NETGEAR®

Connect with Innovation™

V7610

TELSTRA BUSINESS GATEWAY

VPN Configuration Guide

Date: Oct 16, 2015

Revision Num: 1.0

Revision History

Date	Release	Author	Description
Oct 16, 2015	1.0	Hardie Zhang	Initial Release

TABLE OF CONTENTS

1. Introduction

The V7610 gateway's VPN server feature supports both remoteclient-to-GW and site-to-site VPN tunnels using IPsec IKEv1 (PSK/XAuth) as well as IPsec IKEv2 (Certs). This document outlines the various configurations needed to have VPN working in these two modes. In the following sections, detailed steps along with screen shots (where needed) are furnished to help you configure the VPN feature on the V7610 gateway as well as configure various clients to work with the gateway.

2. VPN Connection Type

The V7610 gateway supports the types of VPN connections described in the following sections:

2.1 Remote Client-to-Gateway VPN

In this mode, the V7610 (GW) connects to the public network either through DSL or a WAN uplink. Remote users on the Internet can create an IPSec tunnel from their computers to the GW using the WAN IP address of the GW. Once connected, the remote user can access the LAN-side resources of the GW.

Currently the GW supports and has been tested to work with the following clients:

a. Windows 7 clients using IKEv2 Certs
b. Inbuilt Cisco VPN clients in MAC OS
c. Inbuilt VPN clients in Android and iOS

2.2 Site-to-Site VPN

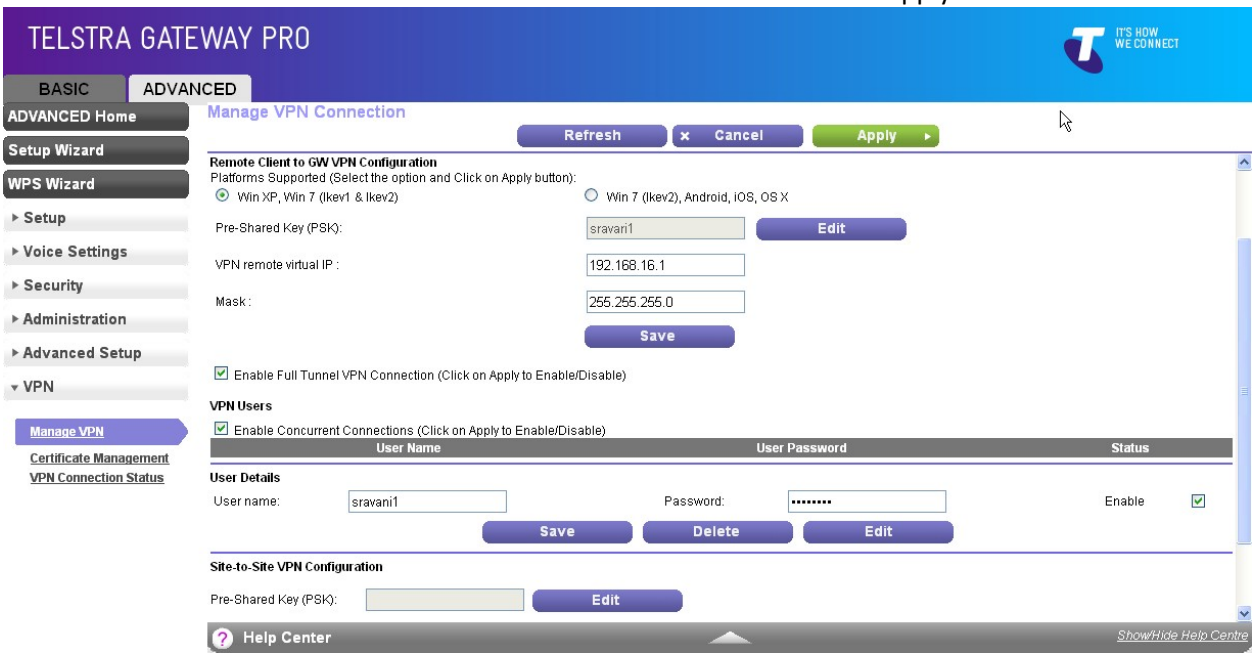
Similar to the remote client-to-gateway VPN configuration, an IPSec tunnel can be established between two GWs. In this configuration, the LAN-side users of either GW can access the other through the site-to-site VPN tunnel. When you configure the site-to-site VPN tunnel, each GW has a unique IP address range for its LAN side.

3. Remote Client to GW Configuration

This section describes the connection configuration details for the remote client-to-GW connection type.

3.1 Configuring the Gateway

- **Adding Remote VPN Users**
  - Select VPN > Manage VPN from the ADVANCED tab.
  - Under VPN users, click Add
  - In the User Details section, enter the user name and password, select or clear the Enable check box, and click the Save button.
  - Add as many users (a maximum of 10) as needed following the previous steps and click Save.
  - To enable concurrent connections to the user login credentials, select the "Enable Concurrent Connections" check box and click the Apply button.



- **b) VPN Connection Information**

  - At the top of the Manage VPN Connection page, click the Edit button next to the Pre-Shared Key field. Enter a pre-shared key that will be used for the Phase 1 negotiation and click the Save button next to the Pre-Shared Key field. Only one key can be used. All end users will share this same key. The key can be any ASCII character string with a minimum length of 8 characters and maximum length of 32 characters. Only alphanumeric characters are allowed. Spaces and special characters cannot be used.

  - In the VPN remote virtual IP field, enter an IP address and mask and click Save. This is the range of IP addresses that the remote clients will be configured with

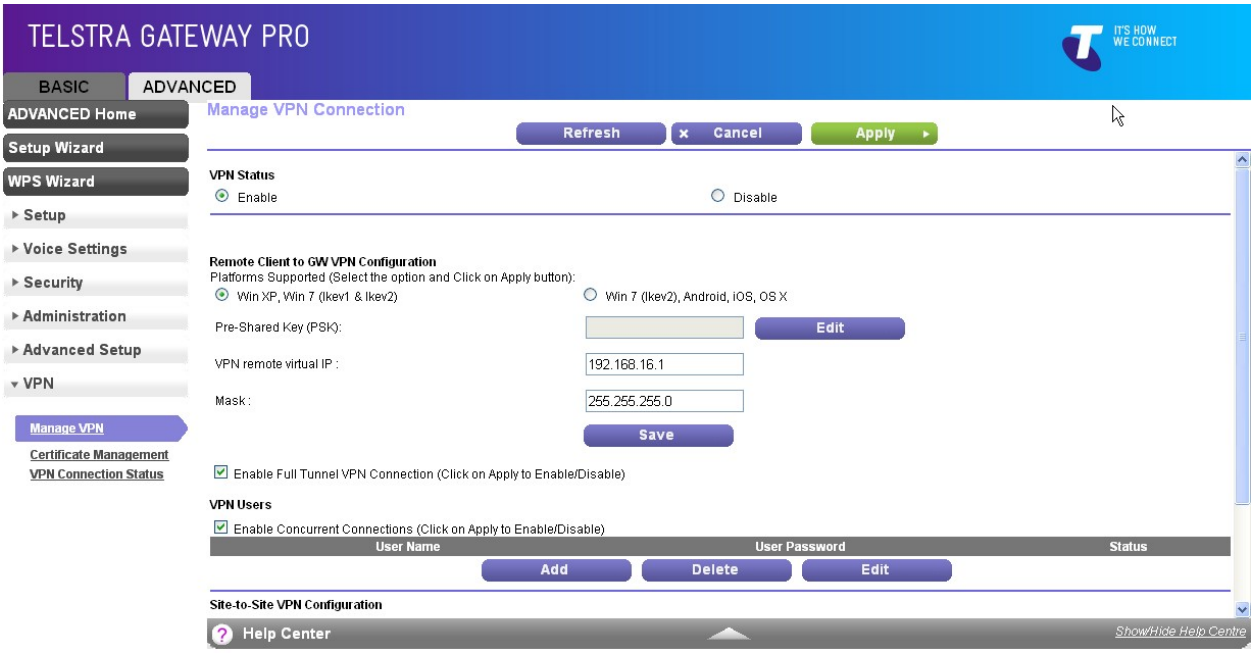
when the VPN tunnel is set up. Note that this range must not be in the range of LAN IP addresses set up for the V7610 device.

- ### c) Platforms Supported

a) If Windows 7 remote client-to-GW configurations are to be supported, then select the Win 7 (Ikev1 & Ikev2) radio button under Platforms Supported and click Apply.
b) If Windows 7 using Certs, Android, iOS and MAC OS remote client-to-GW configurations are to be supported, then select the Win 7 (Ikev2), Android, iOS, OS X radio button under Platforms Supported and click Apply.

- ### d) VPN Status

  - Select the Enable radio button on the top section of the page and hit on Apply.



At this point, the remote client to GW VPN server feature is configured and running on the device.

To stop the VPN server running on the device, select the Disable radio button in the top section of the page and click Apply.

3.2 Configuring the Remote Client – Android Platform – Native VPN Client

To use the native Android VPN client, you must manually configure the Android VPN client settings to match the settings configured on the gateway.

To manually configure the native VPN client on the Android device:

a) On the Settings page, in the Wireless & Networks section, select More and then tap VPN.

b) Tap Add VPN Network. The Edit VPN network page appears.

c) Configure the following settings in the Edit page:

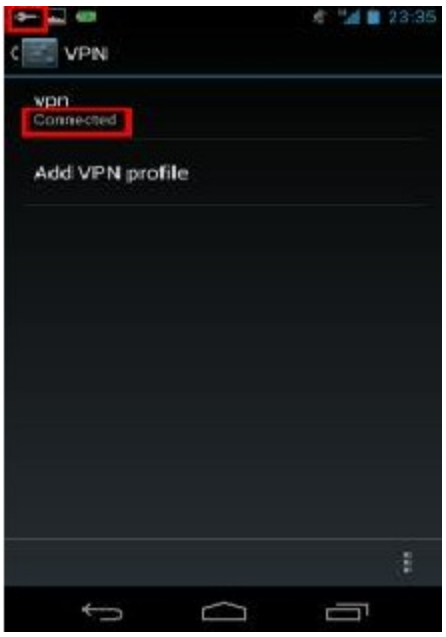
- **Name** — Enter a name to identify this VPN connection on the Android device.
- **Type** — Select IPSec Xauth PSK.
- **Server address** — Enter the WAN IP address of the gateway.
- **IPSec Identifier** —Leave this blank.
- **IPSec pre-shared key** — This is the secret used while the tunnel is being established. Enter the remote client-to-GW pre-shared key configured in the gateway.

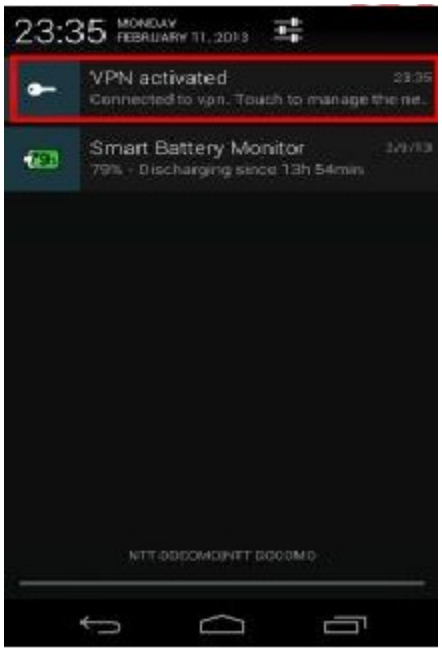
d) Tap Save.

e) Tap the VPN connection you created and type the user name and password configured in the gateway in the Username and Password fields as shown in the following screen shot.

f) Tap Connect to start the VPN connection.

g) After the VPN connection is established, the string Connected is displayed corresponding to the VPN connection settings, and the status indication area of Android shows the VPN activated message. You can tap the message to see the current status of the VPN connection.





h) At this point, your Android client device can access the LAN-side resources of the V7610 GW including access to the V7610 web interface.

i) To disconnect the VPN connection, tap VPN Connected and select Disconnect. The VPN is disconnected.

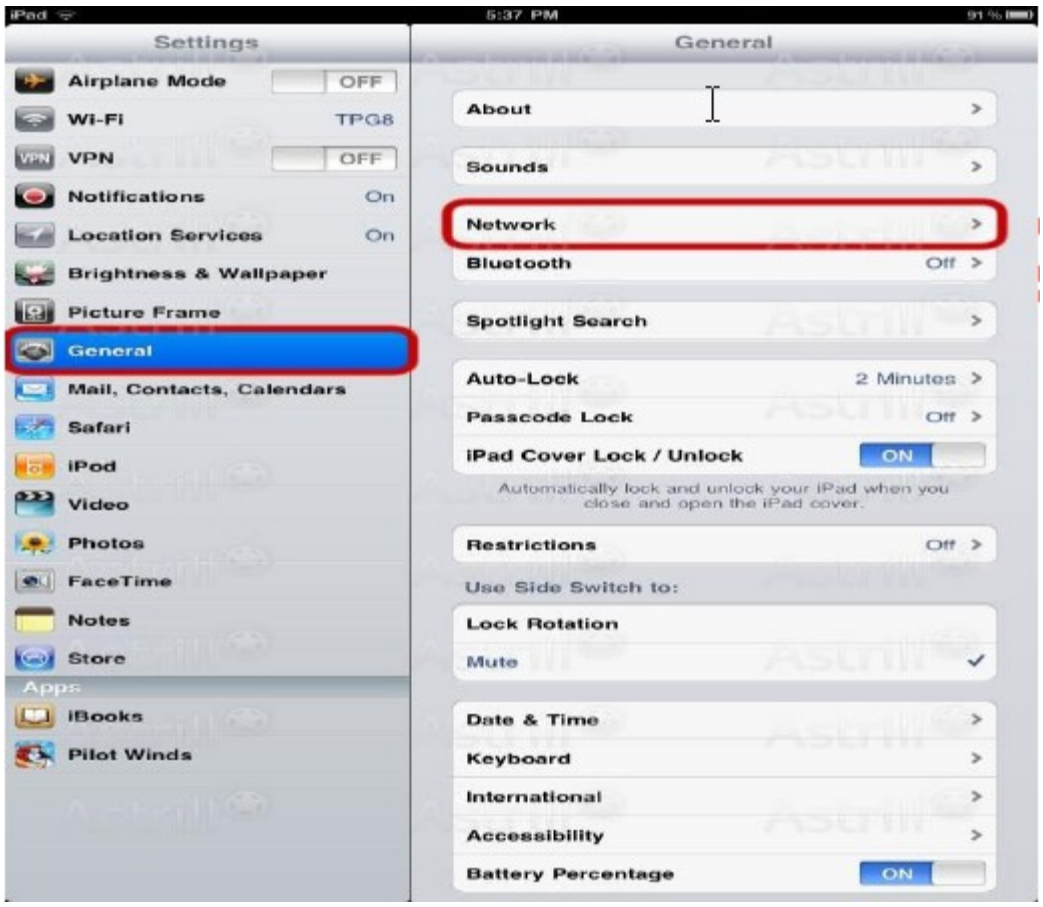
Note: The client configuration navigation may vary for different versions of Android.

3.3 Configuring the Remote client – iOS Platform – Native VPN Client

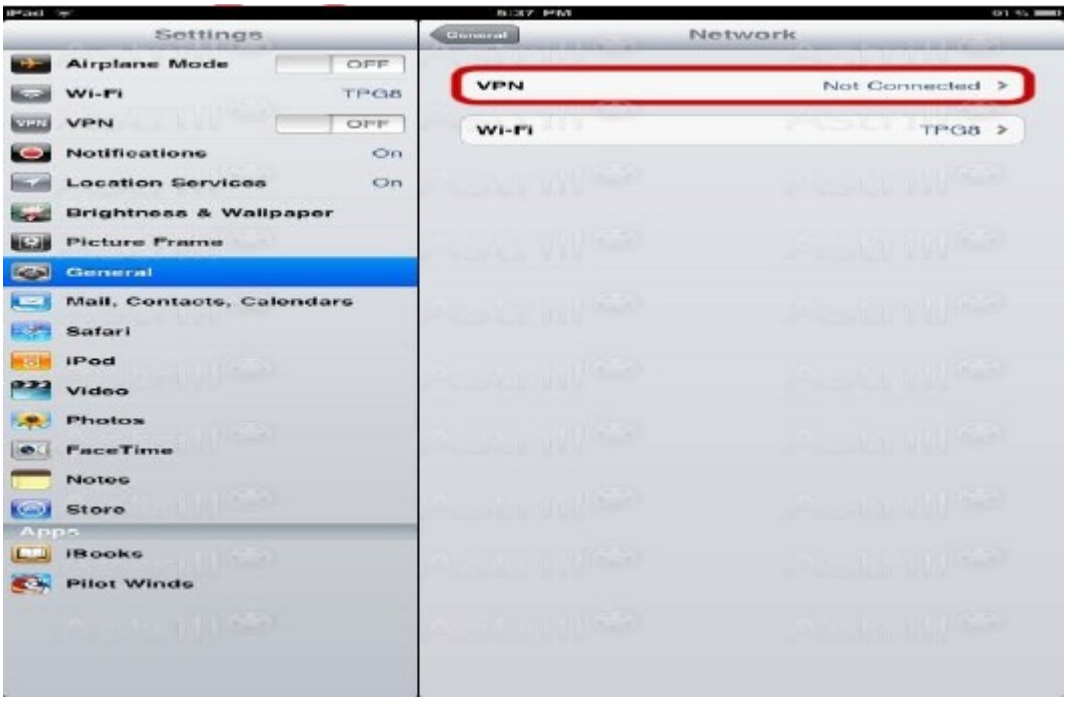
To connect the remote iOS client to the V7610 gateway, you must configure the settings as follows:

a) On the main screen tap the Settings icon as shown in the following screen shot.

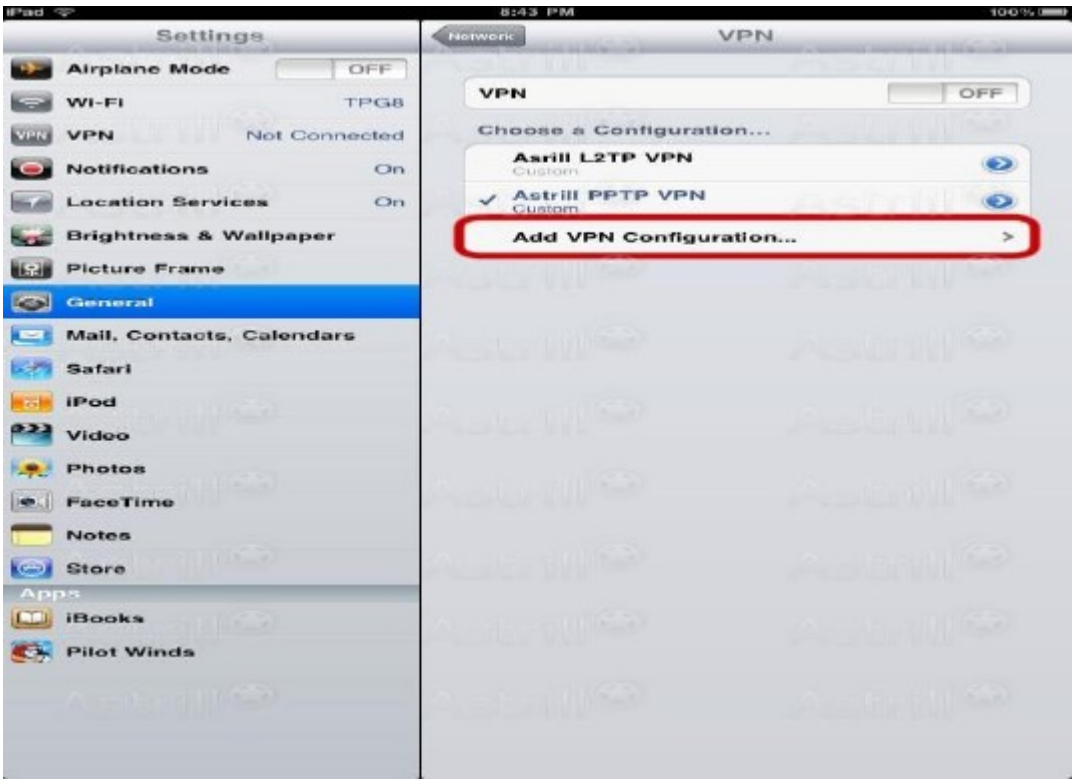
b) Tap General, and then tap Network.


iPad
5:37 PM
91 %
Settings
Airplane Mode
OFF
Wi-Fi
TPG8
VPN
OFF
Notifications
On
Location Services
On
Brightness & Wallpaper
Picture Frame
General
Mail, Contacts, Calendars
Safari
iPod
Video
Photos
FaceTime
Notes
Store
Apps
iBooks
Pilot Winds
General
About
Sounds
Network
Bluetooth
Off
Spotlight Search
Auto-Lock
2 Minutes
Passcode Lock
Off
iPad Cover Lock / Unlock
ON
Automatically lock and unlock your iPad when you close and open the iPad cover.
Restrictions
Off
Use Side Switch to:
Lock Rotation
Mute
Date & Time
Keyboard
International
Accessibility
Battery Percentage
ON

c) Tap on VPN.


