Enabling WPA2-Enterprise in Windows Vista and Windows 7

- In Windows, navigate to Control Panel > Network and Internet > Network and Sharing Center.
- 2. Click Manage Wireless networks.
- 3. Click Add.
- 4. Choose Manually create a network profile.



- 5. On the next page, enter the following:
 - Network name: This is the SSID name. It is case sensitive.
 - Security type: Choose WPA2-Enterprise.
 - Encryption type: Choose AES.
 - Check **Start this connection automatically** if you want Windows to connect to this network automatically.
 - Check **Connect even if the network is not broadcasting** if the SSID is hidden and you want Windows to connect to this network automatically.
- 6. Click Next.

Manually connect	to a wireless network	
Enter information for	the wireless network you want to add	
Network name:	Meraki - WPA2	
Security type:	WPA2-Enterprise	
Encryption type:	AES	
Security Key:	Fide	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 b	e at risk.

On the "Successfully added" page, click Change connection settings.

- 7. Choose the **Security** tab.
- 8. Click **Settings**.
- 9. Uncheck **Validate server certificate** if the wireless client may not trust the RADIUS server certificate.
- 10. For the Authentication Method, choose **EAP-MSCHAP v2**.

hen connecting:	
Validate server certificate	
Connect to these servers:	
1	
Trusted <u>Root</u> Certification Authorities:	
AddTrust External CA Root	
Baltimore CyberTrust Root	
Class 3 Public Primary Certification Authority	
corp-AUSDC01-CA	
corp-AUSDC01-CA	
corp-SFODC01A-CA	
Corp-SFODC01A-CA	•
Do not prompt user to authorize new servers or t certification authorities.	rusted
elect Authentication Method:	
	C
ecured password (EAP-MSCHAP v2)	<u>Configure</u>
ecured password (EAP-MSCHAP v2)	<u>C</u> onngure
Ecured password (EAP-MSCHAP v2)	<u>Configure</u>
Enable East Reconnect	TLV
Enable East Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding Enable Identity Privacy	TLV
Enable East Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding Enable Identity Privacy) TLV

11. Click Configure.

12. Uncheck Automatically use my Windows logon on name and password.



- 14. Click Advanced settings.
- 15. Select the 802.1X settings tab.
- 16. Check Specify authentication mode.
- 17. Choose User or computer authentication.

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

18. Click **OK** to close out.