## **Connecting to UDel Secure with Windows 7**

1. In the system tray, lower-right of your screen, click on the wireless network icon



If UDel Secure is listed on the wireless access points list, right-click on it. If Properties is available, click on it and skip to step 7. Otherwise, click on the link, "Open Network and Sharing Center" and follow the directions in sequential order.

Open Network	and Sharing Center
n the Network and	a Sharing Center dialog window, click on Manage wireless hetwo
🕥 - 🕎 « Network and Inte	rnet 🔸 Network and Sharing Center 🗸 49 Search Control Panel 🔎
Control Panel Home	
Manage wireless petworks	
Change adapter settings	💌 — 🗶 🔮
Change advanced sharing	OET09-GLT Internet
settings	
	View your active networks Connect to a network You are currently not connected to any networks.
	Characterization attices
	Set up a new connection or network Set up a wireless broadband dial-up ad boc or VPN connection; or set up a router or access
	point.
	Connect to a network
	Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
	Choose homegroup and sharing options
	Access files and princers located on other network computers, or change sharing settings.
	Troubleshoot problems
	Diagnose and repair network problems, or get troubleshooting information.
See also	
HomeGroup	
Internet Options	
Windows Firewall	

3. Within Manage wireless networks, click on **Add** to add a connection for UDel Secure.

G ⊃ <mark>⊮1</mark> « Net	work and Internet 🕨 Manage	Wireless Network	5	• •4	Search Manage Wireless Networks
Manage wirele Windows tries to c	ess networks that use (V onnect to these networks in the	Vireless Netw e order listed belo	ork Connection) w.		
Add Remove Mo	ove up Adapter properties	Profile types	Network and Sharing (	Center	
Networksyou can view	v, modify, and reorder (2) Security: Unsec	ured	Type: Any supp	oorted	Manually connect

4. Within the Manually connect to a wireless network window, click on **Manually create a network** profile.



5. Enter the following information in the Manually connect to a wireless network dialog window and click **Next**.

Enter mornadon	for the wheless network you want to	uuu
Network name:	UDel Secure	
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Security Key:	E Hi	de characters
👿 Start this connec	tion automatically	
🔲 Connect even if	the network is not broadcasting	
Warning: If you	select this option, your computer's privacy might	t be at risk.

6. Click on Change connection settings.



7. In the UDel Secure Wireless Network Properties window, verify that **Connect automatically when this network is in range** is checked then click on the **Security** tab.



8. Verify that the following settings are selected. Click on the **Settings** button.

el Secure Wireless N	letwork Properties	2
Connection Security	]	
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Choose a network au Microsoft: Protected W Remember my cro time I'm logged of	uthentication method: HEAP (PEAP) Settings edentials for this connection each n	
(magazara)	S	
Advanced setting		

9. In the Protected EAP Properties window, under Trusted Root Authentication Authorities, check **Thawte Premium Server CA**. Next, click on the **Configure** button.