Settings
Airplane Mode
OFF
Wi-Fi
TPG8
VPN
OFF
Notifications
On
Location Services
On
Brightness & Wallpaper
Picture Frame
General
Mail, Contacts, Calendars
Safari
iPod
Video
Photos
FaceTime
Notes
Store
Apps
iBooks
Pilot Winds
General
Network
VPN
Not Connected
Wi-Fi
TPG8

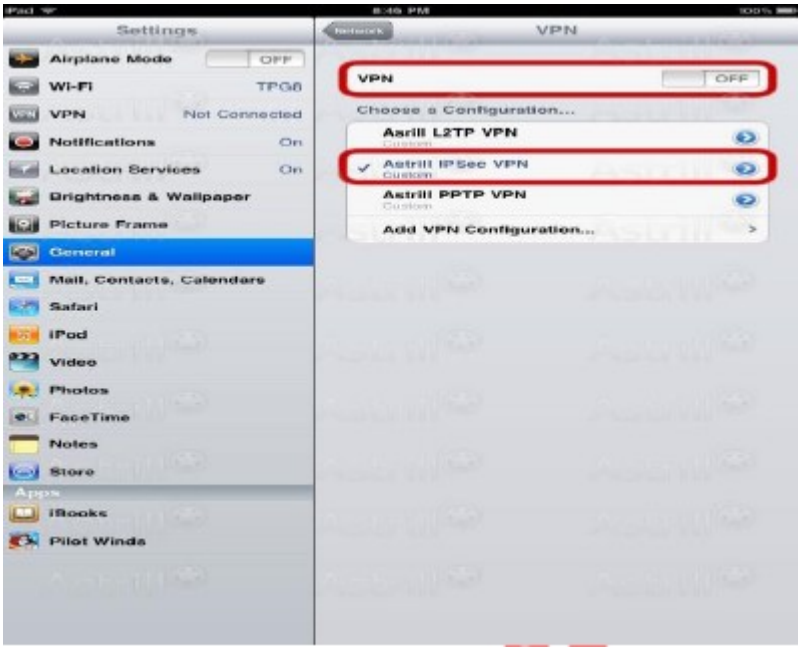
d) Under VPN you can add as many VPN connections as you need. Tap Add VPN Configuration as shown below.



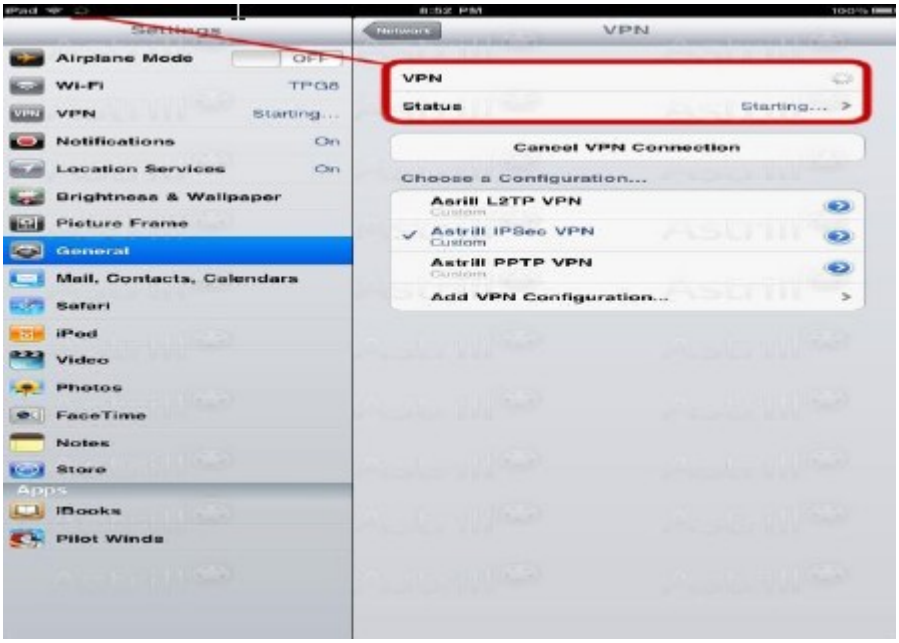
e) Configure the settings as follows:

- Tap IPSec.
- In the Description field, enter a name, for example, Astrill IPSec VPN. This is the name of your VPN connection.
- In the Server field, enter the WAN IP address of the gateway.
- In the Account field, enter the user name.
- In the Password field, enter the password.
- This user name and password should be the ones configured in the gateway. In the Secret field, enter the PSK configured for the remote client-to-GW VPN
- configuration in the gateway.
- Tap the Save button.

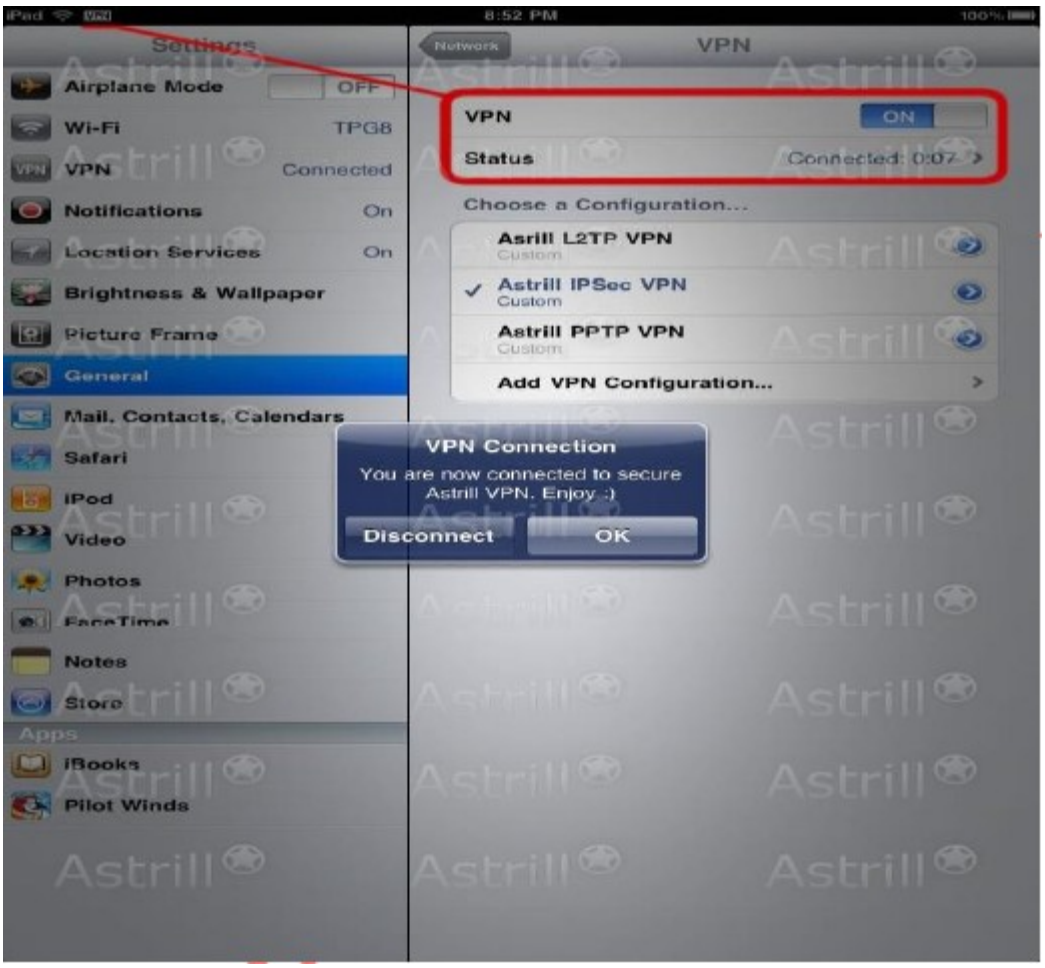
f) Tap Astrill IPSec VPN to select the VPN connection you created, then slide the VPN OFF button to turn VPN on.



g) You will now see the status change from Starting..., Connecting..., and Authenticating...



h) When the connection is established, you see the VPN icon in the title bar. This indicates that the VPN connection is on.



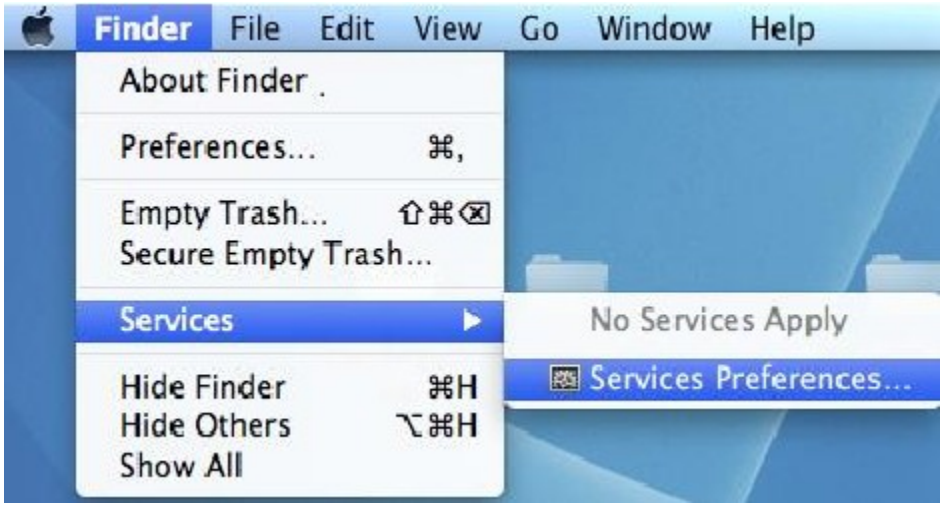
i) At this point, the remote iOS client device can access the LAN-side resources of the V7610 GW including access to the V7610 web interface.

j) To disconnect the tunnel established, slide the VPN ON button to turn VPN off.

Note: The client configuration navigation may vary for different versions of iOS.

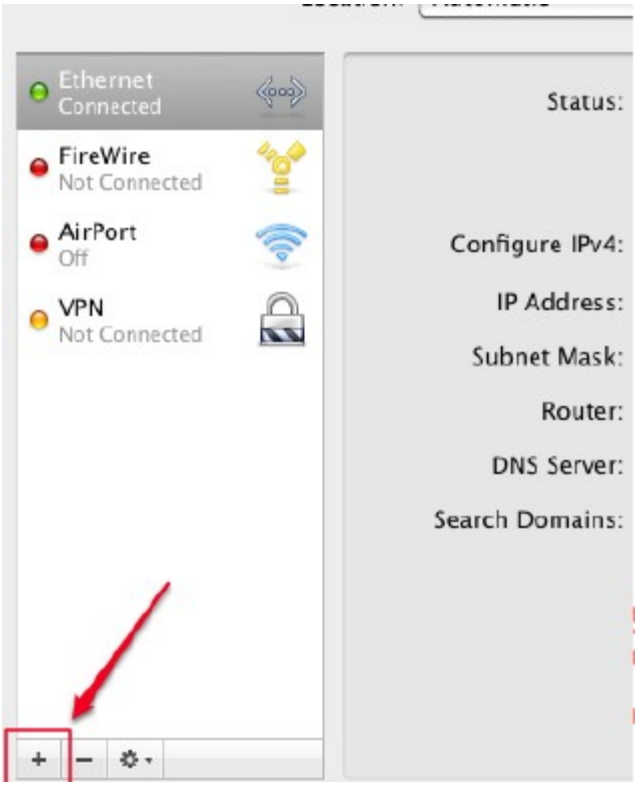
3.4 Configuring the Remote client –Mac OS Platform – Native Cisco VPN Client

a) Select Finder on the menu bar and select Services. Select Service Preferences.

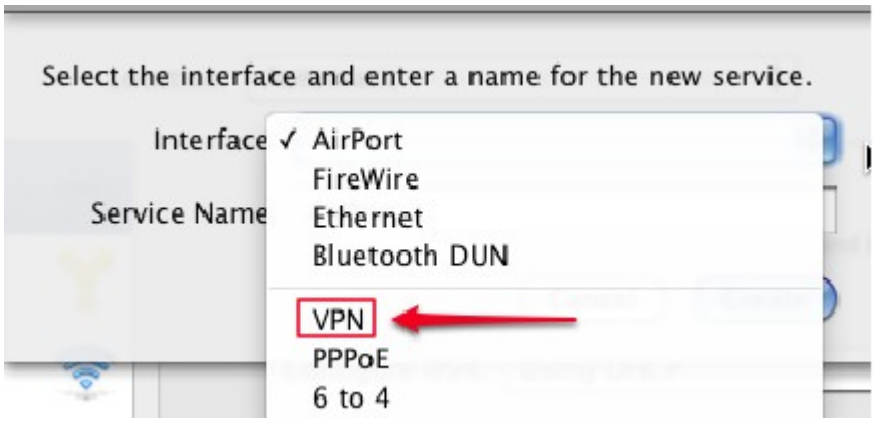


b) Click Show All on the top pane and click the Network icon.

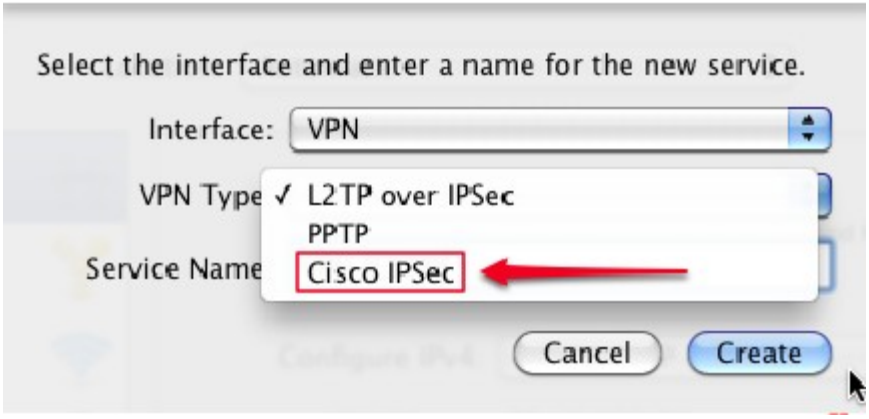
c) On the Network screen, click the + symbol in the lower left:



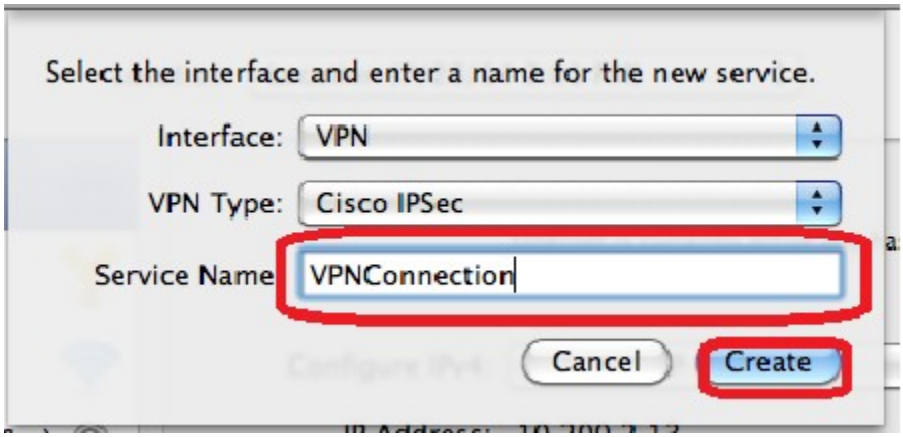
d) In the pop-up window that appears, select the VPN interface as shown below:



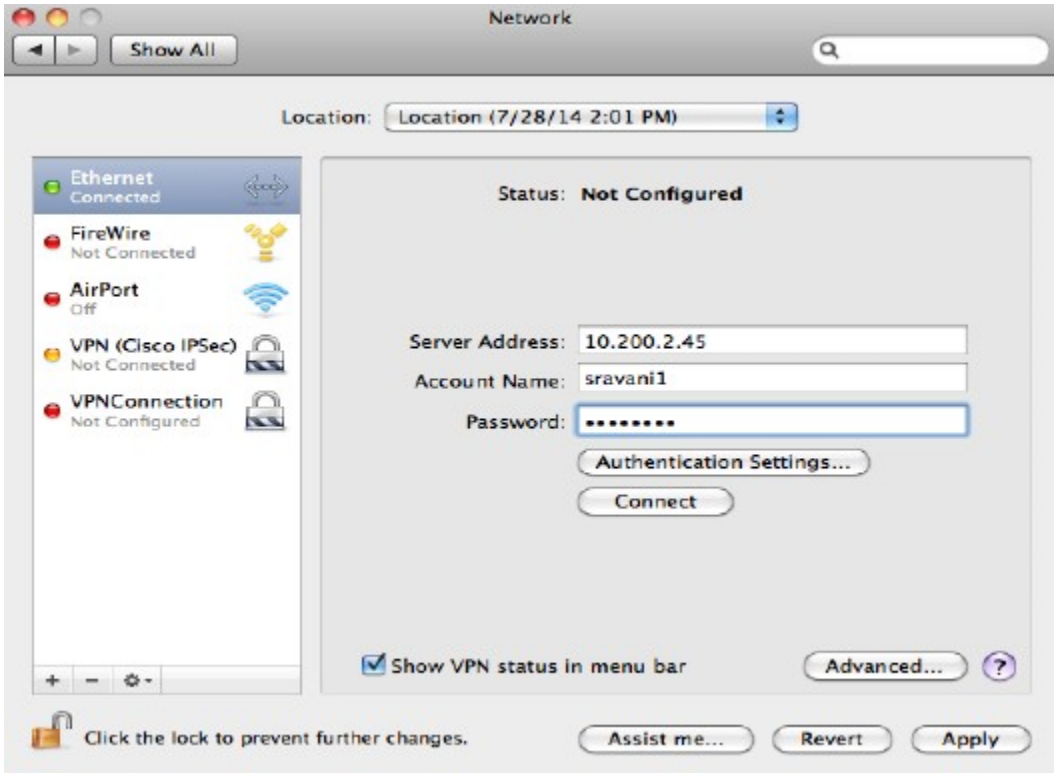
e) Click the VPN Type menu and select Cisco IPSec:



f) Provide any VPN connection name in the Service Name field and click Create.

