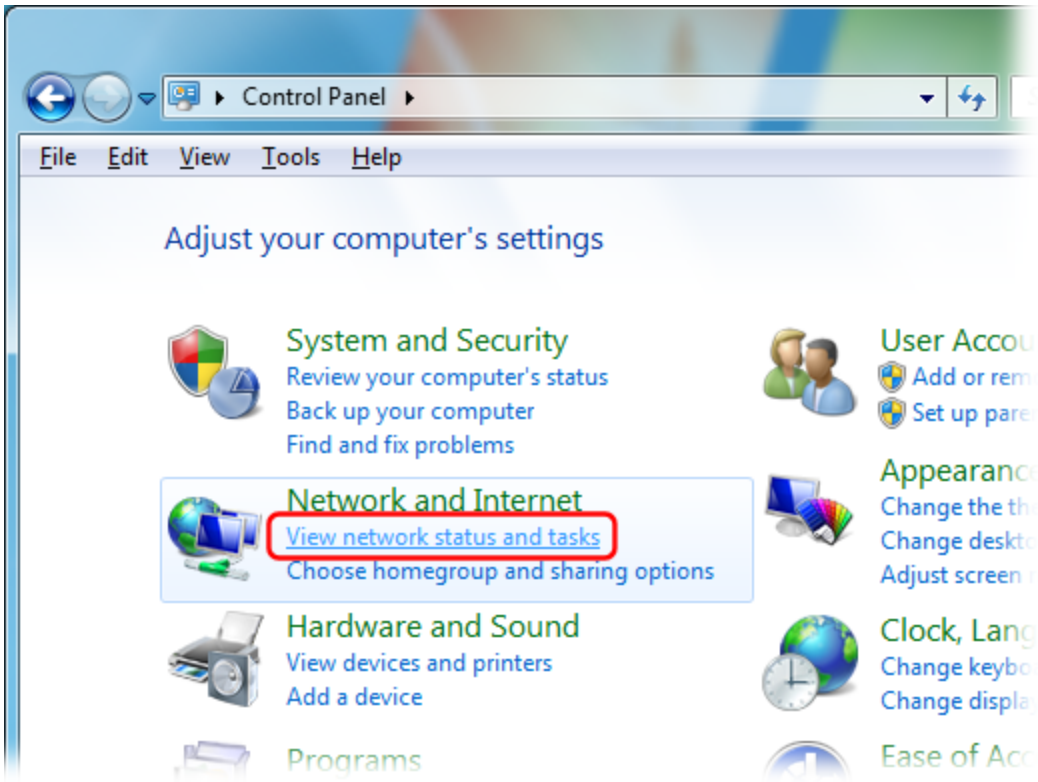
By using our private DNS servers you can take advantage of our malicious domain filtering service which will detect and block all DNS requests to known malicious sites obtained from various user contributed sources such as malware and phishing sites as part of our service. Once connected to our OpenVPN servers, access to these known malicious sites are automatically blocked at the DNS level (DNS sinkhole) thereby preventing the sites from loading in your browser. You will be automatically redirected to our malware alert page when a DNS request is made for a malicious domain listed in our database.

Our custom DNS sinkhole system is currently blocking over 300,000 malicious domains. To see these blocked domains, please go to our Malware DNS Sinkhole web portal at: https://www.anonyproz.com/dnssinkhole/

