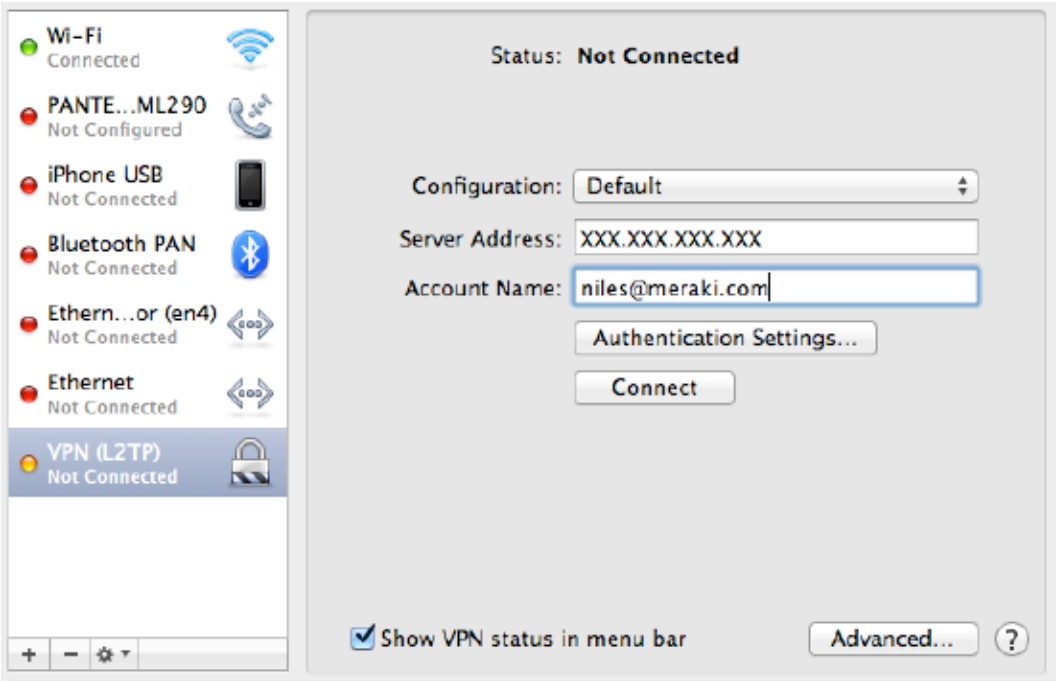
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) **is the user email address** entered in the Dashboard.

The instructions below are tested on Mac OS 10.7.3 (Lion).

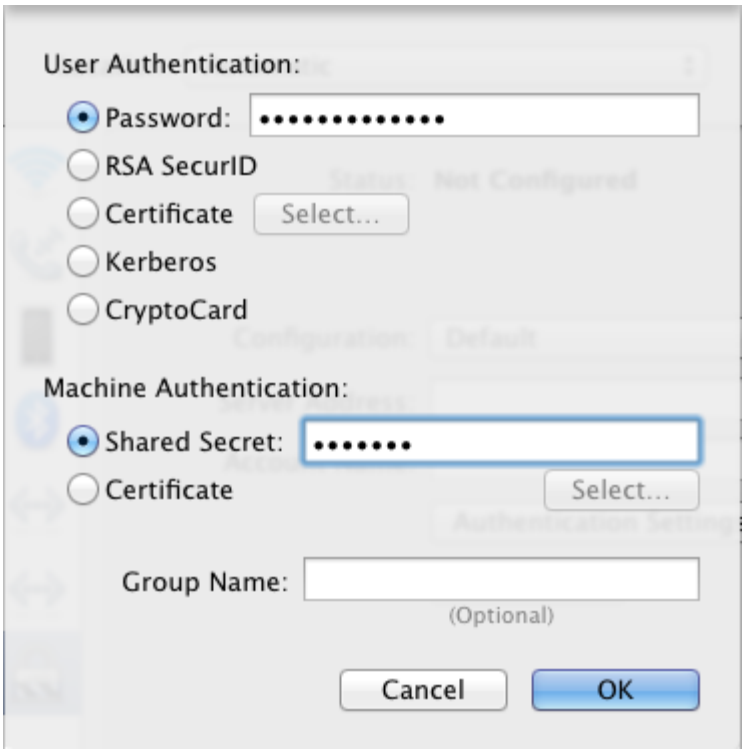
Open **System Preferences > Network** from Mac applications menu. Click the "+" button to create a new service, then select VPN as the interface type, and choose **L2TP over IPsec** from the pull-down menu.

- **Server Address:** Enter the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.
- **Account Name:** Enter the account name of the user (based on AD, RADIUS or Meraki Cloud authentication).

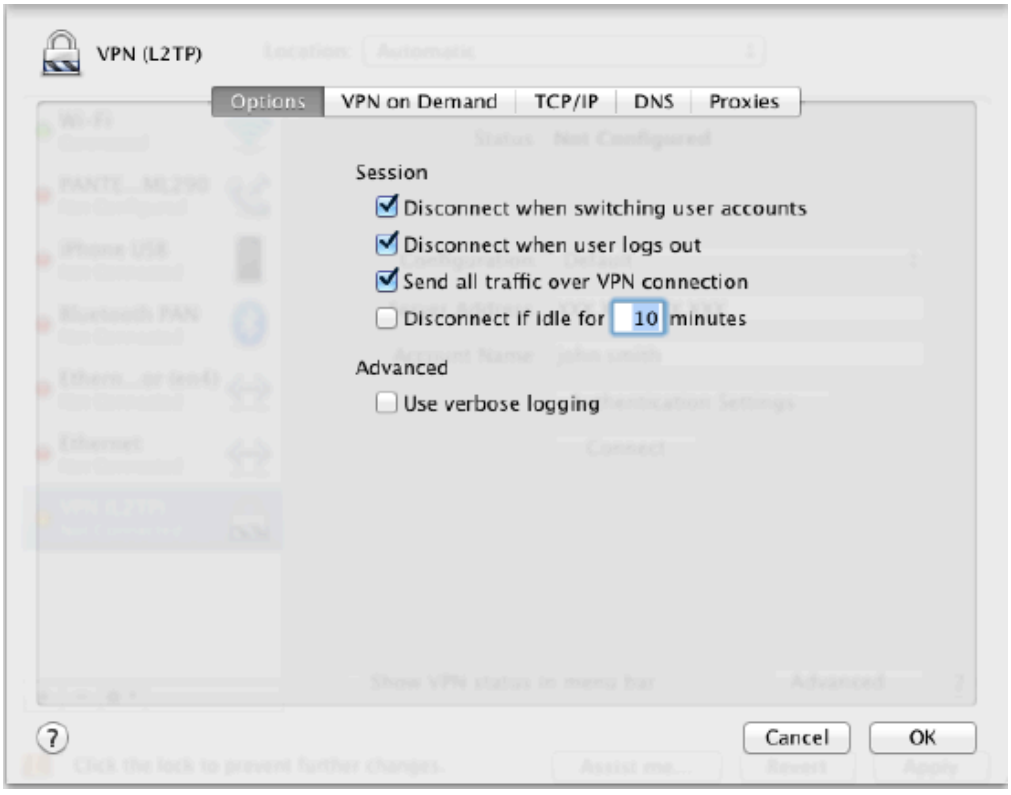


Click **Authentication Settings** and provide the following information:

- **User Authentication > Password:** User password (based on AD, RADIUS or Meraki Cloud authentication).
- **Machine Authentication > Shared Secret:** Enter **shared secret** that admin created in Security appliance > Configure > Client VPN settings.



Click **OK** to go back to the main VPN settings page, then click **Advanced** and **enable the Send all traffic over VPN connection** option.



The VPN connectivity will not be established if you don't enable the **Send all traffic over VPN connection** option!

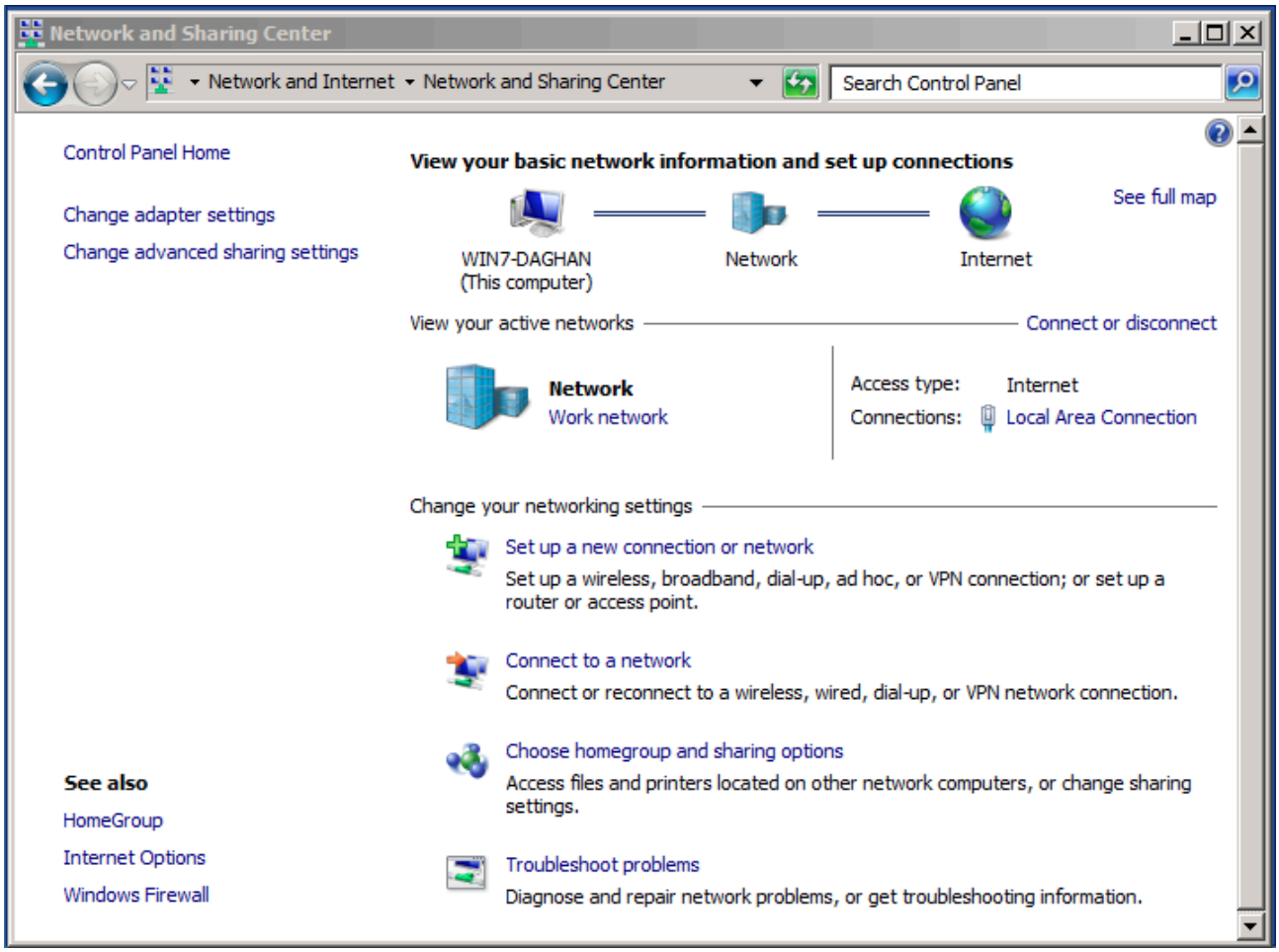
Windows 7

Currently only the following authentication mechanisms are supported:

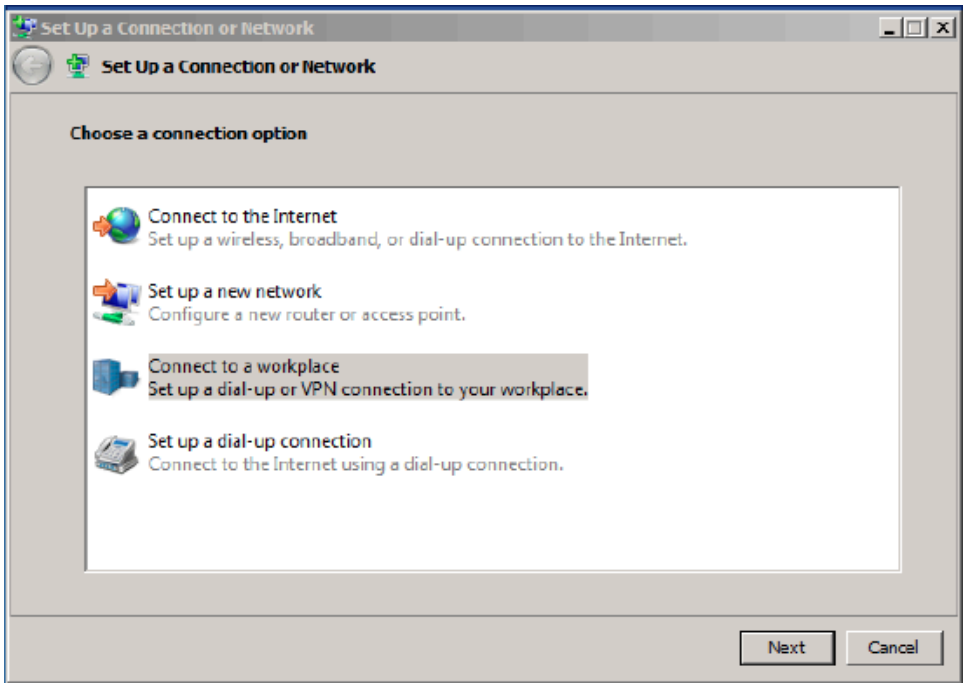
- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) **is the user email address** entered in the Dashboard.

