Wireless Connection Installation for windows 8.1- UWU Wi-Fi Zone



IT UNIT

1. Go to the start menu and search for "Control Panel" (Figure 01)



2. "Network and Sharing Center", click "Set up a new connection or network". (Figure 02)



3. Enter the network name "UWU Staff, Security Type WPA2- Enterprise, Encryption type should be AES and click "Next" (**Figure 03**)

_

	_ 🗆 🗡		
📀 🔮 Manually connect	to a wireless network		
Enter information fo	or the wireless network that you want to add		
Network name:	UWU Students		
Security type:	WPA2-Enterprise V		
Encryption type:	AES 🗸		
Security Key:	Hide characters		
✓ Start this connection automatically			
Connect even if the	network is not broadcasting		
Warning: If you select this option, your computer's privacy might be at risk.			
	Next Cancel		

4. Click next, and then choose "Change connection settings" (Figure 04)

	_ □	×
📀 🔮 Manually connect to a wireless network		
Successfully added UWU Staff		
Change connection settings Open the connection properties so that I can change the settings.		
	CI	ose

5. Click the Security" tab on the top and "Microsoft: Protected EAP (PEAP)" is selected in the drop down, then click Settings (**Figure 05**)

Successfully added UWU Staff UWU Staff Wireless Network Properties Connection Security gs.
UWU Staff Wireless Network Properties
Connection Security
Encryption type: AES V
Choose a network authentication method: Microsoft: Protected EAP (PEAP) ✓ Settings ✓ Remember my credentials for this connection each time I'm logged on
Advanced settings
OK Cancel

 Click off the "verify the Servers identity by validation the certificate Select authentication method "Secured password (EAP-MSCHAP v2)" and click the "configure " (Figure 06)

ntly connected to any networks.	Protected EAP Properties
	When connecting:
	Verify the server's identity by validating the certificate
🕑 🔄 🔮 Manually conne	Connect to these servers (examples:srv1;srv2;,*\.srv3\.com):
^{is} Successfully added	Trusted Root Certification Authorities: AddTrust External CA Root Baltimore CyberTrust Root
UWU Stat	Certum CA
Connection Securit	COMODO KSA Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA
Security type:	S 2
Encryption type:	Tell user if the server's identity cannot be verified V
	Select Authentication Method:
Choose a network	Secured password (EAP-MSCHAP v2) V Configure
Microsoft: Protect	Enable Fast Reconnect
Remember my time I'm logge	Perforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy
	OK Cancel
Advanced setti	ngs

7. A smaller window will appear, uncheck the only check box there, and click OK (Figure 07)

	Protected EAP Properties
	EAP MSCHAPv2 Properties
	When connecting: Automatically use my Windows log-on name and password (and domain if any).
UWU Staff Connection Security Security type:	Certum CA Class 3 Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA Collect High Assured PUblic CA Notifications before connecting:
Encryption type: Choose a network ; Microsoft: Protecte Remember my time I'm logged	Tell user if the server's identity cannot be verified Select Authentication Method: Secured password (EAP-MSCHAP v2) Enable Fast Reconnect Enable Fast Reconnect Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK

8. Network Properties window, click the "Advanced Settings" button. Choose "User Authentication" from the drop down, then click "save credentials" (Figure 08)

Successfully addec	l UWU Staff		Advanced settings	
UWU Stat	f Wireless Network Properties	×	802.1X settings 802.11 settings	
Connection Securit	y	gs.	Specify authentication mode:	ve credential
Security type:	WPA2-Enterprise V		Delete credentials for all user:	
Choose a network	authentication method:		Enable single sign on for this network Perform immediately before user log-on Perform immediately after user log-on	
Microsoft: Protect	ed EAP (PEAP) V Settings credentials for this connection each d on		Maximum Delay (seconds): 10 May additional dialogues to be displayer single sign on This network uses separate virtual LANs and user authentication	d during
Advanced setti	ngs			

9. Enter your user name and password, then click OK (Figure 09)

 Networks
Checking network requirements
Cancel
Sign in
thisraa
Domain:
OK Cancel

10. Finally change the proxy setting and browse the internet (Figure 10)

	Connection Settings		×		
Configure Proxies to Access the Internet					
O No proxy					
○ Auto-detect proxy settings for this net <u>w</u> ork					
○ <u>U</u> se system pro	O Use system proxy settings				
<u>M</u> anual proxy of the second sec	configuration:				
<u>H</u> TTP Proxy:	cache.uwu.ac.lk Port: 3128				
	✓ Use this proxy server for all prot	ocols			
<u>S</u> SL Proxy:	cache.uwu.ac.lk	P <u>o</u> rt:	3128 💂		
<u>F</u> TP Proxy:	cache.uwu.ac.lk	Po <u>r</u> t:	3128 💂		
SO <u>C</u> KS Host:	cache.uwu.ac.lk	Por <u>t</u> :	3128 💂		
	SOC <u>K</u> S v4 SOCKS <u>v</u> 5 Remote <u>D</u> NS				
No Proxy for:					
localhost, 127.0.0.1					
Example: .moz	illa.org, .net.nz, 192.168.1.0/24				
O <u>A</u> utomatic proxy configuration URL:					
			R <u>e</u> load		
Do not prompt for authentication if password is saved					
	OK Cance	el	<u>H</u> elp		