

*unlimited  
possibilities*



**UNIVERSITY HALL**  
THE UNIVERSITY OF WESTERN AUSTRALIA

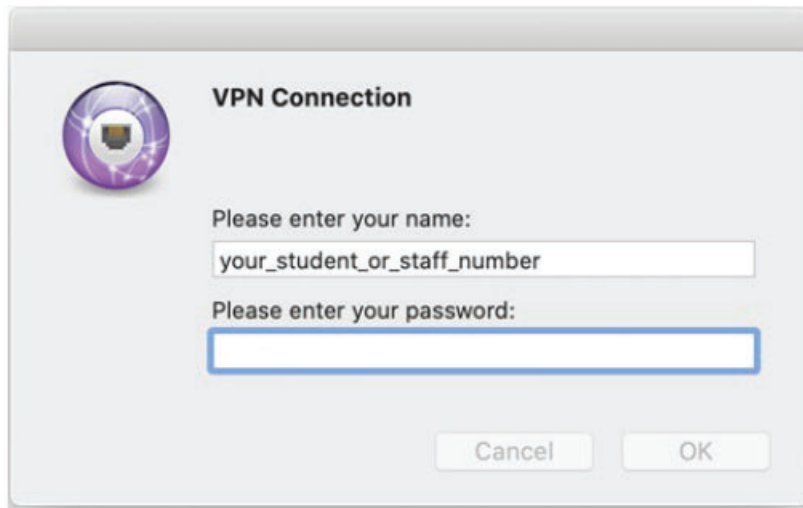


**UNIVERSITY HALL**  
THE UNIVERSITY OF WESTERN AUSTRALIA

# UniConnect Instructions for UWA Students







5. You will receive a prompt for you Microsoft Multifactor Authenticator (MFA) application. Approve the connection.
6. When connected the only way to see this is if you have enabled “Show Time Connected” in the menu bar VPN menu.
7. When the VPN connection is no longer needed, click the **VPN icon**, then click **Disconnect UniConnect** (or whatever name you’ve set your VPN connection to) to disconnect from the VPN.



## Windows 10 Devices

## Before you Begin

- You must use the Authenticator App for Multi-factor Authentication. Other methods, including SMS or Yubikey, will not work.
- Log on to <https://aka.ms/mfasetup> and confirm that the default sign-in method is set to Microsoft Authenticator - Notification.

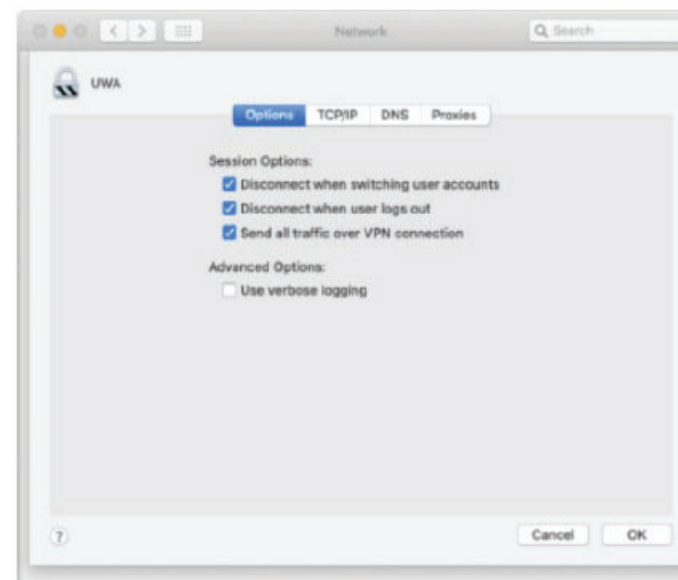
You can switch to using the Authenticator App by following the MFA Quick Setup Guide.

## Create a VPN Profile

- Select the Start button, then click Settings (gear icon) > Network & Internet > VPN > Add a VPN connection.

- In add a VPN connection:
  - For VPN provider, choose Windows (built-in).
  - In the Connection name box, enter the name UniConnect. This is the VPN connection name you'll look for when connecting.
  - In the Server name or address box, enter studentremoteaccess.uwa.edu.au.
  - For VPN type, choose L2TP/IPsec with pre-shared key.
  - Use UNIWA as the Pre-shared Key (note that this is case-sensitive – you must use all capitals).
  - For Type of sign-in info, choose Username and password.
  - For the Username box, enter your staff or student ID.
  - Click Remember my sign-in info.
  - Click Save.

