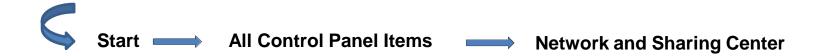
WIRELESS NETWORK CONFIGURATION

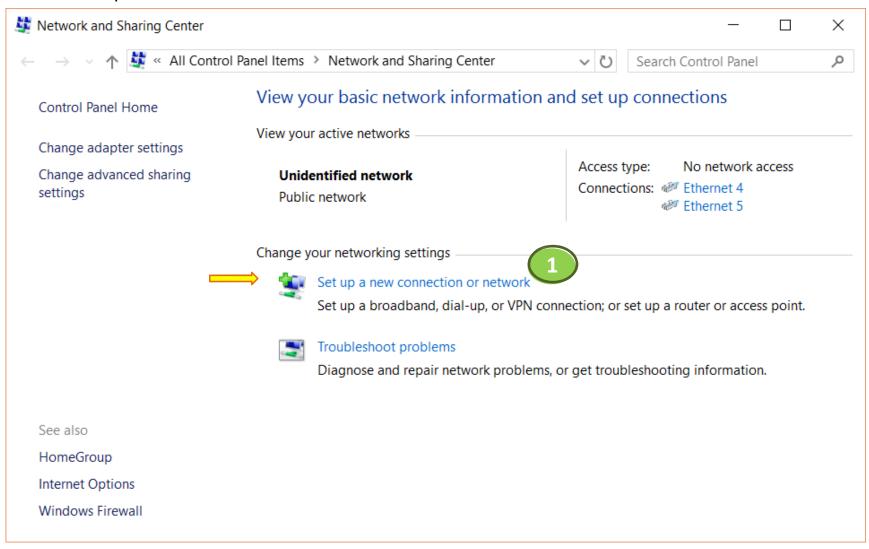
(Windows 10)

Prepared by:

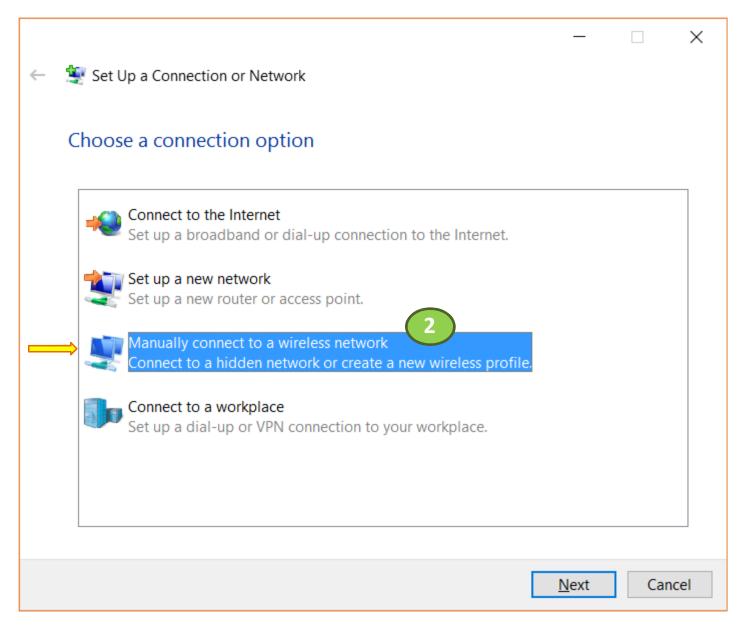
Centre for Digital Technology
(DiTec)
PUSAT TEKNOLOGI DIGITAL
Universiti Malaysia Pahang AL-Sultan Abdullah