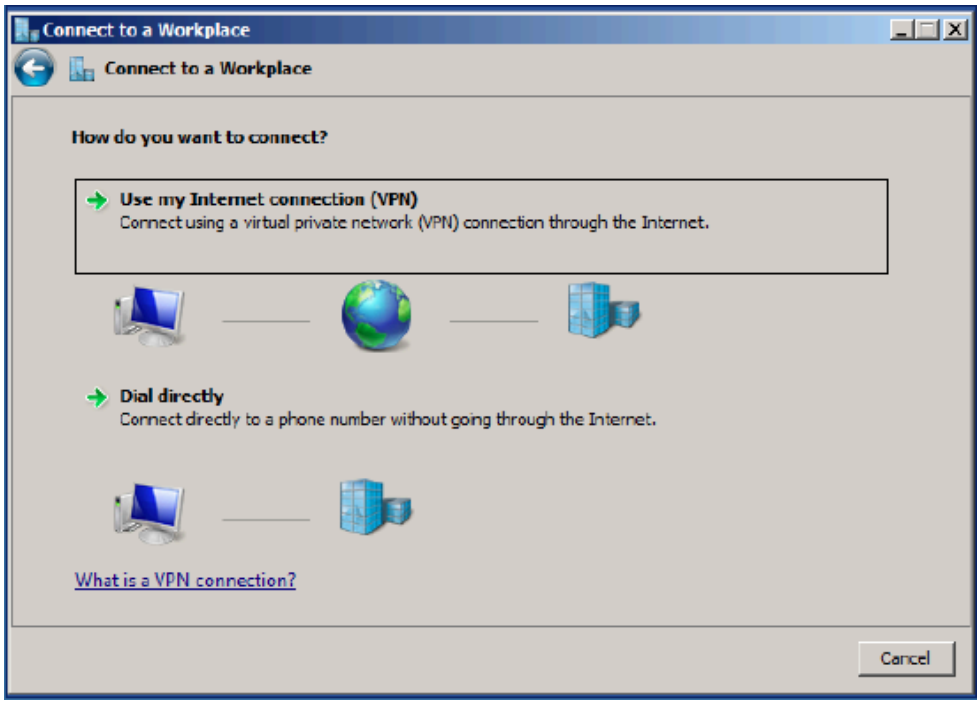
Open **Start Menu > Control Panel**, click on **Network and Internet,** click on **View network status and tasks**.



In the **Set up a connection or network** pop-up window, choose **Connect to a workplace** (Set up a dial-up or VPN connection to your workplace).

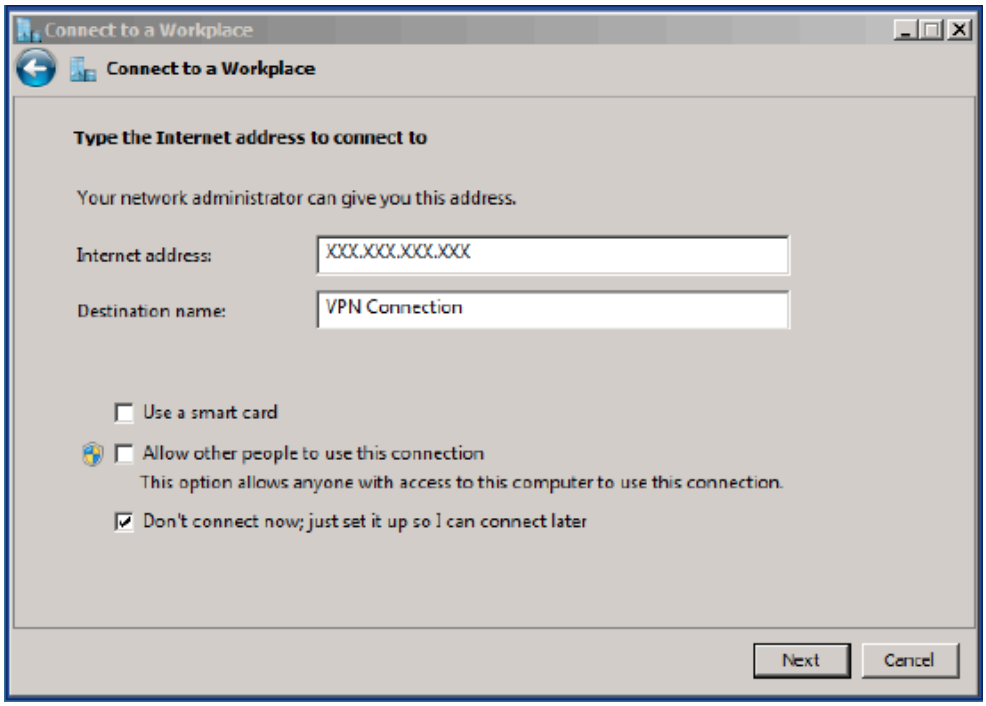


Choose **Use my Internet connection (VPN)**, in the **Connect to a workspace** dialog window.



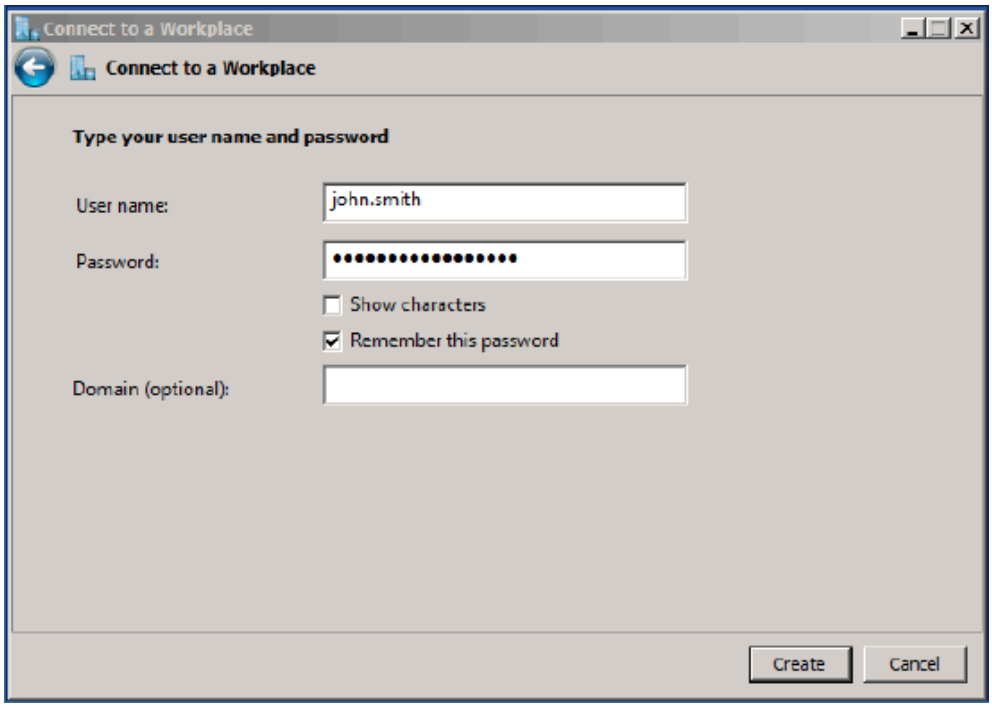
In the **Connect to a Workplace** dialog box, enter:

- **Internet address:** Enter the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.
- **Destination name:** This can be anything you want to name this connection, for example, "Work VPN."

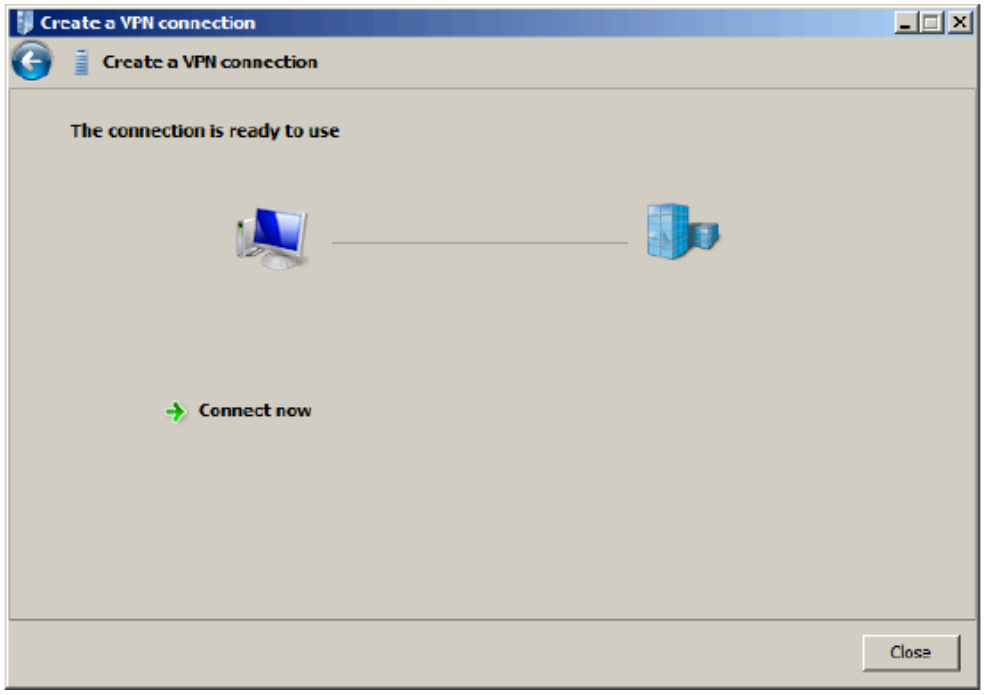


Choose "**Don't connect now; just set it up so that I can connect later**" option.

