Windows Devices

Right click on the wirless icon in the task bar and select "open Network Sharing Center





Click "Set up new connection or Network"

Select "Manually Connect....." from the pop up window



	📀 🚊 Manually conr	_ 🗆 🗙		
	Enter information	n for the wireless network you want to add		
	Network name:	IMG		
	Security type:	WPA2-Enterprise		
	Encryption type:	AES ~		
9	Se <u>c</u> urity Key:	Hide characters		
	✓ Start this conne	ction automatically		
	Connect even if	the network is not broadcasting		
	Warning: If you select this option, your computer's privacy might be at risk.			
		<u>N</u> ext Cancel		

Fill in the Network Name which is

"GHCS-Wireless " (case sensitive).

Use the dropdown security type box and select "WPA2-Enterprise".

Check the "Start this connection automatically" Box.

Click "Next"

Note: Leave the security Key blank



Select the "Security" tab, and then select "Settings".

Select "Change connection settings" from the pop up

MG2 W	ireless Network P	roperties	×
Connection Security			
Security type:	WPA2-Enterprise	~	
Encryption type:	AES	\checkmark	
Ch <u>o</u> ose a network a	uthentication method:		
Microsoft: Protecte	d EAP (PEAP) 🗸 🗸	<u>S</u> ettings	
time I'm logged	redentials for this connection	ction each	
A <u>d</u> vanced setting	S		
	(OK Cancel	

Protected EAP Properties	>
When connecting:	
<u>V</u> erify the server's identity by validating the certificate	
Connact to these convers (avamples and son() *) and) con	.
	J.
Trusted <u>R</u> oot Certification Authorities:	
AddTrust External CA Root	^
Baltimore CyberTrust Root	
Certum CA	
Class 2 Primary CA	
DigiCert Assured ID Root CA	
	~
Notifications before connecting:	
Tell user if the server's identity can't be verified	\vee
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) V Configu	re
✓ Enable <u>Fast</u> Reconnect	
Enforce Network Access Protection	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Can	el

Uncheck the "Verify the server's Identity..."

These Steps are only for Peronally owned Window NON-DOMAIN Computers!

When connecting:						
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com): Trusted Root Certification Authorities: AddTrust External CA Root America Online Root Certification Authority 1 Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
Trusted Root Certification Authorities: AddTrust External CA Root America Online Root Certification Authority 1 Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured D Root CA						
Trusted Root Certification Authorities: AddTrust External CA Root America Online Root Certification Authority 1 Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
Trusted Root Certification Authorities: AddTrust External CA Root America Online Root Certification Authority 1 Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
AddTrust External CA Root America Online Root Certification Authority 1 Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
America Online Root Certification Authority 1 Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DiglCert Assured ID Root CA						
Baltimore CyberTrust Root Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
Certum CA Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
Class 2 Primary CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA						
DigiCert Assured ID Root CA						
Notifications before connecting:						
Tell user if the server's identity can't be verified $$						
Select Authentication Method:						
Secured password (EAP-MSCHAP v2) V Configure						
✓ Enable Fast Reconnect						
England Fast Record Protection England Network Access Protection						
Disconnect if server does not present contabinding TW						
Enable Identity Brivan						
OK Cancel						

Additional steps for domain devices:

Click the "Configure" Button and from the pop-up UNcheck the box "automatically use my windows logon...."

Click ok, and OK again

EAP MSCHA	Pv2 Properties	
When connecting:		
Automatically use my password (and domain	Windows logon name and n if any).	
ОК	Cancel	
testy Wireless Net	work Properties	
Connection Security		
Security type: WPA2-Enter	prise V	
Encryption type: AES	~	
Choose a network authentication Microsoft: Protected EAP (PEAP	Advanced settings	×
Choose a network authentication Microsoft: Protected EAP (PEAP Remember my credentials for	Advanced settings	×
Choose a network authentication Microsoft: Protected EAP (PEAP Remember my credentials for time I'm logged on	Advanced settings	×
Choose a network authentication Microsoft: Protected EAP (PEAP Remember my credentials for time I'm logged on	Advanced settings 802.1X settings 802.11 settings Specify authentication mode: User or computer authenticatior V Save credentials	×
Choose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials fo time I'm logged on	Advanced settings 802.1X settings 802.1X settings Secify authentication mode: User or computer authentication User or computer authentication Computer authentication Computer authentication	×
Choose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials for time I'm logged on Advanced settings	Advanced settings 802.1X settings 802.1X settings Specify authentication mode: User or computer authentication User or computer authentication Computer authentication User authentication Guest authentication Guest authentication	×
Ch <u>o</u> ose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials for time I'm logged on	Advanced settings 802.1X settings 802.1X settings 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	×
Choose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials for time I'm logged on Advanced settings	Advanced settings 802.11 settings	×
Ch <u>o</u> ose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials for time I'm logged on Advanced settings	Advanced settings 802.1X settings 802.1X settings 802.11 settings Specify authentication mode: User or computer authentication User or computer authentication User authentication User authentication User authentication Guest authentica	×
Ch <u>o</u> ose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials for time I'm logged on Advanced settings	Advanced settings 802.1X settings 802.1X settings Secify authentication mode: User or computer authentication User or computer authentication Computer authentication User authentication Guest	×
Choose a network authentication Microsoft: Protected EAP (PEAP ✓ Remember my credentials for time I'm logged on Advanced settings	Advanced settings 802.1X settings 802.1X settings 802.11 settings Specify authentication mode: User or computer authentication User or computer authentication User authentication User authentication Guest authenticati	×
Ch <u>o</u> ose a network authentication Microsoft: Protected EAP (PEAP	Advanced settings	×
Choose a network authentication Microsoft: Protected EAP (PEAP	Advanced settings 802.1X settings Specify authentication mode: User or computer authentication Computer authentication User or computer authentication User or computer authentication Guest authentication Guest authentication © Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Image: Sign on This network uses separate virtual LANs for machine and user authentication	×
Ch <u>o</u> ose a network authentication Microsoft: Protected EAP (PEAP	Advanced settings 802.1X settings 802.11 settings Specify authentication mode: User or computer authentication Computer authentication Guest authentication Guest authentication Cuest authentication Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Image: Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication	×
Ch <u>o</u> ose a network authentication Microsoft: Protected EAP (PEAP	B02.1X settings 802.11 settings Specify authentication mode: User or computer authentication User or computer authentication Computer authentication User authentication Guest authentication Guest authentication Perform immediately before user logon Maximum delay (seconds): 10 Image: Allow additional dialogs to be displayed during single sign on This network uses separate yirtual LANs for machine and user authentication	×
Choose a network authentication Microsoft: Protected EAP (PEAP	Advanced settings 802.1X settings Image: Specify authentication mode: Image: Specify authent	×

ОК

Cancel

Back at the Security Tab, Click "Advanced Settings"

On the Advanced settings pop-up, check the "Specify authentication mode" and also select "User authentication" from the drop down list.

Click "OK, and OK again and then close the connection setting. You must now log off and then back on or restart your computer for the settings to take effect.