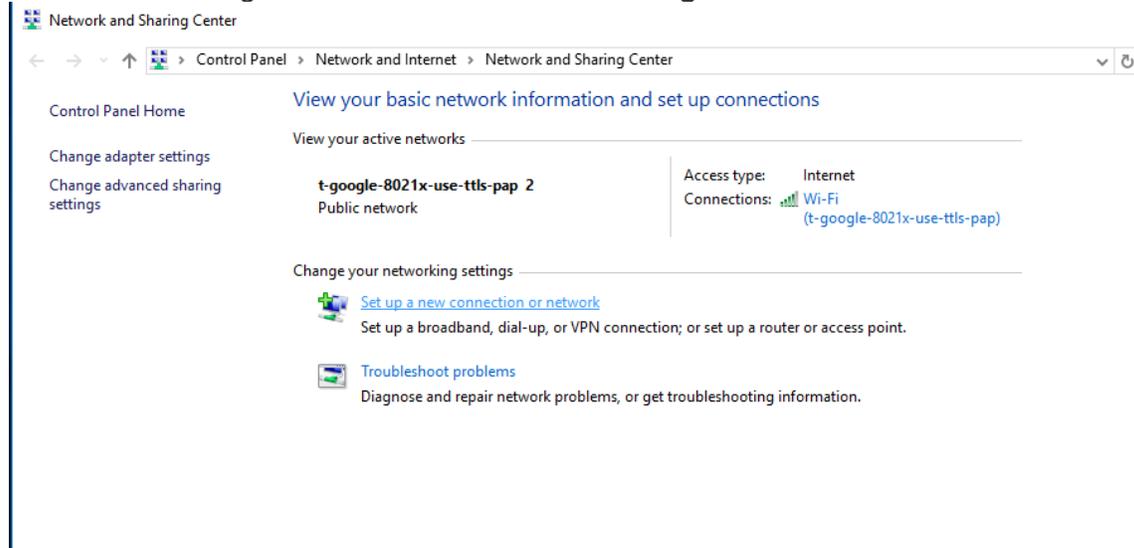


# Configuring EAP-TTLS + PAP Authentication on Windows 8 and 10

The following steps outline how to configure a Windows 8 or 10 device to authenticate to a Meraki wireless network configured to use [WPA2-Enterprise 802.1X with Google Auth](#):