- Now select the Options tab and tick the box **Send all traffic over the VPN connection**.

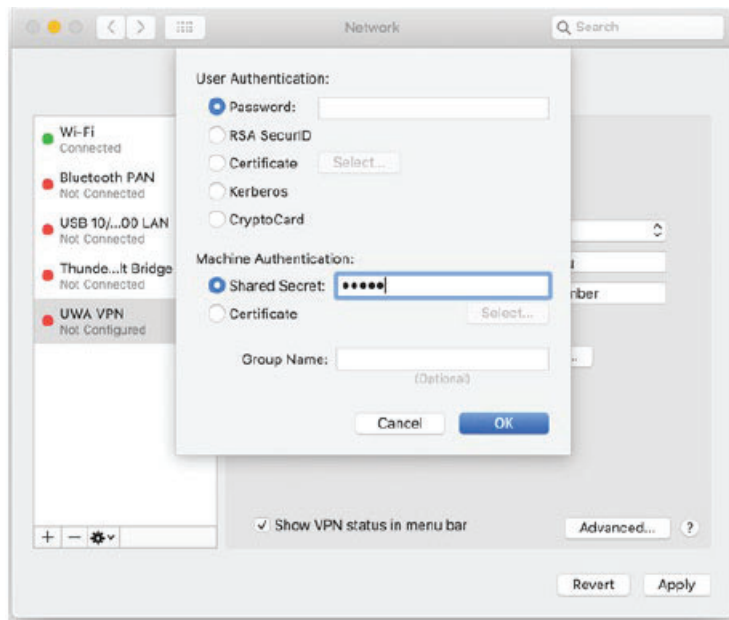


- Click **OK**.
- Click **Apply**.

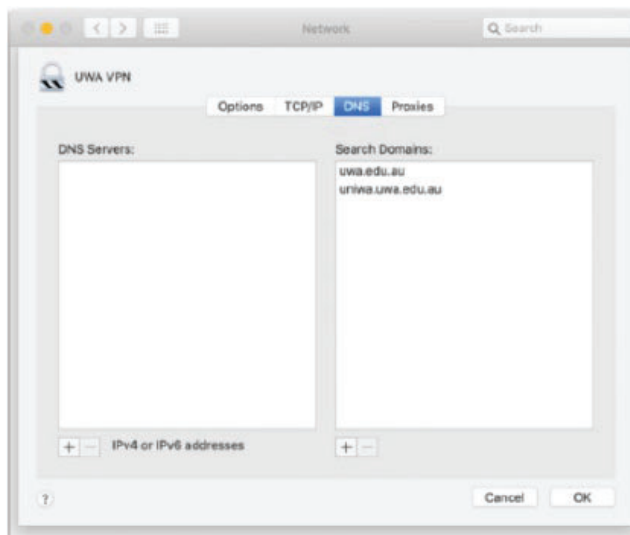
## Connect to the VPN

- Have your mobile phone handy – you'll need it close by for MFA.
- You can connect from this window using the Connect button or from the button at the top right of the menu bar; if you click it, it will expand. We recommend ticking the "Show Time Connected" as it's the only indicator to show you are connected.
- Click **Connect UniConnect**.
- In the VPN Connection window, complete the following steps:
  - In the Please enter your name box, enter your student ID.
  - In the Please enter your password box, enter your PHEME password.
  - Click **OK**.

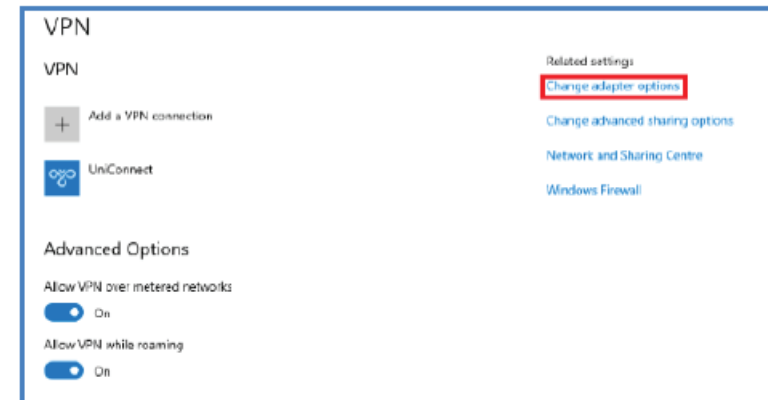
6. Select Shared Secret and enter UNIWA in the box. Click OK.



