

ICT DEPARTMENT

Wireless Authentication Procedures for Windows 7 & 8 Users

For Linux and windows XP users visit ICT office

Requirements:

- 1. Wireless enable laptop with Valid Anti-Virus
- 2. Configure your wireless network card using the below procedures
- 3. Domain Account (Username & Password).
 - NB// Your Username is composed of your firstname.lastname e.g john.kimani
 Obtain these credentials from the ICT office,
 For Inquiries visit ICT office or E-mail ict@pu.ac.ke

Windows 7

Step 1:

Open the Wireless Connection and Click "Open Network and Sharing Center"



On Network and Sharing Center dialog box "Click Manage Wireless Networks"



Step 3

Click ADD button



Click Manually Create a Network Profile

do you want to add a network?	
Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).	
Create an ad hoc network This creates a temporary network for sharing files or an Internet connection	

Step 5

NB// The Network name can either be PU WIFI or eduroam. Choose ONLY one depending on signal strength

Key-in the following and Click Next

Enter the Network Name	PU WIFI
Enter Security Type	WPA2-Enterprise
Encryption Type	AES

G 📲 Manually connect to a v	vireless network
Enter information for	the wireless network you want to add
Network name:	PU WIFI
Security type:	WPA2-Enterprise 🔹
Encryption type:	AES 👻
Security Key:	Hide characters
Start this connection	automatically
Connect even if the	network is not broadcasting
Warning: If you sele	ct this option, your computer's privacy might be at risk.
	Next Cancel

Successfully added PU WIFI information is displayed

Click Change Connection Settings.

🕜 💷 Mar	nually connect to a wireless network	
Succe	ssfully added PU WIFI	
•	Change connection settings Open the connection properties so that I can change the settings.	0
		Close

Step 7

Click Security tab, Choose a network authentication method:- Microsoft: Protected EAP (PEAP) then Click Settings

Connection Security]	
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	ĸ
Choose a network a	umentication method:	
Microsoft: Protecte	d EAP (PEAP)	h
Microsoft: Protecte	d EAP (PEAP) Settings edentials for this connection each n	D s
Microsoft: Protecte	d EAP (PEAP) Settings edentials for this connection each in	Dis
Microsoft: Protecte	d EAP (PEAP) Settings edentials for this connection each n	n s

On the pop up window Uncheck Validate Server Certificate; Select Authentication Method as Secured password (EAP-MSCHAP V2) on the combo box

Click **Configure** Button and Uncheck **Automatically use my windows logon name and password......** and click Ok

rotect	ed EAP Properties				×
When	connectina:				
	/alidate server certific	ate			
1	Connect to these ser	vers:			
Tru	isted Root Certificatio	n Authorities:			
The second second	AddTrust External C	ARoot			<u>^</u>
1000	Baltimore CyberTrus	t Root			=
	Class 3 Public Primar	v Certification A	uthority		
	DigiCert Assured ID	Root CA			
Press.	DigiCert High Assura	ance EV Root CA			
	DST Root CA X3				
					·
	Do not prompt user to certification authoritie	o authorize new : es.	servers of t	rusted	
Select	Authentication Meth	od:			
Secu	red password (EAP-M	ISCHAP v2)	-	Confi	aure
	able Fact Decomposit				
E	force Network Acces	s Protection			
Di	sconnect if server doe	es not present cr	yptobinding	ILV	
E Di	sconnect if server doe able Identity Privacy	es not present cr	yptobinding	ILV	16
E Di	able Identity Privacy	es not present cr	yptobinding		
E Di	able Identity Privacy	es not present cr	OK		ancel
E Di	sconnect if server doe able Identity Privacy	es not present cr	OK		ancel
	able Identity Privacy	es not present cr	OK		ancel
	sconnect if server doe able Identity Privacy	es not present cr	OK		ancel
	EAP Properties	es not present cr	OK		ancel
tected	EAP Properties	es not present cr			ancel
tected When	EAP Properties CHAPv2 Properties	es not present cr	OK		ancel
tected When	EAP Properties CHAPv2 Properties	es not present cr			ancel
tected When	EAP Properties CHAPv2 Properties connecting:	es not present cr	OK		ancel
tected P MSC When	EAP Properties CHAPv2 Poperties connecting:	es not present cr			ancel
tected AP MSC When	EAP Properties CHAPv2 Poperties connecting: uromatically use my Windo assword (and domain if an	es not present cr			ancel
	EAP Properties CHAPv2 Properties connecting: unomatically use my Windo assword (and domain if an OK	es not present cr			ancel
	EAP Properties CHAPv2 Properties connecting: unomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certif giCert Assured ID Root C/ giCert High Assurance EV	es not present cr	OK		ancel
	EAP Properties CHAPv2 Properties CHAPv2 Properties connecting: unomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certif giCert Assured ID Root C/ giCert High Assurance EV ST Root CA X3	es not present cr	OK		ancel
tected When	EAP Properties CHAPv2 Properties connecting: utomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certif giCert Assured ID Root Co giCert High Assurance EV ST Root CA X3	es not present cr			ancel
	EAP Properties CHAPv2 Properties CHAPv2 Properties connecting: unomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certifi giCert Assured ID Root CA giCert High Assurance EV ST Root CA X3	es not present cr	OK OK		ancel
	EAP Properties CHAPv2 Properties connecting: unomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certifi giCert Assured ID Root C/ giCert High Assurance EV ST Root CA X3	es not present cr	OK OK OK Tusted		ancel
	EAP Properties CHAPv2 Properties CHAPv2 Properties connecting: unomatically use my Window assword (and domain if an OK ass 3 Public Primary Certif giCert Assured ID Root C/ giCert High Assurance EV ST Root CA X3 mot prompt user to author tification authorities.	es not present cr	OK OK CK CK		ancel
tected P MSC When P C C C C C C C C C C C C C	EAP Properties CHAPv2 Poperties CHAPv2 Poperties connecting: unomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certifi giCert Assured ID Root CA giCert High Assurance EV st Root CA X3 mot prompt user to authout tification authorities.	es not present cr	OK OK Configur		ancel
tected P MSO When P C C C C C C C C C C C C C	EAP Properties CHAPv2 Poperties CHAPv2 Poperties connecting: unomatically use my Windd assword (and domain if an OK ass 3 Public Primary Certific giCert Assured ID Root CA giCert High Assurance EV ST Root CA X3 mot prompt user to author tification authorities. uthentication Method: password (EAP-MSCHAP) the Fast Reconnect ce Network Access Protect	es not present cr	OK OK UNDER		ancel
Entor Disco	EAP Properties CHAPv2 Properties CHAPv2 Properties CHAPv2 Properties connecting: unomatically use my Windo assword (and domain if an OK ass 3 Public Primary Certific giCert Assured ID Root CA giCert High Assurance EV ST Root CA X3 mot prompt user to author tification authorities. uthentication Method: I password (EAP-MSCHAP) is Fast Reconnect ce Network Access Protect nect if server does not p	es not present cr			ancel