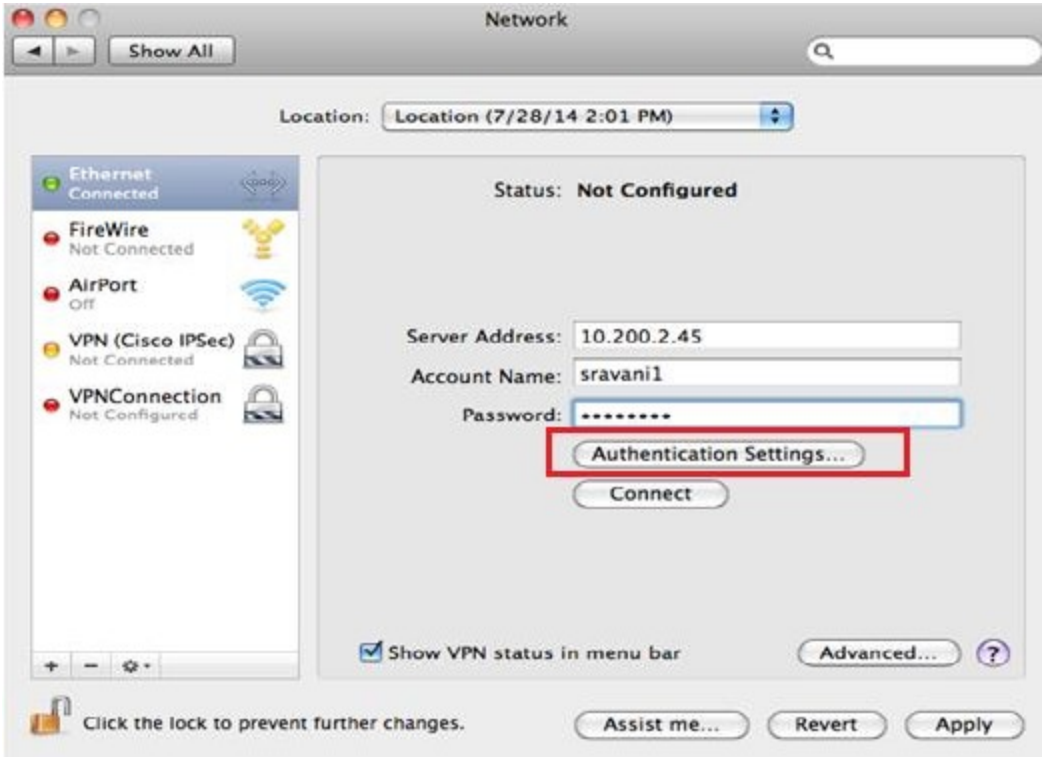


g) You return to the main Network screen. Click your new VPN name (VPNConnection in this example) in the list on the left side.
h) Enter your gateway WAN IP address in the Server Address field.
i) Enter the user name and password configured in the gateway (under VPN Users) in Account Name and Password fields.



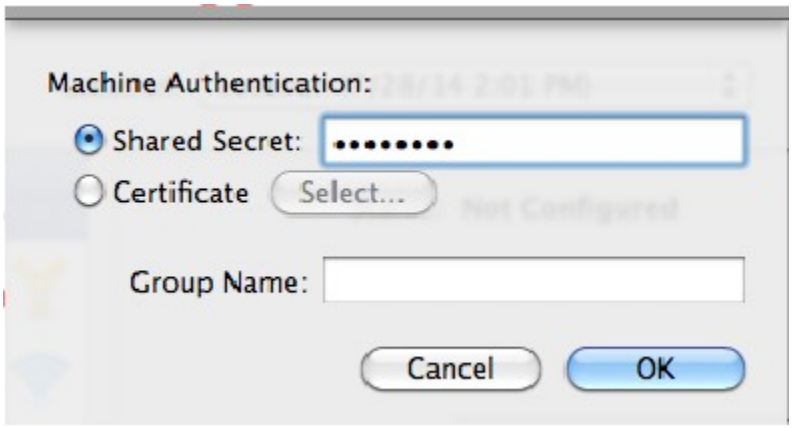
j) Select the Show VPN status in the menu bar check box. A new menu bar icon appears that allows you to quickly turn the VPN connection on and off.

k) Click the Authentication Settings button.

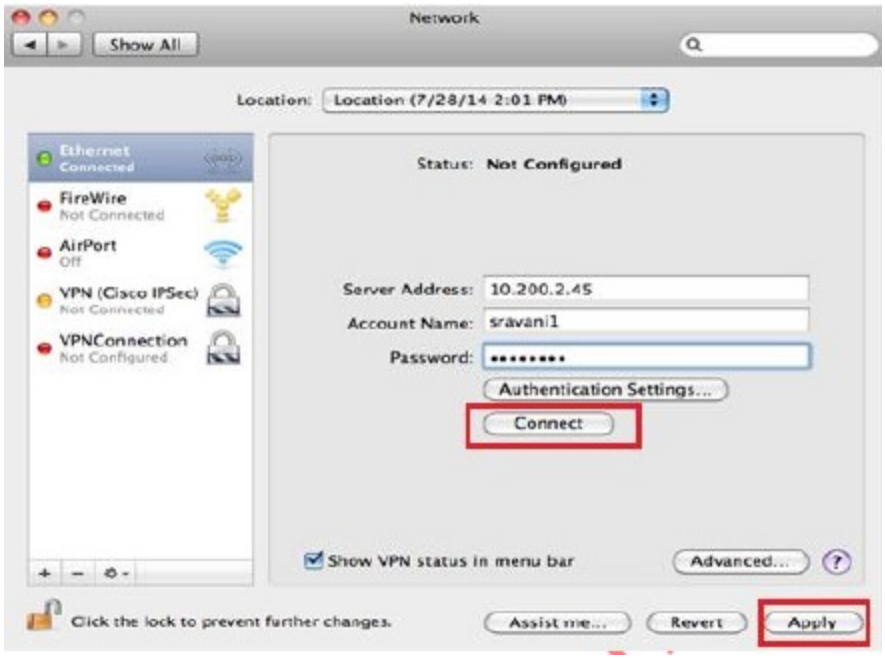


l) Select Shared Secret and enter the pre-shared key (configured under Remote Client to GW Configuration in the Gateway) in the Shared Secret field.

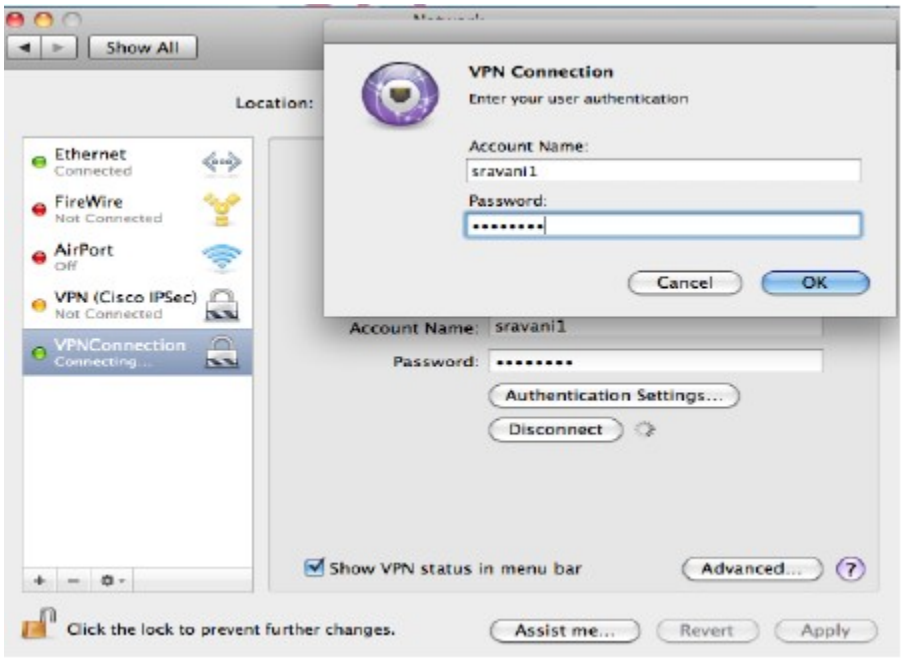
m) Leave the Group Name field blank. Click OK.



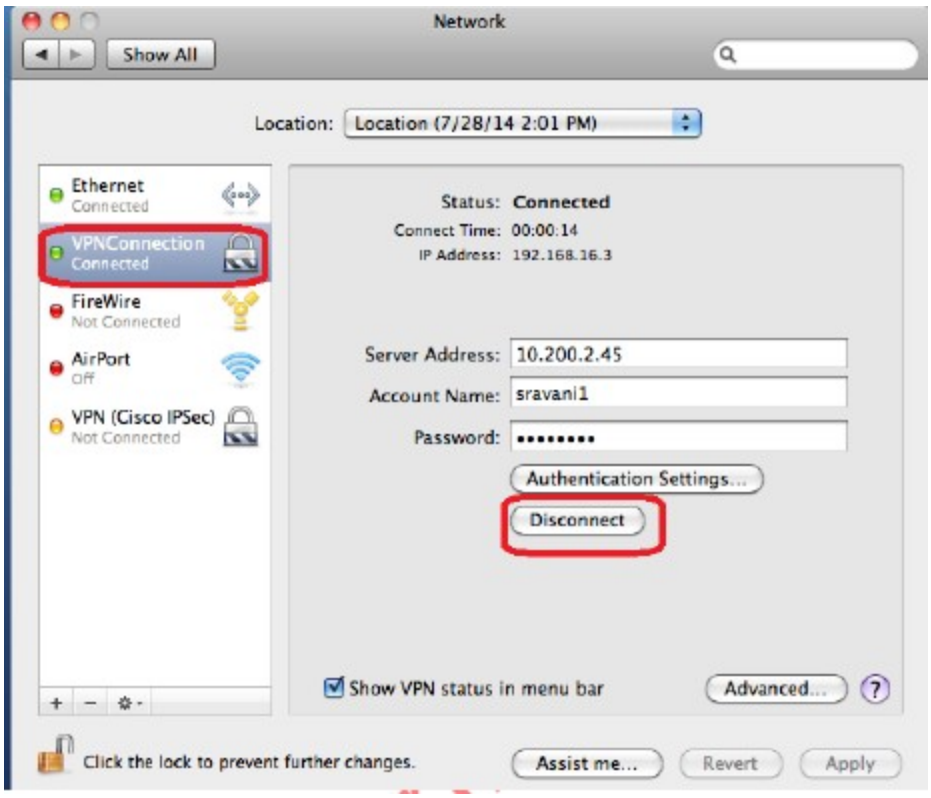
n) Now Click the Apply button and then click Connect.



o) Enter the password configured in the gateway (under VPN Users) in the Password field and click OK



p) The VPN connection starts, and Connected displays when the connection is successful. Successful connection is indicated with green icon as shown in the following screen shot.



q) If the Mac VPN client is connected, the remote Mac client device can access the LAN-side resources of the V7610 GW including access to the V7610 web interface.

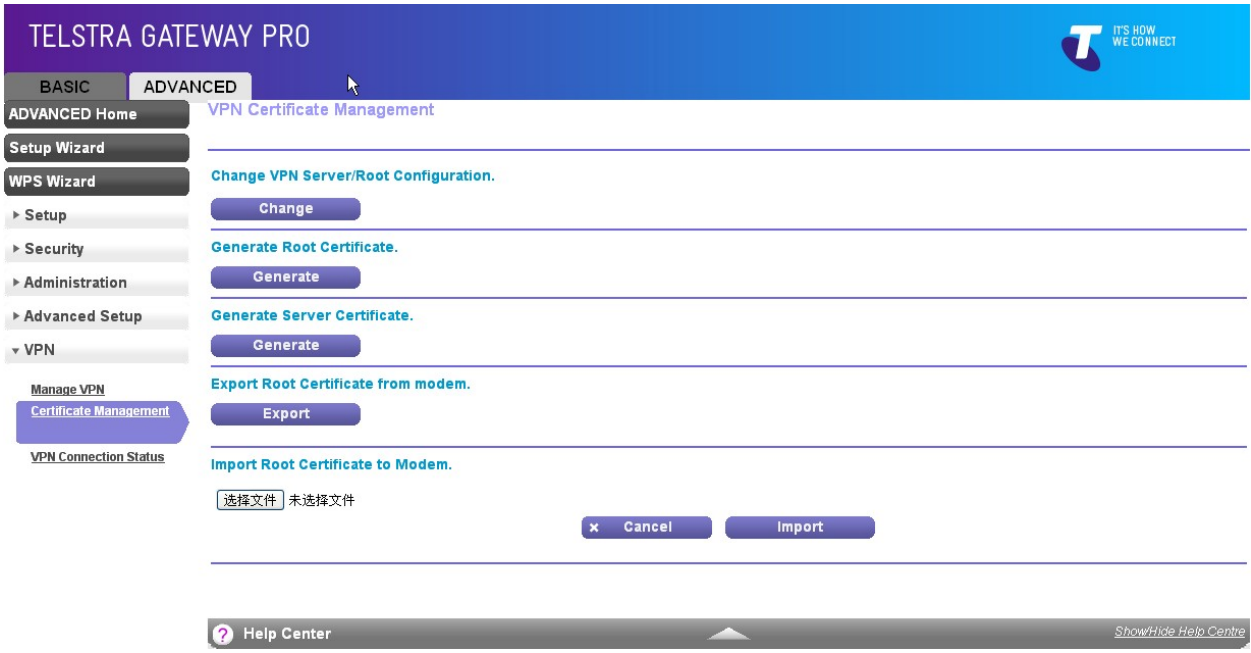
r) To disconnect the VPN tunnel, click the Disconnect button as shown above. The VPN is disconnected.

3.5 Windows 7 Using Certificates

3.5.1 Configuring the Gateway

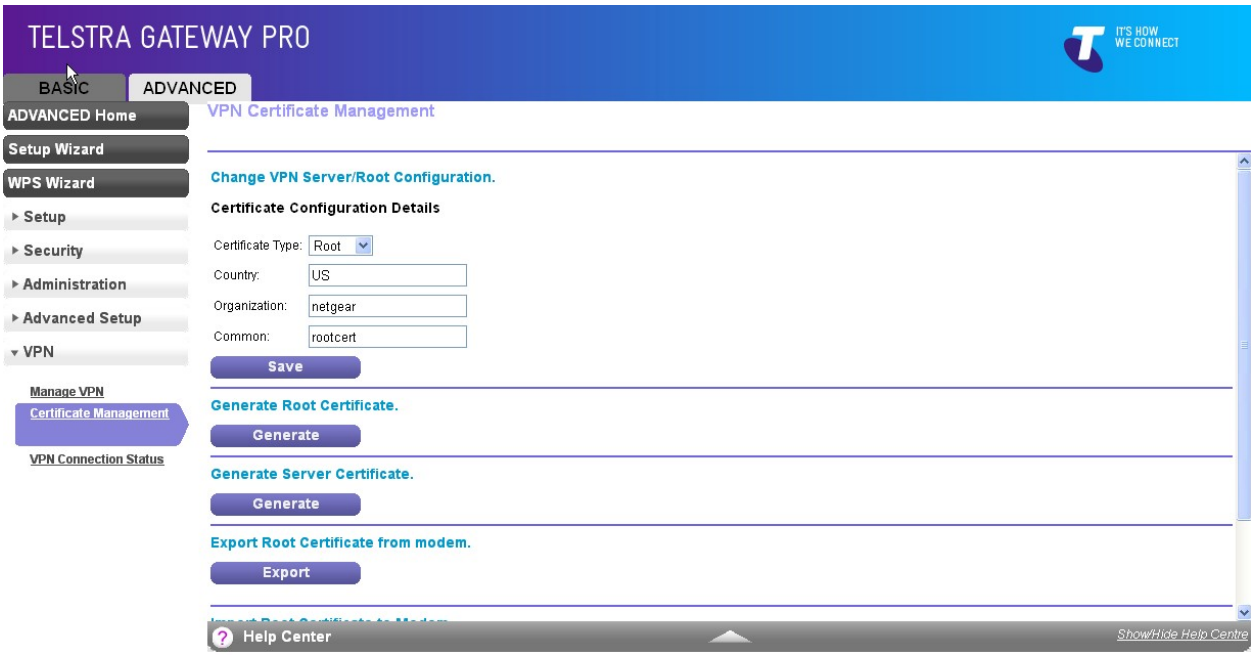
a) Go to Advanced > VPN > Certificate Management in the gateway web interface.

b) Click the Change button under Change VPN Server/Root Configuration.



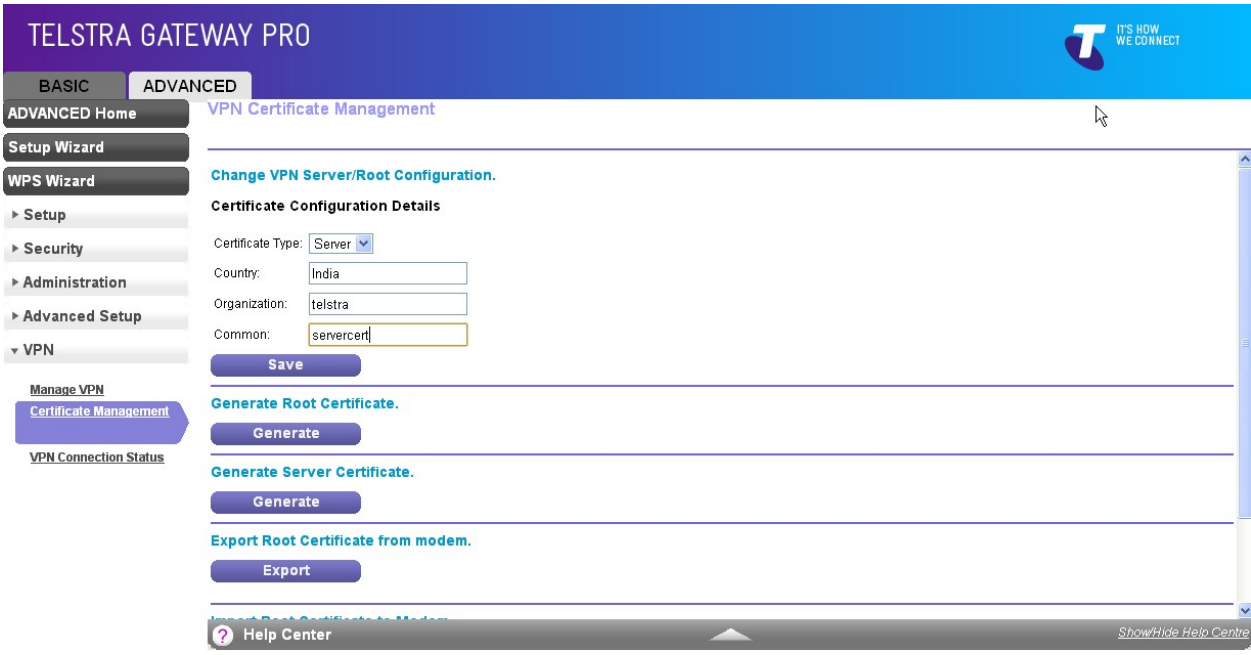
c) In the Certificate Type list, select Root.

d) Complete the Country, Organization, and Common (any unique text for the certificate generation) fields and click the Save button. For example: Country – US, Organization – netgear, Common – rootcert.



e) In the Certificate Type list, select Server.