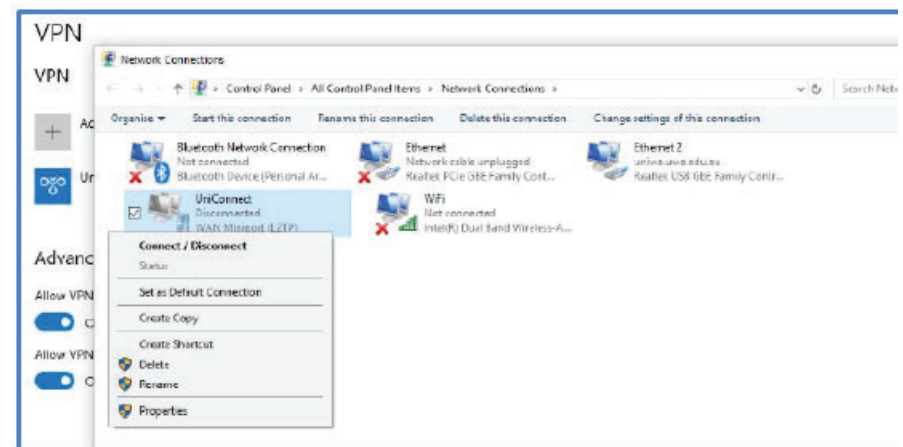
7. Click the Advanced button in the lower right and then select the DNS tab. On the right side of the window click the + and add first uniwa.uwa.edu.au and then uwa.edu.au Then click OK.



