How to make a VPN connection to our servers from Windows 8

Windows 8 is able to make a newer type of VPN connection called a Secure Socket Tunnelling Protocol (SSTP) connection. This works just like a traditional Point-To-Point Tunnelling Protocol (PPTP) VPN except that it uses the same TCP ports and protocol type as a secure website.
This has the advantages that:-

1. Almost all firewalls allow this type of connection to pass through, by default.
2. It's very difficult to block an SSTP VPN and still allow secure websites to function.
3. It's not obvious to anyone monitoring your traffic that that you are using a VPN connection.

Also, by default, Windows 8 tries to make an SSTP connection first and then falls back to a PPTP if SSTP fails. Our VPN servers support both types of VPN but, if you have Windows 8, there no reason *not* to use SSTP. This means you will always be able to make an SSTP VPN connection to our servers, however and wherever you've connected to the Internet.
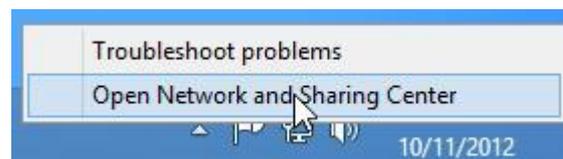
1 - How to Create a new VPN Connection

From the Windows 8 Desktop right-click on the Network icon in the Notification Area:-

If you are using a wireless connection the network icon will look like this instead:-
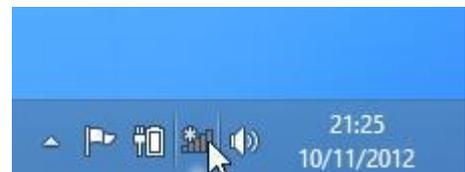
Click: **Open Network and Sharing Center**

Click: **Setup a new connection or network**

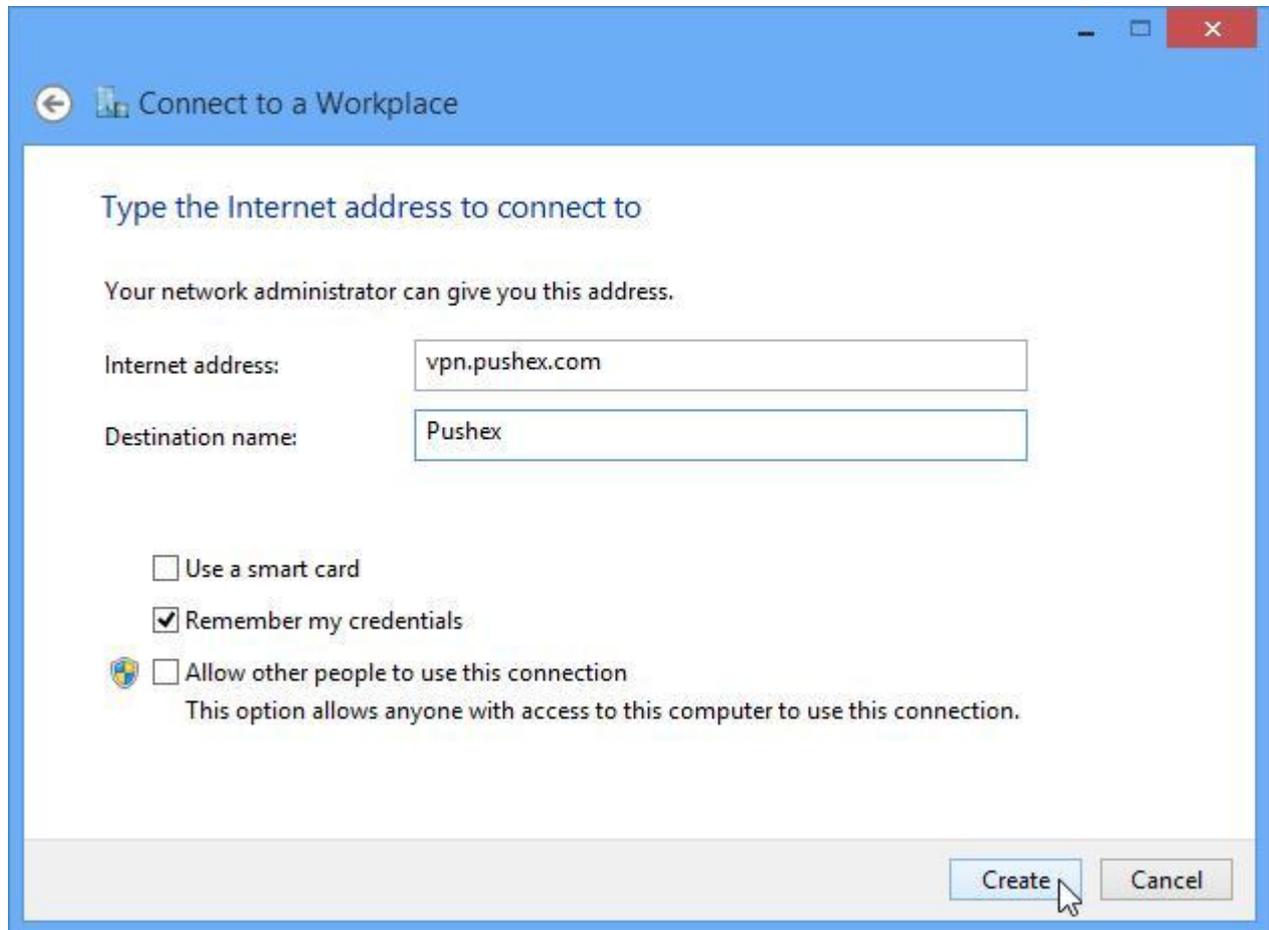and then select: **Connect to a workplace**

