

"eduroam" Configuration Manual

For Windows 7

1. Open 'Network and Sharing '





2. Go to 'Manage Wireless Networks'



3. Click on 'Add'





4. Choose 'Manually Create a network profile'





- 5. On network name write "eduroam"
- 6. Security type 'WPA2-Enterprise'
- 7. Encryption Type 'AES'
- 8. Leave Security Key 'Blank'
- 9. Click on 'Next'

	Manually connect to a wi	reless network	
	Enter information for t	the wireless network you want to add	
	Network name:	eduroam	
	Security type:	WPA2-Enterprise	
•	Encryption type:	AES -	
	Security Key:	Hide characters	
	V Start this connection a	utomatically	
	Connect even if the ne	etwork is not broadcasting	
	Warning: If you select	this option, your computer's privacy might be at risk.	
		Nex	t Cancel



10.Go to 'Change Connection Setting'

🕝 all Manu	ally connect to a wireless network	
Succes	sfully added HEC Smart University	
•	Change connection settings Open the connection properties so that I can change the settings.	
		Close



- 11.Once the wireless properties window has popped up select the "Security" tab and confirm the following:
- **12.Security Type: WPA-2 Enterprise**
- **13.Encryption Type: AES**
- 14.Network Authentication: Microsoft Protected EAP (PEAP).
- **15.Remember My Credentials For This Connection: Checked.**

Connection Security	
Security type:	WPA2-Enterprise
Encryption type:	AES
Microsoft: Protected	EAP (PEAP) Settings
Romember my cre	edentials for this connection each
Microsoft: Protected	s
Microsoft: Protected	s



16.In the PEAP connection window make sure to uncheck the "Validate server certificate" and then click on the "Configure" button

When connecting: Validate sover certificate Connect to these servers: Class 3 Public Primary Certification Authority: GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK	otected EAP Properties	
Validate sever certificate Connect to these servers: Trusted Root Certification Authorities: Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	When connecting:	
Connect to these servers:	Validate sever certificat	te
Trusted Root Certification Authorities: Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. Gelect Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Connect to these serve	ers:
Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. Elect Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Concel OK Cancel	Trusted Root Certification	Authorities:
GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. Elect Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Class 3 Public Primary	Certification Authority
Microsoft Root Authority Microsoft Root Certificate Authority Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. Elect Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	GTE CyberTrust Global	Root
Microsoft Root Certificate Authority Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. ielect Authentication Method: Secured password (EAP-MSCHAP v2) Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Microsoft Root Authori	ity
	Microsoft Root Certino	ate Authority
Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Indivice inneaderinging	CA.
Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Do not prompt user to a certification authorities.	authorize new servers or trusted
Secured password (EAP-MSCHAP v2)	elect Authentication Method	l:
Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Secured password (EAP-MSC	CHAP v2) Configure
Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Tenable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Enforce Network Access P	Protection
Enable Identity Privacy OK Cancel	Disconnect if server does	not present cryptobinding TLV
OK Cancel	Enable Identity Privacy	
OK Cancel		
		OK Cancel



17. Then Click on Advance settings and in the next TAB Specify authentication mode: checked and select User authentication as shown in red mark. Click OK.

Connection Security	Advanced settings
	802.1X settings 802.11 settings
Security type: WPA2-Enterprise	Specify authentication mode:
Encryption type: AES -	User authentication Save credentials
	Delete credentials for all users
Choose a petwork authentication method:	Enable single sign on for this network
Microsoft: Protected FAP (PEAP)	Perform immediately before user logon
	Perform immediately after user logon
time I'm logged on	Maximum delay (seconds):
	☑ Allow additional dialogs to be displayed during single sign on
	This network uses separate virtual LANs for machine and user authentication
Advanced settings	
OK Cancel	OK Cancel

18.As the window pops up make sure to uncheck the "Automatically use my Windows logon name and password" selection and then select ok.

AP MSCHAPv2 Properties	X
When connecting:	
Automatically use my Windows I password (and dom in if any).	ogon name and
OK Car	ncel



19.Select ok on the "PEAP Connection" window.

20.Select ok on the "Network Properties" window.

21.Click close at the bottom of the "Manually connect to a wireless network" window

					× (**)	N 20 40	10-32 A 5/28/20
/indows Security					are co		X
Network Auth Please enter user of	entica redentia	tion Is					
		97 A			3		1
- 100	D Dacci	Studen	t ID	_			
	DPass	word					-