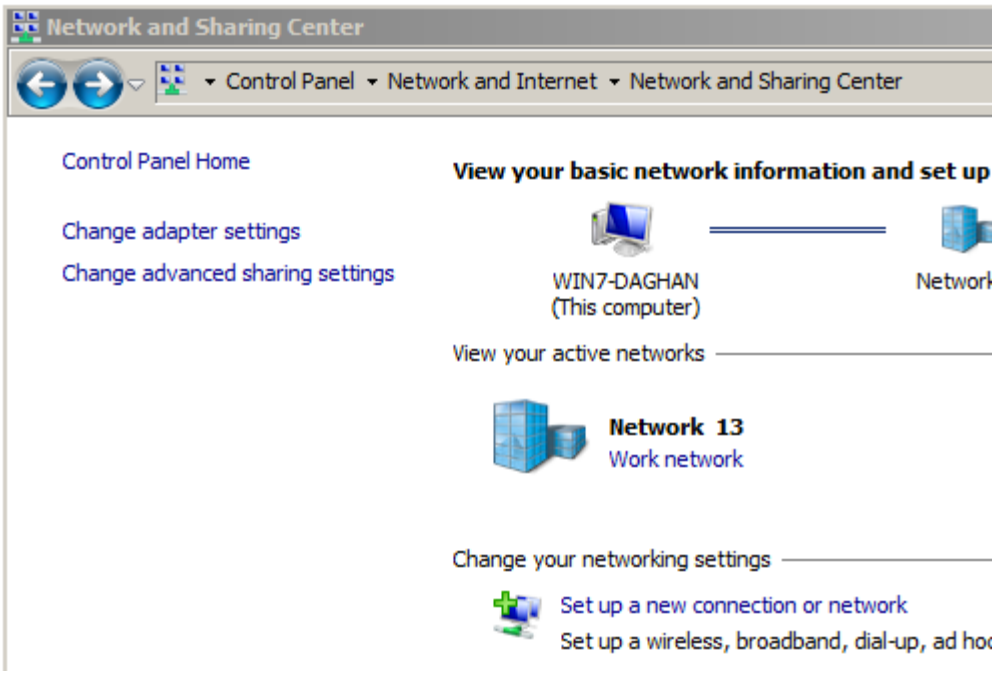
Click **Next**. In the next dialog window, enter the user credentials, and click **Create.**



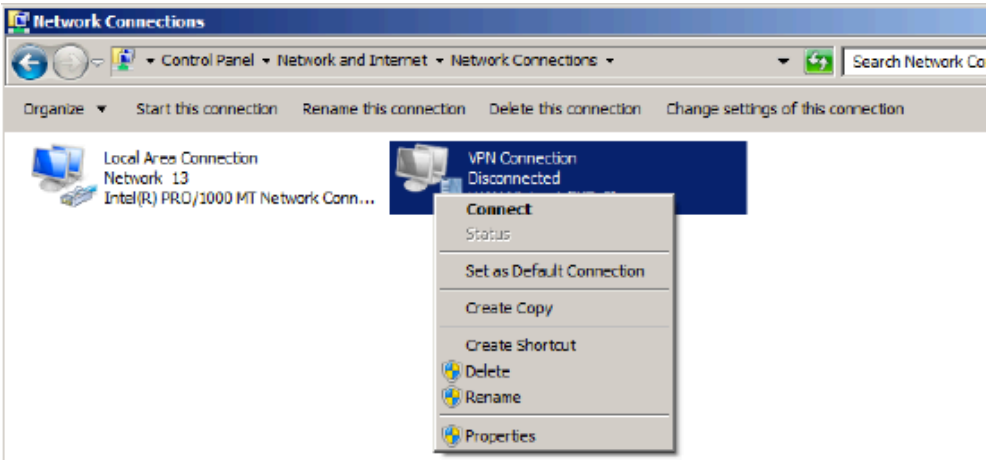
Close the VPN connection wizard.



Go to Networking and Sharing Center and click **Change Adapter Settings**

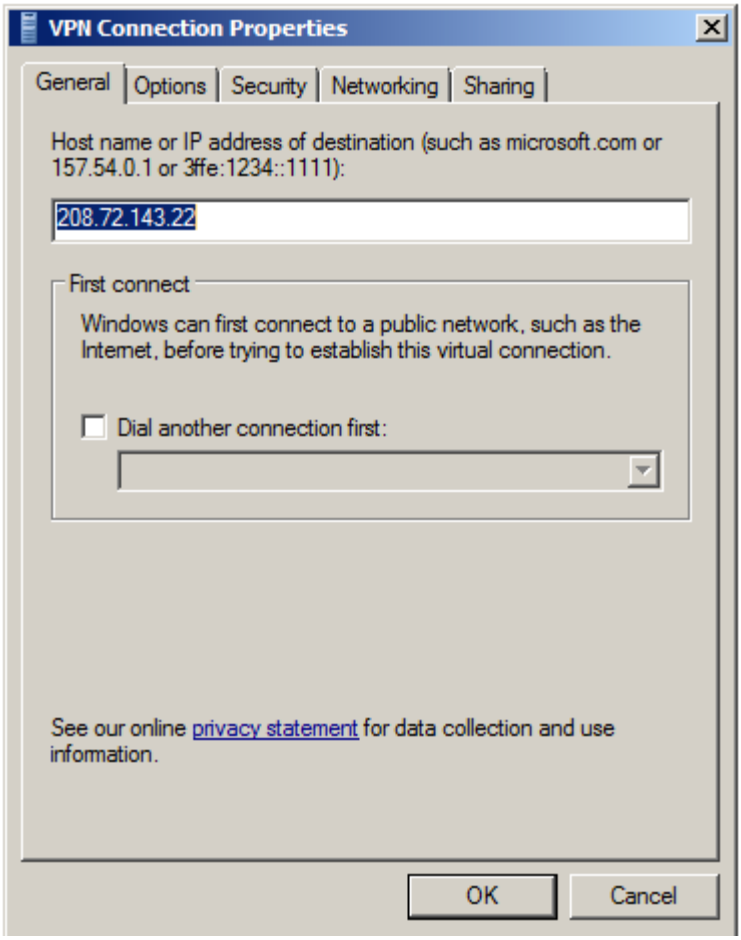


In Network Connections window, right-click on the new VPN connection settings and choose **Properties**

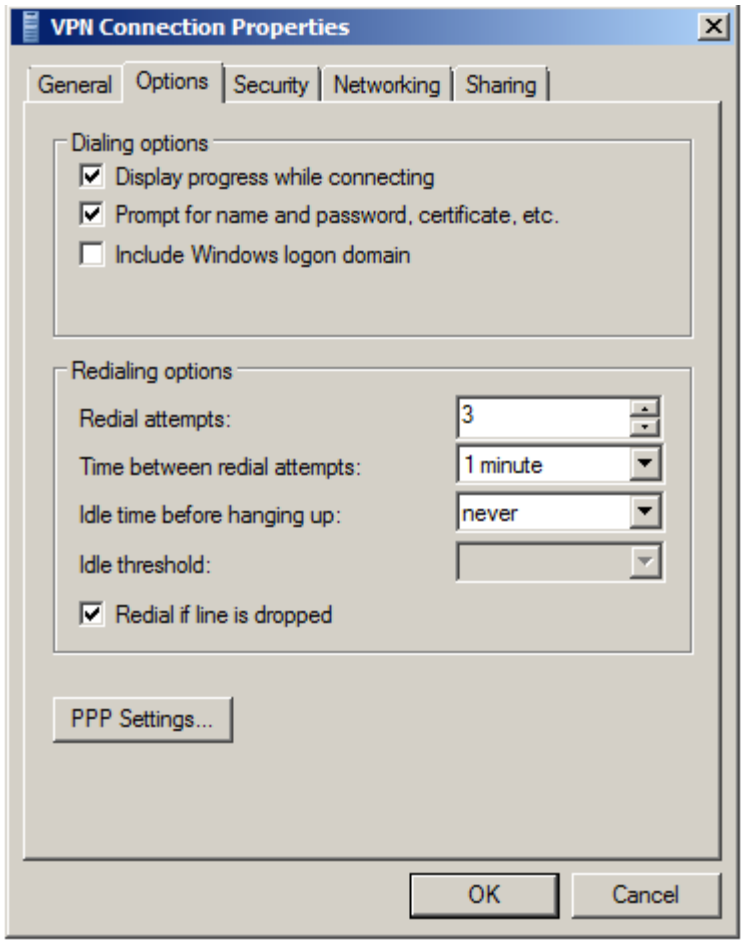


In the **General** tab, verify the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in

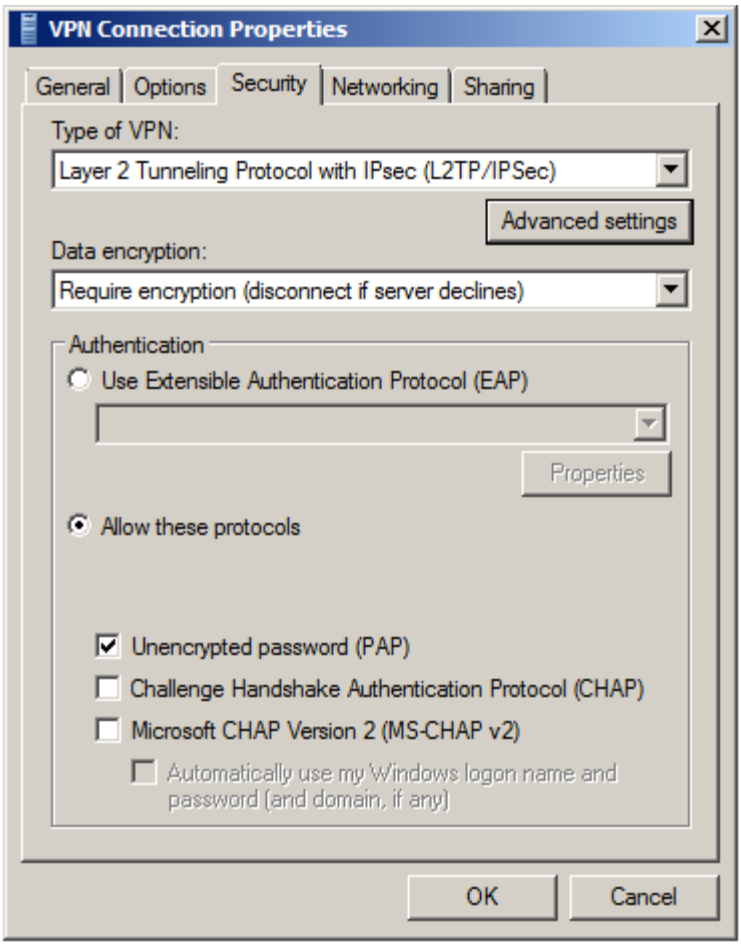
Dashboard, under Security appliance > Monitor > Appliance status.



In the **Options** tab, **uncheck** "**Include Windows logon domain**"



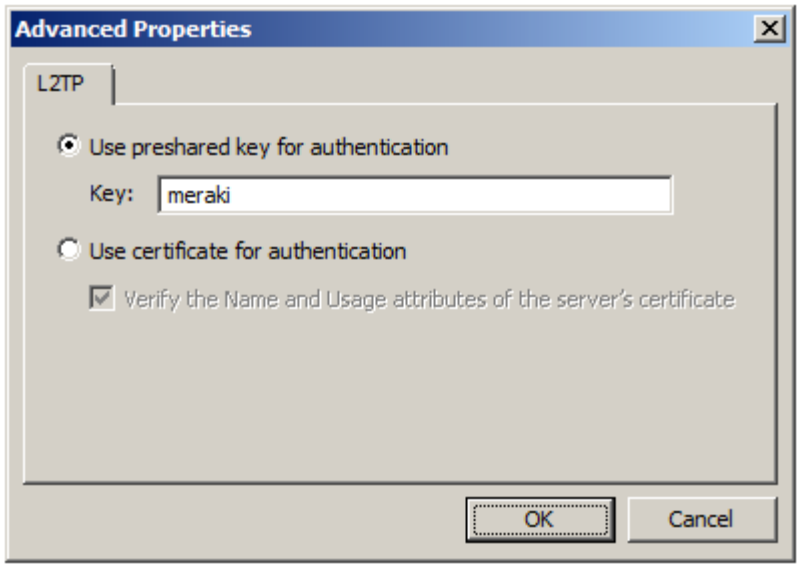
In the "**Security**" tab, choose "**Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**".
Then, check "**Unencrypted password (PAP)**", and uncheck all other options.



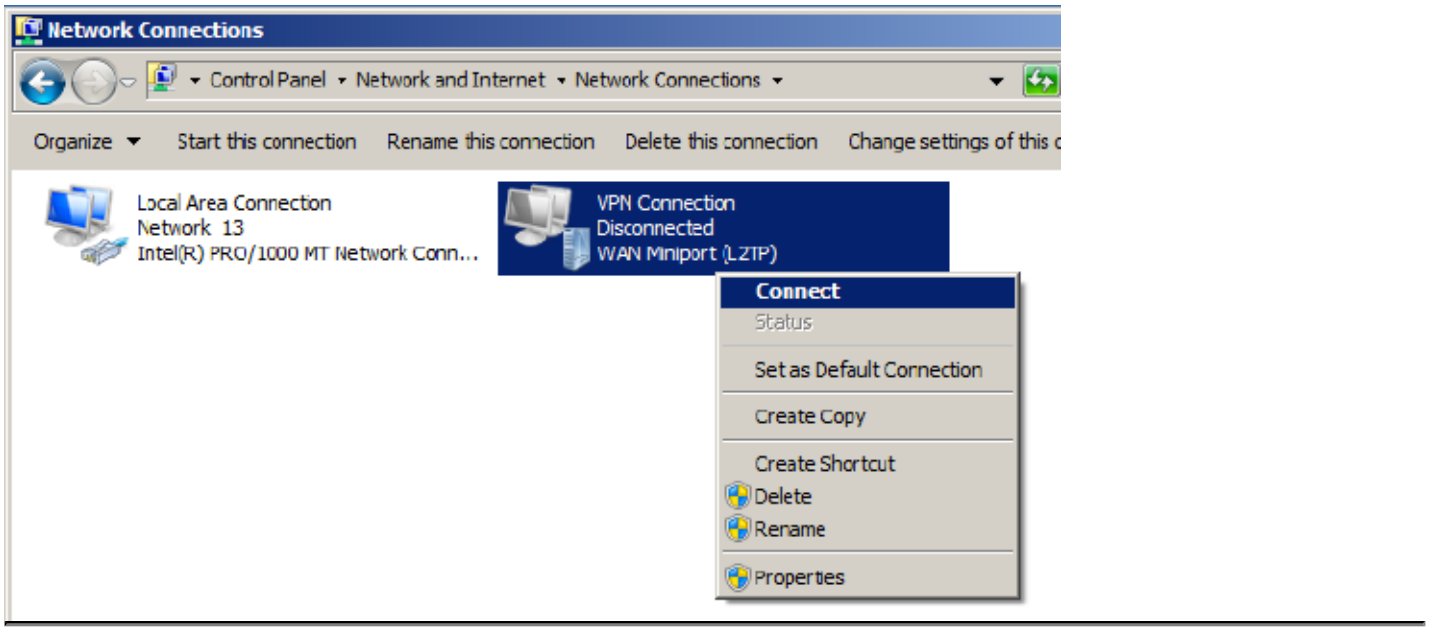
Click on "**Advanced settings**".

Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.

In **Advanced Properties** dialog box, choose "**Use preshared key for authentication**" and enter the pre-shared key that admin created in Security appliance > Configure > Client VPN settings.
Click **OK**.



Back at the **Network Connections** window, right-click on the **VPN connection** and click **Connect**



Verify your user name and click **Connect.**

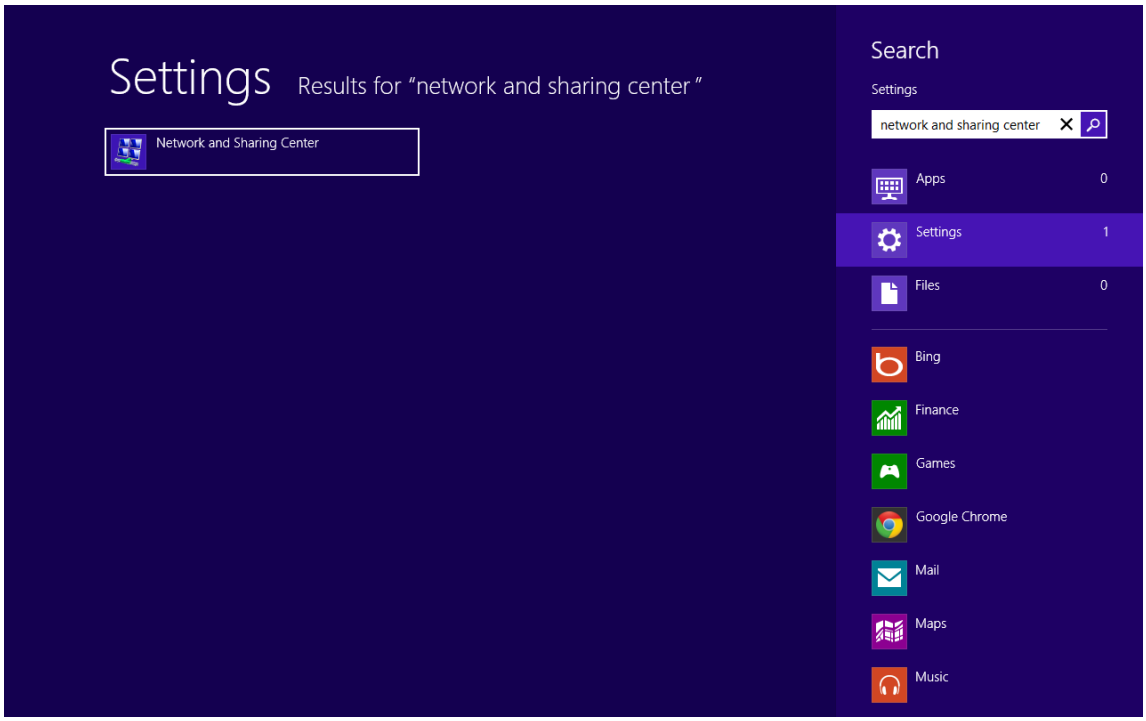
Windows 8

Currently only the following authentication mechanisms are supported:

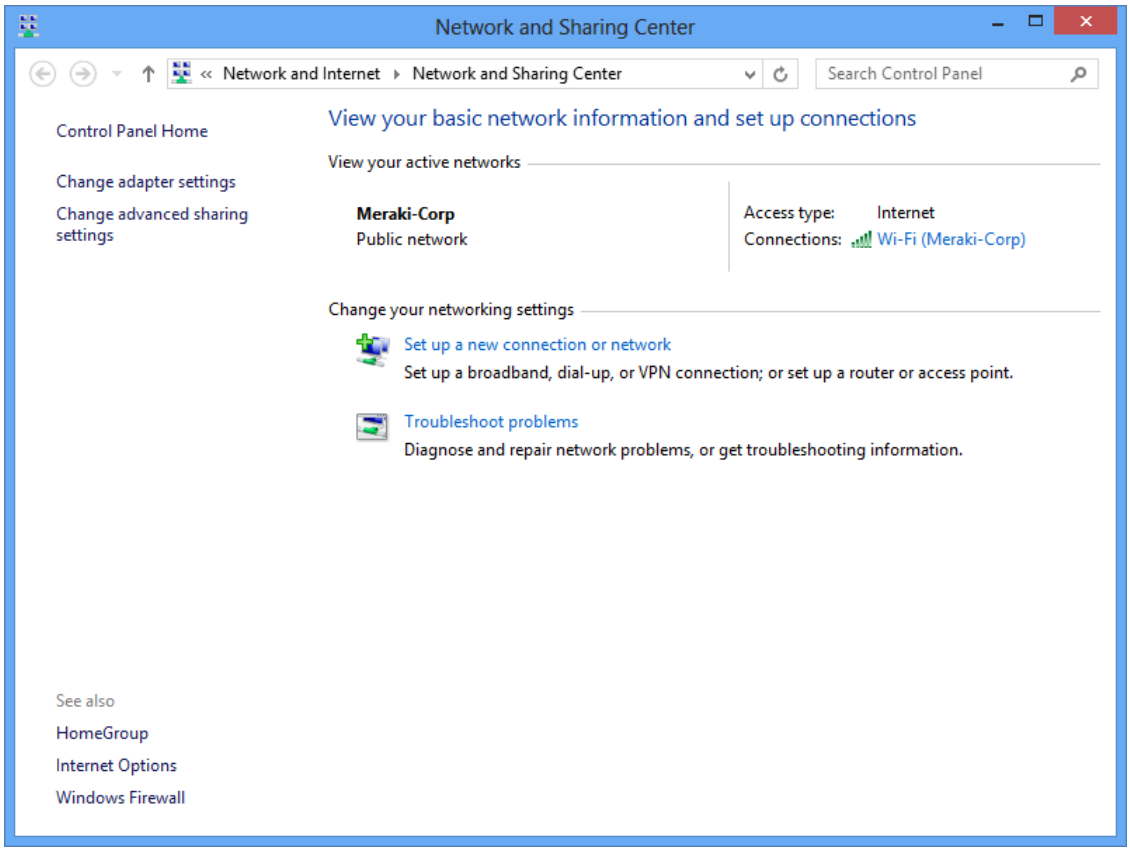
- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) **is the user email address** entered in the Dashboard.

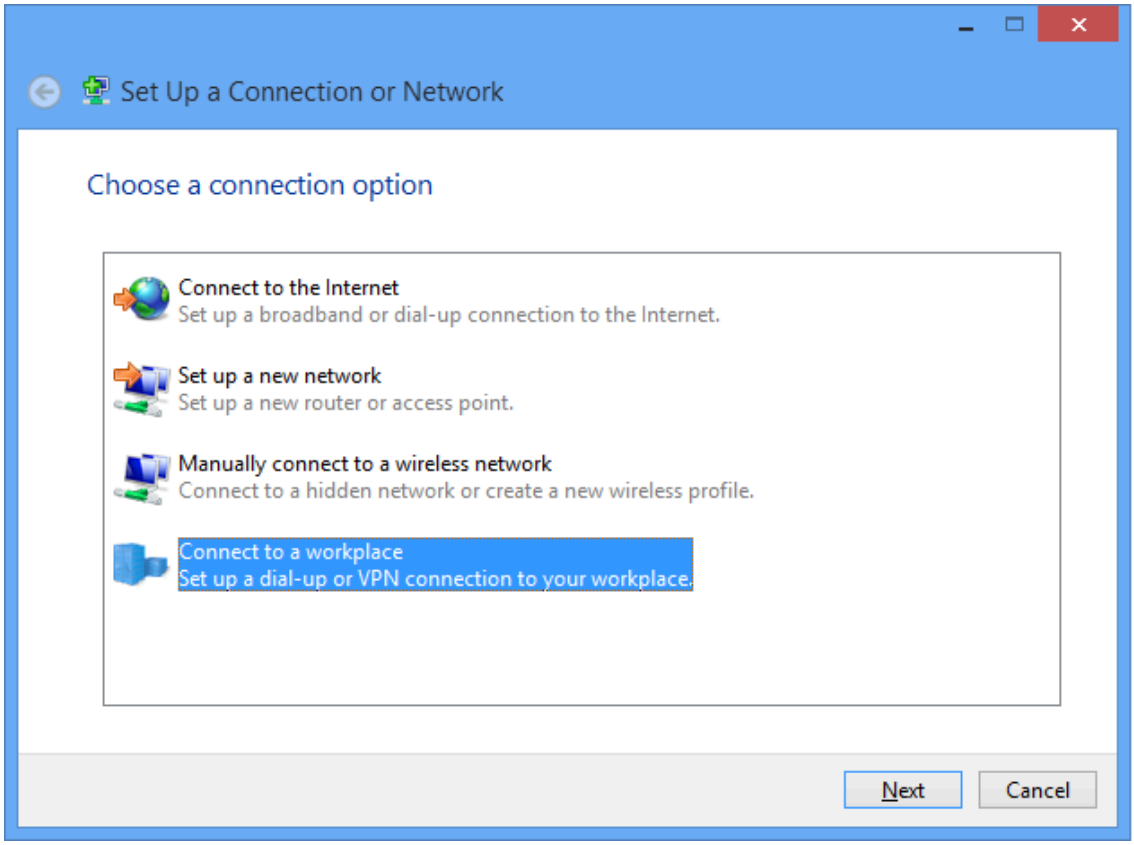
Open **Start Menu > Network and Sharing Center** and click **Settings**.



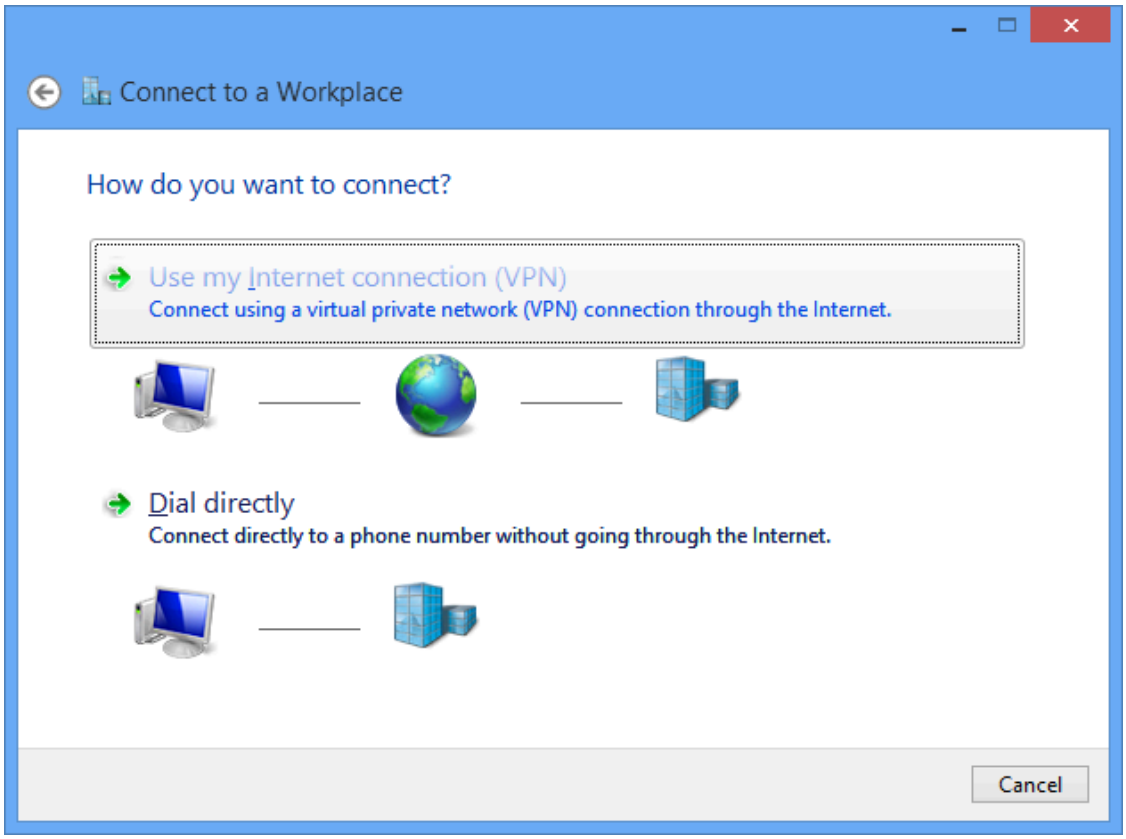
In the **Network and Sharing Center**, click **Set up a new connection or network**.



