Connecting a machine running Microsoft Windows® to the Personal Devices wifi

The screenshots in this guide were taken in Windows 7 Professional. The appearance of your machine may vary slightly.



Select *Open Network and Sharing Center* from the connections menu in the task bar.

In the Network and Sharing Center click **Set up a new connection or network.** On the wizard that open select **Manually connect to a wireless network.**





Devices in the Network name box and select *WPA2-Enterprise* for the security type.

On the following screen, enter Personal

- • ×

	Successfully added Personal Devices	
n't n,	Change connection settings Open the connection properties so that I can change the settings.	
		Close

On the last step of the wizard don't click close, click the big button, *Change connection settings.*

Connecting a machine running Microsoft Windows® to the Personal Devices wifi

The screenshots in this guide were taken in Windows 7 Professional. The appearance of your machine may vary slightly.

Personal Devices Wirel	ess Network Properties			
Connection Security				
Security type:	WPA2-Enterprise -			
Encryption type:	AES 👻			
Choose a network authentication method:				
Microsoft: Protected EAP (PEAP)				
Remember my credentials for this connection each time I'm longed on				
Advanced settings				
	OK Cancel			

In the property window that appears click on the *Security* tab and click the *Settings* button.

Another window is going to be opened titled **Protected EAP Properties**. In this window **un-check** the box labeled **Validate server certificate** and towards the bottom of the page click the button labeled **Configure...**

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK Cancel

This will bring up the last window that we need. Uncheck the box labeled Automatically use my Windows logon name and password.

When connecting:	
Validate server certificate	
Connect to these servers:	
Trusted Poot Certification (utborities)	
Trasted Root Certification Additionales.	
Add trust External CA Root	Â
Baltimore Cyber Irust Root	=
Class 3 Public Primary Certification Authority	
ClabelGas Bash CA	
Gobalsign Root CA	
Go Daddy Class 2 Certification Authority	
GTE Cyber Irust Global Root	
	,
Do not prompt user to authorize new servers or trusted	
Do not prompt user to authorize new servers or trusted certification authorities.	,
Do not grompt user to authorize new servers or trusted certification authorities.	
Do not grompt user to authorize new servers or trusted certification authorities.	,
Oo not grompt user to authorize new servers or trusted certification authorities. Select Authentication Method:	
Do not grompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2)	onfigure
Con not grompt user to authorize new servers or trusted certification authorities. Select Authentication Method: [Secured password (EAP-MSCHAP v2) Contemporation Contemp	onfigure
Con not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Contemporate Context Contemporate Context	onfigure
Oo not grompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Fable Fast Reconnect Enforce Network Access Protection	onfigure
Oo not grompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Finable East Reconnect Enforce Bytwork Access Protection Disconnect if server does not present cryptobinding TLV	onfigure
Oo not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Snable East Reconnect Enable East Reconnect Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	onfigure
Oo not grompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Enable East Reconnect Fnforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	onfigure
O not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Finable East Reconnect Finforce Network Access Protection Disconnect if server does not present cryptobinding TLV Finable Edentity Privacy OK	onfigure Cancel
Oo not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP v2) Fnable East Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK	onfigure) Cancel

Now, click OK to dismiss all of the open windows. When you get back down to the desktop, Windows should start connecting to the wireless network. If you are within

range of the network you should see a bubble appear from the task bar telling you that more information is needed.

Additional information is needed to connect Personal Devices. * × Click to provide additional information.	
- 18 B	()) 11:15 AM 2/6/2014

Windows Securit	y		×
Network Au Please enter us	uthentication er credentials		
	b_davis		
		OK Cance	:

Click on the bubble and you will be presented with a box asking for credentials to connect. Enter you Marlington username and password and click OK.



That's it! Provided all went well, you can verify that you are connected to the Personal Devices network.