Click: **Next**

Click: **Use my Internet connection (VPN)**

When the window below appears, enter: **vpn.pushex.com** as the Internet address.

The **Destination name:** is just what *you* want to call this connection.
It can be anything, but **Pushex** is good:-

Select: **Remember my credentials** if you don't want to enter your password each time you connect.
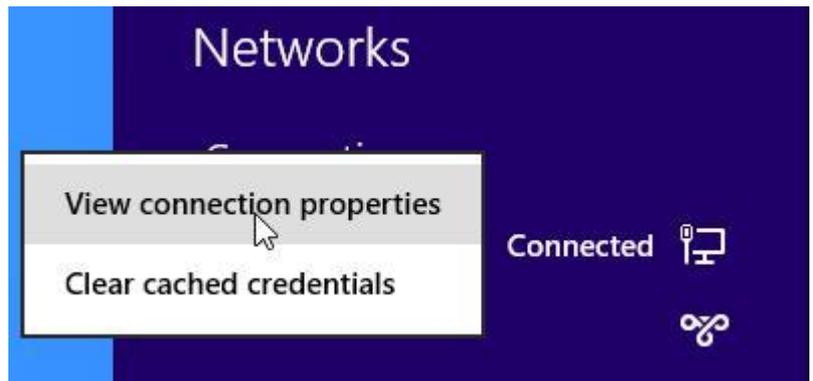
Select: **Create** and the **Networks** list will pop out from the right of the screen showing the new VPN connection you've just created:-
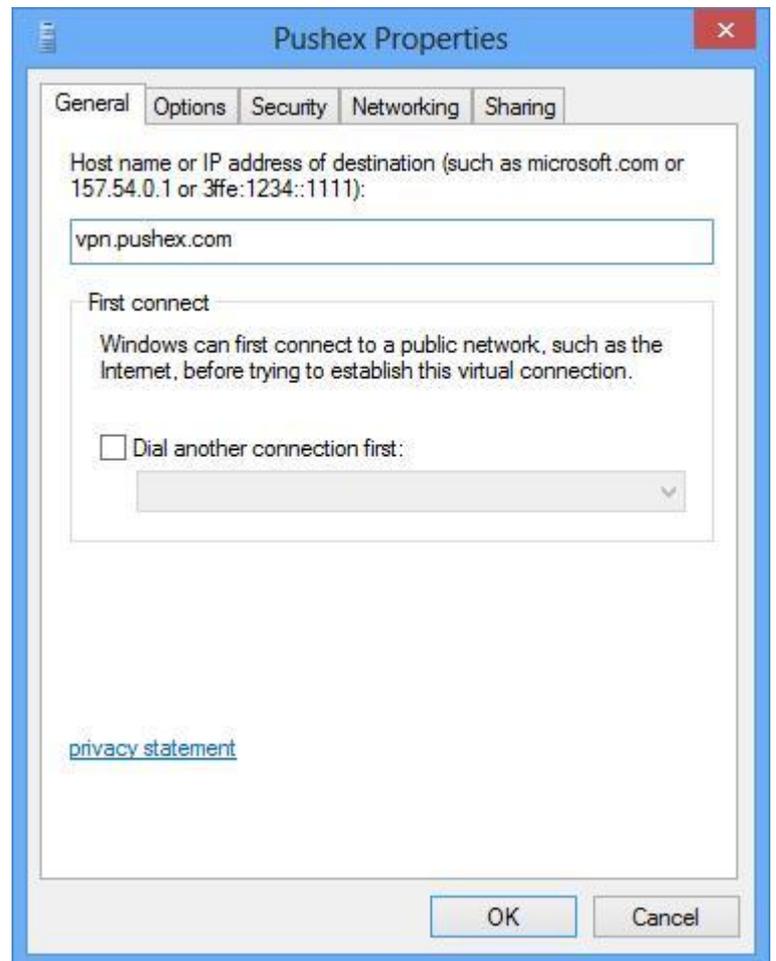