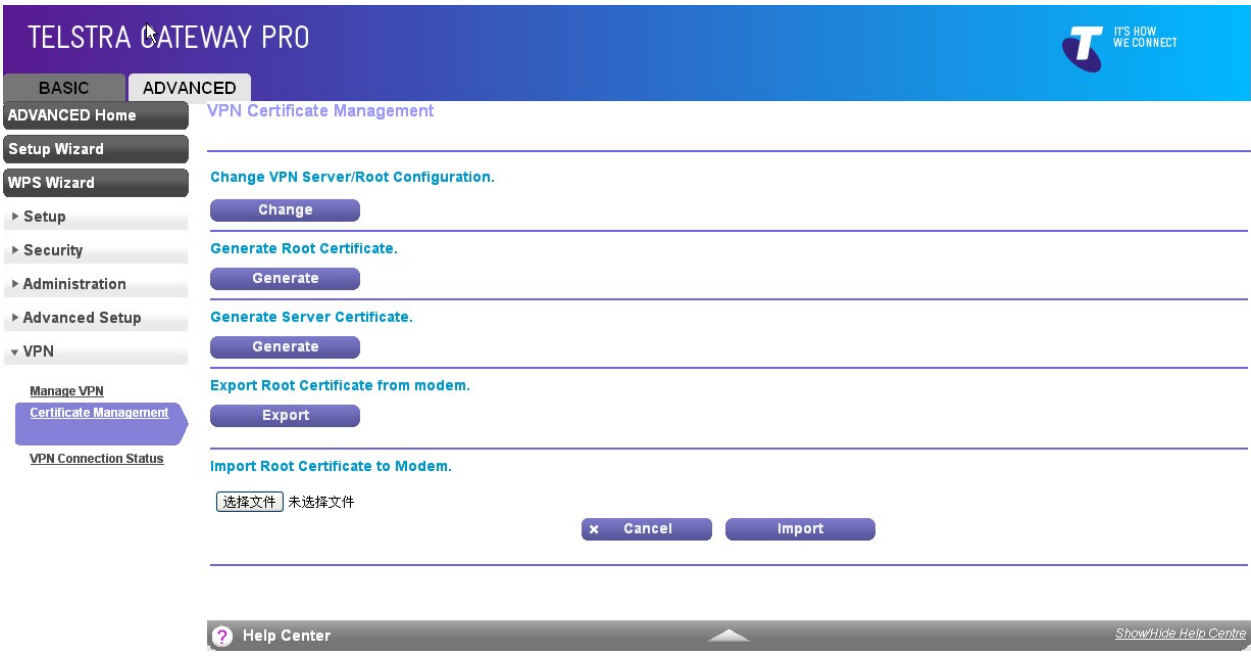
f) Complete the Country, Organization, and Common (any unique text for the certificate generation) fields and click the Save button. For example: Country – India, Organization – Telstra, Common – servercert.



g) Click the Generate button under Generate Root Certificate.

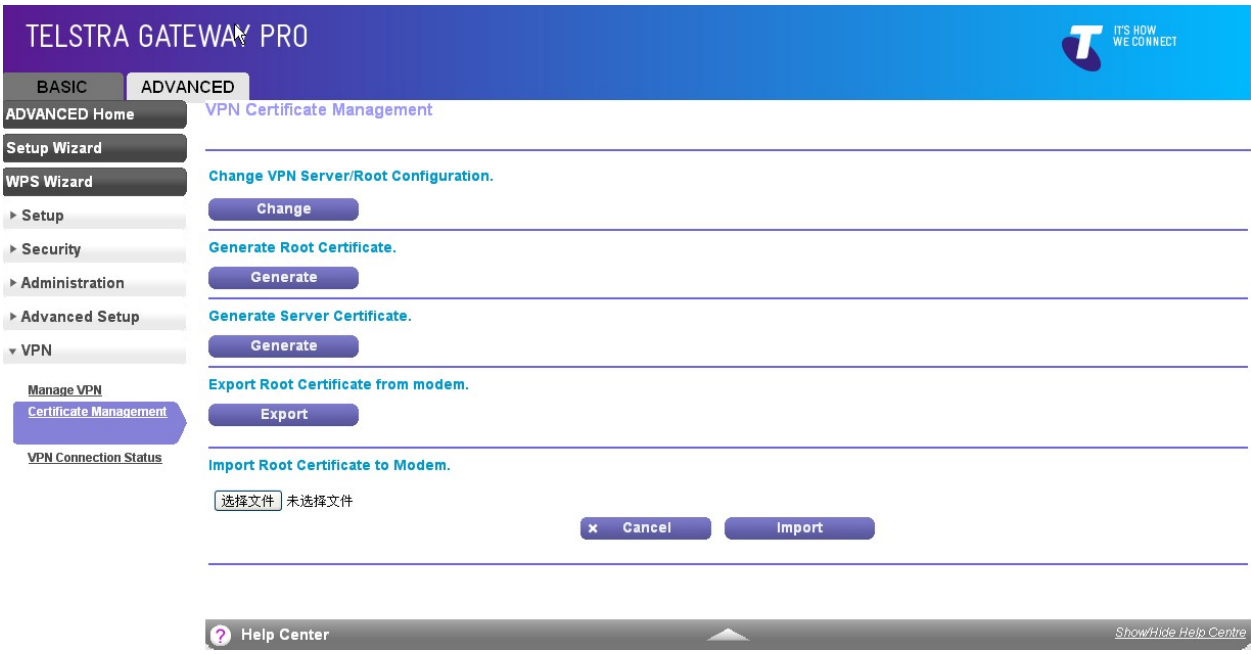
h) Click the Generate button under Generate Server Certificate.

i) Click the Export button under Export Root Certificate from modem and save the file on the local hard drive. This is the certificate that will be used on your Windows 7 computers for the VPN connection through IKEv2 Certs.



If you reset the V7610 gateway to factory defaults, the certificates generated are lost. It is possible to import the root certificate from a client computer back into the V7610. You can use the Import button on this page to restore the VPN root certificate.

j) For you to import the root certificate to the modem, a computer with the root certificate must be connected on the LAN side of the product. Click the Browse button (as shown below) and select the root certificate saved on the hard drive.



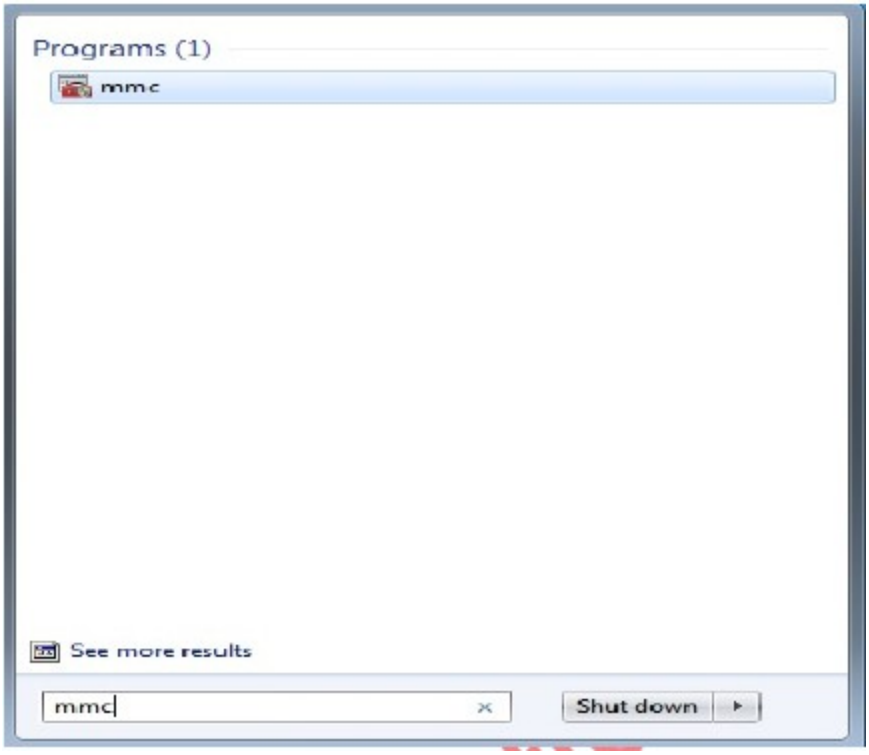
k) Click the Import button to import the selected certificate.

l) Generate the server certificate by configuring the server details (Country, Organization, and Common fields) as shown in Step f.

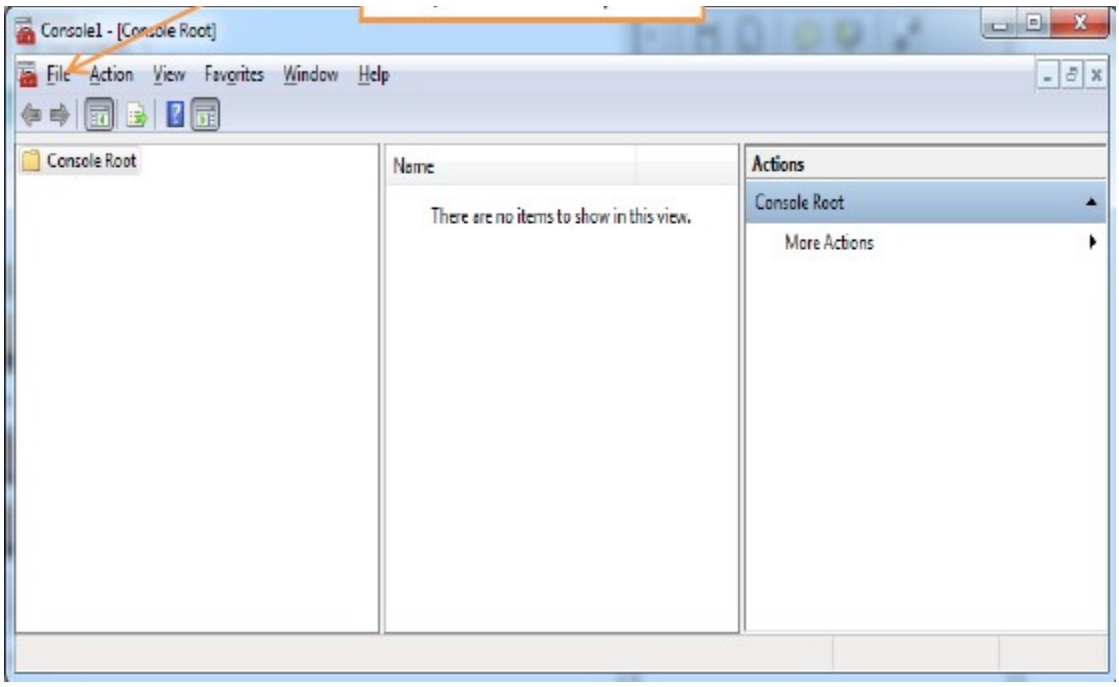
3.5.2 Configuring the Remote Client – Windows 7 Platform – Using Certificates

3.5.2.1 Storing a Windows 7 Machine Certificate

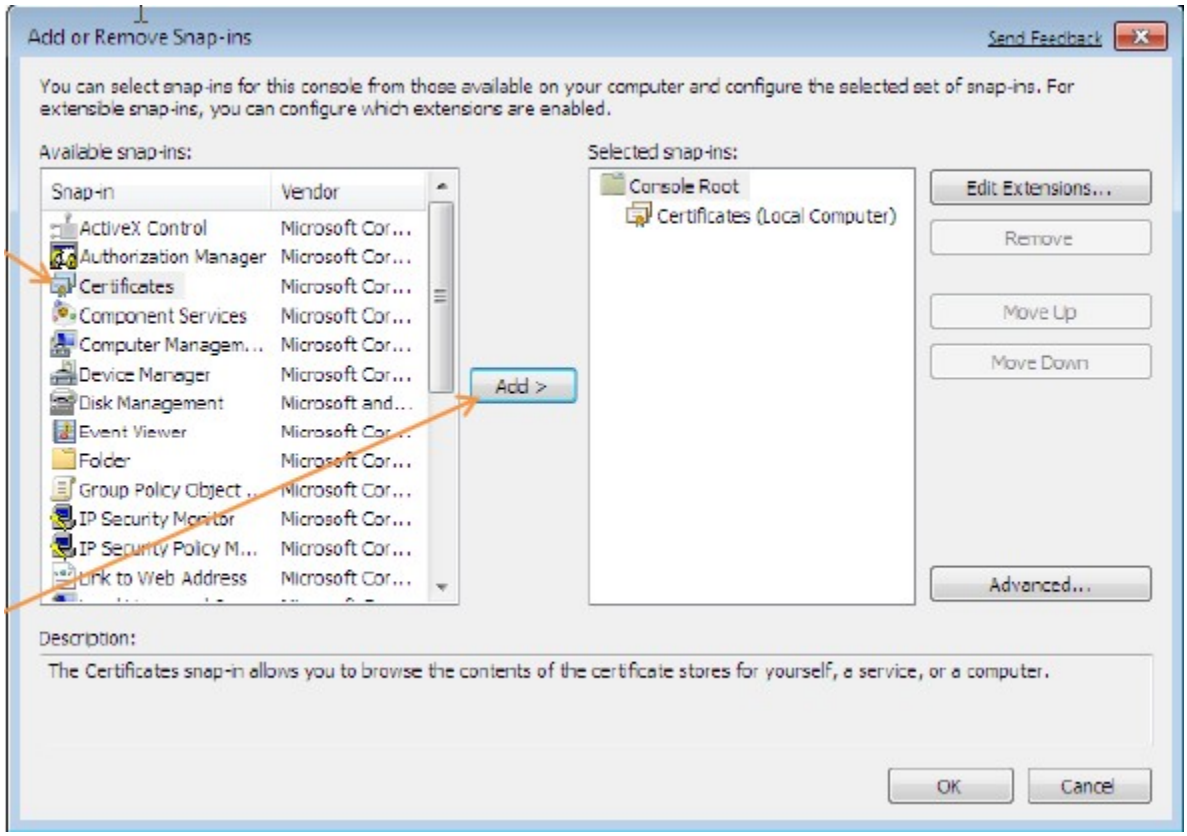
a) Select Start > Run, type mmc, and press Enter.



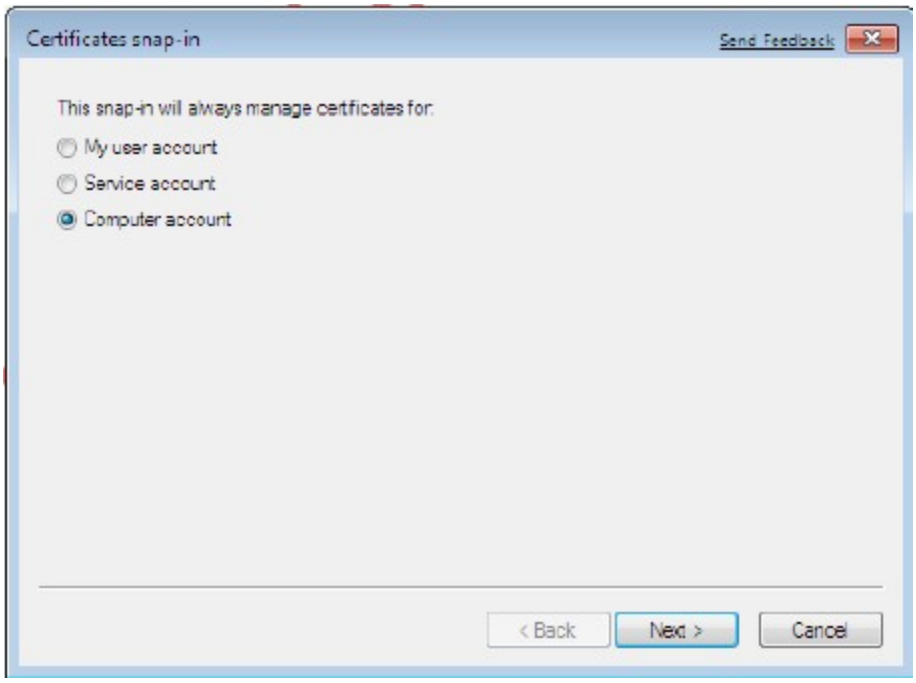
b) Click File and then select Add/Remove Snap-in as shown below.



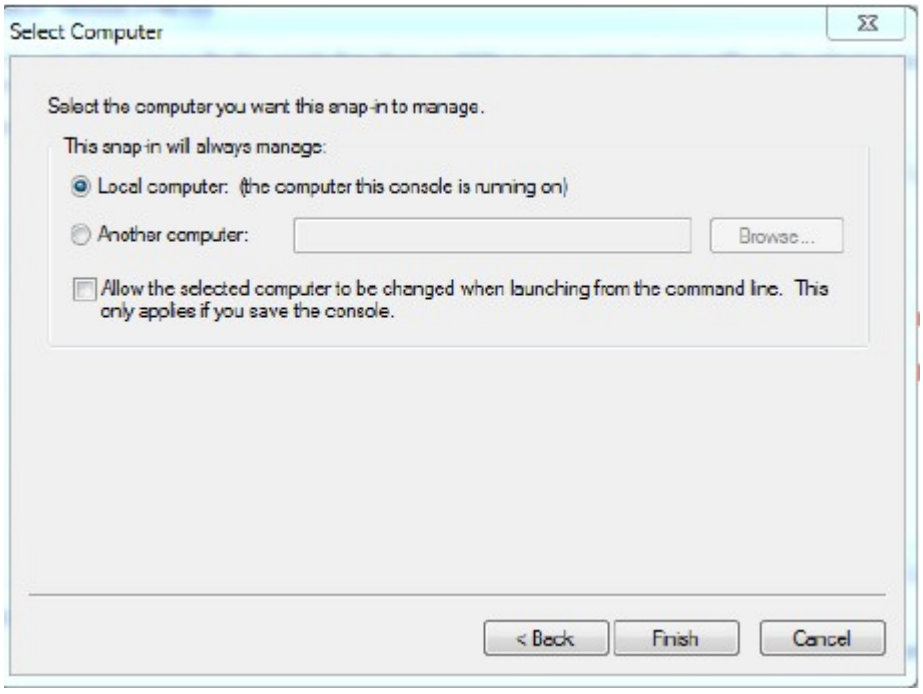
c) Select Certificates and click Add as shown below.



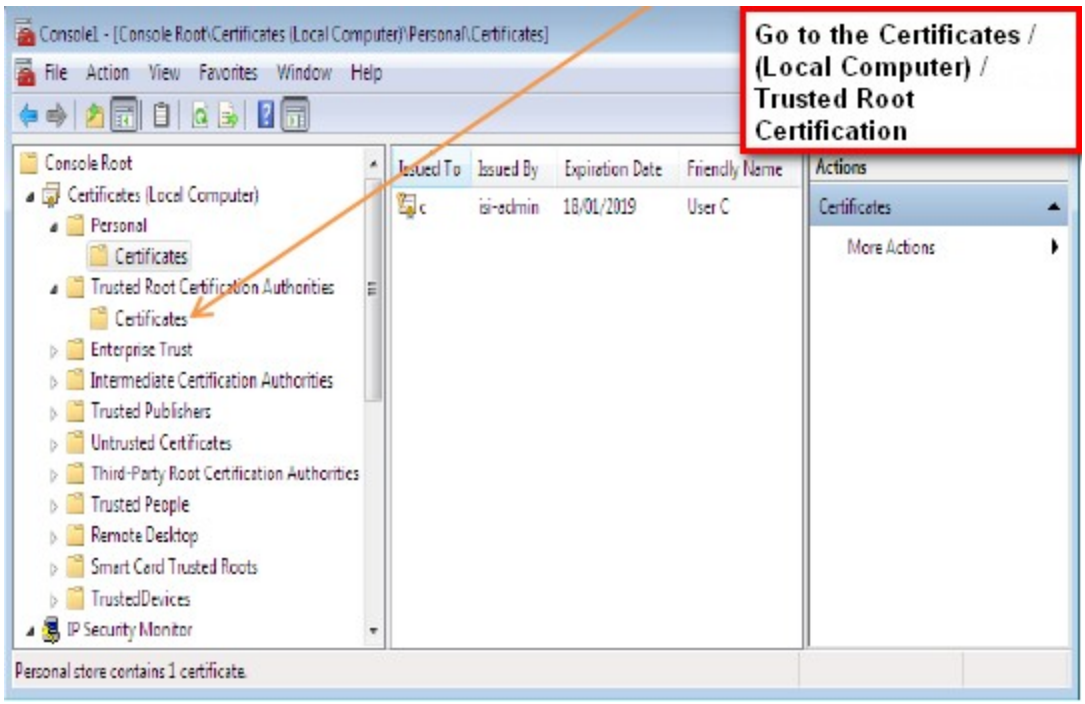
d) In the screen that displays, select the Computer account radio button and click Next.



e) Click Finish. Then click OK.