3. While still in the VPN window, click **Change adapter options**.

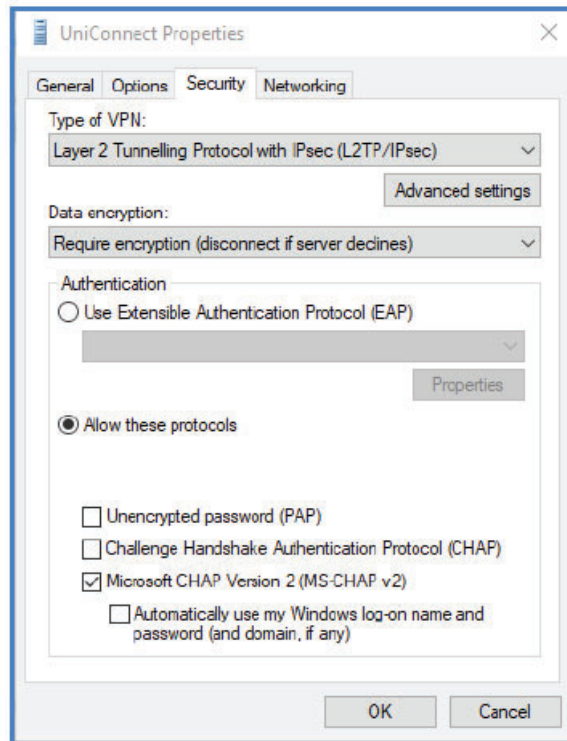


4. Right click on the new VPN you just set-up and click Properties.

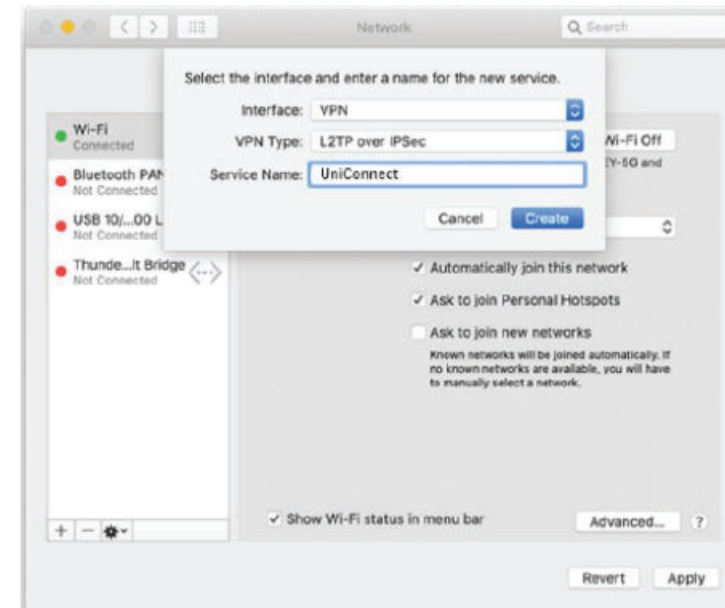
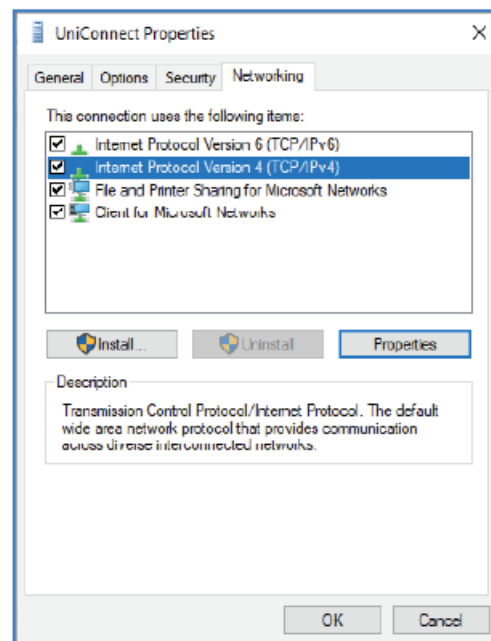


5. Go the **Security** tab:
- In the **Data encryption** drop down, ensure that **Require encryption** is selected.
  - In the **Authentication** section, select **Allow these protocols**, untick **Unencrypted password (PAP)** and tick **Microsoft CHAP Version 2 (MS-CHAP v2)**.

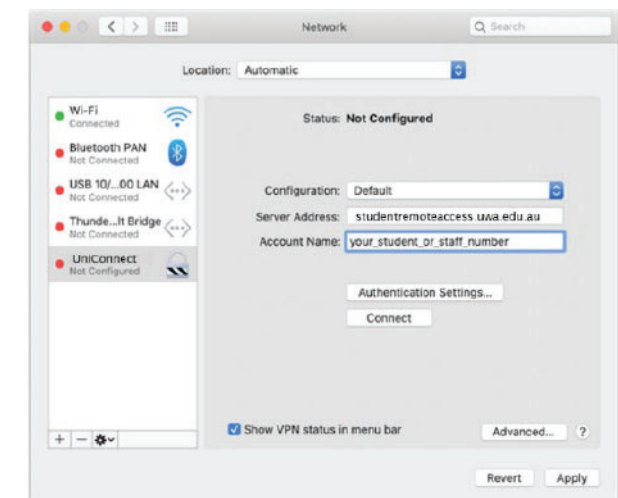




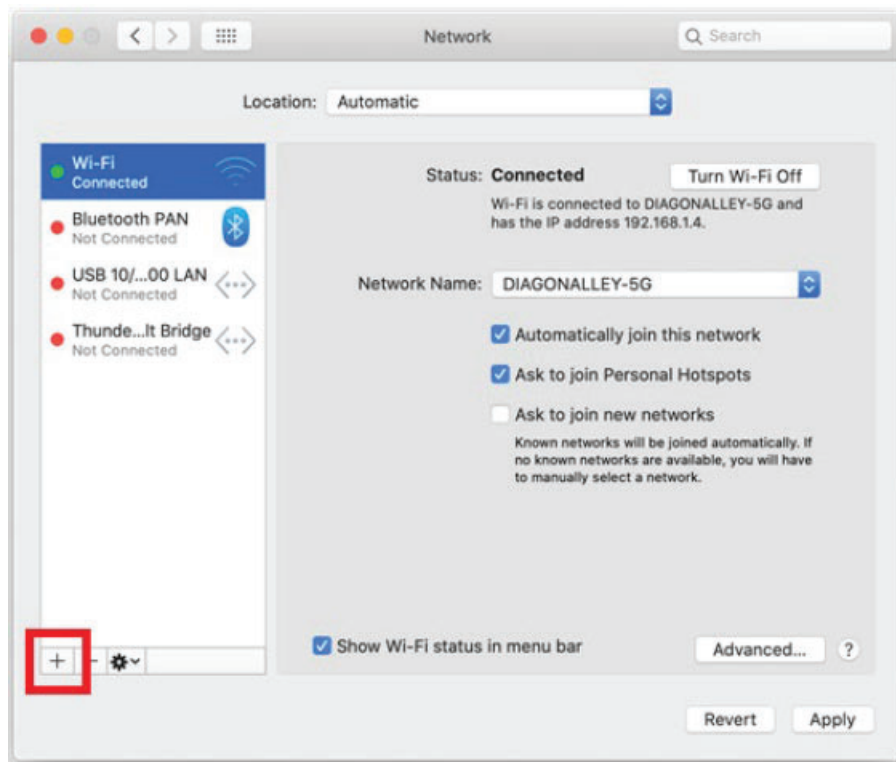
6. Go to the **Networking Tab**, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