Close the **Network and Sharing Center** window.

Click on the Network icon in the Notification Area to display the **Networks** list.

Right-click on the word **Pushex** and select **View connection properties**.

This window will then appear:

There's nothing to do on the **General** and **Options** tabs so go to the **Security** tab.

For **Type of VPN:** Automatic is usually the best choice.

Our servers will accept connections of type Point to Point Tunnelling Protocol (PPTP) and Secure Socket Tunnelling protocol (SSTP).

When set to Automatic, Windows first tries to make an SSTP connection and if this doesn't work it tries a PPTP connection.

While equally secure, an SSTP connection hides the fact that you are actually using a VPN connection and so, if this is important, you could set the **Type of VPN:** to SSTP so that *only* SSTP connections are attempted.
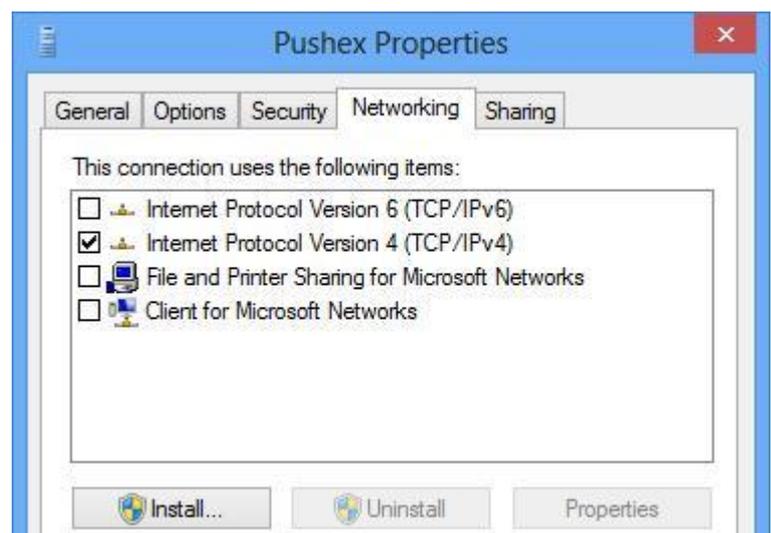
Select: **Allow these protocols**

