

Connecting to KHSC Corporate Wi-Fi

Microsoft Windows Instructions

July 2017 v1.0

- 1. <u>Open Network and Sharing Center</u>: Navigate to the 'Control Panel', click 'Network and Internet', click 'Network and Sharing Center', then click 'Manage wireless networks' on the left-hand pane
- 2. Click 'Add' on the top left-hand pane, then click 'Manually create a network profile'



- 3. Enter the below details, click 'Next', then click 'Change connection settings':
 - Network name: KHSC

Security type: WPA2-Enterprise

Checkmark 'Connect even if network is not broadcasting'

🚱 🏨 Manually connect to	o a wireless network	Manually connect to a wireless network
Enter information	for the wireless network you want to add	Successfully added KHSC
N <u>e</u> twork name:	KHSC	
Security type:	WPA2-Enterprise	 Change connection settings Open the connection properties so that I can change the settings.
Encryption type:	AES 🔹	
Segurity Key:	Hide characters	
☑ Start this connect	tion automatically	
Connect even if t	the network is not broadcasting	
Warning: If you s	select this option, your computer's privacy might be at risk.	
	Next Cancel	Close
-		











23

Settings

OK Cancel

the nen up plick the 'Security' teh plick the 'Settings' button ->	KHSC Wireless Network Properties
the pop-up, click the Security tab, click the Settings button \rightarrow	Connectic Security
	Security type: WPA2-Enterprise
	Encryption type: AES
	Choose a network authentication method
	Microsoft: Protected EAP (PEAP)
	Remember my credentials for this con time I'm logged on
	Advanced settings

4. In

5. In the new pop-up, un-checkmark 'Validate server certificate', then click 'Configure' and uncheckmark 'Automatically use my Windows logon name and password (and domain if any)'; click 'OK' then click 'OK' again to close the pop-ups shown below

Note: This will allow you to be prompted for your HDH/KGH credentials

Protected EAP Properties	8	EAP MSCHAPv2 Properties	X
Validate server certificate		When connecting: Automatically use my Windows log- password (and domain if any).	on name and
Trusted Root Certification Authorities: AddTrust External CA Root Baltimore CyberTrust Root Class 3 Puble Primary Certification Authority DigiCert Assure dI Root CA DigiCert High Assurence EV Root CA Configu Finable Fast Reconnect Finders High Assurence EV Root Ca Disconnect If server does not present cryptobinding TLV Enable Identity Privacy OK Cam	ure	OK Cance	



6. Click 'Advanced settings'; in the pop-up, checkmark 'Specify authentication mode' and select 'User authentication' in the dropdown

(
KHSC Wireless Network Properties	Advanced settings
Connection Security	802.1X settings 802.11 settings
Sgcurity type: WPA2-Enterprise Encryption type: AES	User authentication mode: User authentication Save gredentials
Chgose a network authentication method: Microsoft: Protected EAP (PEAP) ▼ Settings ✓ Remember my credentials for this connection each time I'm logged on	Enable gingle sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 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 Cance	el OK Canc

- 7. Click 'OK' or 'Close' until all pop-ups are closed
- Connect to the "KHSC" Wi-Fi option through your internet settings and enter your HDH or KGH credentials as "hoteldieu\USERNAME" or "kgh\USERNAME"



- 9. Once connected, open Internet Explorer and enter a website in the address bar (e.g. <u>www.kgh.on.ca</u>), you will be redirected to the "KHSC BYOD Portal"
- Read the Acceptable Use Policy, then click 'Start'
- 11. Enter a 'Device name' and optionally a 'Description', then click 'Continue'





- 12. Open the downloaded file "NetworkSetupAssistant.exe" and click 'Run'
- 13. Click 'Start', follow the instructions and click 'Yes' to accept/install each certificate; you will be prompted to enter your HDH/KGH credentials for additional information

Cisco Network Setup Assistant		
Root Certificate Store Image: State S	Security Warning You are about to install a certificate from a certification authority (CA) claiming to represent: ciscoisepv1.kgh.on.ca Windows cannot validate that the certificate is actually from "ciscoisepv1.kgh.on.ca". You should confirm its origin by contacting "ciscoisepv1.kgh.on.ca". The following number will assist you in this process: Thumbprint (sha1): FBFDC7BF 53E8143F E9491AEB 30783258 0D861453 Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?	X
•	Yes No	

14. On the last setup screen, click 'Exit' and your device is ready to use the internet