1. Click Set up a new connection or network



2. Select Manually connect to a wireless network



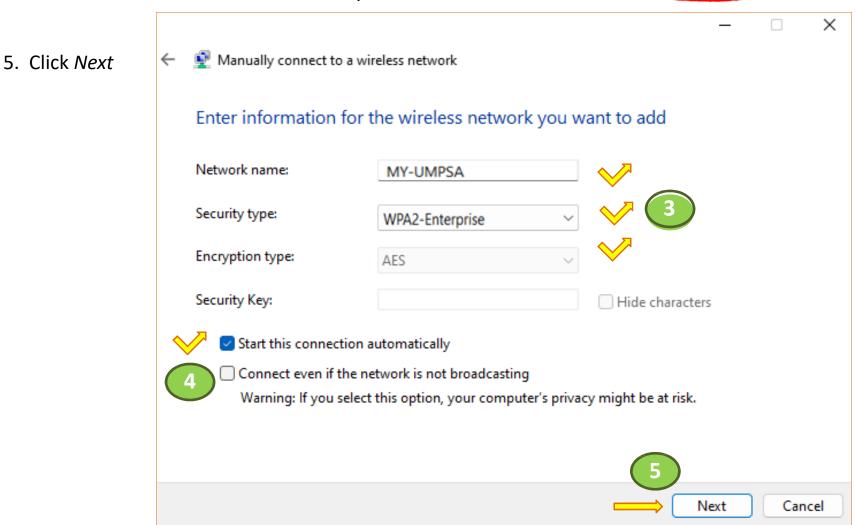
3. Enter the following details: Network name: MY-UMPSA

Security type: WPA2-Enterprise

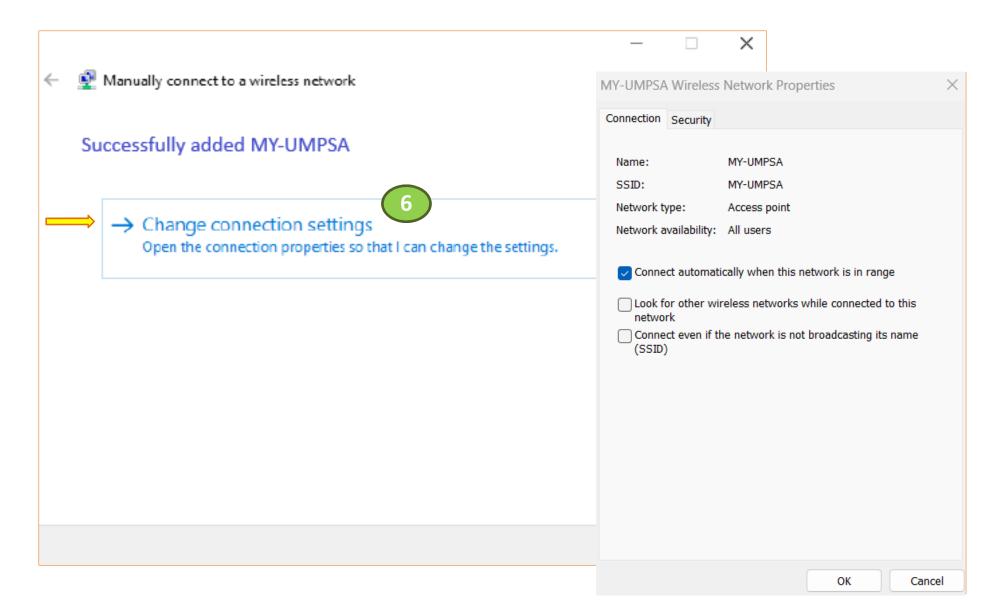
Encryption type: **AES**

4. Tick Start this connection automatically

*capital letter for 'MY'
with dash '-'



6. Click Change connection settings



7. Click the Security tab. Ensure that the Security type is set to WPA2-Enterprise and Encryption type is set to AES.

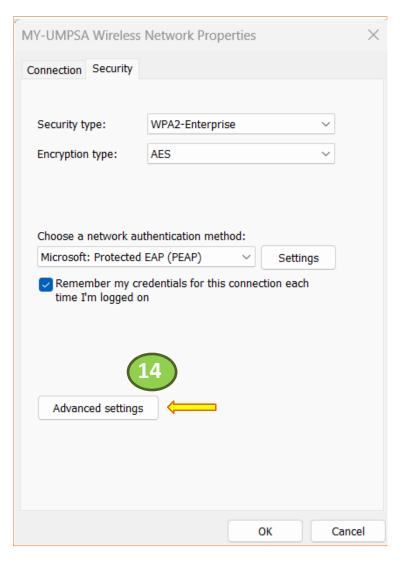
10. Untick Verify the server's identity by validating the certificate

- 8. Ensure that the network authentication method is set to Microsoft: Protected EAP (PEAP)
- 9. Click Settings