and **Microsoft CHAP version 2**

Now go to the **Networking** tab.
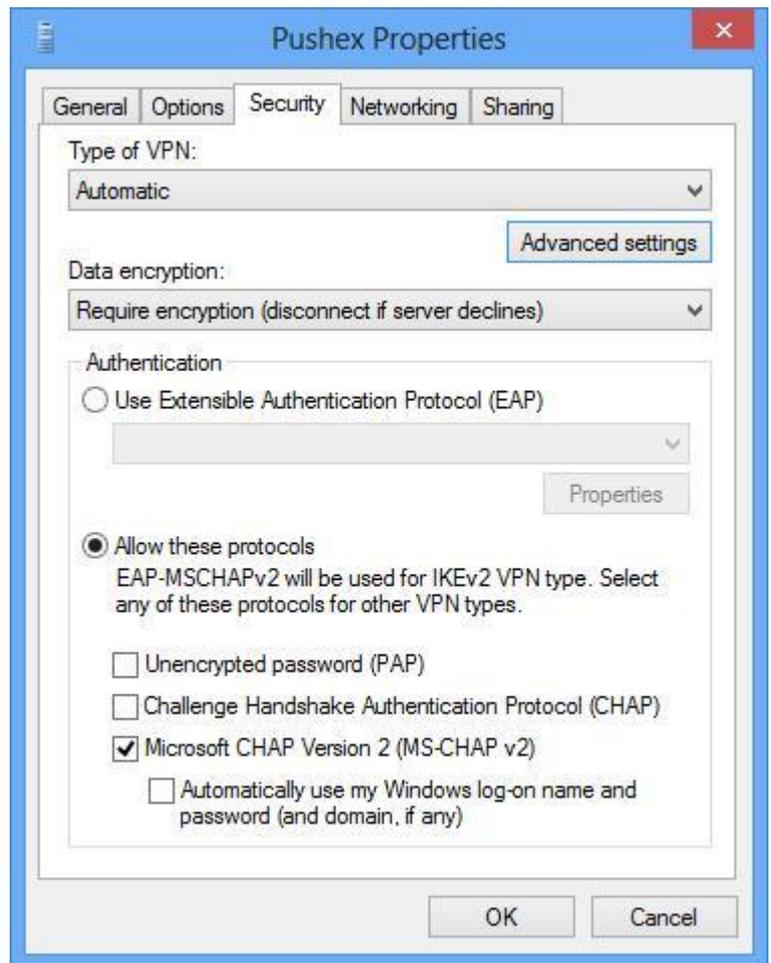
Although not strictly necessary, for greater efficiency and to avoid problems, we advise that you *deselect* everything on this tab except **Internet Protocol Version 4 (TCP/IPv4)**

(There may be additional items to deselect as well as the ones shown here.)

There's nothing to do on the **Sharing** tab so click: **OK** to close the Properties window.

The VPN connection setup procedure is now complete.

2 – Connecting to the VPN

Click on the Network icon in the Notification Area to display the **Networks** list.

Click on the word **Pushex** and then the **Connect** box when it appears.
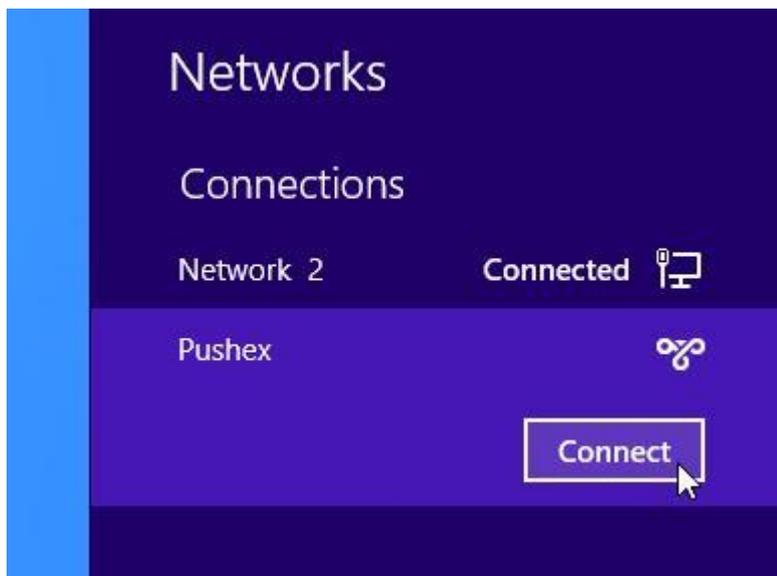
The first time you connect you have to enter your Pushex username and password.

If you selected **Remember my credentials** during the setup process you won't need to do this step when connecting in future.

If you didn't select **Remember my credentials** during setup but now wish to do so, this setting is on the **Options** tab of the connection properties window in Section 1.

It is correct that the **Domain:** shown opposite is blank.

Click: **OK** to connect

When you've successfully connected, the Networks list will appear like this:

The regular network connection is now listed as **Limited** which just means that it is not being used to access the Internet. You will still be able to access devices on your local network such as printers, NAS drives, other PCs or servers.


When connected, to check that your PC is sending all its Internet traffic over the VPN, go to the website:-
http://www.whatismyipaddress.com

and it should show your computer as being located in the UK.