5. Back in the Network window, select the new VPN connection and do the following:
- In the Server Address box, enter **studentremoteaccess.uwa.edu.au**.
  - In the Account Name box, enter your staff or student ID.
  - Tick the **Show VPN status in menu bar** box.
  - Click **Authentication Settings....**

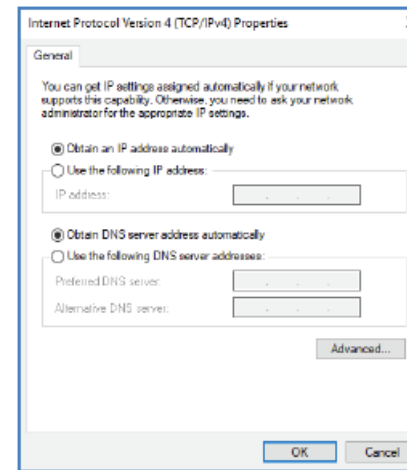


- Click the + button in the lower left of Network to add the VPN connection.

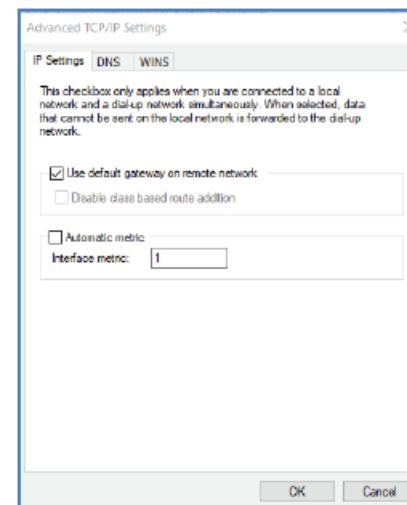


- In new connection window, complete the following steps:
  - For the Interface, select **VPN**.
  - For VPN Type, select **L2TP over IPSec**.
  - In the Service Name box, enter a name you'll recognize (for example, UWA VPN). This is the VPN connection name you'll look for when connecting.
  - Click **Create**.

- Click the **Advanced** Button.



- Uncheck the **Automatic metric** checkbox and then set **Interface metric** to 1.



- Click **OK** to confirm.
- Click **OK** to close the **Internet Protocol Version 4** window.
- Click **OK** to close the **UniConnect Properties** window.
- Close the Network Connections and Settings windows.

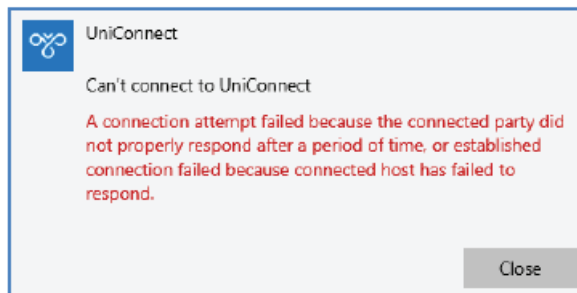
## Connect to UniConnect

1. Have your mobile phone handy – you'll need it close by for MFA.
2. On the far right of the taskbar, select the Network icon.
3. Select the **UniConnect** connection and then select **Connect**.
4. If you're prompted, enter your username (student number) and password.
5. You will receive a prompt via the Microsoft Multifactor Authenticator (MFA) app on your mobile device. Approve the connection to connect.
6. When connected, the VPN connection name will display **Connected** underneath it. To see if you're connected to the VPN while you're doing things on your PC, select the Network icon (either or ) on the far right of the taskbar, then see if the VPN connection says **Connected**.
7. When the VPN connection is no longer needed click **Disconnect** to disconnect from the VPN.

## Troubleshooting

### Q1. "A connection attempt failed" or "The L2TP connection failed."

One of the following messages are displayed when the connection is launched:



Ensure that you are not connected to the on-campus University network, the UniFi Wi-Fi network, or another VPN service – the UniConnect is only required when you're **not on campus**, and cannot be used in conjunction with another VPN service.