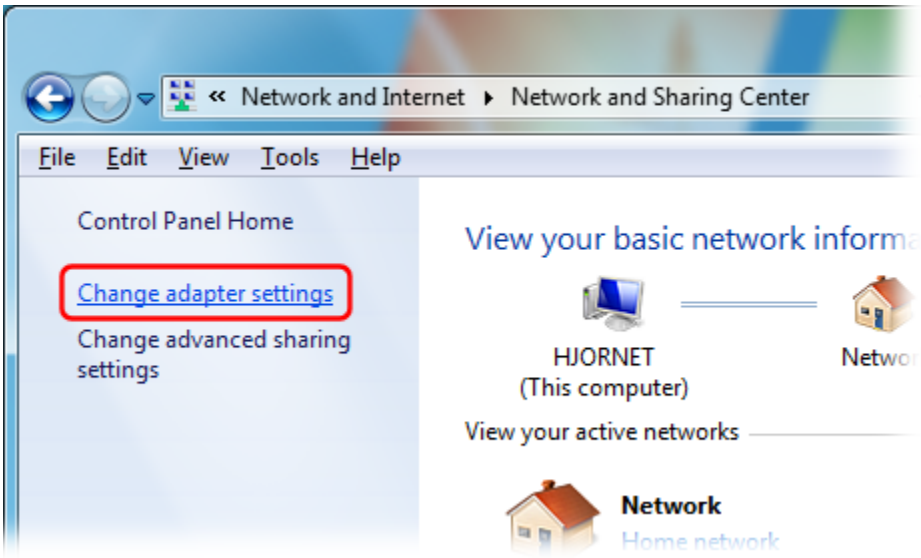
DNS Switching Pre-requisites

To ensure that the DNS switching feature works correctly and reliably, there are certain pre-requisites that are necessary. These are as follows:

1. Ensure that the OpenVPN TAP adapter name for your computer LAN (Local Area Network) settings 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":



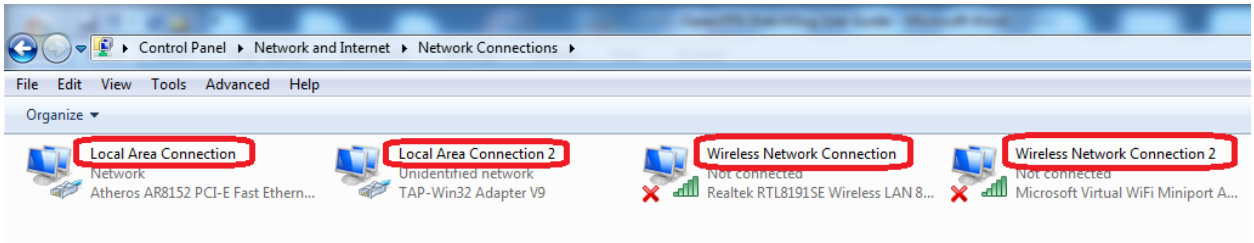
Click "Change adapter settings":



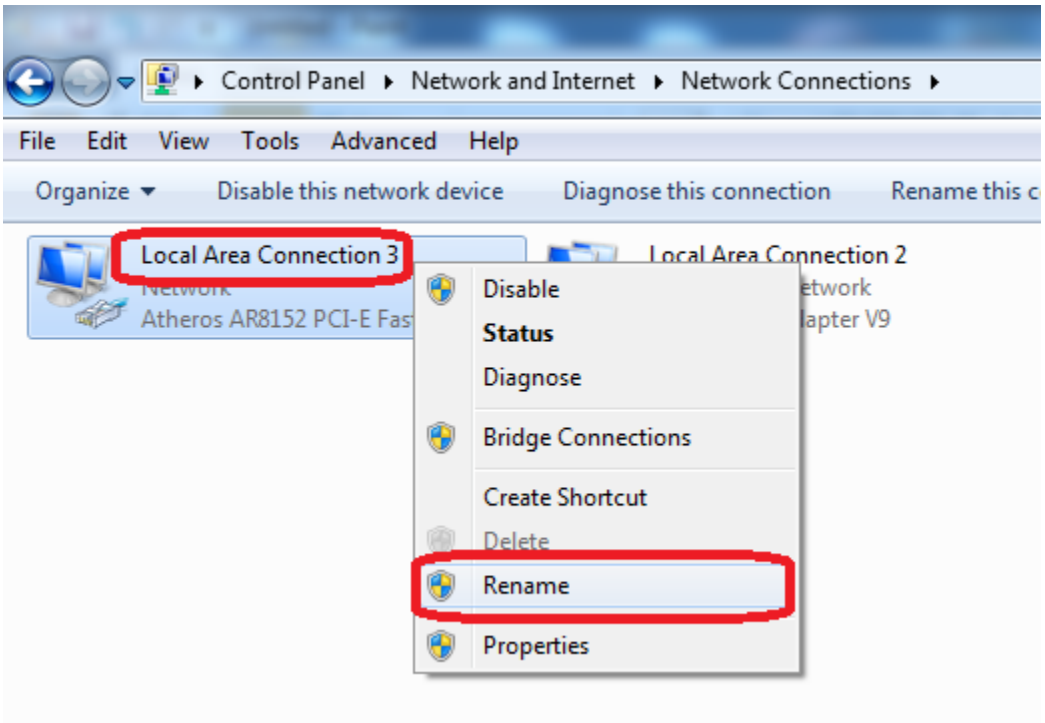
Then check the names of the Internet connection's icon as highlighted in the screenshot below. You can easily identify the active adapters by looking beneath the icons. Those will a red cross indicates that they are not active or in use. For example, as shown in the screenshot below, there are 2 active network

adapters; the LAN adapter for your normal internet connection and the TAP adapter for your OpenVPN connection.