1. In Windows, navigate to the **Network and Sharing Center**:

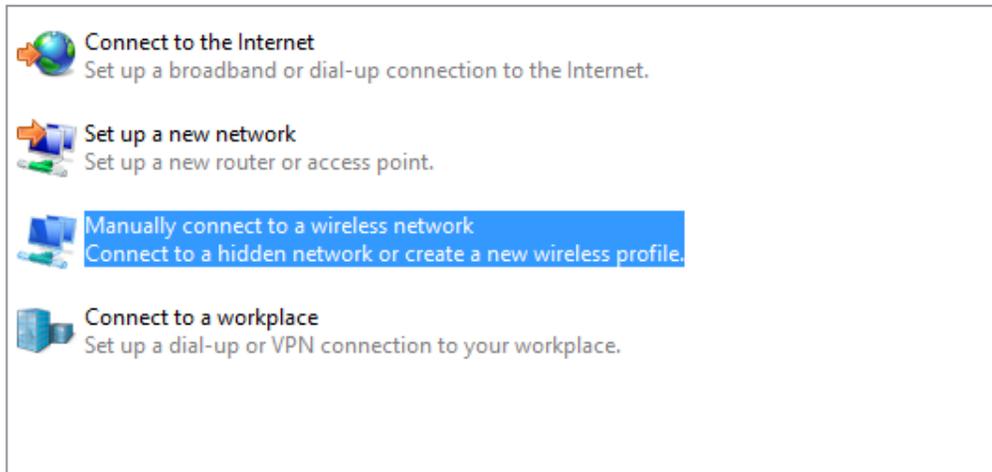


2. Click **Set up a new connection or network**.

3. Select *Manually connect to a wireless network*:

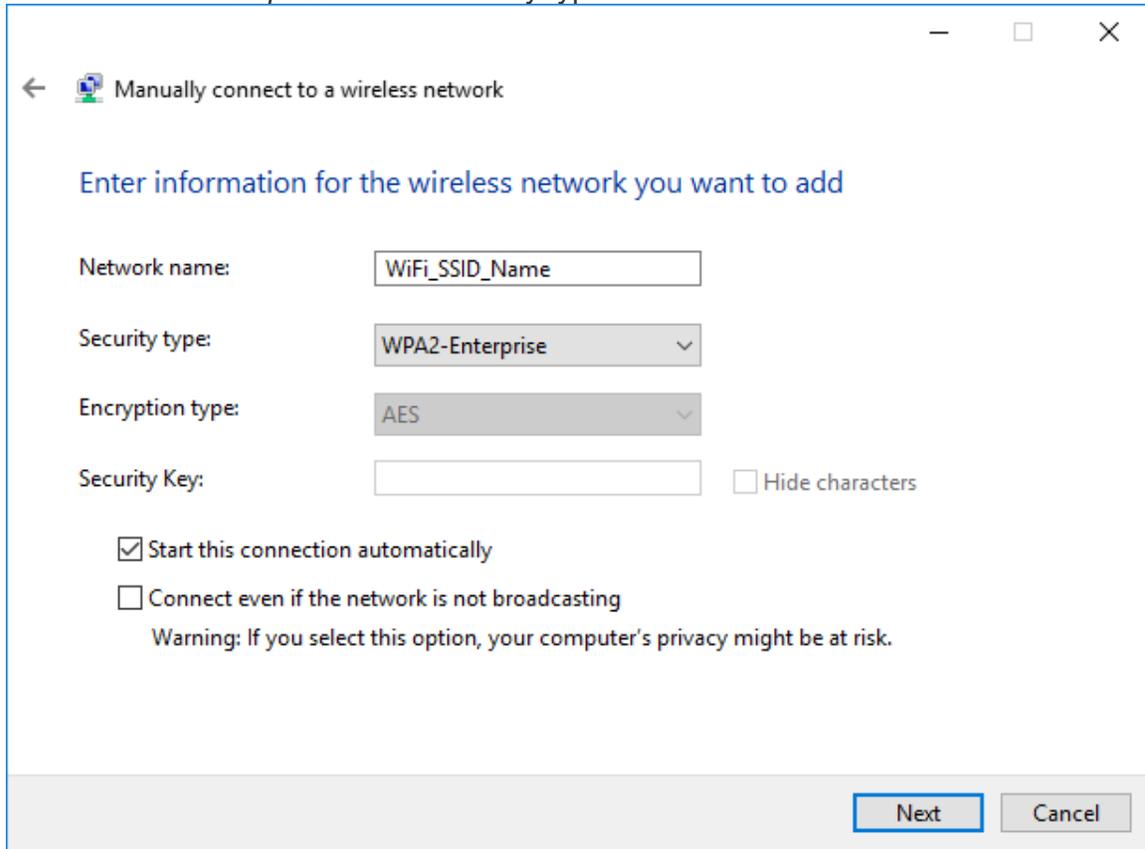
←  Set Up a Connection or Network

Choose a connection option



4. Enter information for the wireless network:
- Specify your SSID name.

- Select *WPA2-Enterprise* as the security type:

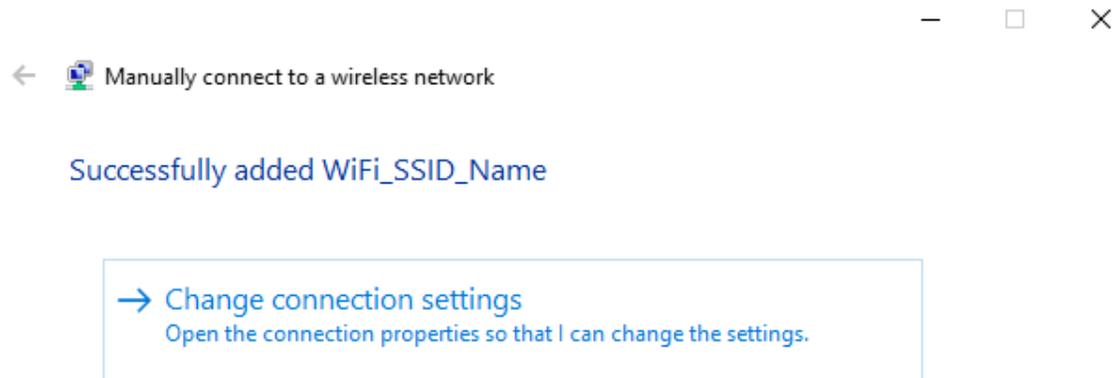


The screenshot shows a Windows Network Setup wizard window titled "Manually connect to a wireless network". The window contains the following fields and options:

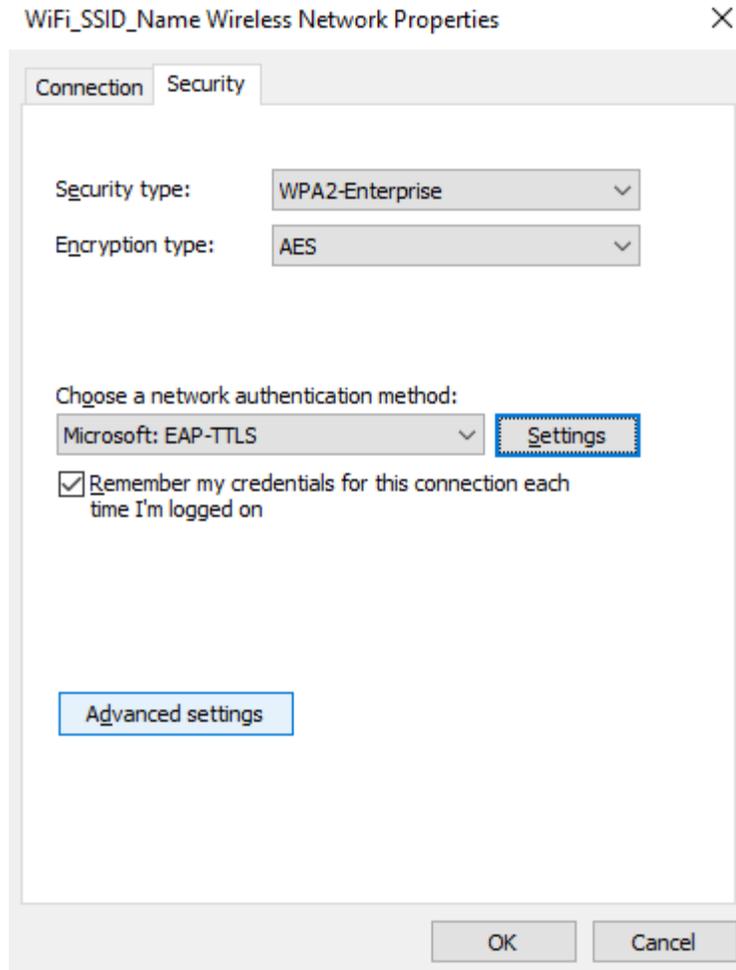
- Network name:** A text input field containing "WiFi\_SSID\_Name".
- Security type:** A dropdown menu set to "WPA2-Enterprise".
- Encryption type:** A dropdown menu set to "AES".
- Security Key:** An empty text input field with a "Hide characters" checkbox to its right.
- Start this connection automatically
- Connect even if the network is not broadcasting
- Warning: If you select this option, your computer's privacy might be at risk.

At the bottom right of the window, there are two buttons: "Next" and "Cancel".

5. After the new WiFi configuration is successfully added, click **Change connection Settings** to open the connection properties:



6. Go to the **Security** tab under the connection properties page.
  - a. Choose *Microsoft: EAP-TTLS* as the authentication method.
  - b. Click **Settings**:



- c. Uncheck **Enable identity privacy**.
- d. Select **PAP** as the non-EAP method for authentication:

TTLs Properties

Enable identity privacy

anonymous

Server certificate validation

Connect to these servers:

Trusted Root Certification Authorities:

- AddTrust External CA Root
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA

Don't prompt user if unable to authorize server

Client authentication

Select a non-EAP method for authentication

Unencrypted password (PAP)

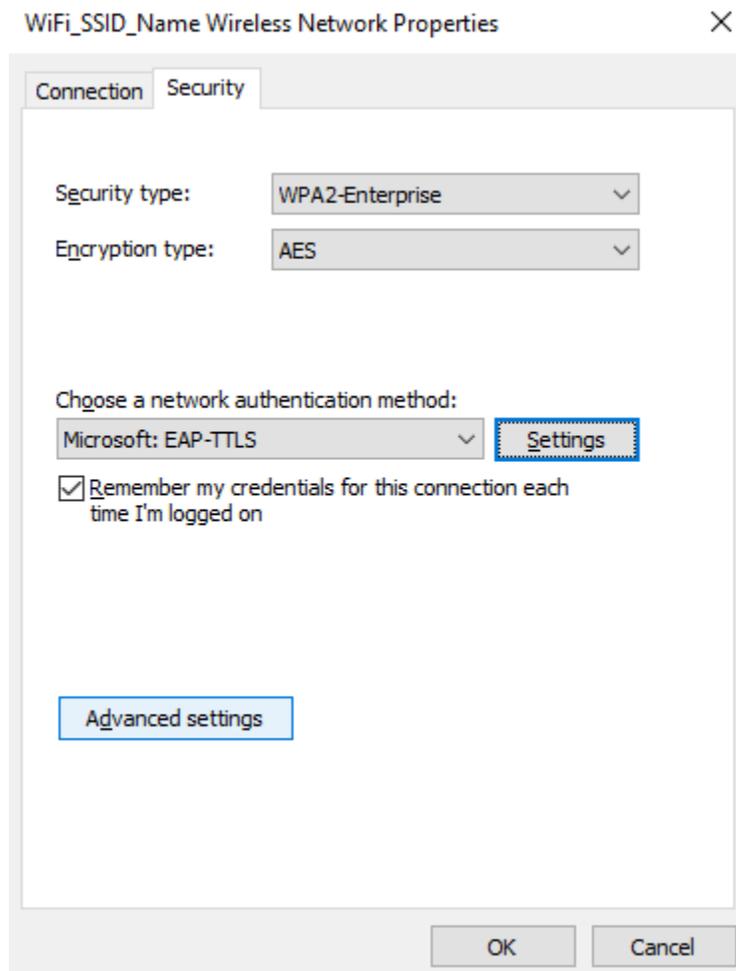
Automatically use my Windows account name and password (and domain, if any)

Select an EAP method for authentication

Microsoft: Smart Card or other certificate

Configure

2. Close the **TTLS Properties** window, then select **Advanced Settings**:



- a. Check **Specify authentication mode**.
- b. Select *User authentication*.
- c. Click **Save credentials**.
- d. Enter the user's credentials:

