

## **Configuring Windows 8 on the new Cisco Wireless network**

- 1. From the Desktop, Move the mouse to the bottom-right corner and bring up the Charms menu.
- 2. Click or tap on "Settings".





3. Click on "Control Panel".





4. Click on "Network and Internet",

<b>9</b>	Contr	ol Panel	- C ×
(e) → ↑ I Control Panel	>		V C Search Control Panel D
File Edit View Tools Help			
Adjus	t your computer's settings		View by: Category 🔻
	System and Security Review your computer's status Save backup copies of your files with File History Find and fix problems	<b>.</b>	User Accounts and Family Safety Change account type Set up Family Safety for any user
	Network and Internet Connect to the Internet View network status and tasks Choose homegroup and sharing options	<b>N</b>	Appearance and Personalization Change the theme Change desktop background Adjust screen resolution
-	Hardware and Sound     View devices and printers     Add a device	Ð	Clock, Language, and Region Add a language Change input methods Change date, time, or number formats
	Programs Uninstall a program	G	Ease of Access Let Windows suggest settings Optimize visual display



5. Click on "Network Sharing Center".





## 6. Click on "Set up a new connection or a network"

2	Network and Sharing Center	- 🗆 🗙
🛞 🍥 👻 🛉 ີ 💺 🕨 Control Pane	el > Network and Internet > Network and Sharing Center v 🖒 Search Control Panel	م
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> ools <u>H</u> elp		
Control Panel Home	View your basic network information and set up connections	
Change adapter settings	View your active networks	
settings	Change your networking settings	
	Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point.	
	Troubleshoot problems	
	Diagnose and repair network problems, or get troubleshooting information.	
See also		
iCloud		
Internet Options		
Windows Firewall		



7. Click on "Manually connect to a wireless network", then click "Next".





8. Input "lehman\_college" as the Network Name, Choose "WPA2-Enterprise" as security type and choose "AES" as the encryption type, then click "Next".

📀 🖳 Manually connect	t to a wireless network		- • ×
Enter information f	or the wireless netwo	rk you want to add	
N <u>e</u> twork name:	lehman_college		
<u>S</u> ecurity type:	WPA2-Enterprise	~	
Enc <u>r</u> yption type:	AES	~	
Se <u>c</u> urity Key:		<u>H</u> ide characters	
$\checkmark$ Start this connecti	on automatically		
Connect even if th	e network is not broadcastin	g ter's privacy might be at risk	
wanning: It you se	sect this option, your compu	iter's privacy might be at risk.	
		Ne	xt Cancel



9. Click on "Change connection settings".

	-		×
Manually connect to a wireless network			
Successfully added lehman_college			
<ul> <li>Change connection settings</li> <li>Open the connection properties so that I can change the settings.</li> </ul>			
		Clo	se



10. Click on the "Secirity" tab, and make sure that "Microsoft: Protected EAP (PEAP) is selected.

lehman_college Wireless Network Properties			es ×
Connection Security			
S <u>e</u> curity type:	WPA2-Enterprise	~	
Encryption type:	AES	~	
Choose a network aut	hentication method:		
Microsoft: Protected	EAP (PEAP) V	Settings	
Remember my credentials for this connection each time I'm logged on			
A <u>d</u> vanced settings			
		ОК Са	ancel



11. Click on "Setting", Uncheck the "Verify the server's identity by validating the certificate"

	Protected EAP Properties	×
When	connecting:	
	erify the server's identity by validating the certificate	
	Connect to these servers (examples:srv1;srv2;.*\.srv3\.	com):
Trus	sted Root Certification Authorities;	
	AddTrust External CA Root	^
	America Online Root Certification Authority 1	
	Baltimore CyberTrust Root	
	Class 3 Public Primary Certification Authority	
	Class 3 Public Primary Certification Authority	
	Default CA	
	Default CA	~
<		>
No <u>t</u> if	fications before connecting:	
Tell	user if the server's identity can't be verified	$\sim$
Select	Authentication Method:	
Secur	red password (EAP-MSCHAP v2)	fours
Secur		ingure
Ena	able <u>F</u> ast Reconnect	
Ent	force Network Access Protection	
	connect if server does not present cryptobinding TLV	
Ena	able <u>I</u> dentity Privacy	
	OK	Cancel



12. Click on "Configure".

Protected EAP Properties
When connecting: Verify the server's identity by validating the certificate Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities;
<ul> <li>America Online Root Certification Authority 1</li> <li>Baltimore CyberTrust Root</li> <li>Class 3 Public Primary Certification Authority</li> <li>Class 3 Public Primary Certification Authority</li> <li>Default CA</li> <li>Default CA</li> </ul>
< > Notifications before connecting:
Tell user if the server's identity can't be verified
Secured password (EAP-MSCHAP v2) V Configure
Enable East Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel

13. Uncheck "Automatically use my Windows logon name and password (and domain if any). Click "OK".



14. Click "OK" again.

When connecting:
Verify the server's identity by validating the certificate
verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted <u>Root</u> Certification Authorities:
AddTrust External CA Root
America Online Root Certification Authority 1
Baltimore Cyber I rust Root
Class 3 Public Primary Certification Authority
Default CA
🗌 Default CA 🗸 🗸
< >
Notifications before connecting:
Tell user if the server's identity can't be verified V
Select Authentication Method:
Secured password (EAP_MSCHAP v2)
Configure
Chapter Past Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel



15. Click on "Advanced Settings".

lehman_college Wireless Network Properties		
Connection Security		
Security type:	WPA2-Enterprise V	
Encryption type:	AES 🗸	
Choose a network aut	hentication method:	
Microsoft: Protected	EAP (PEAP) V Settings	
<u> </u>	dentials for this connection each	
A <u>d</u> vanced settings		
	OK Cancel	

16. Check the "Specify authentication mode" box and choose "User authentication".

Advanced settings	×	
802.1X settings 802.11 settings		
Specify authentication mode:	- I.	
User authentication V Save gredentials		
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 <u>v</u> irtual LANs for machine and user authentication		
OK Cance	4	



## 17. Click on "Save Credentials"

Advanced settings		
802.1X settings 802.11 settings		
Specify authentication mode:		
User authentication  V Save credentials		
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):		
Allow additional dialogs to be displayed during single sign on		
This network uses separate <u>v</u> irtual LANs for machine and user authentication		
OK Cancel		

18. Input your Lehman Username and password to save.

Windows Security		×
Save credentials Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).		
P	User name Password	
	OK Cance	



19. Wireless network "lehman\_college" is connected.



20. Skip Step 17 and 18, if you don't want to save the credentials. When connecting to "lehman\_college", it will prompt for username and password.



If you have any questions please contact the Help Desk by phone at (718) 960-1111 or by coming into the Academic IT Center in Carman Hall Room 108.