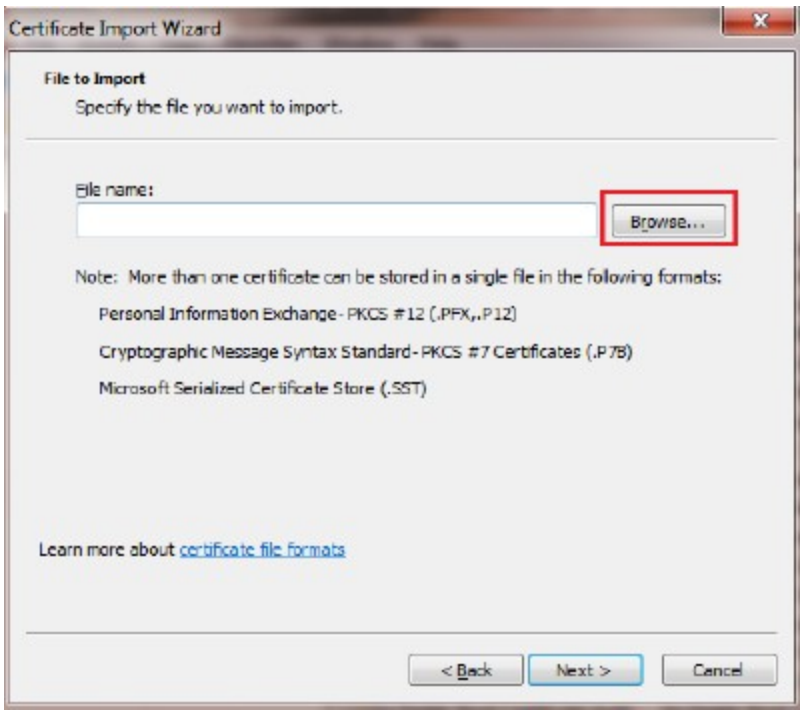


f) Under Trusted Root Certification Authorities, select certificates as shown below.

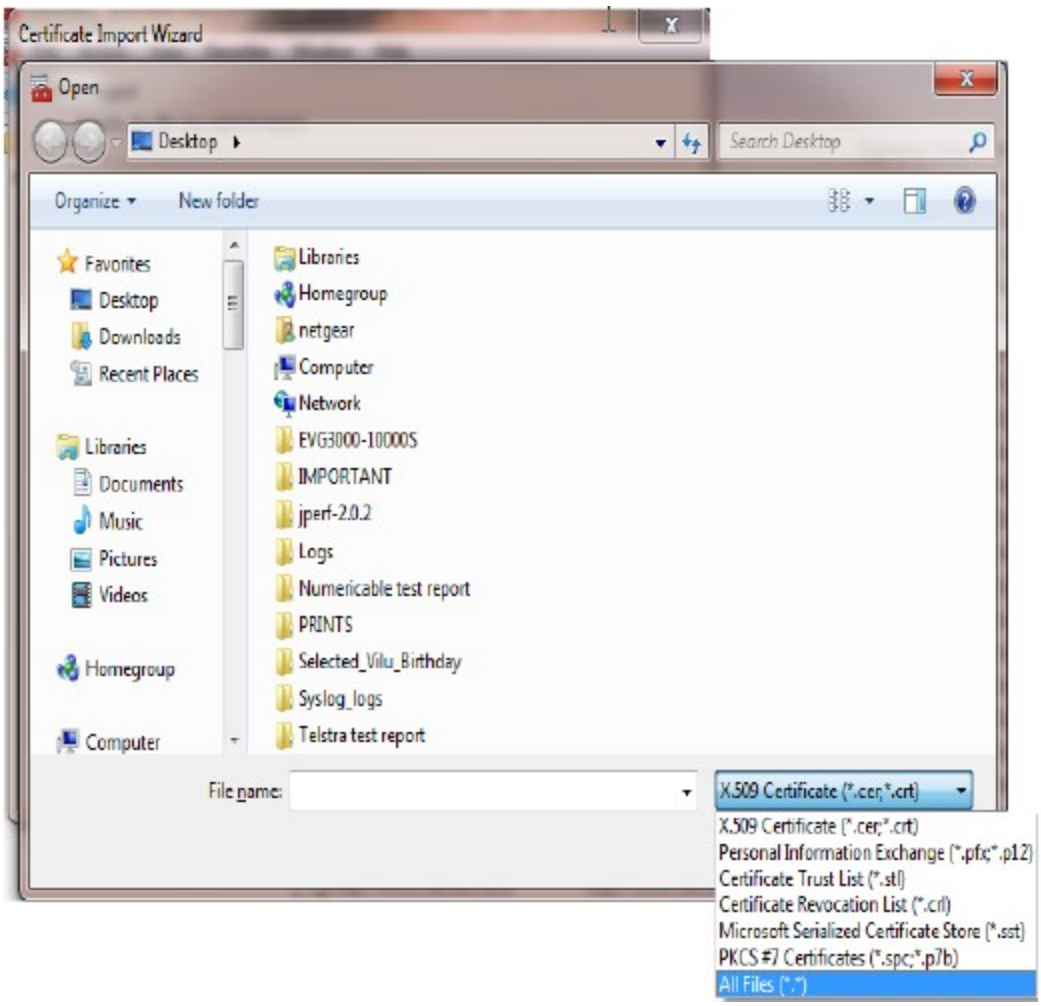


g) Right-click Certificates > Select All Tasks and select Import to start the Certificate Import Wizard.

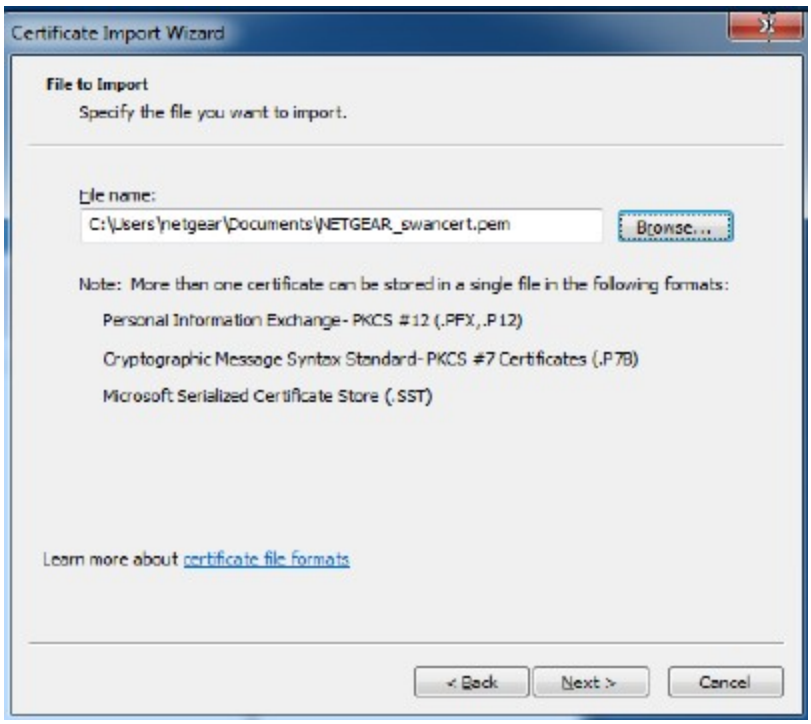
h) Click Next.
i) Click the Browse button.



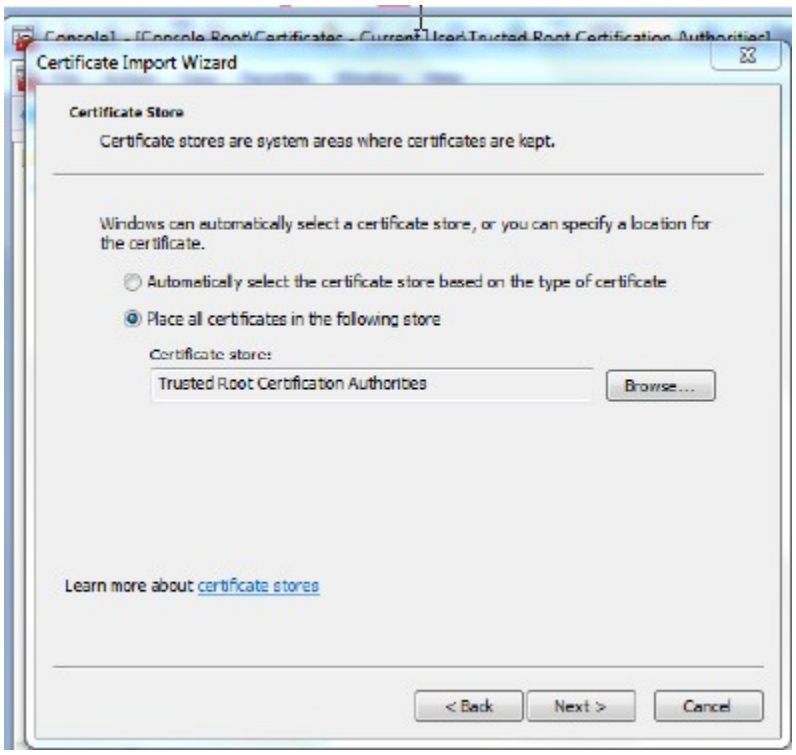
j) Select the certificate that was generated and saved in the Windows computer (.pem extension) by selecting All files from the File name list, and click Open.


Certificate Import Wizard
Open
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Libraries
Homegroup
netgear
Computer
Network
EVG3000-10000S
IMPORTANT
jperf-2.0.2
Logs
Numericable test report
PRINTS
Selected_Vilu_Birthday
Syslog_logs
Telstra test report
File name:
X.509 Certificate (*.cer;*.crt)
X.509 Certificate (*.cer;*.crt)
Personal Information Exchange (*.pfx;*.p12)
Certificate Trust List (*.stl)
Certificate Revocation List (*.crl)
Microsoft Serialized Certificate Store (*.sst)
PKCS #7 Certificates (*.spc;*.p7b)
All Files (*.*)

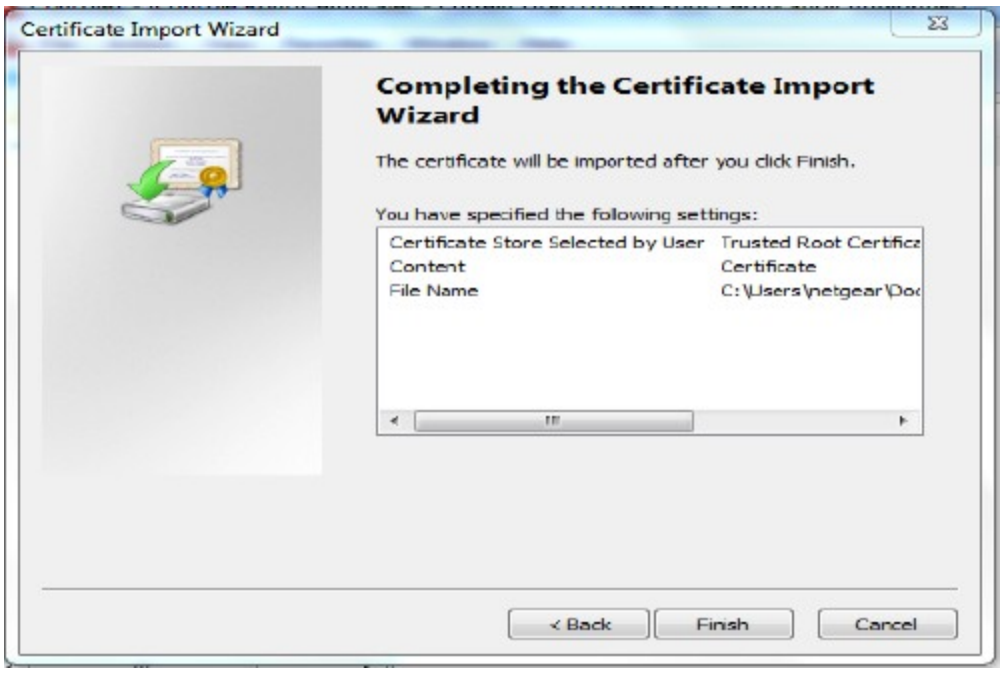
k) Click Next.



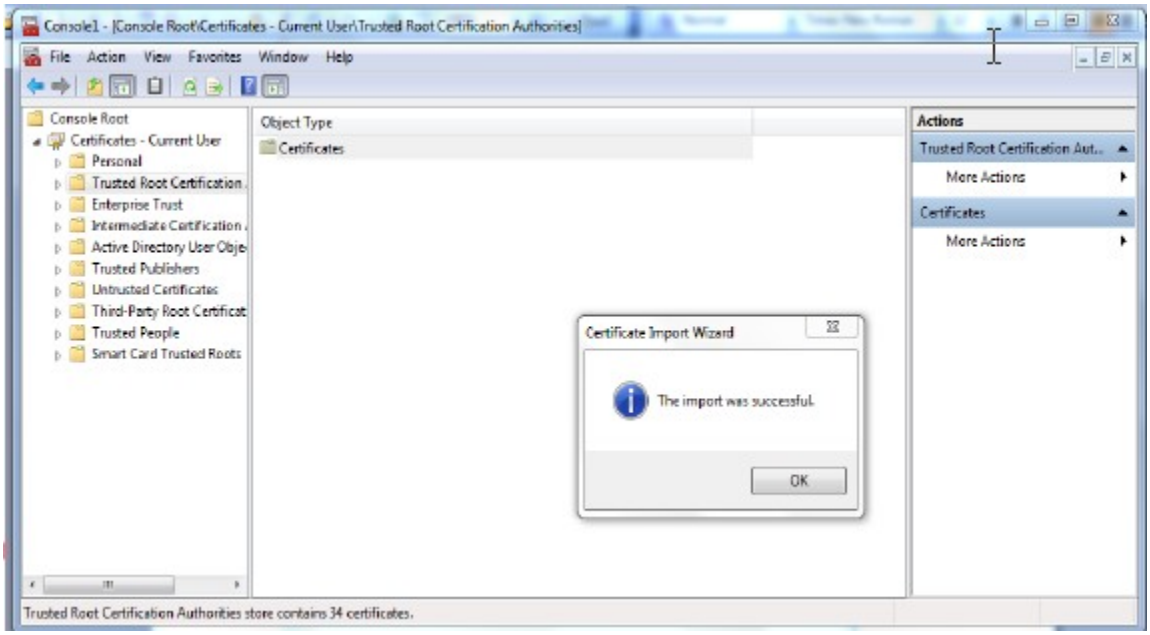
l) Select the Place all certificates in the following store radio button as shown below and click Next.



m) Click Finish.

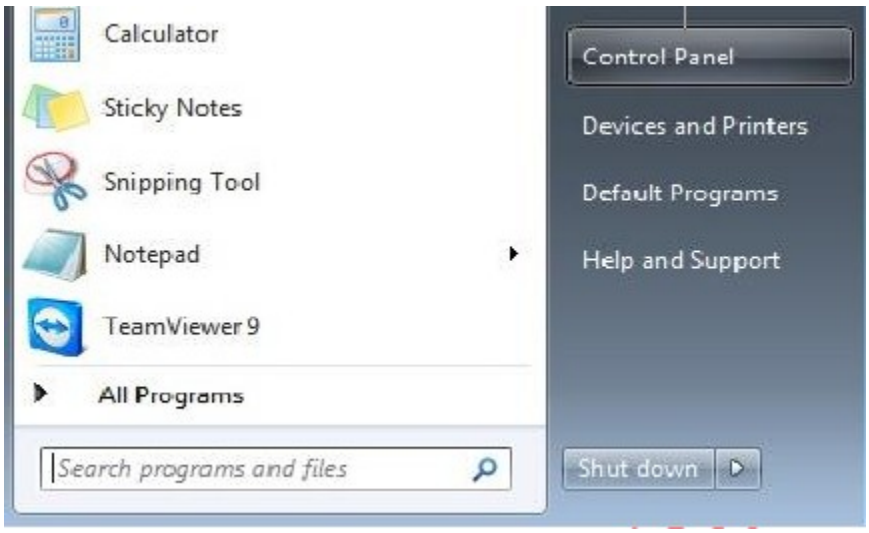


n) A pop-up window saying The import was successful displays as shown.

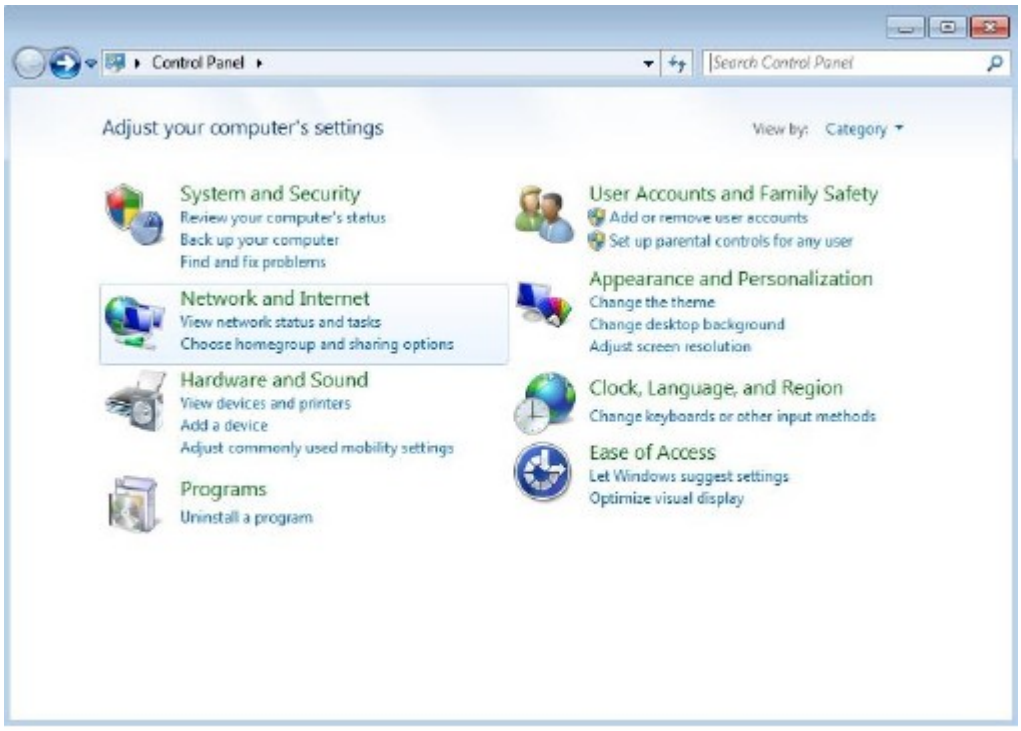


3.5.2.2 Configuring a Windows 7 Agile VPN Connection

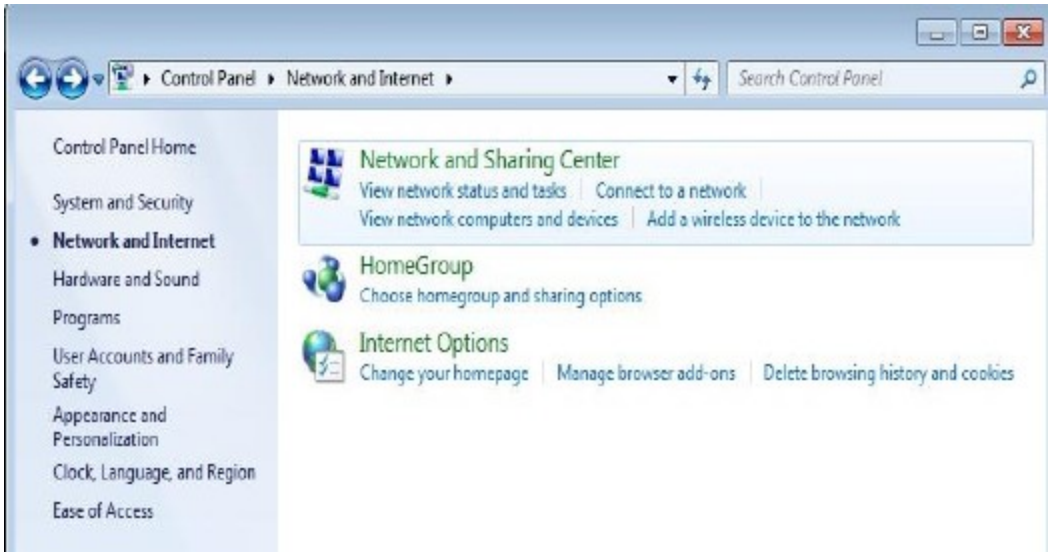
a) Click Start and select Control Panel.