To disconnect from the VPN, click the Network icon in the Notification Area to display the **Networks** list,

Click on the word **Pushex** to make the **Disconnect** box appear,

then click: **Disconnect**
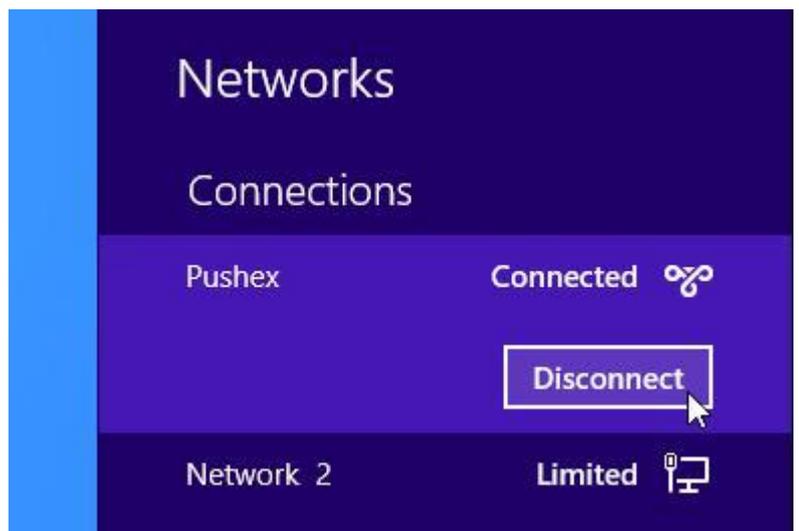
After disconnection, your regular network connection will now show as **Connected** again.

3 – The VPN over VPN trick

It's so amazing that this actually works we've given it a section of its own.

If your work has a VPN setup for you to access company files when you're away from the office, you may find that it can't always connect. This is because most VPNs need specific ports to be open on any firewalls they pass through and these ports can sometimes be blocked, either on purpose or through ignorance.
An SSTP VPN uses Port 443 which is almost certain to be open on all firewalls. What you can do, therefore, is to first make an SSTP VPN to our servers and then make a second VPN connection to your office, over our SSTP VPN, which has all the ports open that your VPN requires.

The picture opposite shows two VPNs connected simultaneously.

This also works on a Mac running Windows 7 using Parallels. You first make an SSTP connection with Windows 7 and then make a PPTP connection from the Mac OS.

We haven't tested all types of VPN to see if they will connect over an SSTP VPN connection but a PPTP VPN over SSTP VPN will.
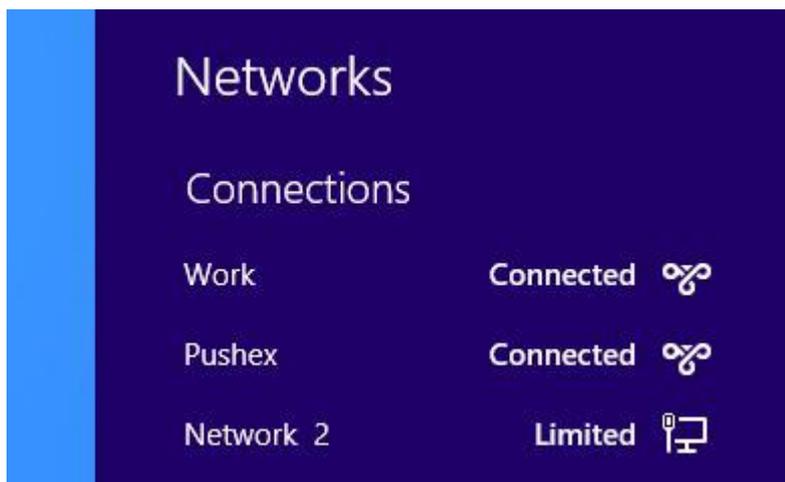
4 - Troubleshooting Tips

Certificate Revocation List problem

A valid commercial digital certificate is required on our VPN server to make an SSTP connection, which, of course, we have in place.
Valid means the certificate was issued by an authority Windows trusts, the name on the certificate is **vpn.pushex.com** and the certificate hasn't expired.
It could be possible that someone's stolen our certificate from us and is using it to *pretend* to be our company.
When a certificate is stolen or compromised in some way, it can be reported to the issuer who will then revoke the certificate and, until it expires, add it to its list of invalid certificates on the Certificate Revocation List or CRL.

So, before Windows will allow an SSTP connection to connect, it goes out onto the Internet to check the CRL to see if our certificate is on it. It isn't, of course, but it's possible that there could be a problem downloading the CRL from your location.

If Windows can't access the CRL then it will refuse to make the VPN connection – simple as that.