Click Ok to quit Protected EAP Properties

OK

Cancel

Click on Advanced Settings Tab

Check the checkbox to Specify authentication mode, Scroll the combo box and select User Authentication. Click 802.11 settings tab. Check that Enable Pairwise Master Key (PMK) caching is NOT TICKED. Click Ok to quit advance setting window

onnection Security]	
Security type:	WPA2-Enterprise	-
Encryption type:	AES	-
Choose a network au	uthentication method:	
Bemember my cre	edentials for this connection	settings
time I'm logged or	s	
	ОК	Cancel
lvanced settings		•
802.1X settings	802.11 settings	
		· · · · · · · · · · · · · · · · · · ·
	ouz. 11 setungs	
Specify au	thentication mode:	
Specify au	thentication mode:	Save credential
Specify au User auth	thentication mode: mentication credentials for all users	Save credential
Specify au User auth Delete	thentication mode: nentication credentials for all users gle sign on for this netwo	Save credential
Specify au User auth Delete	thentication mode: mentication credentials for all users gle sign on for this netwo	Save credential ork er logon
Enable sing Perforr	thentication mode: mentication credentials for all users gle sign on for this netwo mimmediately before user	Save credential ork er logon
Specify au User auth Delete Enable sing Perforr Perforr Maximum o	thentication mode: nentication credentials for all users gle sign on for this netwo m immediately before user delay (seconds):	Save credential
Specify au User auth User auth Delete Enable sing Perforr Maximum o Allow a sign on	thentication mode: nentication credentials for all users gle sign on for this netwo m immediately before user delay (seconds): additional dialogs to be d	Save credential
Specify au User autt User autt Delete Enable sing Perforr Perforr Maximum o Xallow a sign on This ne and use	thentication mode: nentication credentials for all users gle sign on for this netwo m immediately before user delay (seconds): additional dialogs to be d twork uses separate vir er authentication	Save credential
Specify au User auth Delete	thentication mode: nentication credentials for all users gle sign on for this netwo n immediately before user delay (seconds): additional dialogs to be d twork uses separate vir er authentication	Save credential

Click Close button to quit manually connect to wireless network window



Click on a pop up window (Additional Information is needed to connect PU WIFI) as shown below



Provide your username and password and click OK

Windows Security	
Network Au Please enter us	Ithentication er credentials
	User name Password
	OK Cancel

Windows 8 Authentication

Step 1

Move your mouse pointer to the top or bottom right corner without clicking and **Charms bar** will appear. Click on **Settings** then **Control Panel**



