Windows 10 EAP-TTLS Configuration

You can create a new wireless connection which uses EAP-TTLS as the authentication method manually.

On Windows 10, go to Control Panel > Network and Sharing Center > Set up a new connection or network > Manually connect to a wireless network. Enter a Network name and set Security type to WPA2-Enterprise. The Encryption type is set to AES.

				_		\times
←	👰 Manually connect to a wi	reless network				
	Enter information for t	the wireless network you want to add				
	N <u>e</u> twork name:	<my network="" wifi=""></my>				
	Security type:	WPA2-Enterprise \checkmark				
	Enc <u>ryption</u> type:	AES ~				
	Se <u>c</u> urity Key:	<u>H</u> ide char	acters			
	Start this connection a	utomatically				
	Connect even if the new Warning: If you select	etwork is not broadcasting this option, your computer's privacy might be at r	risk.			
			<u>N</u> e	t	Canc	el

Once created, you have the option to modify the wireless connection. Select **Change connection settings**.

		-		×
~	Manually connect to a wireless network			
	Successfully added <my network="" wifi=""></my>			
	→ C <u>h</u> ange connection settings Open the connection properties so that I can change the settings.			
	L			
			Clo	se

In the Security tab, Choose a network authentication method to Microsoft: EAP-TTLS, and select Settings.

TekRADIUS - Windows 10 EAP-TTLS Configuration

My WiFi Network> W	Vireless Network Properties	C TTLS Properties
Connection Security		Enable identity privacy
S <u>e</u> curity type: Encryption type:	WPA2-Enterprise ~	Server certificate validation Connect to these servers:
Choose a network au	thentication method:	Trusted <u>R</u> oot Certification Authorities:
Microsoft: EAP-TTLS	Settings edentials for this connection each	Anuvu Anuvu Anun Anuvu Anuvuu Anuvuuu Anuvuuu Anuvuu Anuvuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
		Client authentication
Advanced settings	5	Automatically use my Windows account name and password (and domain, if any)
		Select an <u>E</u> AP method for authentication Microsoft: Smart Card or other certificate
		Configure
	OK Cancel	OK Cancel

Note that, for simplification purposes, **Enable identity privacy and Don't prompt user if unable to authorize sever** options are disabled. However, EAP-TTLS allows the client to validate the server. To enable this, you will need to import the CA certificate to the Windows 10 computer and make sure that it is enabled as a Trusted Root Certification Authority in the Windows Certificate Store If your RADIUS server is not using a certificate from a known CA.

802.1X settings Specify authentication mode: User authentication Save gredentials Delete credentials for all users Enable single sign on for this network Perform immediately before 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	dvanced settings	>			
Sgecify authentication mode: User authentication Delete credentials for all users Enable gingle sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication	802.1X settings 802.11 settings				
User authentication Save gredentials 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 Sign on This network uses separate virtual LANs for machine and user authentication	Specify authentication mode:				
 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 	User authentication	✓ Save gredentials			
Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication	Delete credentials for all users				
 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 	Enable single sign on for this net	work			
 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 	Perform immediately before u	iser logon			
Maximum delay (seconds): Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication	Perform immediately after use	er logon			
 Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication 	<u>M</u> aximum delay (seconds):	10 🌲			
 This network uses separate virtual LANs for machine and user authentication 	Allow additional dialogs to be sign on	displayed during single			
	This network uses separate <u>v</u>	irtual LANs for machine			
	and user authentication				
		Cancel			

Click advanced settings and specify authentication as **User authentication**. You can optionally enter username and password by clicking **Save credentials** button.

Select OK for all dialog windows to confirm all settings. The configuration for the Windows 10 computer has been completed and the user should be able to authenticate to Wi-Fi using their username and password.

You can optionally configure EAP-TLS using TekWiFi. Double click on the Wi-Fi network listed in Wireless Network tan and set EAP-TLS parameters. The Wi-Fi network Mesut be configured for WPA-Enterprise.

🕪 TekWiFi	– 🗆 ×				
File Help					
🚧 Wireless Networks 🧕 Connection	🗳 Diagnostic 🔒 Cipher Suites				
MiniAP					
IP Address : N/A	DNS 1: N/A				
Subnet Mask : N/A	DNS 2 : N/A				
Default Gateway : N/A	Security : WPA2 Enterprise				
Authentication Method	EAP-TTLS				
Username	myusername				
Password					
Trusted Certificate Authority	DigiCert Trusted Root G4				
Authentication Method					
Select authentication method for EAP.					
	Connect				
MiniAP is not connected.	.::				

You can download TekWiFi from KaplanSoft Web site. Please see https://www.kaplansoft.com/tekwifi/ for more information.