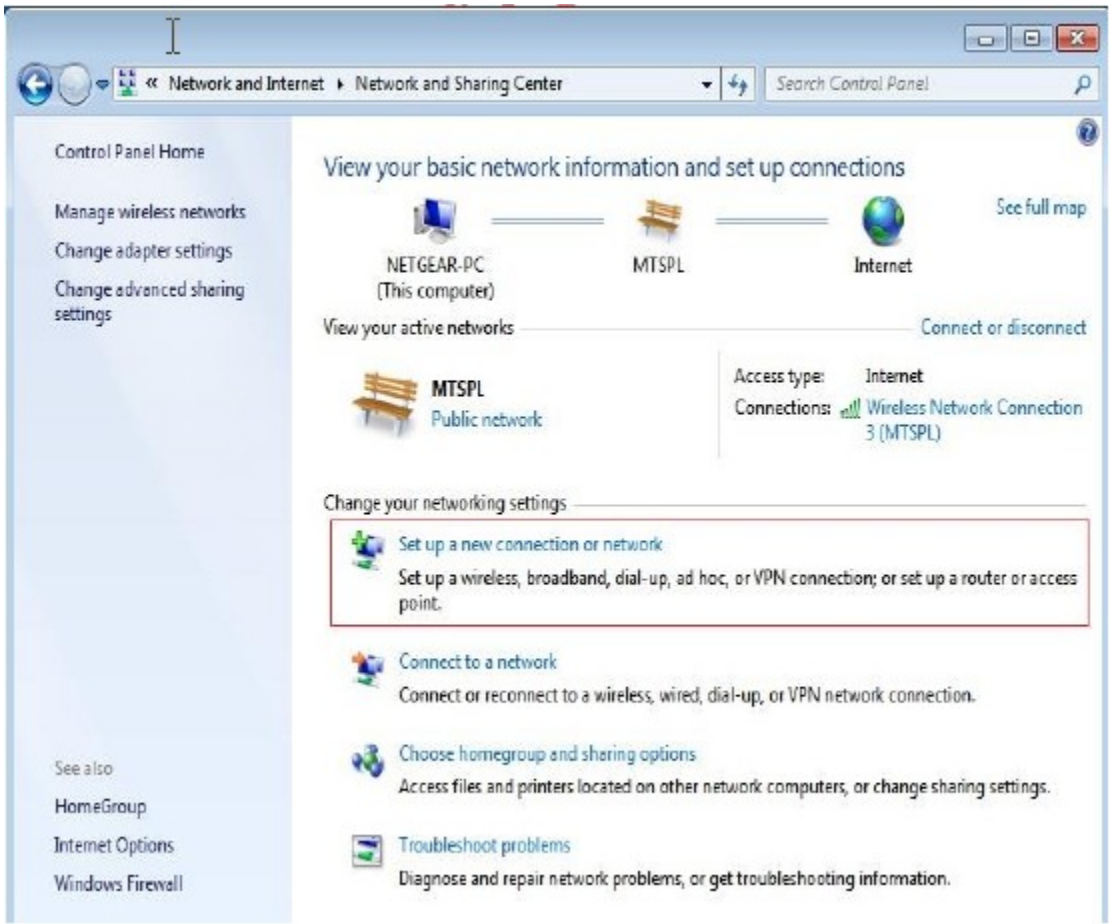
b) Select Network and Internet.



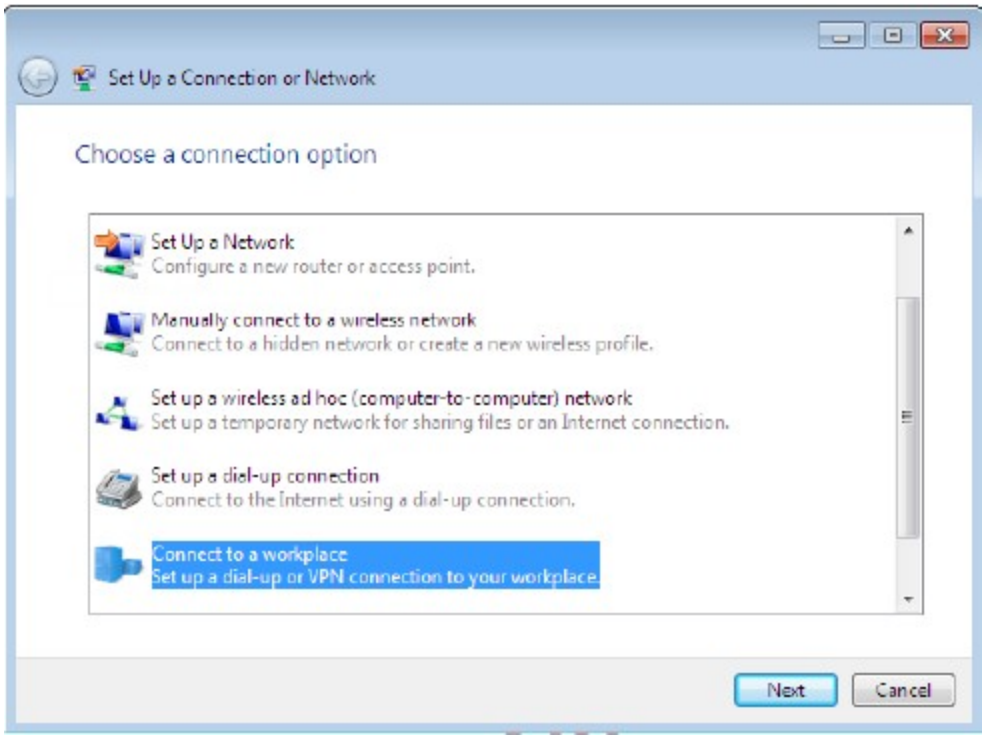
c) Select Network and Sharing Center.



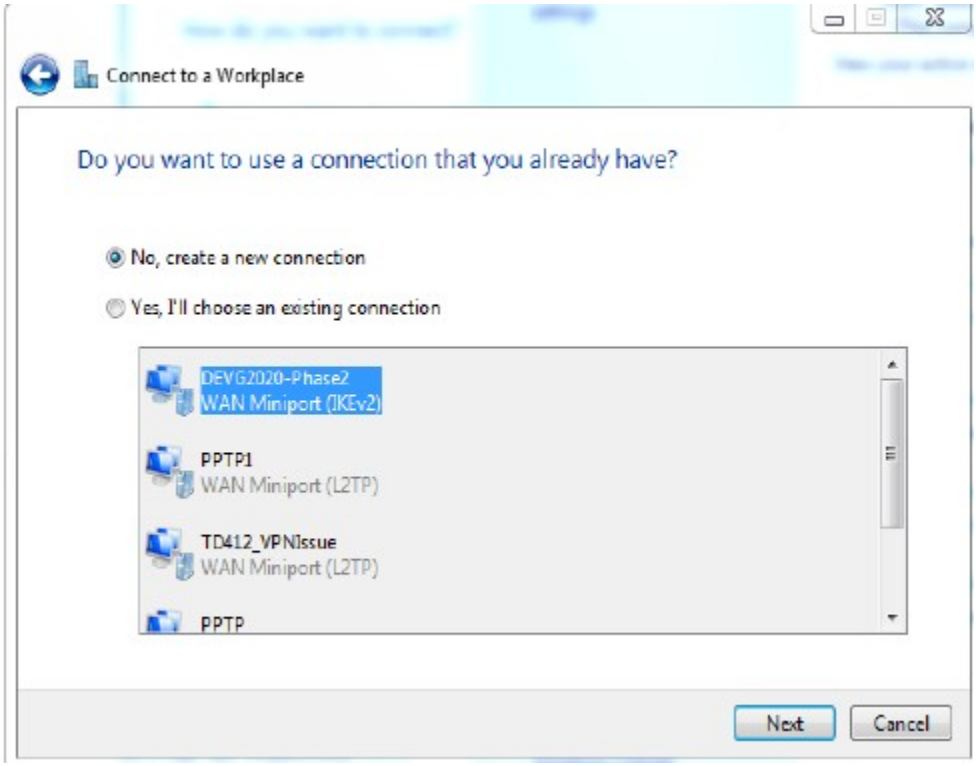
d) In the Network and Sharing Center screen, select Set up a new connection or network as shown.



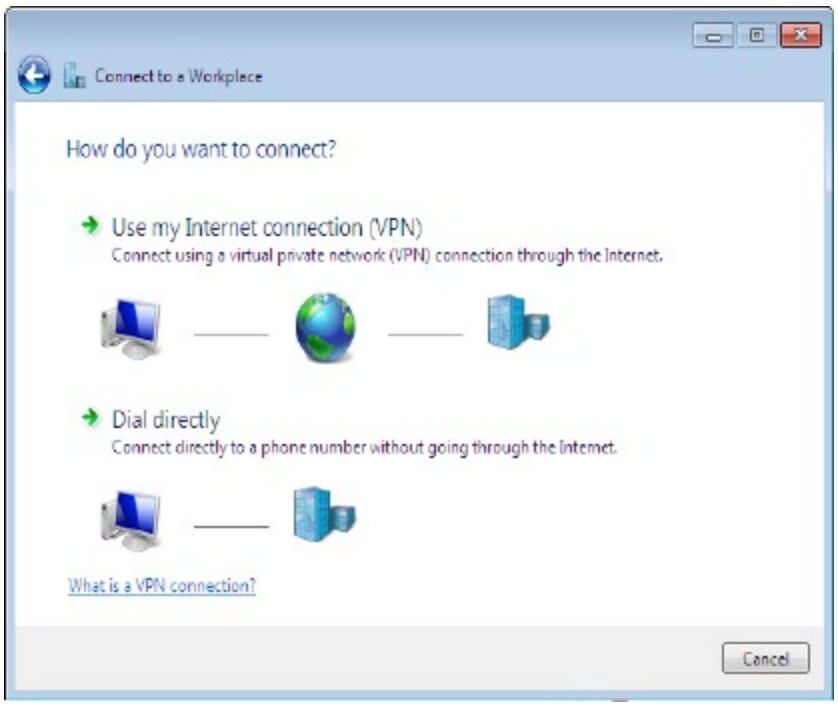
e) Select the Connect to a workplace option and click Next.



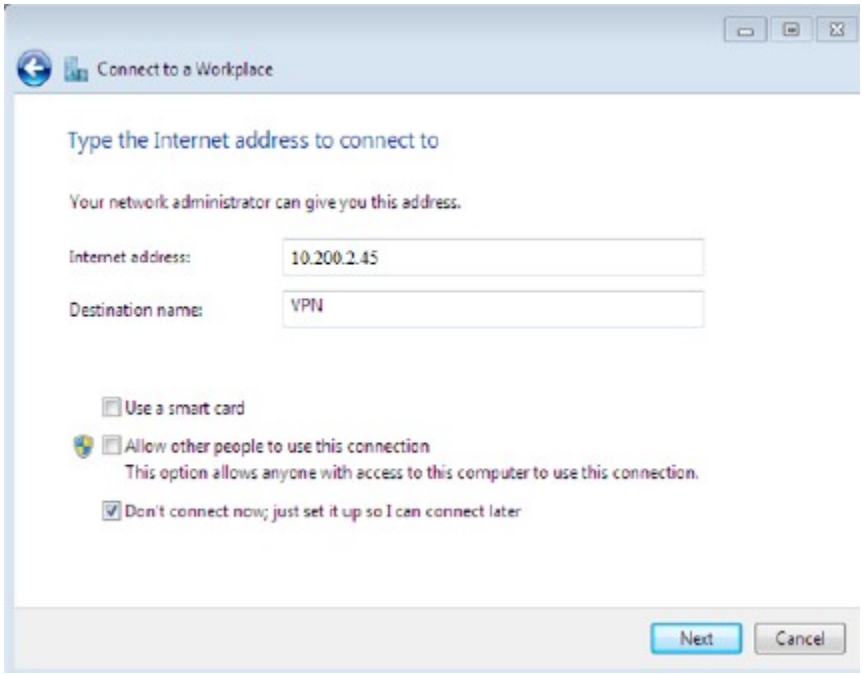
f) Select No, create a new connection and click Next.



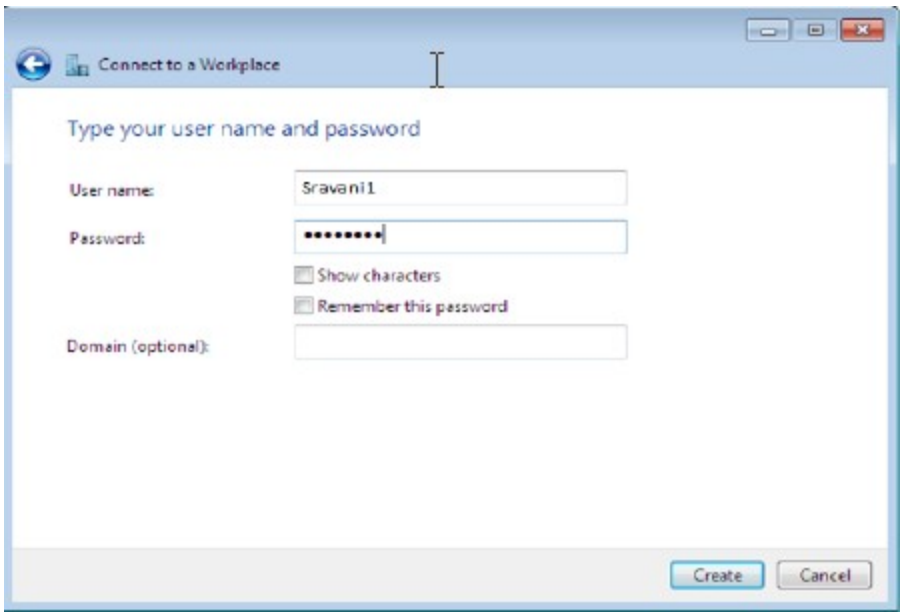
g) Click Use my Internet connection (VPN).



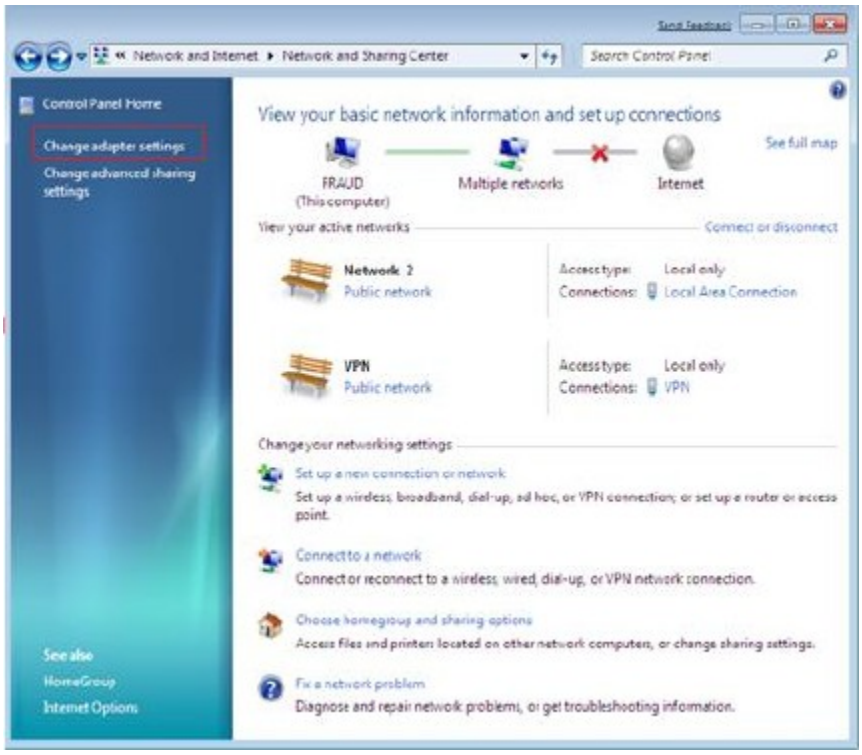
h) Enter the WAN IP address of the gateway in the Internet address field.
i) The destination name can be any string, for example, VPN.
j) Select the Don't connect now; just set it up so I can connect later check box and click Next.



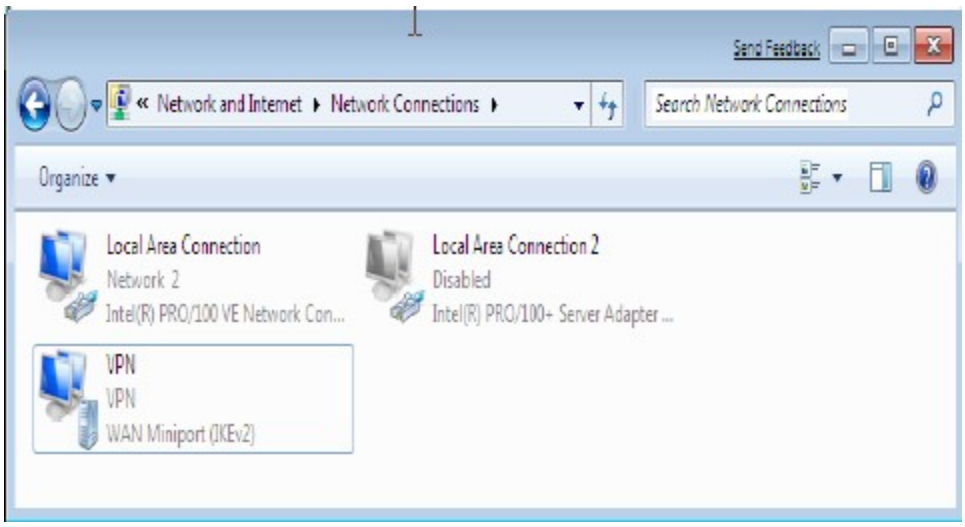
k) Enter your remote VPN user name and password from the V7610 (under VPN users) and click Create.



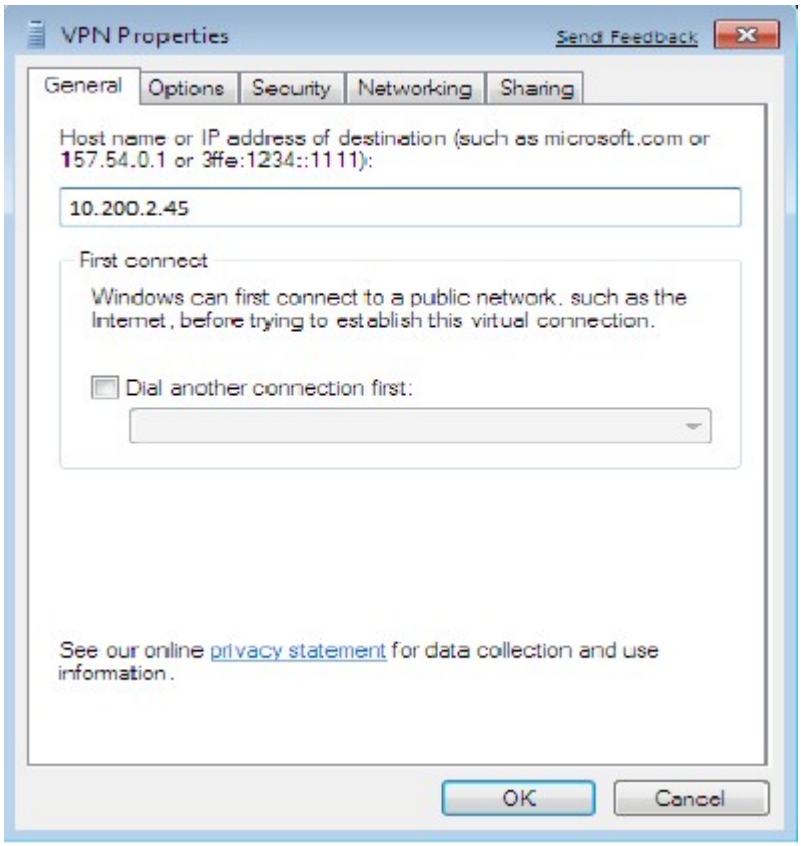
l) Click Close.
m) Navigate to the VPN you created.
n) Click Start and select Control Panel. Select Network and Internet. Select Network and Sharing Center (see Steps a, b, and c in this section).
o) Click Change adapter settings.



p) Right-click the VPN you created and select Properties.



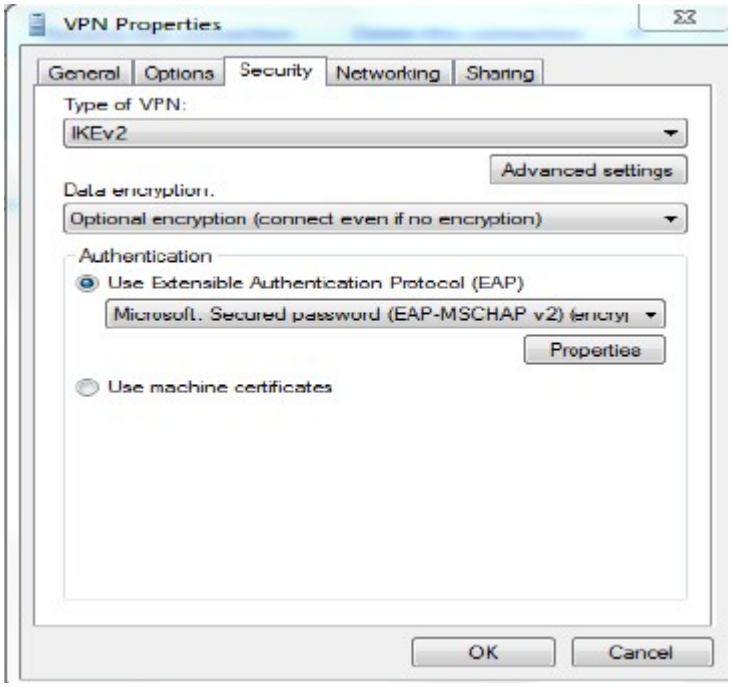
q) In the General tab of the VPN Properties screen, the WAN IP address of the VPN gateway has already been entered, but you can edit it at any time.



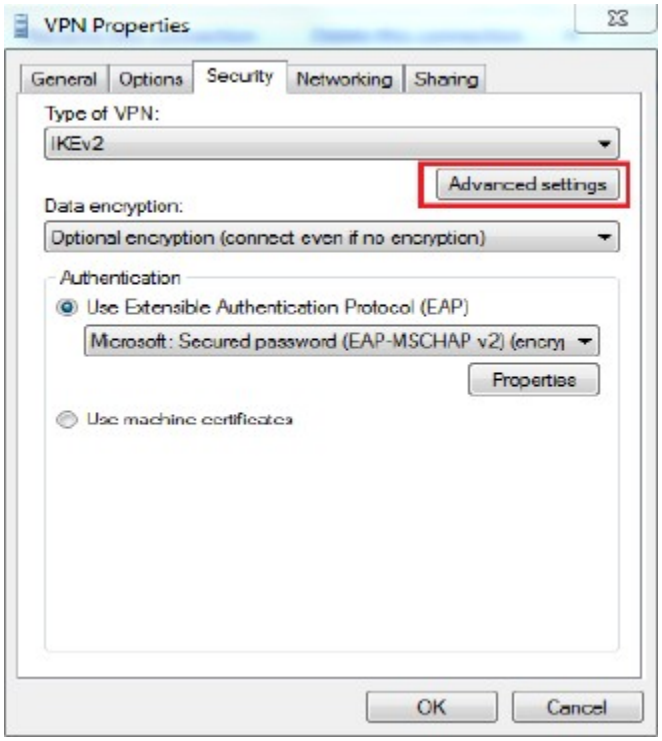
r) In the Security tab of the VPN Properties screen, make the following changes:

- In the Type of VPN list, select IKEv2.

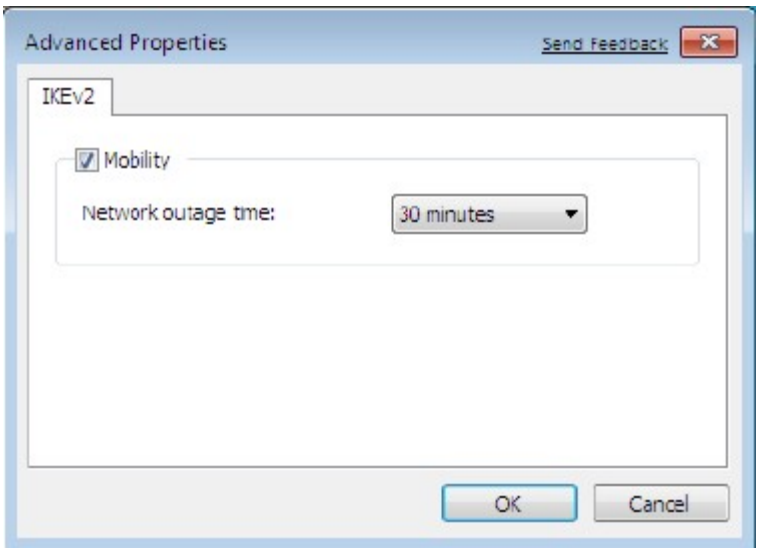
- In the Data encryption list, select Optional encryption (connect even if no encryption).



- Click Advanced settings as shown below.



- In the screen that appears, select the Mobility check box. Click OK as shown.



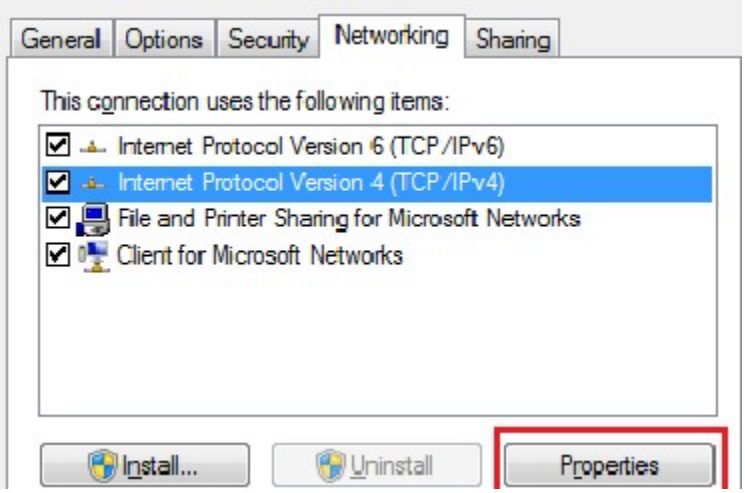
The configuration of the Windows & Agile VPN connection is complete.

3.5.2.3 Configuring Split Tunnel in Windows

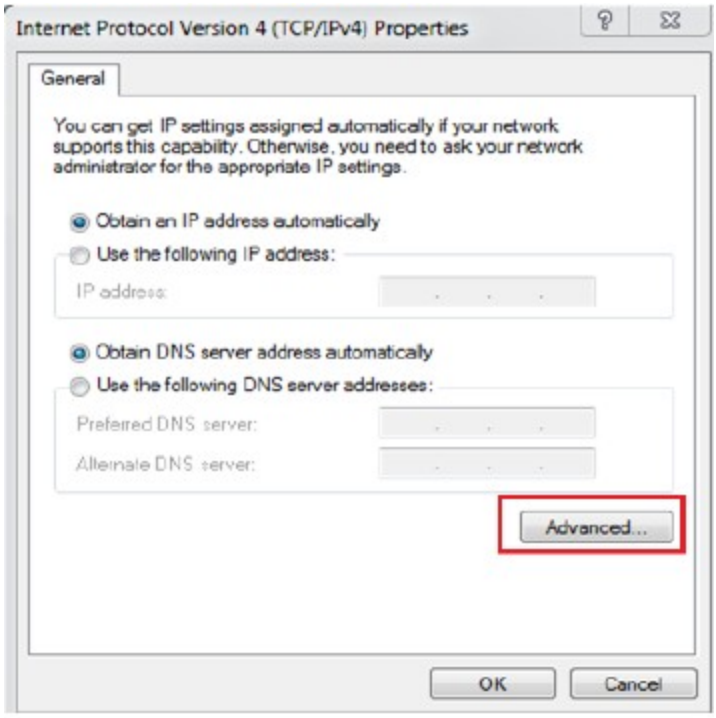
The split tunnel allows users to access the Internet as well as the remote LAN subnet after the VPN tunnel is established. To set up a split tunnel, follow these instructions:

a) Modify the properties of the VPN connection created in the Windows 7 host so that it will not use the remote network default gateway for routing Internet traffic:

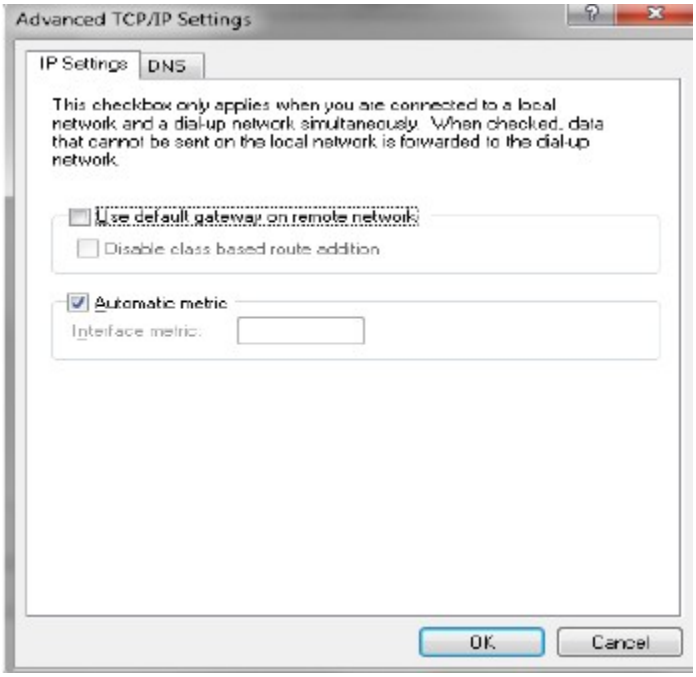
- Select Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings.
- Right-click the VPN connection, then select Properties.
- Select the Networking tab.
- Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.



- Click Advanced.



- Clear the Use default gateway on remote network check box and click OK. Apply
- the changes.



b) Split tunneling is enabled for the VPN on your Windows 7 host. If the VPN remote virtual pool configured in the V7610 GW (as shown in the following screen shot) is same as the LAN IP pool of the GW, then the VPN configuration for the split tunnel is complete. Otherwise, go to Step c.

c) If the VPN remote virtual pool configured in the V7610 GW is different from the LAN IP address pool of the GW, as shown in the following screen shot, add a static route.

Open command prompt on your Windows 7 host and enter the following text to add a static
route to the remote network LAN pool:

route add <Modem LAN subnet> mask <subnet mask> <VPN remote virtual IP of the gateway>

```
C:\Users\netgear>Route add 192.168.15.0 mask 255.255.255.0 192.168.16.1
```

Important notes:

i) In the example above 192.168.16.1 is the virtual IP gateway configured in your router and 192.168.15.0 is modem's LAN IP subnet.

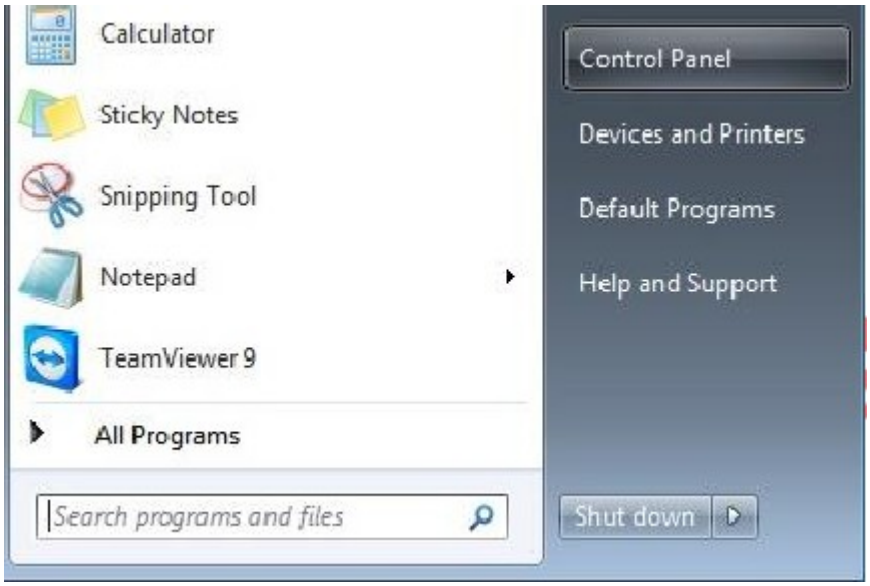
ii) The route will be deleted when the Windows host reboots. To make the route persistent, append a -p flag to the command as shown below.

```
C:\Users\netgear>Route add -p 192.168.15.0 mask 255.255.255.0 192.168.16.1
```

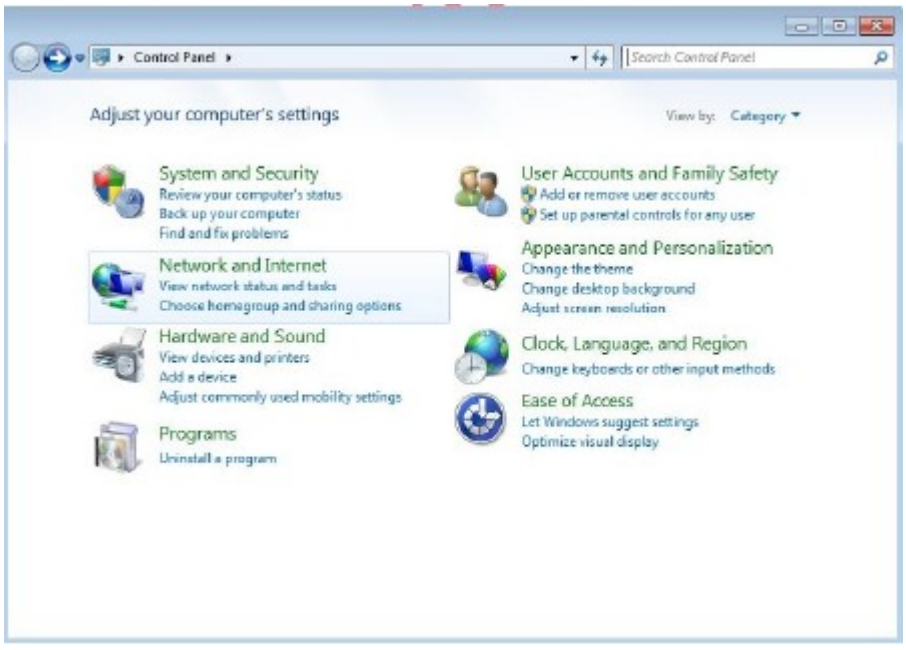
iii) If you need to delete this static route for any reason, run the following command:

3.5.2.4 Starting a Windows 7 Agile VPN Connection

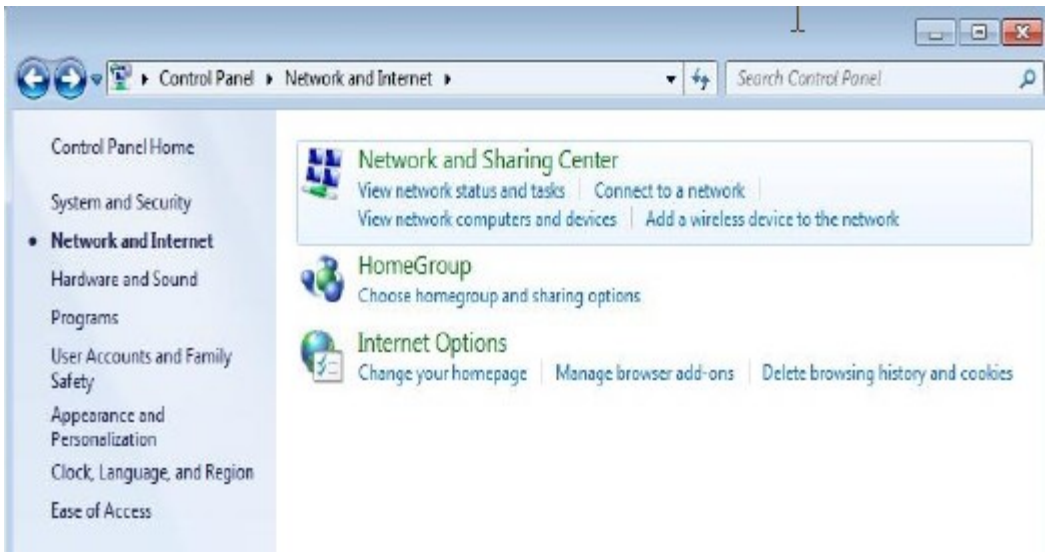
a) Click Start and select Control Panel.



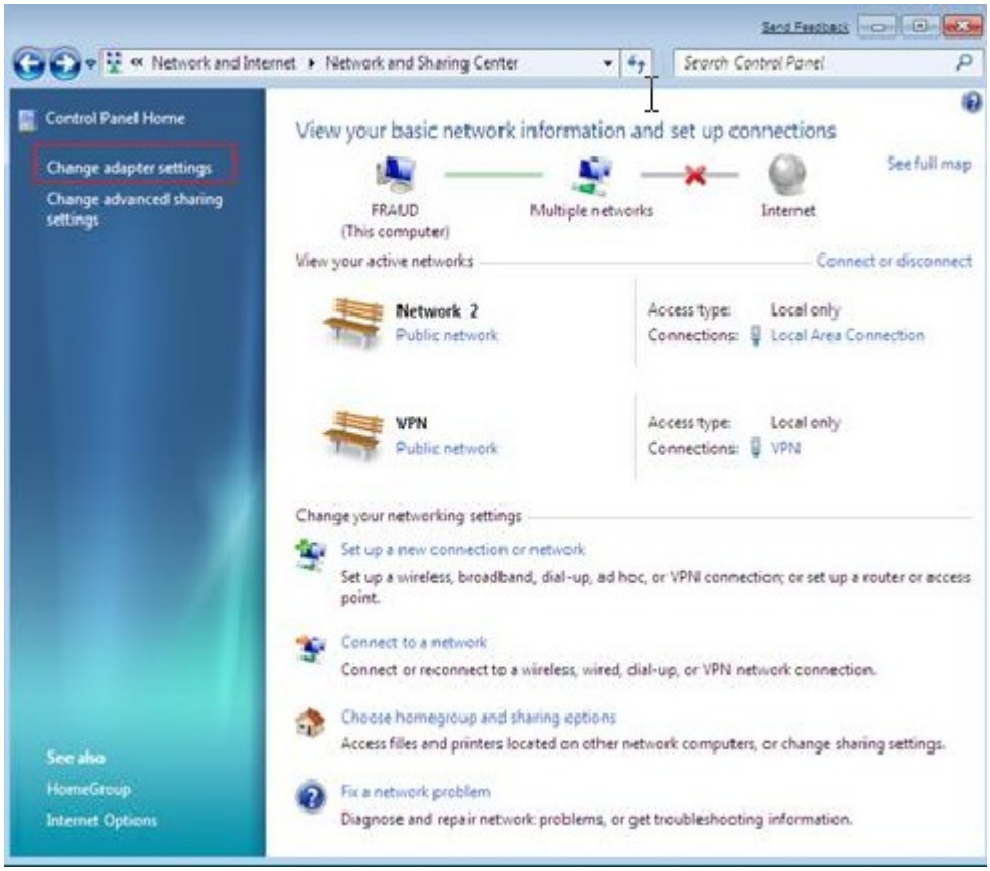
b) Select Network and Internet.