Image: Second	stected EAP Properties	23
Validate server certificate Connect to these servers: Connect to these servers: Cass 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Server CA Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. elect Authentication Method: secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Disconnect if server does not present cryptobinding TLV Concel OK Cancel	Vhen connecting:	
Connect to these servers: Connect to these servers: Connect to these servers: Connect to these servers: Connect if cation Authorities: Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Server CA Do not prompt user to authorize new servers or trusted certification authorities.  elect Authentication Method: elect Authentication Method: Enable Fast Reconnect Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Validate server certificate	
Connect to these servers:  Trusted Root Certification Authorities:  Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Server CA Do not prompt user to authorize new servers or trusted certification authorities.  elect Authentication Method: Enable Fast Reconnect Fnforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel		
Trusted Root Certification Authorities:         Class 3 Public Primary Certification Authority         GTE CyberTrust Global Root         Microsoft Root Authority         Microsoft Root Certificate Authority         Microsoft Root Certificate Authority         Thawte Premium Server CA         Thawte Server CA         Thawte Server CA         Do not prompt user to authorize new servers or trusted certification authorities.         elect Authentication Method:         Secured password (EAP-MSCHAP v2)         Enable Fast Reconnect         Enforce Network Access Protection         Disconnect if server does not present cryptobinding TLV         Enable Identity Privacy         OK       Cancel	Connect to these servers:	
Class 3 Public Primary Certification Authority The CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities.  Elect Authentication Method: Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Trusted Root Certification Authorities:	
GTE CyberTrust Global Root  Microsoft Root Authority  Microsoft Root Certificate Authority  Thawte Premium Server CA  Thawte Server CA  Thawte Server CA  Do not prompt user to authorize new servers or trusted certification authorities.  elect Authentication Method:  cecured password (EAP-MSCHAP v2)  Configure  Enable Fast Reconnect  Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV  Concel  OK  Cancel	Class 3 Public Primary Certification Authority	
Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. elect Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	GTE CyberTrust Global Root	
Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Microsoft Root Authority	
Thawte Premium Server CA Thawte Server CA Thawte Server CA Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. elect Authentication Method: secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Microsoft Root Certificate Authority	
Thawte Server CA Thawte Timestamping CA Do not prompt user to authorize new servers or trusted certification authorities. elect Authentication Method: secured password (EAP-MSCHAP v2)  Configure Enable Fast Reconnect Enable Fast Reconnect Bisconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Thawte Premium Server CA	
Thawte Timestamping CA  Do not prompt user to authorize new servers or trusted certification authorities.  elect Authentication Method: Secured password (EAP-MSCHAP v2)  Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Thawte Server CA	1
Do not prompt user to authorize new servers or trusted certification authorities.  elect Authentication Method: Secured password (EAP-MSCHAP v2)  Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Thawte Timestamping CA	
elect Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Do not prompt user to authorize new servers or trusted certification authorities.	
Secured password (EAP-MSCHAP v2)  Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	elect Authentication Method:	
Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Secured password (EAP-MSCHAP v2)	figure
Enforce Network Access Protection     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy     OK Cancel	TEnable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel	Enforce Network Access Protection	
Enable Identity Privacy OK Cancel	Disconnect if server does not present cryptobinding TLV	
OK Cancel	Enable Identity Privacy	T
OK Cancel	- · · · L	
	ОК С	ancel
		No.

10. In the EAP MSCHAPv2 Properties window, uncheck **Automatically use my Windows logon name and password (and domain if any)** and click **OK**. Click **OK** again in the Protected EAP Properties window.

EAP MSCHAPv2 Properties	<b>X</b>
When connecting:	
When connecting.	
Automatically use my Windows logon name password (and domain if any).	e and
OK Cancel	

11. In the UDel Secure Wireless Network Properties window, click the Advanced Settings button.

onnection Security		
Security type:	WPA2-Enterprise	¥
Encryption type:	AES	•
Choose a network a Microsoft: Protecte	uthentication method: d EAP (PEAP)	tings
Remember my cr time I'm logged c	redentials for this connection each on	r
Remember my cr time I'm logged c	edentials for this connection ead	ו
Remember my cr time I'm logged c	redentials for this connection each	1
Remember my cr time I'm logged c           Advanced setting	redentials for this connection each	1
Remember my cr time I'm logged c           Advanced setting	redentials for this connection ead	1
<ul> <li>Remember my cr time I'm logged c</li> <li>Advanced setting</li> </ul>	redentials for this connection ead	1

12. In the Advanced Settings window, check **Specify authentication mode** and select **User authentication** from the drop-down menu. Click on the **Replace Credentials** button.

802.1X settings	802.11 settings	
Specify a	uthentication mode:	
User au	thentication	<ul> <li>Replace credentials</li> </ul>
💹 Delet	e credentials for all users	
Enable sir	ngle sign on for this netwo	ork
@ Perfo	rm immediately before use	er logon
O Perfo	rm immediately after user	logon
Maximum	delay (seconds):	10
Allow sign o	additional dialogs to be di n	splayed during single
This n and u	etwork uses separate viri ser authentication	tual LANs for machine
	ſ	OK Care

## 13. Enter your UDel NetID and password. Click OK.

	ty	23
Replace cr Saving your c	redentials credentials allows your computer to connect to the network	k
when you re	not logged on (for example, to download updates).	
	User name	
	Password	

13. Click on the 802.11 settings tab to verify the following configuration. Click **OK**.

Advanced settings		×
802.1X settings 802.11 settings		
Fast roaming		
Enable Pairwise Master Key (PMK) caching		
PMK time to live (minutes):	720	
Number of entries in PMK cache:	128	
This network uses pre-authentication		
Maximum pre-authentication attempts:	3	A. V
compliance for this network		

14. Click **OK** in the UDel Secure Wireless Network Properties window.

	Network Properties	23
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Choose a network a	uthentication method:	
Remember my cr time I'm logged c	redentials for this connection each	
Advanced setting	25	
Advanced setting	35	

15. Click on the wireless network icon in the system tray. Click on the **Connect** button next to UDel Secure. That should do it. If you have any questions, contact <u>oet-help@udel.edu</u>.