MY-UMPSA Wireless Network Properties Protected EAP Properties 13. Untick *Automatically use* When connecting: Connection Security my Windows logon name and Verify the server's identity by validating the certificate password (and domain if any). Connect to these servers (examples:srv1;srv2;.*\.srv3\.com): Security type: WPA2-Enterprise Your device will not connect if **AES** Encryption type: this is selected Trusted Root Certification Authorities: AddTrust External CA Roo avast! Web/Mail Shield Root X EAP MSCHAPv2 Properties avast! Web/Mail Shield Root Choose a network authentication method: Baltimore CyberTrust Root Microsoft: Protected EAP (PEAP) Certum CA When connecting: Class 3 Public Primary Certification Authority Remember my credentials for this connection each. DigiCert Assured ID Root CA Automatically use my Windows logon name and time I'm logged on password (and domain if any). Notifications before connecting: Tell user if the server's identity OK Cancel Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure... Advanced settings 12. Click Configure Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel OK. Cancel

11. Ensure Authentication Method is set to Secured password (EAP-MSCHAP-v2)

Advanced settings

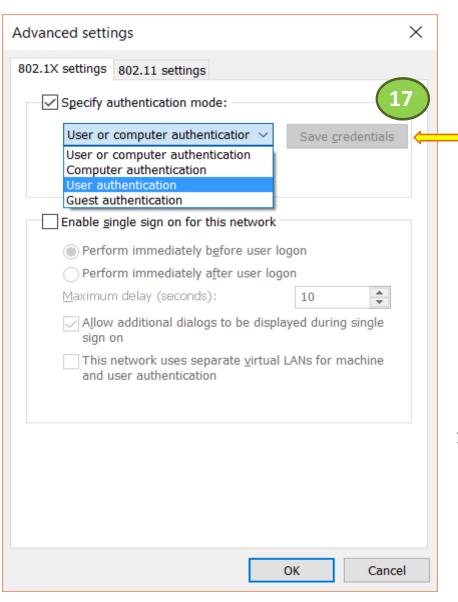


2.1X settings 802.11 settings Specify authentication mode: User or computer authentication > Save credentials User or computer authentication Computer authentication User authentication Guest authentication Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication OK Cancel

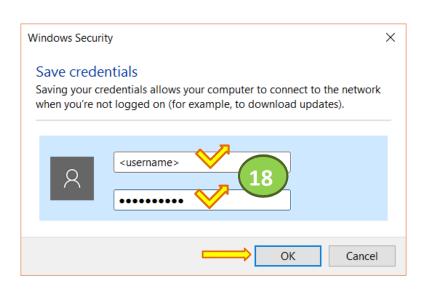
 \times

14. Click Advanced settings

- 15. Select *Specify authentication mode*
- 16. From the drop down menu, choose *User authentication*



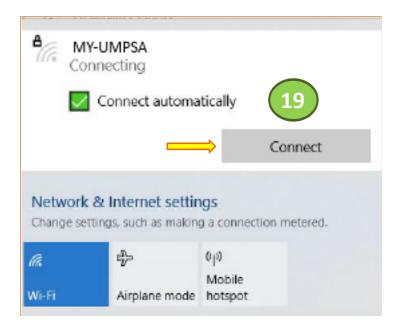
17. Click Save credentials

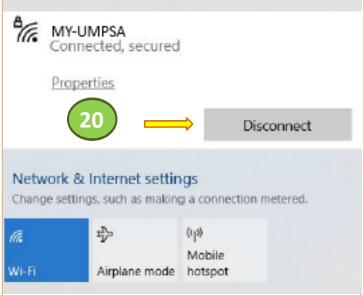


- 18. Enter your UMPSA-ID ecomm Username and Password
 - ** This credentials should be same as logging into your ecomm, email, UMPSA Online Learning, etc.

19. When the device is in range of the wireless network, you can choose to connect to SSID MY-UMPSA which listed under *Wireless Network Connection*.

<u>Note</u>: Tick on the box *Connect automatically* if you want **MY-UMPSA** to connect automatically next time when it's in connection range.





20. Once connected to MY-UMPSA you can click on *Properties* to view the connection settings that you have done.

<u>Note</u>: Click on *Disconnect* button to ensure that **MY-UMPSA** Wi-Fi network session properly terminated after not in use