In the **Set Up a Connection or Network** pop-up window, choose **Connect to a workplace**.
(Set up a dial-up or VPN connection to your workplace).



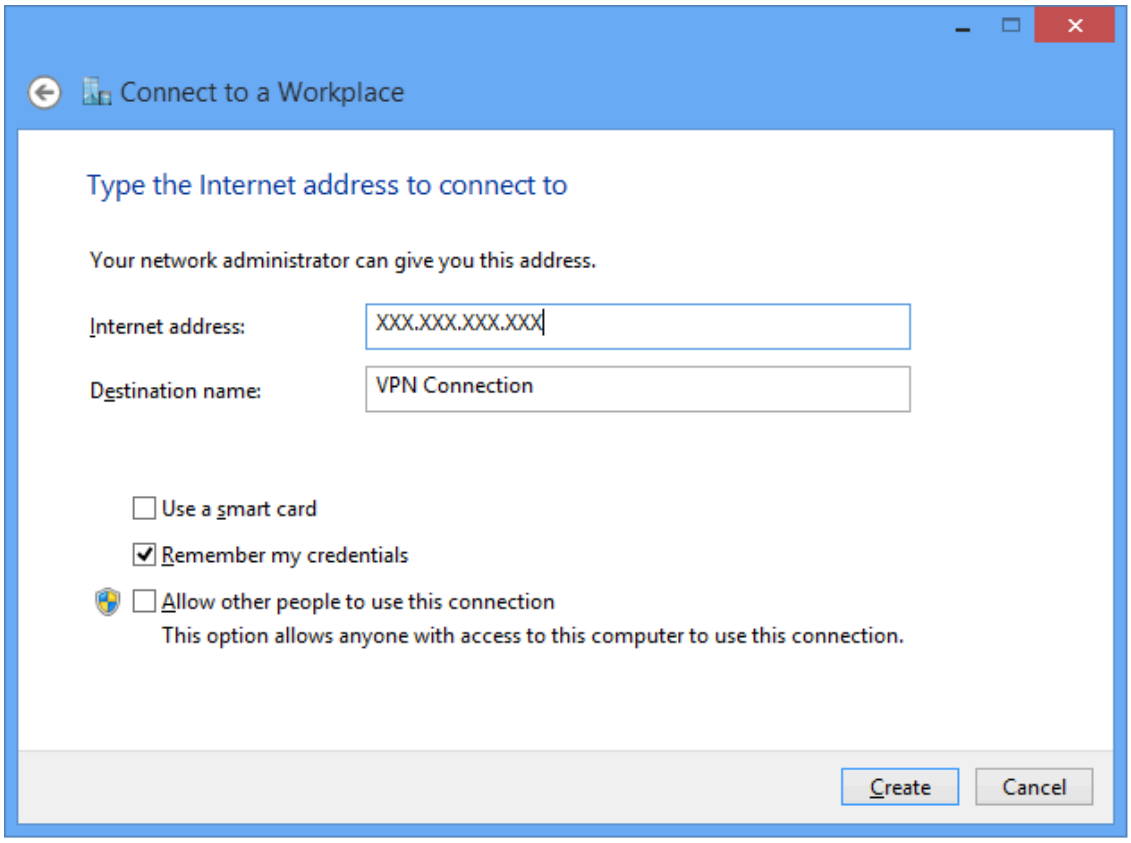
Choose **Use my Internet connection (VPN)**, in the **Connect to a Workspace** dialog window.



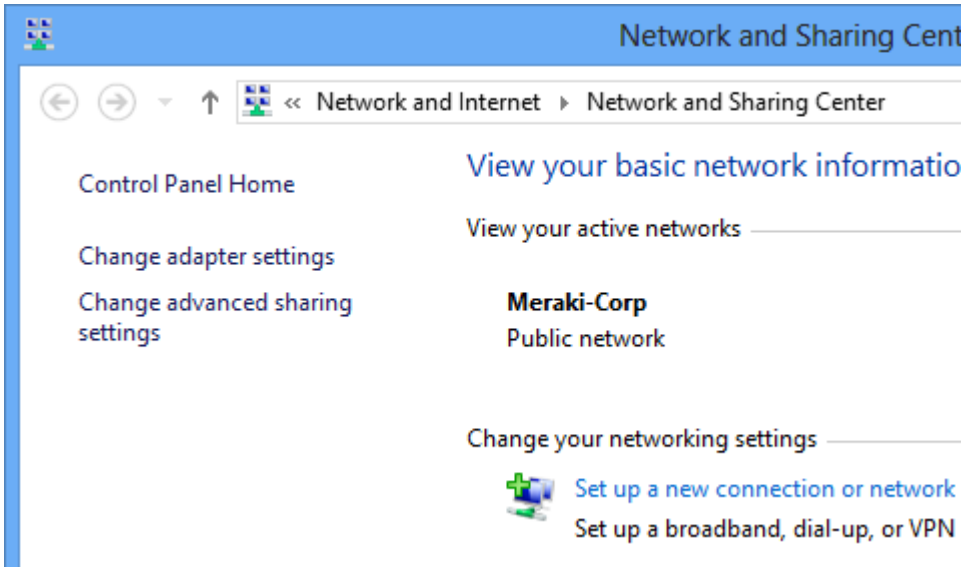
In the **Connect to a Workplace** dialog box, enter:

- **Internet address:** Enter the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.
- **Destination name:** This can be anything you want to name this connection, for example, "Work VPN."

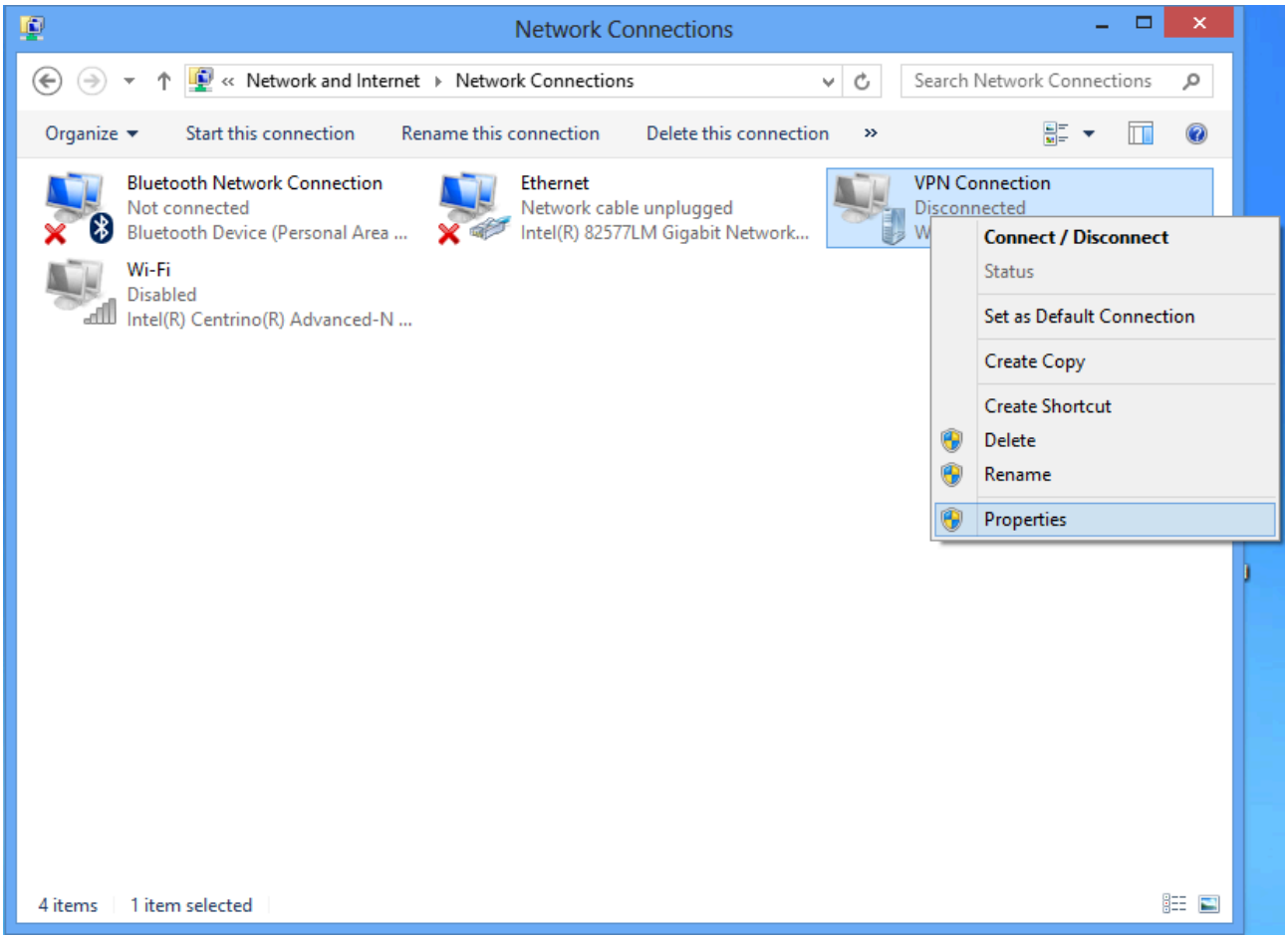
Click **Create.**



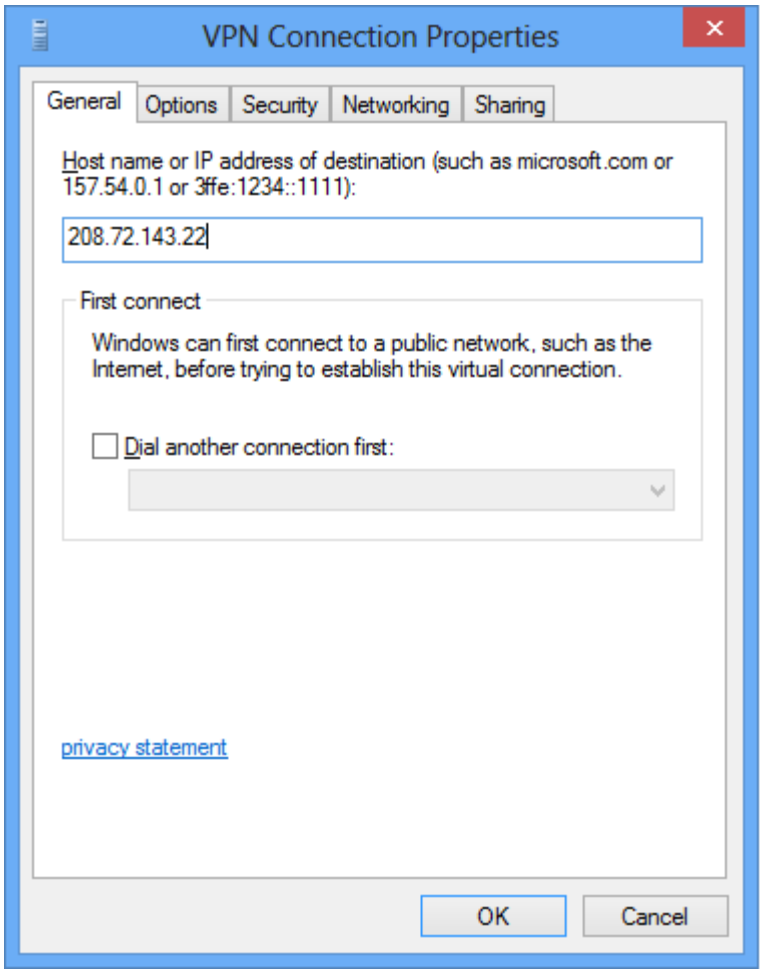
Go back to **Network and Sharing Center** and click **Change Adapter Settings**.