The CRL checking process usually works without a hitch but, if you ever get an error message about a CRL problem, or you just want to save a few seconds during the connection process, you can tell Windows not to bother checking the CRL.

To disable CRL checking you need to edit the Windows registry.
The Registry contains settings which, if changed or deleted, can stop your PC functioning.
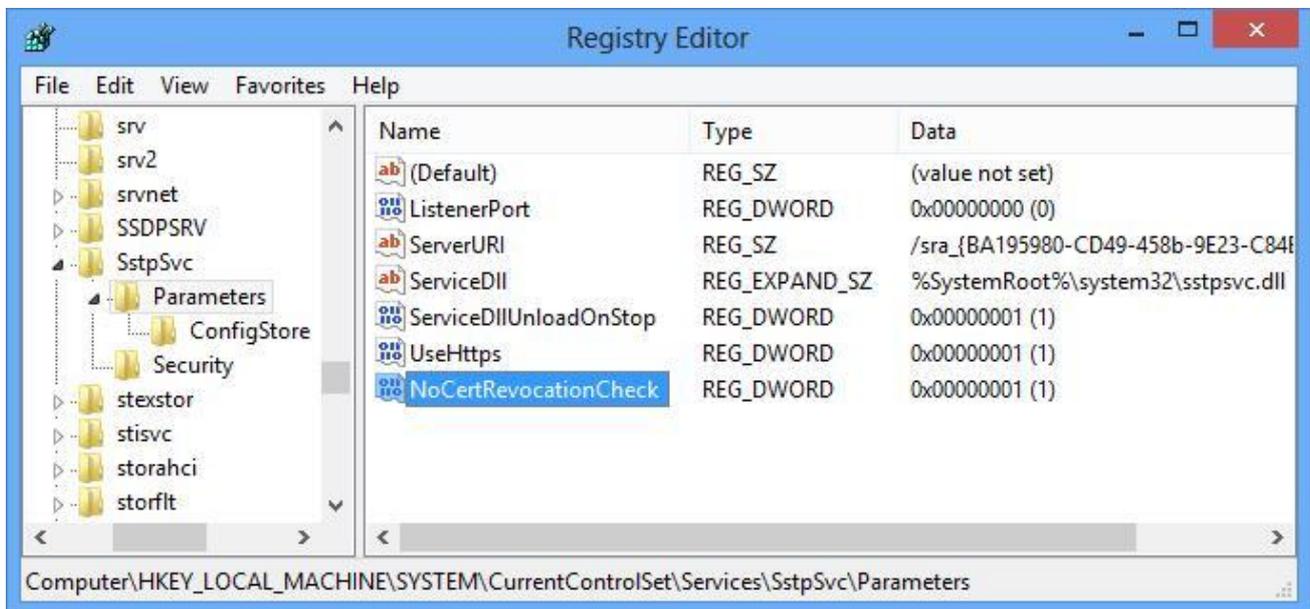Don't be put off by this warning, just make the changes carefully.
To run the Registry Editor click: **Windows Key + R** and type **regedit** into the **Open:** box, then press **OK**

Navigate to the key:-

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Sstpsvc\Parameters

Click: **Edit – New** and create a new DWORD (32 bit) Value called **NoCertRevocationCheck**
and set its value to **1**

Click: **OK** and then **File – Exit** to quit the Registry Editor.

To save you having to edit the Windows Registry, we have a file you can download to create the required registry value automatically.

Download this file:-

http://support.pushex.com/files/NoCertRevocationCheck.reg

Save it to your Desktop and then double-click on it.
Click: **Yes** to the warnings and the required value will be added to your registry.