### Q2. "The connection was terminated."

The following message is displayed when the connection is launched:

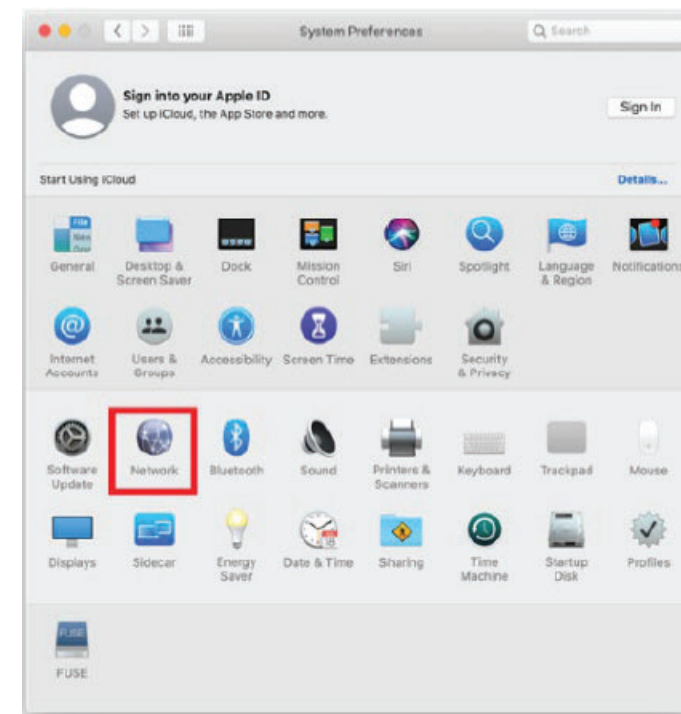
## Before you Begin

- You must use the Authenticator App for Multi-factor Authentication. Other methods, including SMS or Yubikey, will not work.
- Log on to <https://aka.ms/mfasetup> and confirm that the default sign-in method is set to Microsoft Authenticator - Notification.

You can switch to using the Authenticator App by following the MFA Quick Setup Guide.

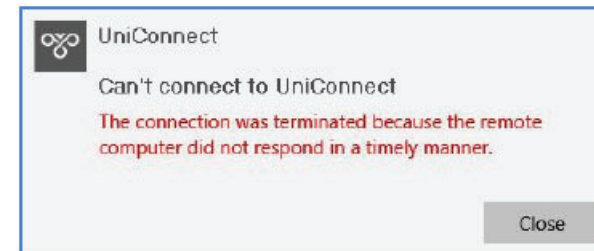
## Create a VPN Service

1. Open System Preferences by selecting the System Preferences application found in the Applications folder or from the Apple menu at the top-left of the screen (click the Apple logo).
2. Click **Network**.





## MacOS Devices



This message is generally displayed when your Multifactor Authentication (MFA) has not been setup correctly for use with UniConnect. Refer to the instructions at the start of this guide to Setup MFA with Authenticator App.

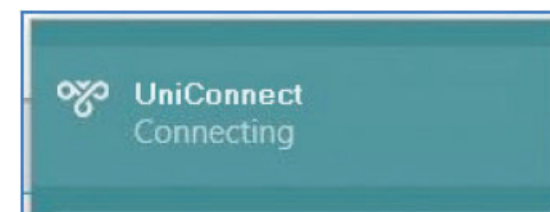
### Q3. "I receive multiple MFA requests, and cannot connect to the VPN."

When you connect to the VPN, an MFA approval will be sent to your mobile phone. If that approval request times out (usually around 30 seconds to a minute), the system will re-prompt for approval. Occasionally, this can result in a multiple MFA approval prompts, and stop you connecting to the VPN completely.

If this occurs, please wait 10 minutes before trying to reconnect to the VPN; try to keep your mobile phone handy when initially connecting, and approve the MFA prompt as soon as it comes though.

### Q4. The connection keeps displaying "Connecting" message and does not appear to complete connection.

On some versions of Windows 10 when you launch the connection from the task bar as shown in earlier instructions, the connection appears to stay connecting displaying the following if you look at your network connections. This is a known issue with some versions of Windows 10. On some versions A



workaround for this known issue is to connect to the VPN as shown below:

Select the **Start** button, then click **Settings > Network & Internet** then select **UniConnect** and Click **Connect**.