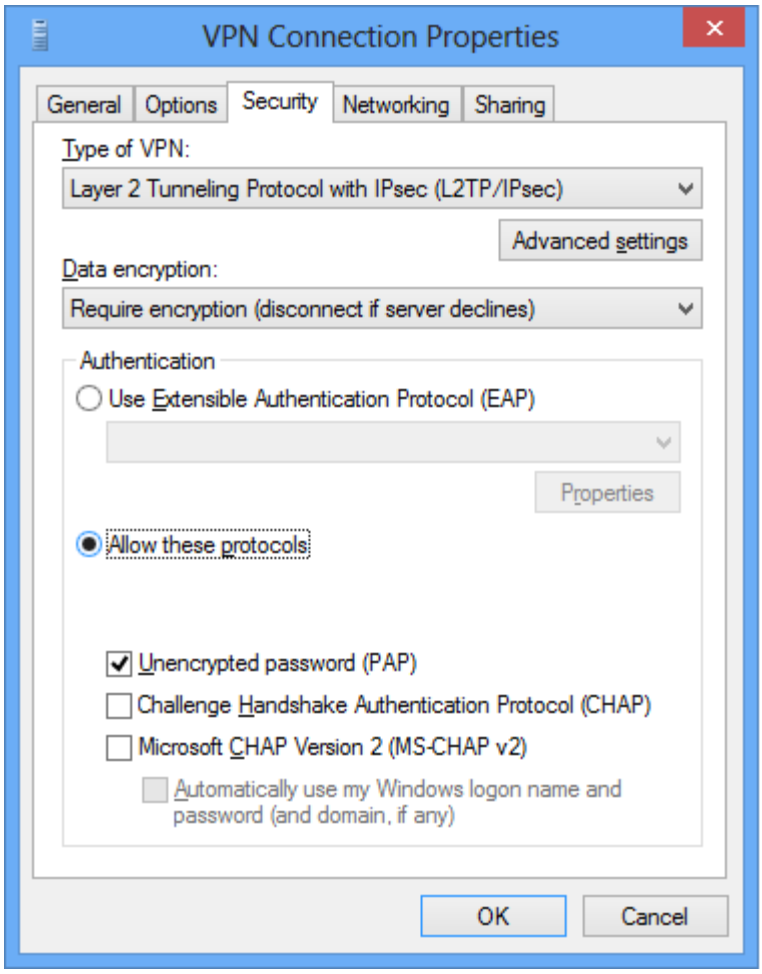
In the **Networks Connections** window, right click on the **VPN connection** icon and choose **Properties**.



In the **General** tab, verify the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.



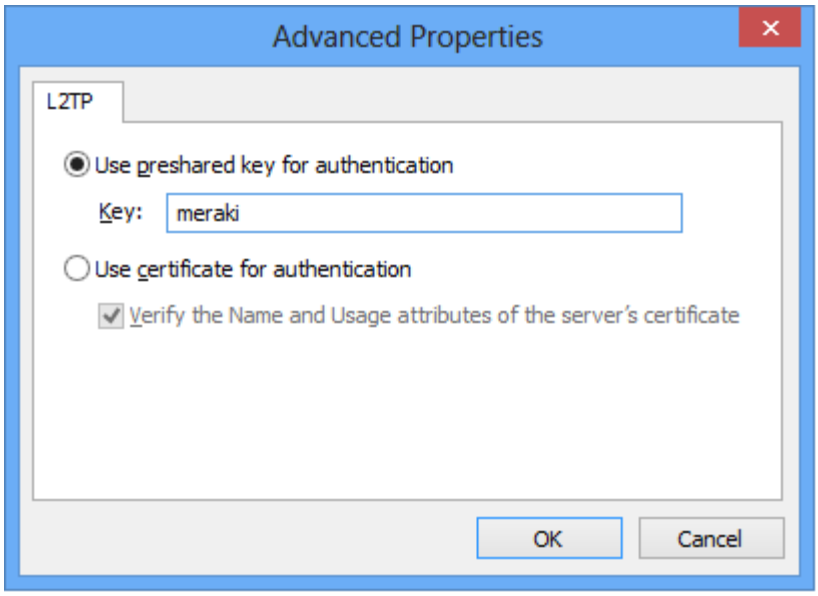
In the "**Security**" tab, choose "**Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**".
Then, check "**Unencrypted password (PAP)**", and uncheck all other options.



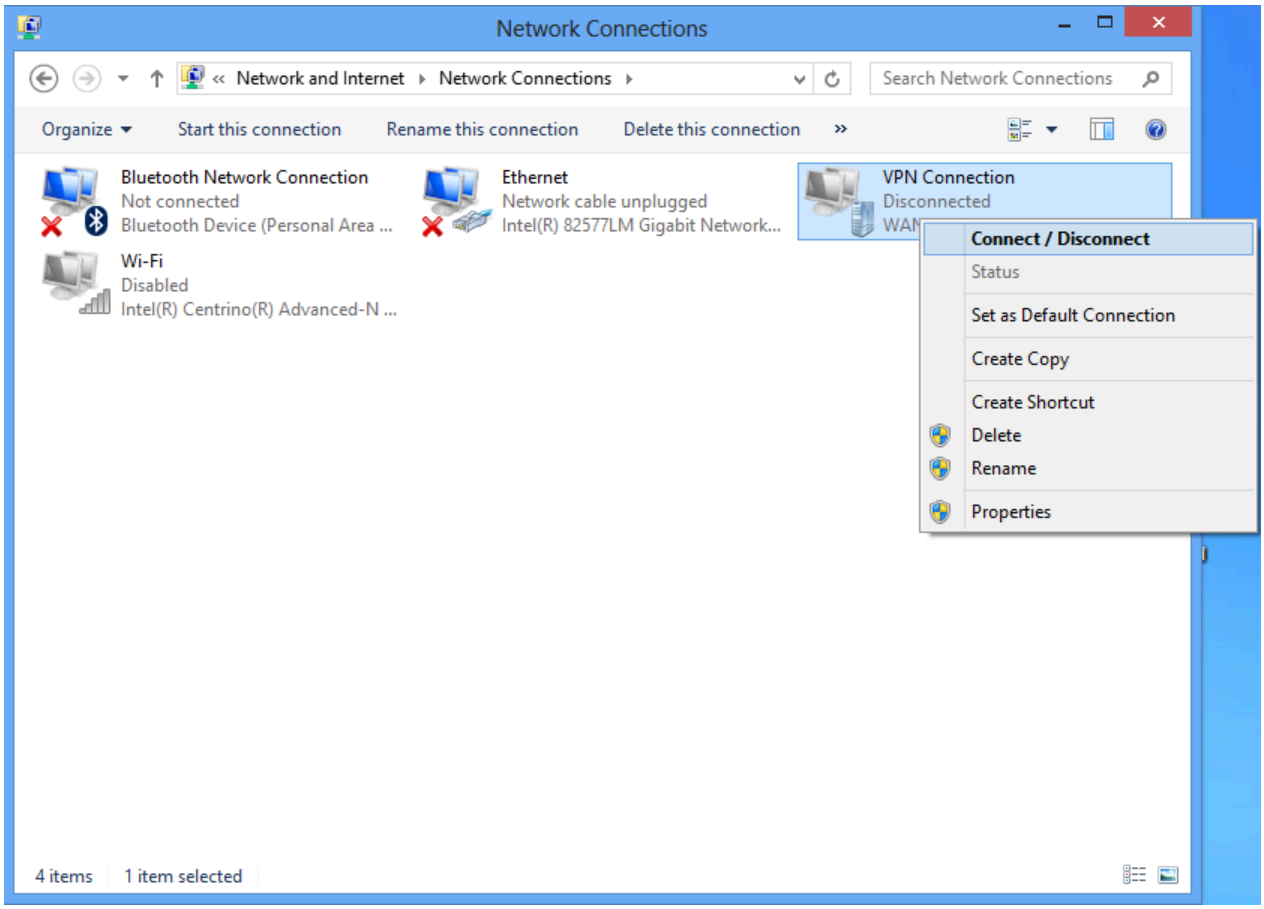
Click on "**Advanced settings**".

Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.

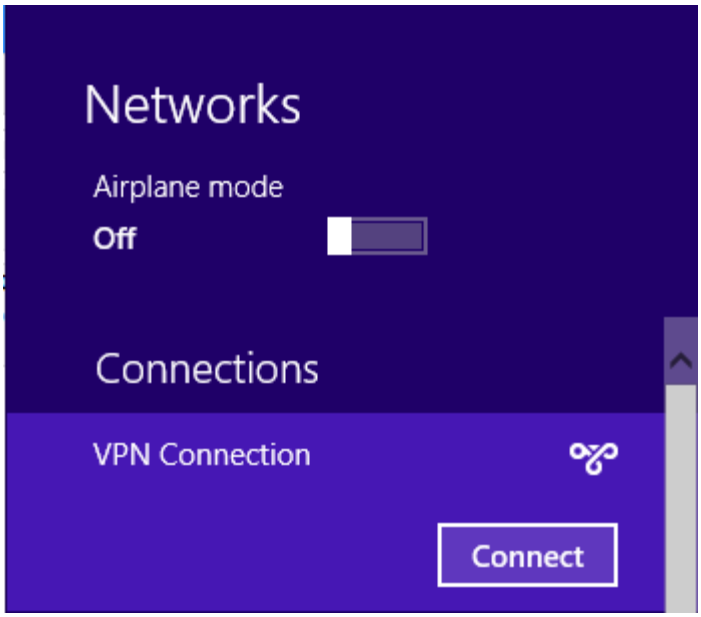
In **Advanced Properties** dialog box, choose "**Use preshared key for authentication**" and enter the pre-shared key that admin created in Security appliance > Configure > Client VPN settings.
Click **OK**.



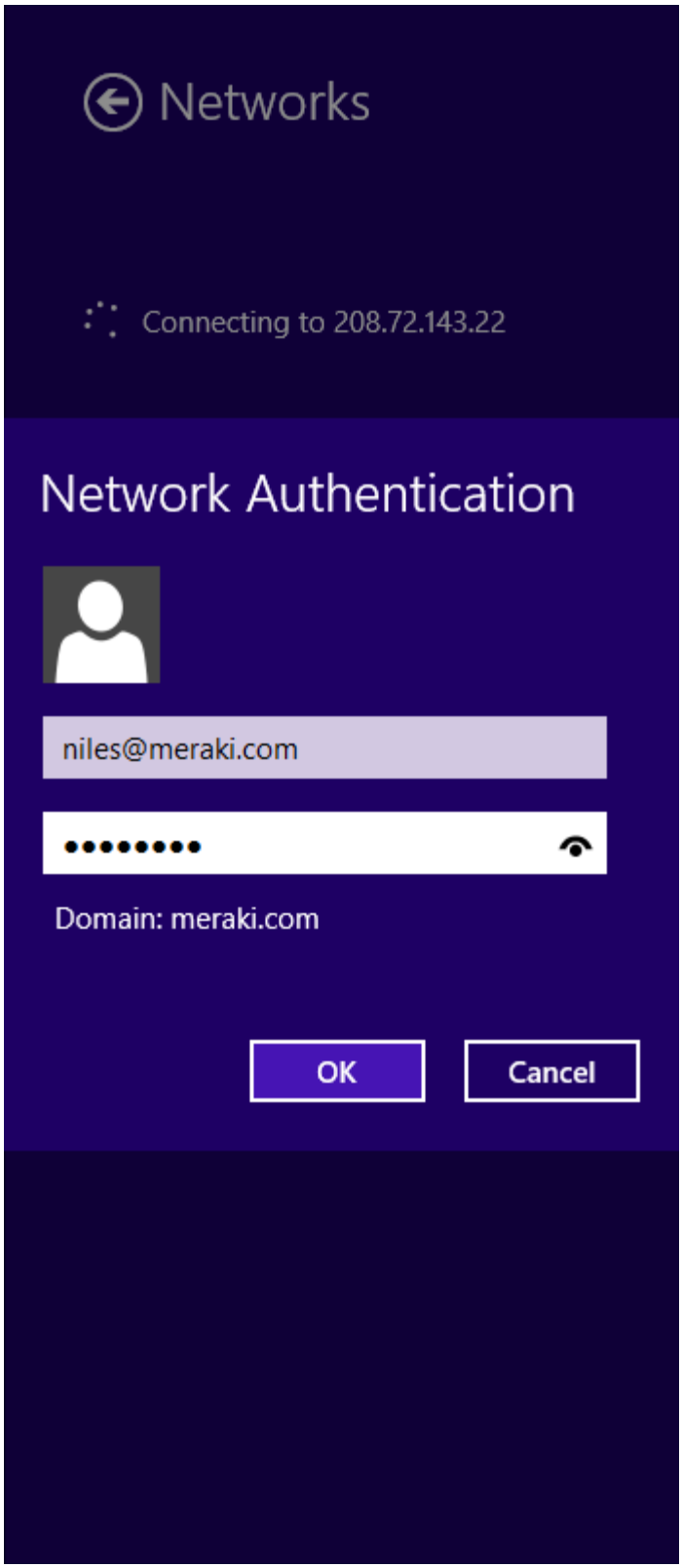
Back at the **Network Connections** window, right-click on the **VPN connection** and click **Connect / Disconnect**.