Connection Error

If you get the error message shown opposite after you have just created a VPN connection and are attempting to connect for the first time, it may be because you missed out a step on the **Security** tab of the connection Properties window.
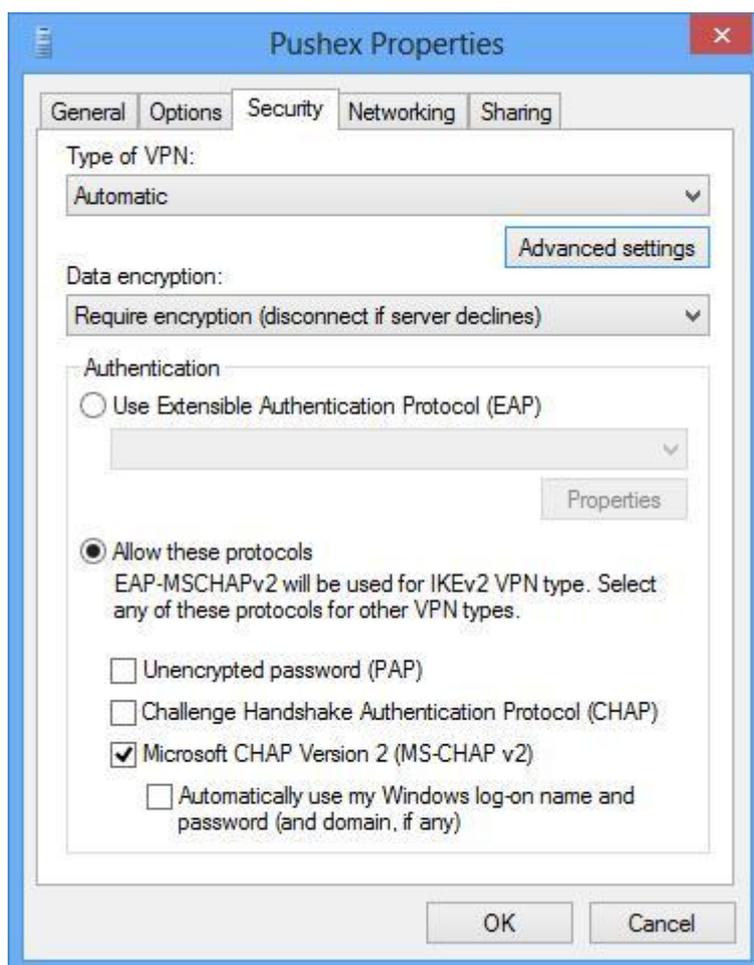
This is a new requirement in Windows 8 which was enabled by default in previous version of Windows.
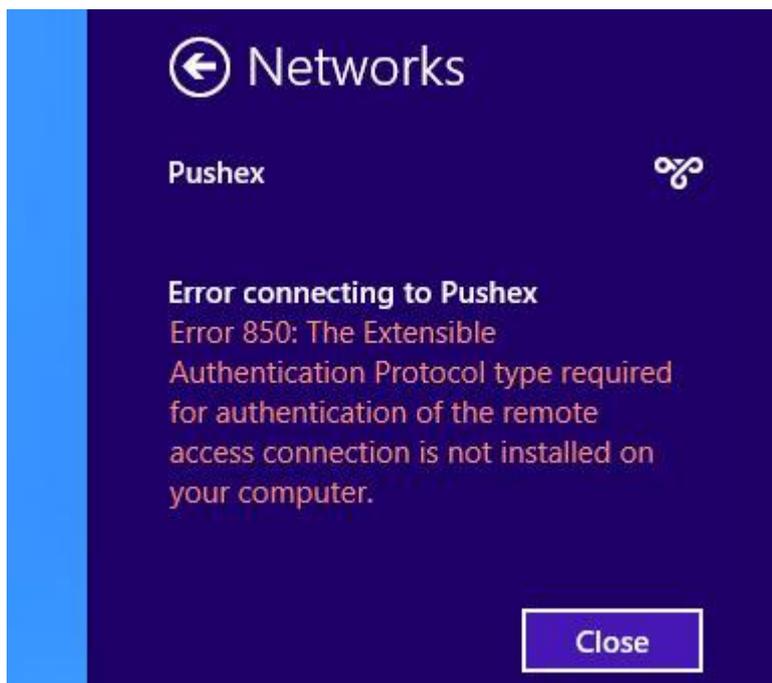
Here's the Security tab again and it is:-

Allow these protocols and
Microsoft CHAP Version 2 (MS-CHAP v2)

that need to be selected.

The VPN connects but your computer isn't using the VPN for Internet access

When connected, if you go to the website:-http://www.whatismyipaddress.com
it should show your computer as being located in the UK, but if it doesn't, it's possible that a setting is wrong on the VPN connection properties.

