

Windows 7 Setup for "TIFRH-WLAN"

1. Windows taskbar click on the Network icon.



2. Click on "Open Network and Sharing Center"



3. Click on "Setup a new connection or Network"





4. Click on "Manually Connect to a wireless Network"



5. Enter Netwrk Name : TIFRH-WLAN Select Security Type : EAP2-Enterprises Encryption Type : AES Click on "Next"



Manually connect to	o a wireless network	add
Enter mormation		auu
Network name:	TIFRH-WLAN	
Security type:	WPA2-Enterprise 2	
Encryption type:	AES 3 -	
Security Key:	Hid	le characters
V Start this connec	tion automatically	
Connect even if	the network is not broadcasting	
Warning: If you	select this option, your computer's privacy might	be at risk.

6. Click on "Change Connection Settings"

and the second s	
🕞 🔮 Manually connect to a wireless network	
Successfully added TIFRH-WLAN	
Change connection settings Open the connection properties so that I can change the settings.	
	Close



7. Select the "Security" tab . Chose network authentication method as "Microsoft : protected EAP (PEAP) " and Click on "Settings"

TIFRH-WLAN Wireless No	etwork Properties
Connection Security	1
Security type: Encryption type:	WPA2-Enterprise AES
Choose a network aut Microsoft: Protected E Remember my cred time I'm logged on	entication method EAP (PEAP) ▼ Settings lentials for this connection each
	OK Cancel



8. Un-select "Validate Server Certificate" and Click on "Configuration"

Protected EAP Properties	×
When connecting:	
Connect to these servers:	
Trusted Root Certification Authorities: AddTrust External CA Root Baltimore CyberTrust Root	
Certum Trusted Network CA Class 3 Public Primary Certification Authority COMODO RSA Certification Authority DisiCert Assured ID Reat CA	
DigiCert Global Root CA III	-
Do not prompt user to authorize new servers or trusted certification authorities.	
Select Authentication Method:	
Secured password (EAP-MSCHAP v2)	ure
Enable Fast Reconnect Enforce Network Access Protection	
Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	

9. Un-select the checkbox and click "OK"

EAP M	ISCHAPv2 Properties
Whe	n connecting:
	Automatically use my Windows logon name and password (and domain if any).
	OK Cancel



10. Click on "Advance Settings"

TIFRH-WLAN Wireless N	letwork Properties	X
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES 🔻	
Choose a network aut	hentication method:	
Microsoft: Protected	EAP (PEAP) Settings	
Remember my creating I'm logged on	dentials for this connection each	
une in logged on		
Advanced settings		
	ОК Са	ncel



11.

- 1. Select the tab "802.1x Settings"
- 2. check the "Specify authentication mode"
- 3. select "User Authentication"
- 4. click on "Save Credentials"

Save credential Save credential Save credential Delete credentials for all users Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10	I terr authorities time	
 Delete credentials for all users Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	User authentication	Save credential
 Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	Delete credentials for all use	rs
 Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	Enable single sign on for this net	work
 Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	Perform immediately before under the second seco	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	Perform immediately after us	er logon
 Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	Maximum delay (seconds):	10 *
This network uses separate virtual LANs for machine and user authentication	Allow additional dialogs to be sign on	displayed during single
	This network uses separate and user authentication	virtual LANs for machine

12. Enter your username and password, Click ok. It will get connected now.