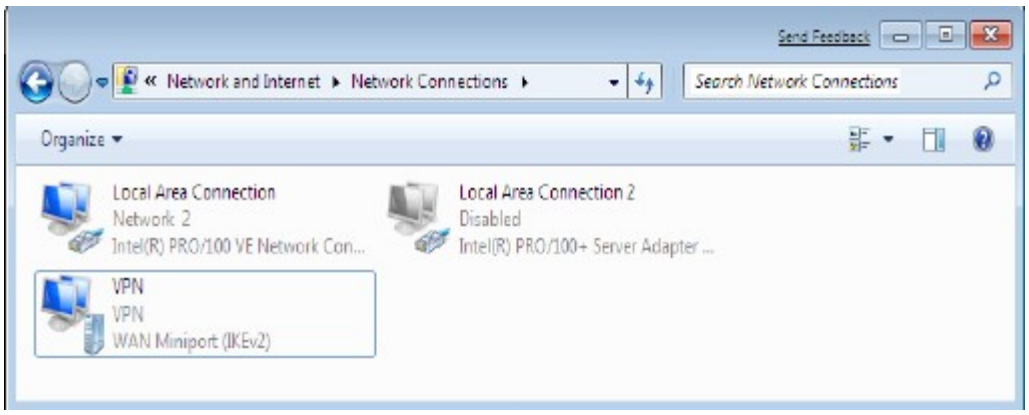
c) Select Network and Sharing Center.



d) Click Change adapter settings.



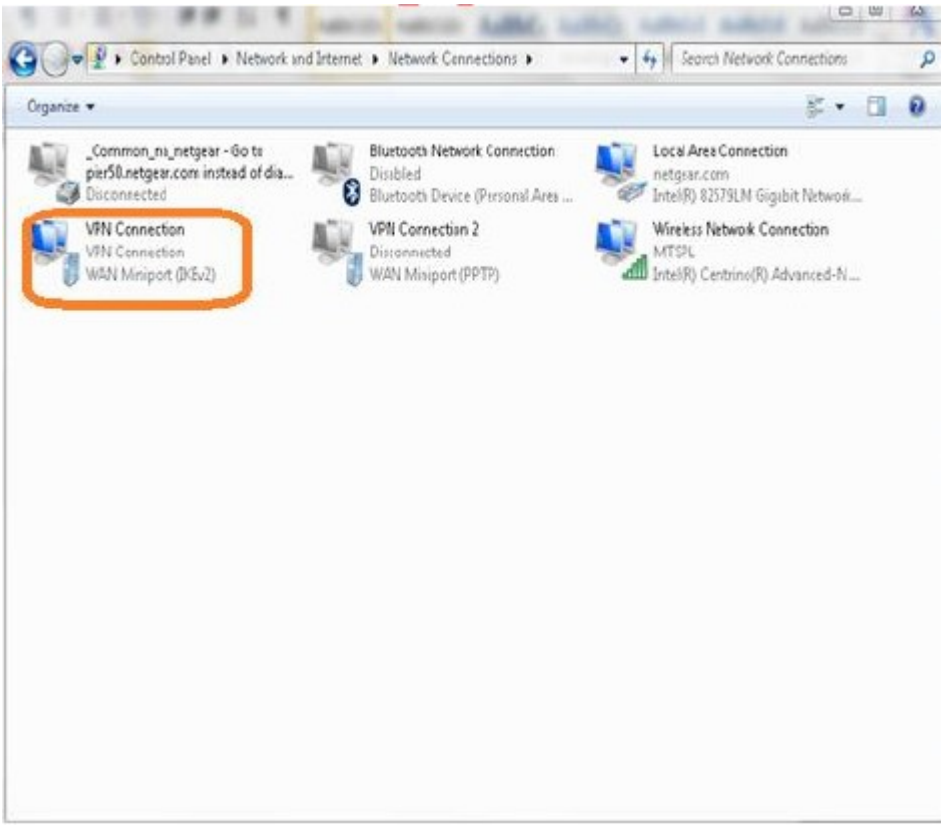
e) Right-click the VPN you created and click Connect.



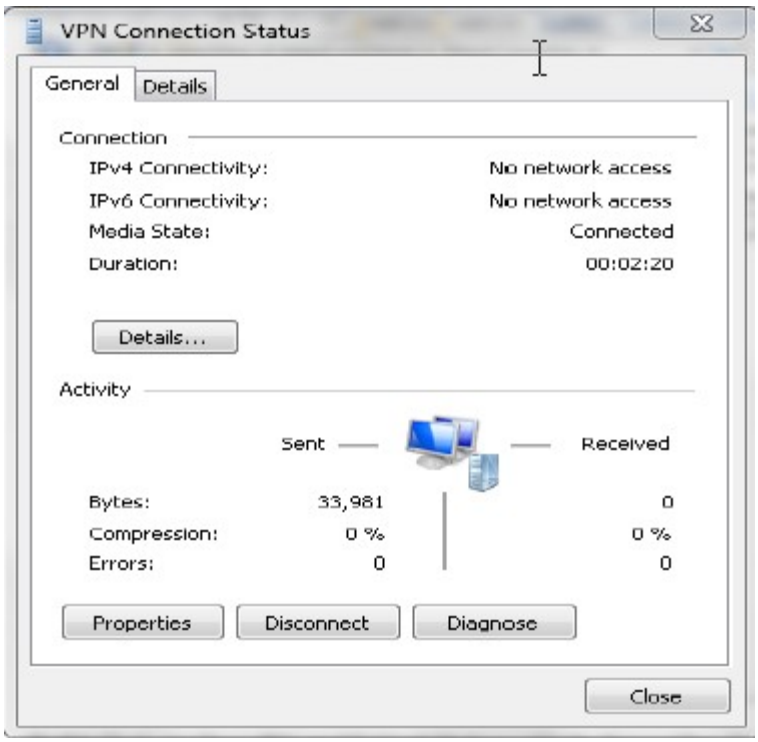
f) Enter the user name and password that are configured in the gateway. Click Connect.

g) You are prompted to reenter the user name and password configured in the gateway. Click OK.

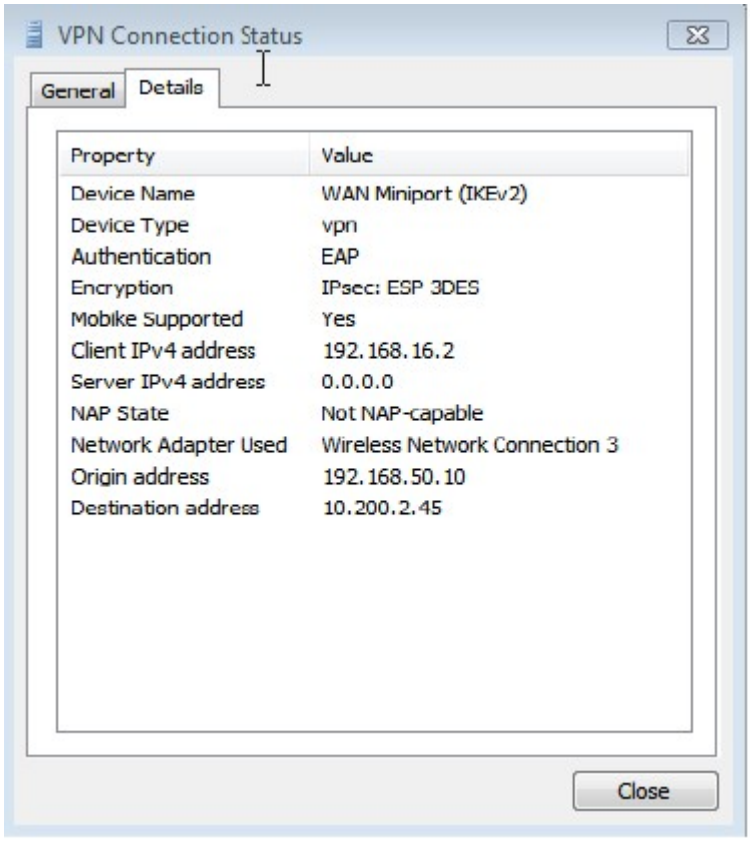
h) The VPN tunnel is established.



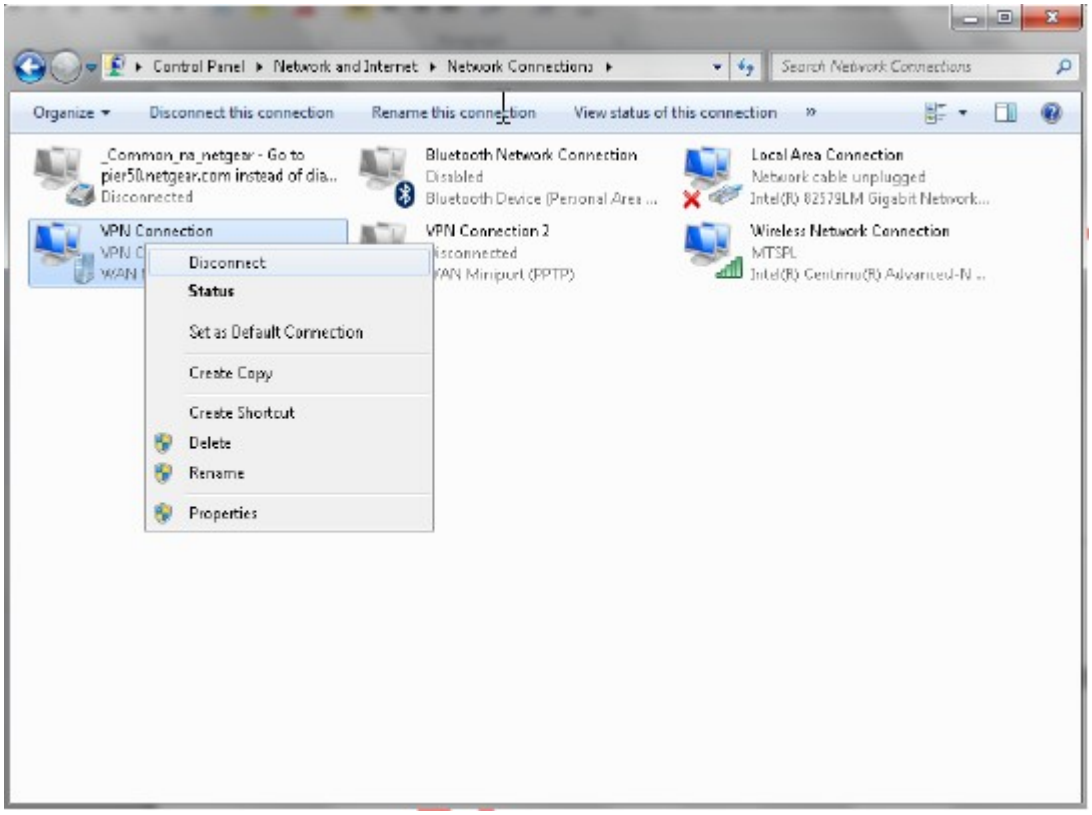
i) Right-click the VPN and select Status to show the status of the VPN tunnel you established.



j) Click the Details tab to view the details as shown below:



k) To disconnect the VPN tunnel you established, right-click the VPN Connection icon in the Network connection page and select Disconnect. The tunnel is disconnected.

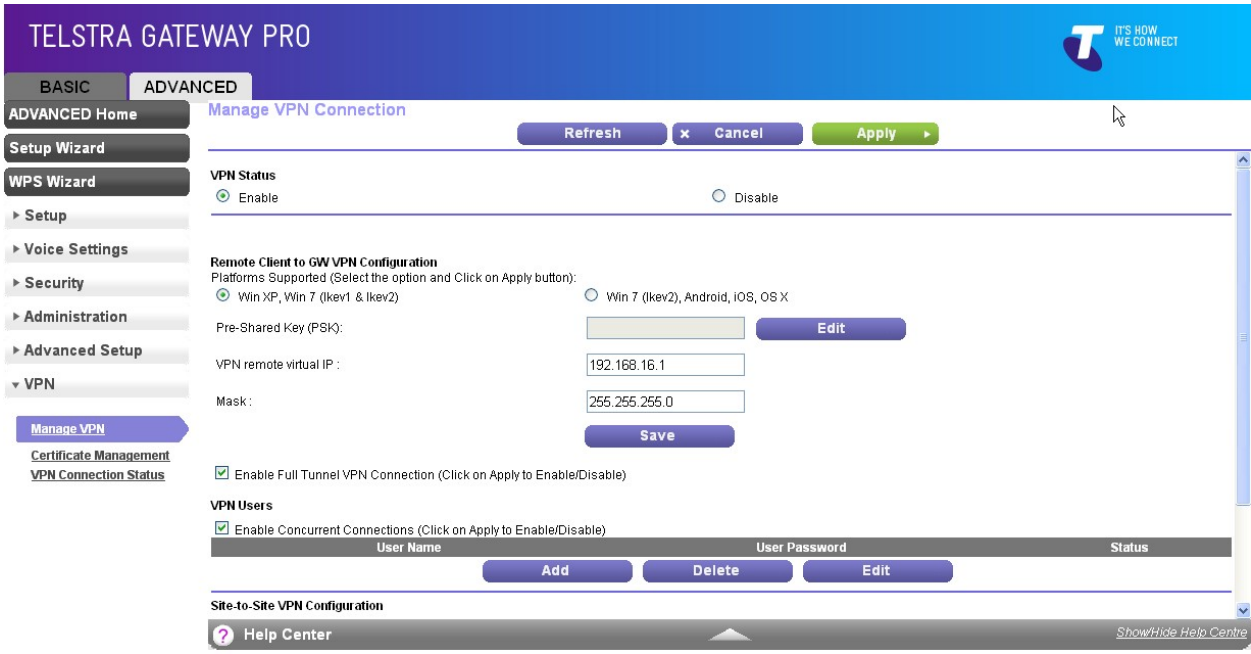


NOTE: The client configuration navigation may vary for different versions of Windows (Enterprise, Professional, and so on).

4. Site-to-Site VPN Configuration

This section describes the connection configuration details for a site-to-site VPN connection between two V7610 GW devices. The LAN subnets of these two devices must each be in a unique range for the connection to be established successfully.

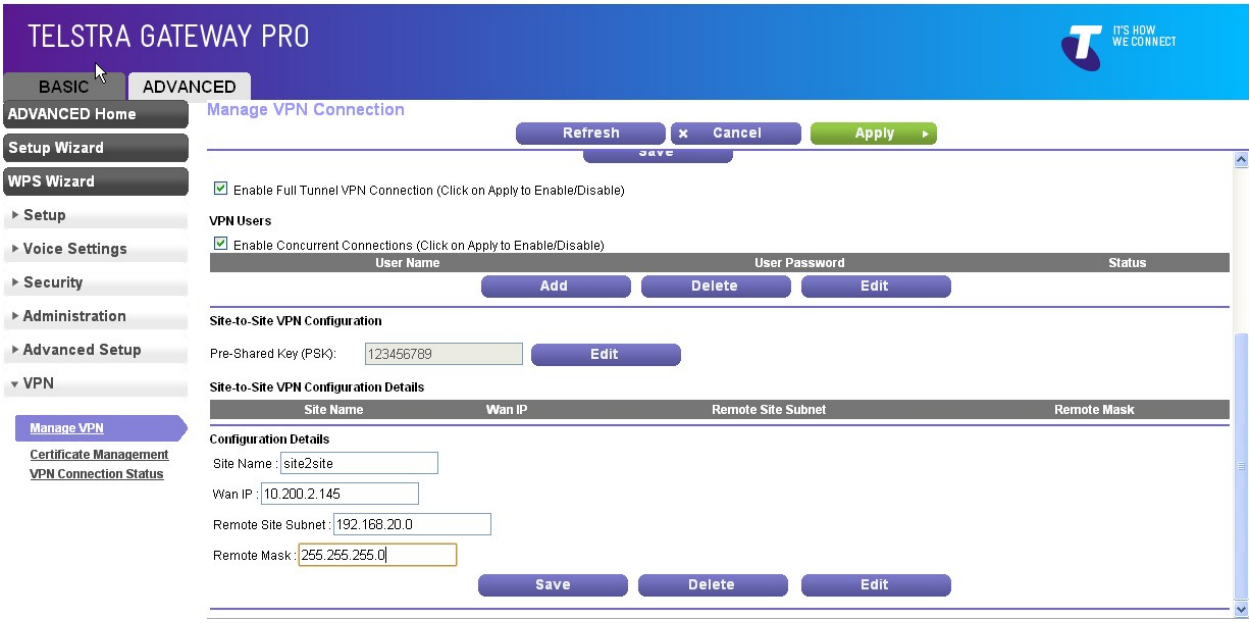
a) On the first V7610 GW device, click the ADVANCED tab and select VPN > Manage VPN on the left pane. Browse down to the Site-to-Site VPN Configuration section of the page.



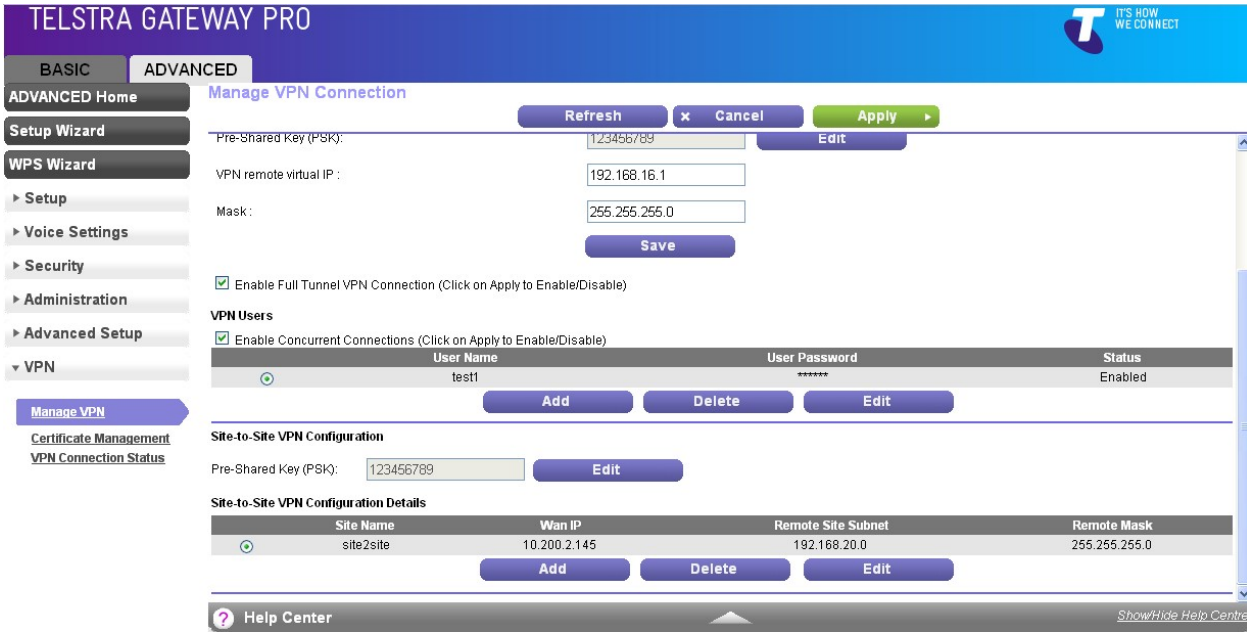
b) Enter an alphanumeric string (a minimum of 8 characters and a maximum of 32 characters) in the Pre-Shared Key (PSK) field. Note that this field applies to the site-to-site VPN configuration, not the remote client-to-GW configuration.

c) In the Configuration Details section, click Add and enter the values in the following fields:

- Site Name – This is a user-friendly name for the connection.
- **WAN IP** – Enter the remote GW WAN IP address.
- **Remote Site IP address and Subnet –** This is the remote GW LAN subnet. As mentioned earlier, each of the two GWs in this configuration must have a unique nonoverlapping IP address range.
- Click Apply to save the changes.



d) An entry is created in the Site-to-Site Configuration table as shown below.



e) On the second V7610 GW device, repeat steps (a) through (c). Note that the pre-shared key for both the V7610 GW devices must be the same.

f) When the configuration is complete, enable VPN on both GWs.

g) The IPSec VPN tunnel is established between the two V7610 GWs, and LAN-side resources from one GW can access the other through this tunnel.