Access the connection Properties window by right-clicking on the Network icon in the notification area and choose **Open Network and Sharing Center** as shown in Section 1.
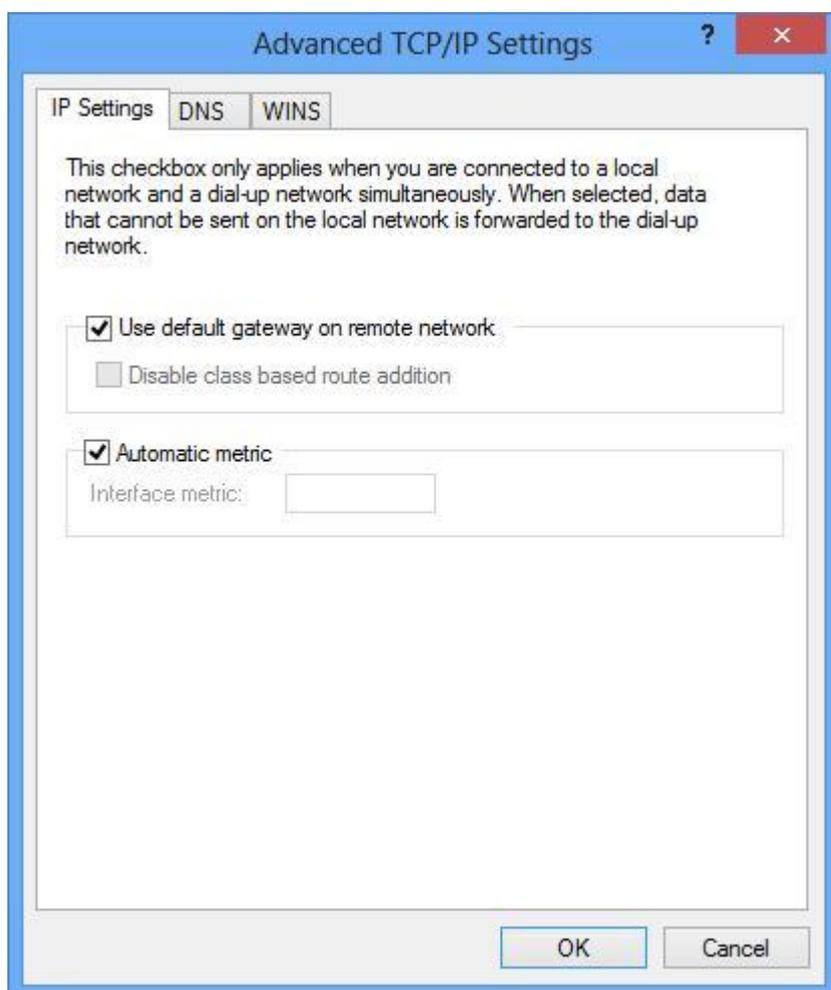
Go to the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)**

Click: **Properties** then **Advanced** to display this window:-

Make sure that:-

Use default gateway on remote network

is selected.

DNS Server Problems

DNS servers convert website names, such as **www.google.com**, into numeric IP addresses, such as **209.85.229.104**

There are several reasons why you want to use the DNS servers on our VPN servers, rather than your local DNS servers, when the VPN is connected:-

1. Your ISP might be giving you the wrong answers to DNS lookup requests, *on purpose*, as an easy way to block access to particular sites.
2. Your ISP could be logging all your DNS requests to check what you are doing.
3. Your ISP could, quite legitimately, be sending you to, for example, your nearest Hotmail server when what you *actually* want, to get the speediest response, is the Hotmail server located nearest to our VPN servers.

Unlike Windows XP, there's usually *no problem* with Windows 8 using the VPN server's DNS servers when connected, and then your local DNS servers when not connected.
All this section is doing, therefore, is to show you a simple way to check which DNS servers your computer is using.

When you're connected to the VPN, you can check that you're using the DNS servers on the VPN server by typing the following into your browser:-

http://www.dns.test

The top-level domain **test** doesn't exist and so no DNS servers on the Internet will be able to find the required IP address, which means the webpage will fail to load.
We've added a dummy record to the DNS servers on our VPN servers so, if your PC is using our DNS servers, the webpage *will* load correctly.

The VPN connection will not connect

If you have followed these instructions carefully and can't connect, here are some suggestions:-

1. If this is the first time you are trying to connect and you've been trying a few times then send us an email and we'll double-check that your account is setup correctly.
   You use the same username and password as you do for your mailbox so check to see if you can still logon to webmail at http://pushex.com from your location.

2. If you have previously been connecting OK but suddenly can't, check to see if your Internet connection has dropped out (go to Google) and that your subscription to the Hosted Exchange service is still current.