Step 2

On the control panel click Network and Internet



Click Network and Sharing shown below



Step 4

Click Set up a New Connection or Network

Network and Sharing Center – 🗆 🗙				
📀 🌛 🔹 🕇 🚆 « Network an	d Internet → Network and Sharing Center	✓ C Search Control Panel P		
Control Panel Home	View your basic network information and	l set up connections		
Change adapter settings	View your active networks			
Change advanced sharing settings	PU WIFI 7 Public network	Access type: Internet Connections: 📶 Wi-Fi (PU WIFI 7)		
See also	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connect Troubleshoot problems Diagnose and repair network problems, or g	ction; or set up a router or access point. net troubleshooting information.		
HomeGroup				
Windows Firewall				

Click Manually Connect to a Wireless Network

		-		×
1	📀 🔄 Set Up a Connection or Network			
e	Choose a connection option			
	Connect to the Internet Set up a broadband or dial-up connection to the Internet.			
	Set up a new router or access point.			
	Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.			
	Connect to a workplace Set up a dial-up or VPN connection to your workplace.			
	Next		Can	cel

Step 6

NB// The Network name can either be PU WIFI or eduroam. Choose ONLY one depending on signal

Key the following details then Click Next

Network Name PU WIFI

Security Type WPA2-Enterprise

Encryption AES

			- 🗆 🗙
IE	📀 🖳 Manually connect to	a wireless network	
11 73	Enter information for t	the wireless network you want to add	
	Network name:	PU WIFI	ר ר
	Security type:	WPA2-Enterprise V	
	Encryption type:	AES 🗸	
	Security Key:	Hide char	acters
	Start this connection a	automatically	
	Connect even if the ne	etwork is not broadcasting	
	Warning: If you select	this option, your computer's privacy might be at r	risk.
			Next Cancel

A successfully added PU WIFI is displayed. Click Change connection Settings

	- 🗆 🗙
) 🔄 🔮 Manually connect to a wireless network	
Successfully added PU WIFI	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

Step 8

Click Security tab, Choose a network authentication method:- Microsoft: Protected EAP (PEAP) then Click Settings

PU WIFI Wireless Network Properties				
Connection Security				
Security type:	WPA2-Enterprise	~		
Encryption type:	AES	~		
Choose a network authentication method:				
Microsoft: Protected E	EAP (PEAP) V	Settings		
Remember my credentials for this connection each time I'm logged on				
Advanced settings				
		ОК Са	ancel	

On the pop up window Uncheck Verify the server's identity by Validating Server Certificate.

Select Authentication Method as Secured password (EAP-MSCHAP V2) on the combo box

Click Configure Button and Uncheck Automatically use my windows logon name and password...... and click Ok

Network and Sha	aring Center
Protected EAP Properties	· · · · · · · · · · · · · · · · · · ·
When connecting:	icate
Connect to these servers (examples:srv1;srv2;.*	*\.srv3\.com): FI 7)
Trusted Root Certification Authorities:	EAP MSCHAPv2 Properties
Class 3 Public Primary Certification Authority GeoTrust Global CA Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority 2010 Microsoft Root Certificate Authority 2011	When connecting: Automatically use my Windows logon name and password (and domain if any).
StartCom Certification Authority	OK Cancel
Tell user if the server's identity can't be verified	
Select Authentication Method:	
Secured password (EAP-MSCHAP v2)	Configure Close
 Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding Enable Identity Privacy 	g TLV
OK	Cancel

Click Ok to quit Protected EAP Properties and Advance settings window

Click Advanced Setting Tab

ſ	PU WIFI 7 Wireless Network Properties				
	Connection Security				
	Security type: WPA2-Enterprise Encryption type: AES				
e	Choose a network authentication method: Microsoft: Protected EAP (PEAP) V Settings Remember my credentials for this connection each time I'm logged on				
	Advanced settings OK Cancel				

Click **802.1x setting** and **Check** the checkbox to **Specify authentication mode**, Scroll the combo box and select **User Authentication**.

Click **802.11 settings** tab. On Fast roaming section, **Uncheck** the checkbox **Enable Pairwise Master Key (PMK)** caching

Click **Ok** to quit advance setting window

Advanced settings	Advanced settings
802.1X settings 802.11 settings	802.1X settings 802.11 settings
Specify authentication mode:	Fast roaming Enable Pairwise Master Key (PMK) caching
Delete credentials for all users	PMK time to live (minutes): 720 Number of entries in PMK cache: 128
	This network uses pre-authentication
Enable single sign on for this network	Maximum pre-authentication attempts: 3 🚔
 Perform immediately before user log-on Perform immediately after user log-on Maximum delay (seconds): 10 Allow additional dialogues to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	Enable Federal Information Processing Standards (FIPS) compliance for this network
OK Cancel	OK Cancel

Click the Network icon on the systems tray, select PU WIFI and click connect. Key in your username and password on the Network Authentication window

NB// Your Username and password is Domain Controlled. It's composed of your **firstname.lastname**

Obtain these credentials from the ICT office,

For Inquiries visit ICT office or E-mail ict@pu.ac.ke

