UTEP Secure Windows 7 Setup



1. Before any Windows 7 device can authenticate on utepsecure, a Windows Service must be started for authentication purposes. Open the start menu, and begin typing "services.msc". Click on Services.

2. Once the window is open, on the bottom there will be two tabs called "Extended" and "Standard". Click on Standard and scroll down until you see Wired AutoConfig.

🔍 Windows Remote	Windows Remote Man		Manual	Network S	
🛸 Windows Search	Provides content indexi	Started	Automatic (D	Local Syste	
🛸 Windows Time	Maintains date and tim		Manual	Local Service	
🧠 Windows Update	Enables the detection,	Started	Automatic (D	Local Syste	
🧠 WinHTTP Web Pr	WinHTTP implements t	Started	Manual	Local Service	
Wired AutoConfig	The Wired AutoConfig		Manual	Local Syste	
🤐 WLAN AutoConfig	The WLANSVC service	Started	Automatic	Local Syste	
🥋 WMI Performance	Provides performance li		Manual	Local Syste	
🥋 Workstation	Creates and maintains	Started	Automatic	Network S	
🤐 WWAN AutoConfig	This service manages		Manual	Local Service	
Extended A Standard					

Wired AutoConfig P	roperties (Local Computer)				
General Log On	Recovery Dependencies				
Service name:	dot3svc				
Display name:	Wired AutoConfig				
Description:	The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X				
Path to executable C:\Windows\syste	e: em32\svchost.exe				
Startup type:	Automatic				
Help me configure	service startup options.				
Service status:	Started				
Start	Stop Pause Resume				
You can specify th from here.	e start parameters that apply when you start the service				
Start parameters:					
	OK Cancel Apply				

3. Double-click it to open a window. Make sure the service has been started, and is set to automatically start each time Windows boots up. If it is not, change the Startup Type to Automatic. If the service is not started, click on the Start button to start the service. Click Apply. Click OK to close the window. This method is used to authenticate you on the wireless network.



4. After completing the previous step, you will be returned to your list of networks and it will show you are connected to utepsecure. It is recommended you Forget utepwl1 so your device will prefer utepsecure as its primary wireless network. Make sure your settings are identical to the image below.



5. After those settings have been set, close those windows and right-click on the network icon in the bottom right corner of your screen and click Open Network and Sharing Center.

Networking Authentication Sharing					
Select this option to provide authenticated network access for this Ethemet adapter.					
Choose a network authentication method:					
Microsoft: Protected EAP (PEAP) Settings					
Remember my credentials for this connection each time I'm logged on					
Fallback to unauthorized network access					
Additional Settings					
OK Cancel					

Local Area Connection Properties					
Networking Authentication Sharing					
Select this option to provide authenticated network access for this Ethemet adapter. Enable IEEE 802.1X authentication					
Choose a network authentication method:					
Microsoft: Protected EAP (PEAP)					
Remember my credentials for this connection each time I'm logged on					
Fallback to unauthorized network access					
Additional Settings					
OK Cancel					
+					

6. In this window, click on Change adapter settings. Right-click on Local area connection and select Properties.

7. From Properties, click on the Authentication tab. If this tab is missing, go back to steps 1 and 2 to repeat the procedure. If steps 1 and 2 are skipped you will not have the Authentication tab under Properties.

Click on Settings next to Choose a network authentication method.

Protected EAP Properties
When connecting:
Validate cerver certificate
Connect to these servers:
Trusted Root Certification Authorities:
AddTrust External CA Root
🔲 avast! Mail Scanner Root
Baltimore CyberTrust Root
Class 2 Primary CA
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA 🗸
۰ III ا
Do not prompt user to authorize new servers or trusted
certification authorities.
Colore Antheory and a standard
Select Authentication Method:
Secured password (EAP-MSCHAP v2) Configure
Enable East Reconnect
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel



8. Make sure your settings are the same as the ones provided in the image. Once complete, click on Configure.

Uncheck the box that says "Automatically use my Windows logon name and password (and domain if any)." Click OK, and click OK again on Protected EAP Properties.

Protected EAP Properties	23
When connecting:	
Validate server certificate	
Connect to these servers:	
EAP MSCHAPv2 Properties	
Trust: When connecting: B C C D When connecting: When connecting: Automatically use my Windows logon name and password (and domain if any).	
Cancel	

- 9. Click Ok once complete, next click on Additional Settings under the Authentication tab. This will open a new window that says Advanced Settings. In this window, check Specify authentication mode and select User authentication. Click on Save credentials. In the new window, enter your UTEP credentials and Click OK. Click OK again once that is done.
- 10. Once these steps have been completed you will be able to connect to utepsecure. Click on the wireless icon and select utepsecure. It will now prompt you for credentials. Enter your UTEP username and password, you may be prompted to trust a certificate once or twice. Click continue and you will be able to connect to the network.