The DNS switching function requires that the OpenVPN connection adapter name be " Local Area Connection 2"



If the name of the OpenVPN TAP adapter is not same as explained above, simply right click on the adapter and change the name.



2. If using Windows 7/Vista, ensure that you run the GUI with proper Administrative rights. This you can do by running the GUI as Administrator.

Preventing DNS and ARP Cache Poisoning by Clearing DNS and ARP Cache:

The GUI includes a feature to clear your DNS and ARP (Address Resolution Protocol) cache which effectively fixes DNS cache poisoning (which is a filtering method commonly used by ISPs to block access

to certain sites) and ARP cache poisoning. 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.

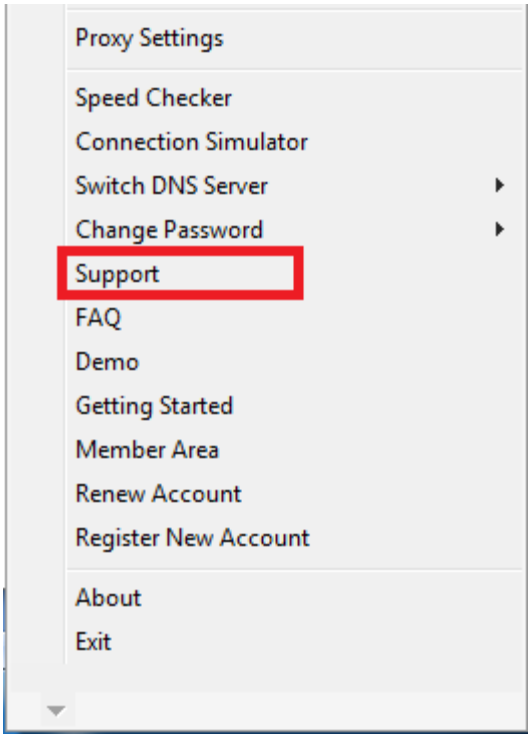
Thus in order to avoid this 5 minutes delay nuisance, you can simply click on the “Clear DNS and ARP cache” menu on the GUI under the “Switch DNS Servers” main menu to effectively clear the DNS resolver cache to remove any corrupted or poisoned DNS entries in your existing resolver cache.

On the other hand, the ARP Cache is a collection of ARP entries that are created when a hostname is resolved to an IP address and then an IP address is resolved to a MAC address thereby enabling the computer to communicate with the IP address. However, with time, ARP cache entries can become stale and it is possible for additional entries to the ARP cache table to be made without removing expired entries from the stored table. Eventually, this will result in errors that can significantly impact computer or network performance and can cause issues with Internet connections and Web page loading. Hence, by clearing the ARP cache, these issues can be resolved.

Important Tip: We recommend that you always clear your DNS and ARP cache before connecting to the VPN server. Doing this will help prevent certain internet connection and website resolution issues!

Contacting Support:

If you have any questions or issues with using the program, you can reach our support center URL by clicking on the “Support” menu in the OpenVPN GUI.



Software Warranty and Third Party Usage:

THIS SOFTWARE IS A FREE SOFTWARE BASED ON THE OPEN SOURCE OPENVPN CLIENT BY MATHIAS SUNDMAN.THE SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE OR USE ARE DISCLAIMED.

FREE UNRESTRICTED USAGE OF THE SOFTWARE IS PERMITTED FOR NON-SUBSCRIBERS OF ANONYPROZ OPENVPN SERVICES. HOWEVER, SOME FEATURES OF THE SOFTWARE MAY NOT WORK FOR THIRD PARTY USAGE. USE AT YOUR OWN DISCRETION.

Credits:

We are grateful to Mathias Sundman for the Open Source OpenVPN GUI without which this modified version of the GUI would not have been possible.

Last Modified: 27/12/2019

http://www.anonyproz.com