Find your VPN profile and click **Connect**.



Enter your user name and password.
Click **OK.**


Networks
Connecting to 208.72.143.22
Network Authentication
niles@meraki.com
Domain: meraki.com
OK
Cancel

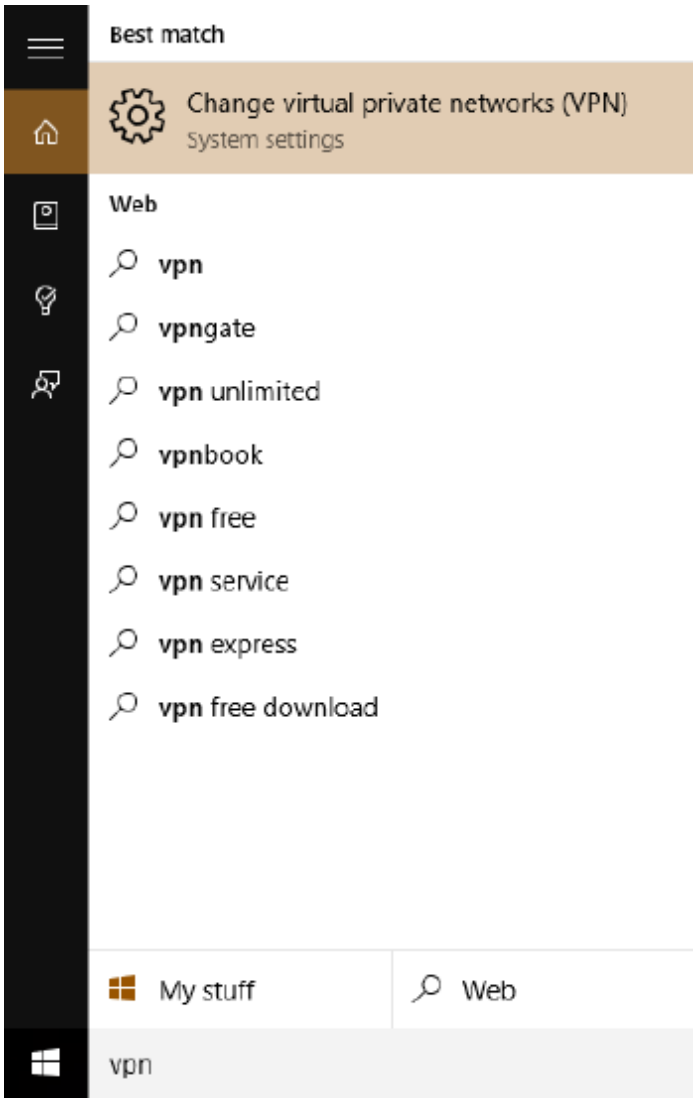
Windows 10

Currently only the following authentication mechanisms are supported:

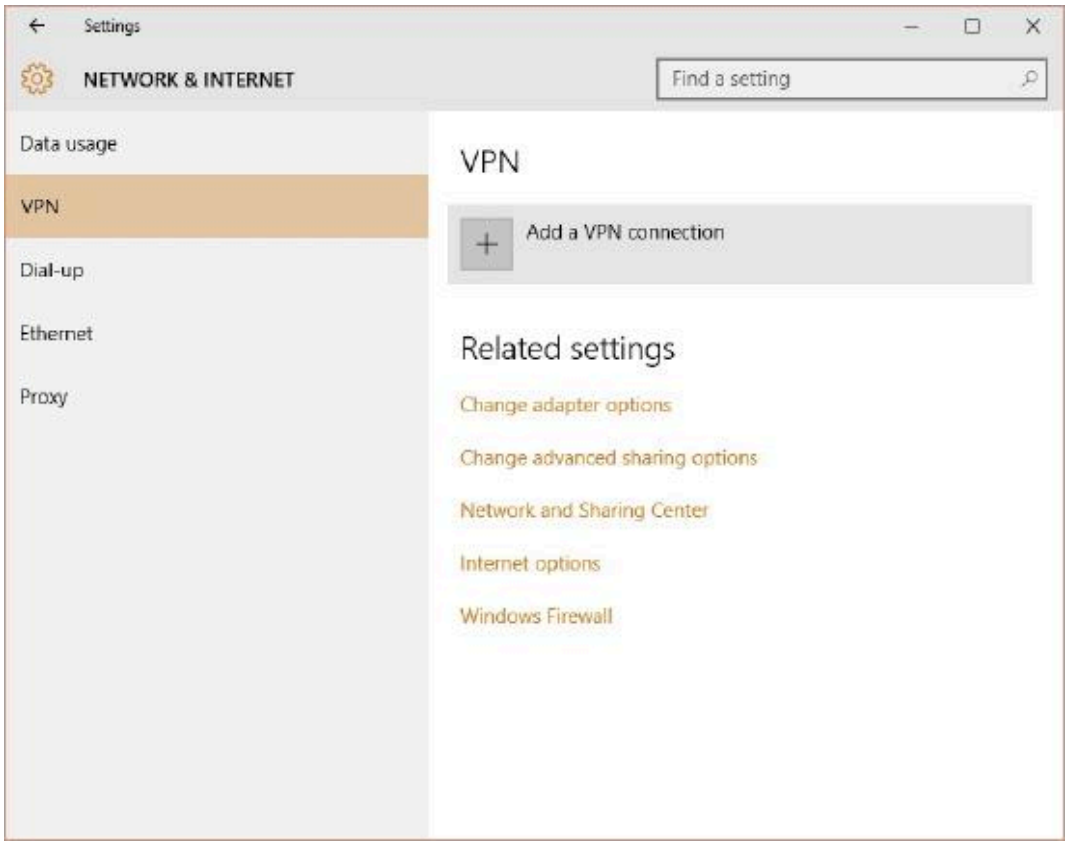
- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) **is the user email address** entered in the Dashboard.

Open **Start Menu > Search "VPN" > Click Change virtual private networks (VPN)**



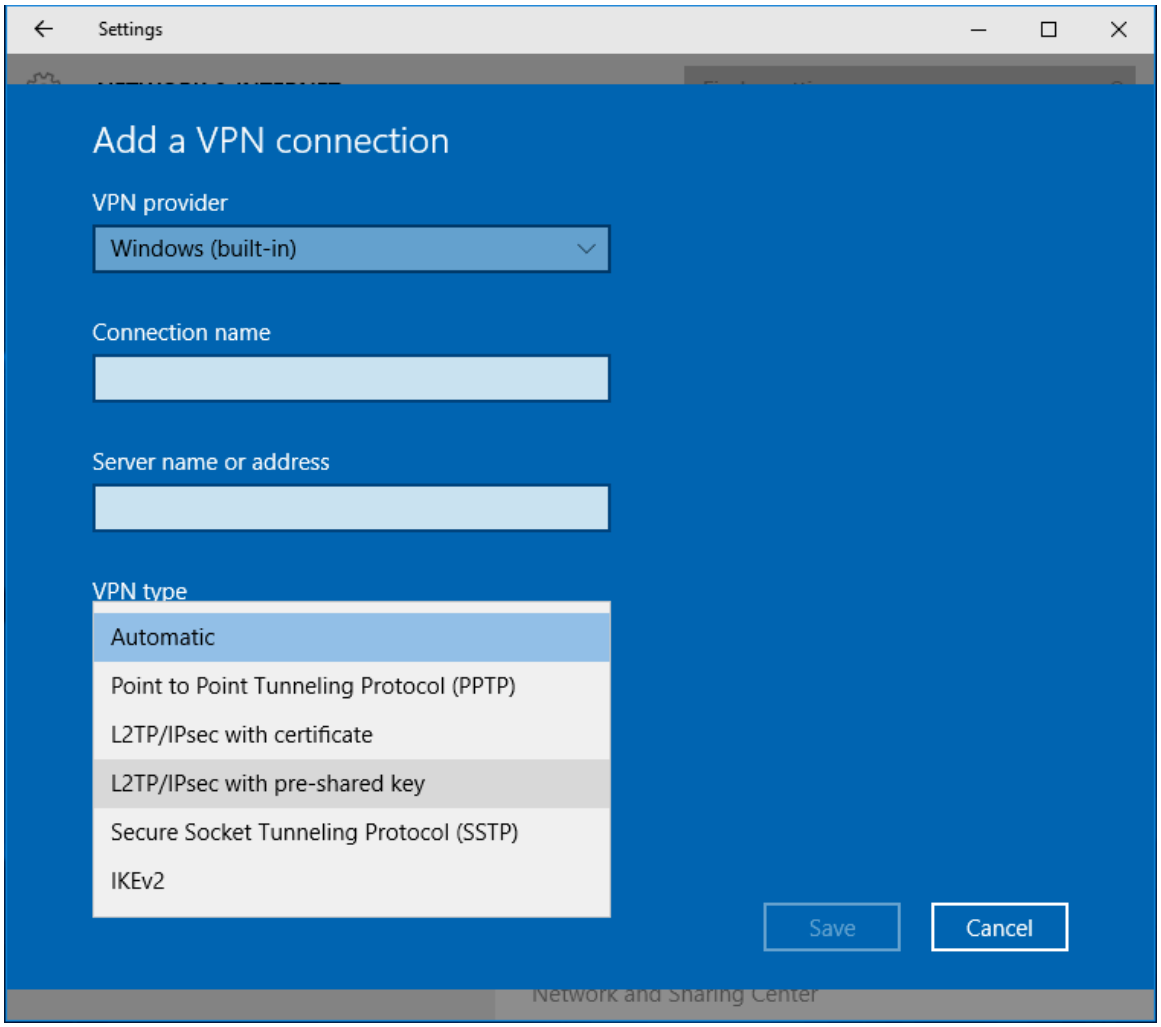
From the VPN settings page, click **Add a VPN connection**.



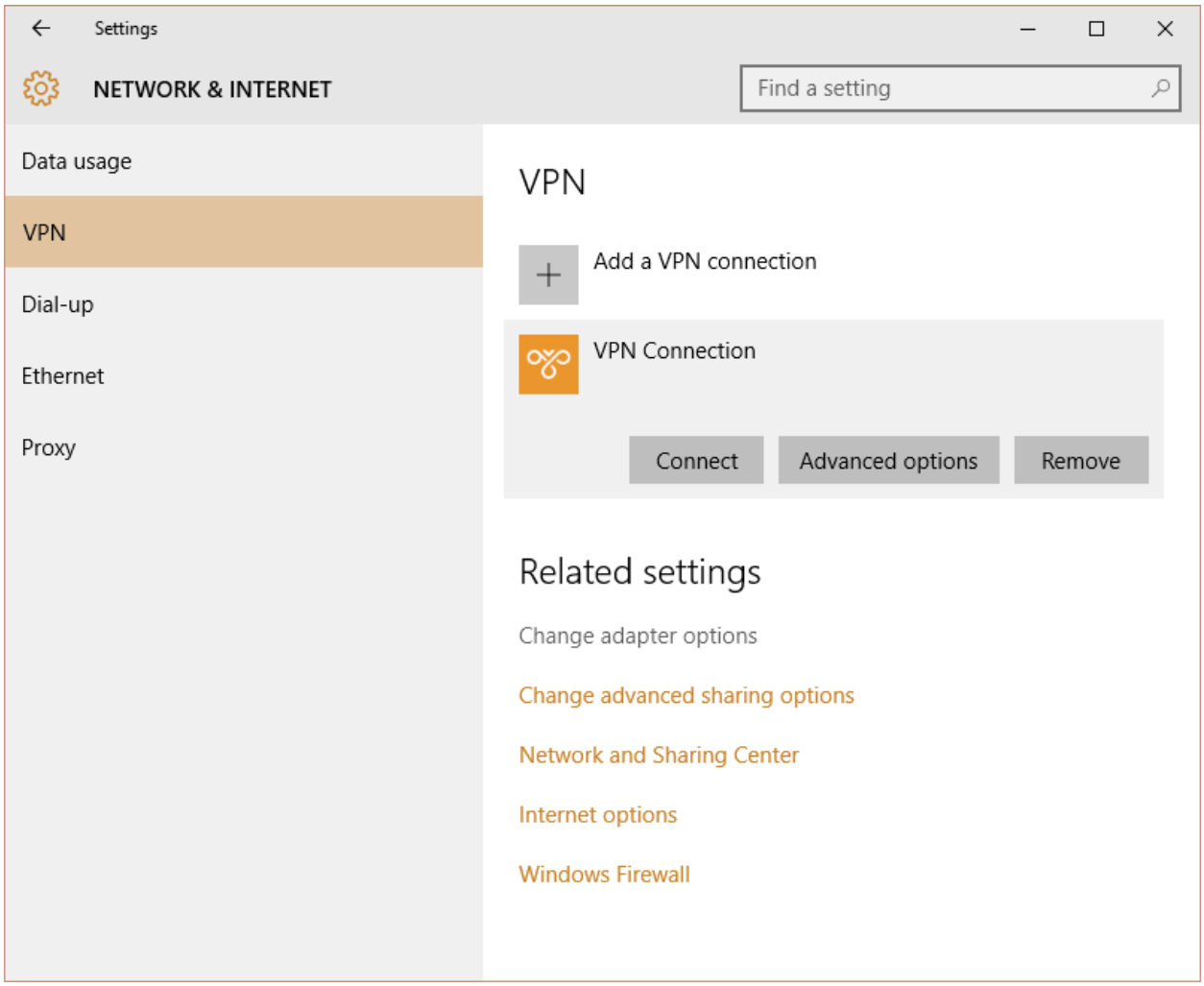
In the Add a VPN connection dialog:

- **VPN provider:** Set to Windows (built-in)
- **Connection name:** This can be anything you want to name this connection, for example, "Work VPN."
- **Server name or address:** Enter the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.
- **VPN type:** Select L2TP/IPsec with pre-shared key
- **User name** and **Password:** optional

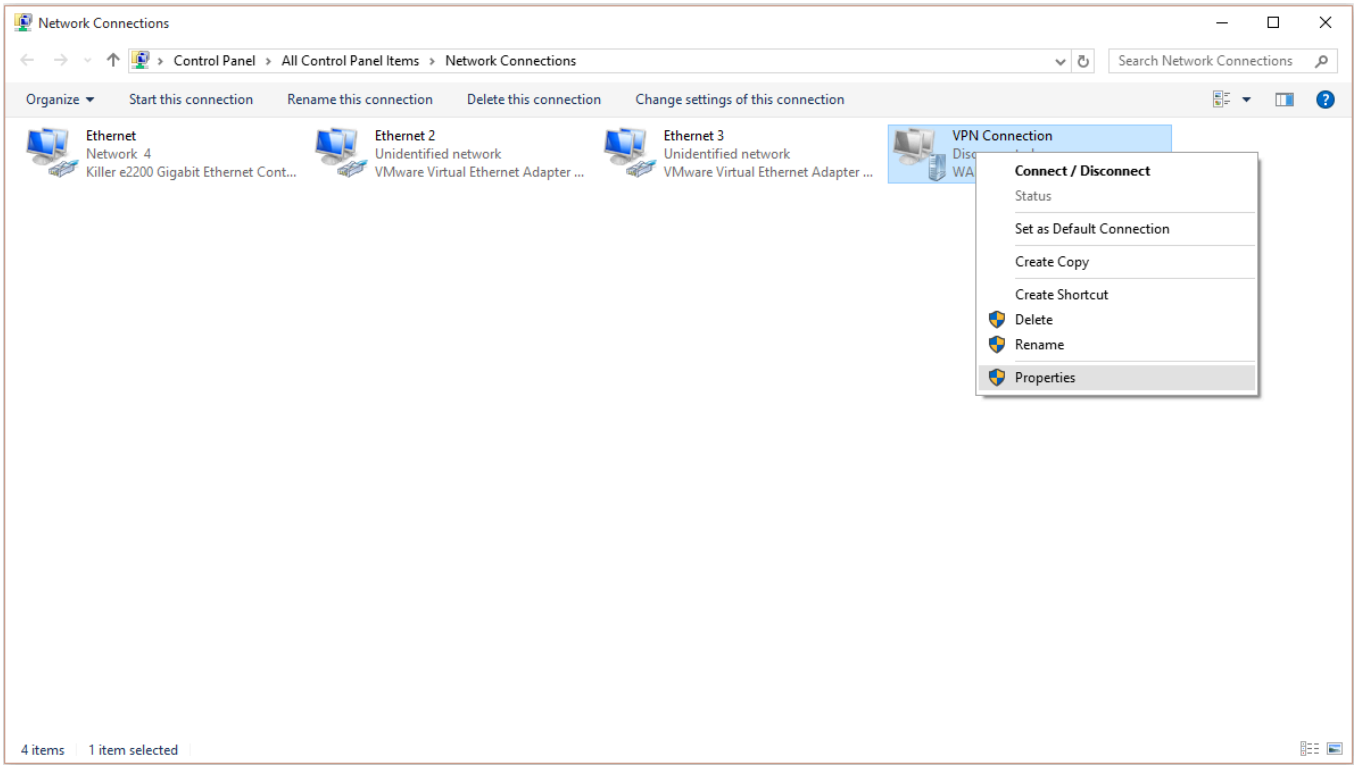
Press **Save.**



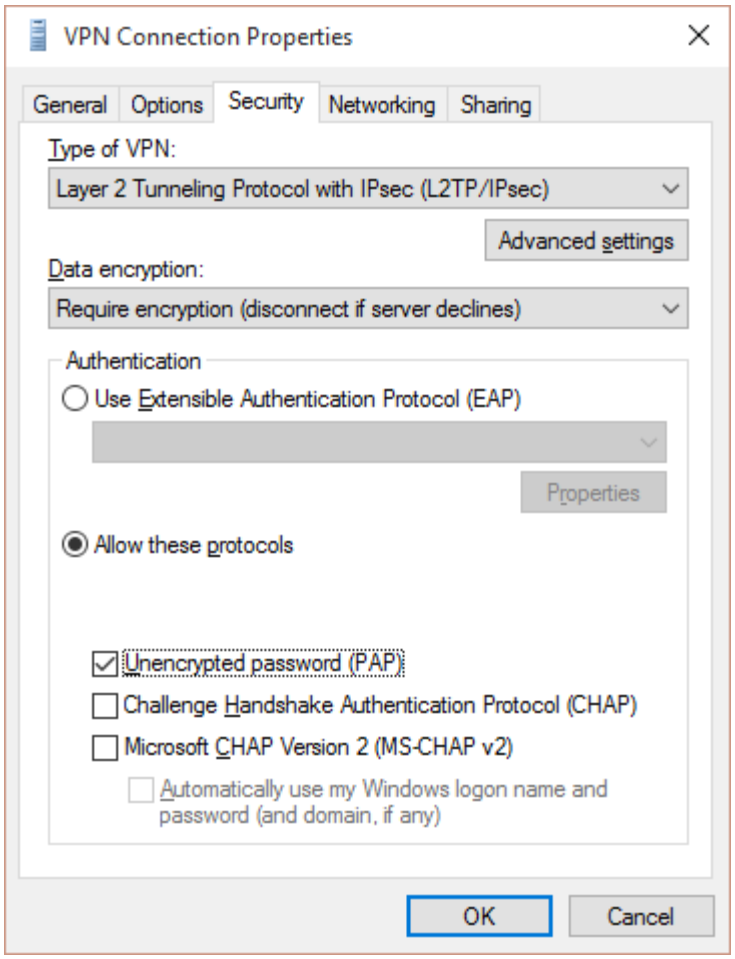
After the VPN connection has been created, click **Change adapter options** under **Related settings**.



Right-click on the **VPN Connection** from the list of adapters and click **Properties**.



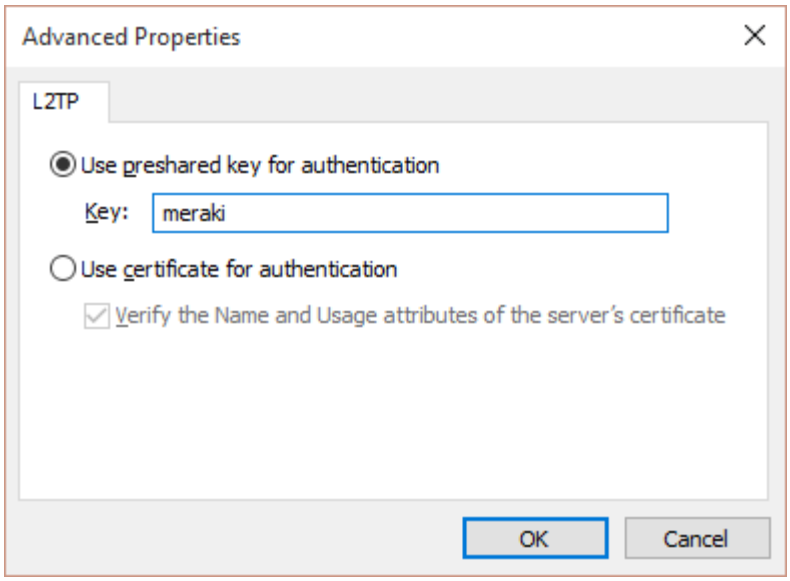
In the **Security** tab, select "**Require encryption (disconnect if sever declines)**" under **Data encryption**. Then, select "**Allow these protocols"** under **Authentication**. From the list of protocols, check "**Unencrypted password (PAP)**", and uncheck all other options.



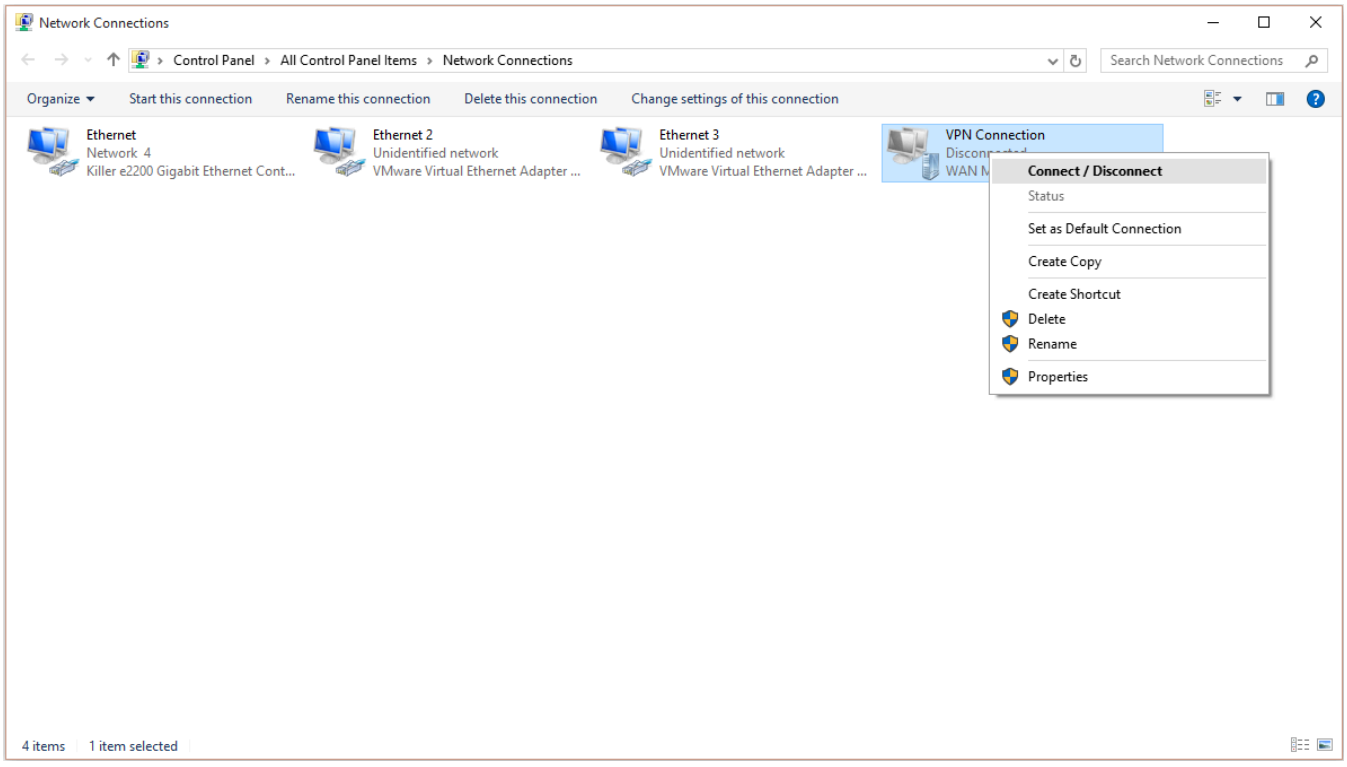
Click on "**Advanced settings**"

Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.

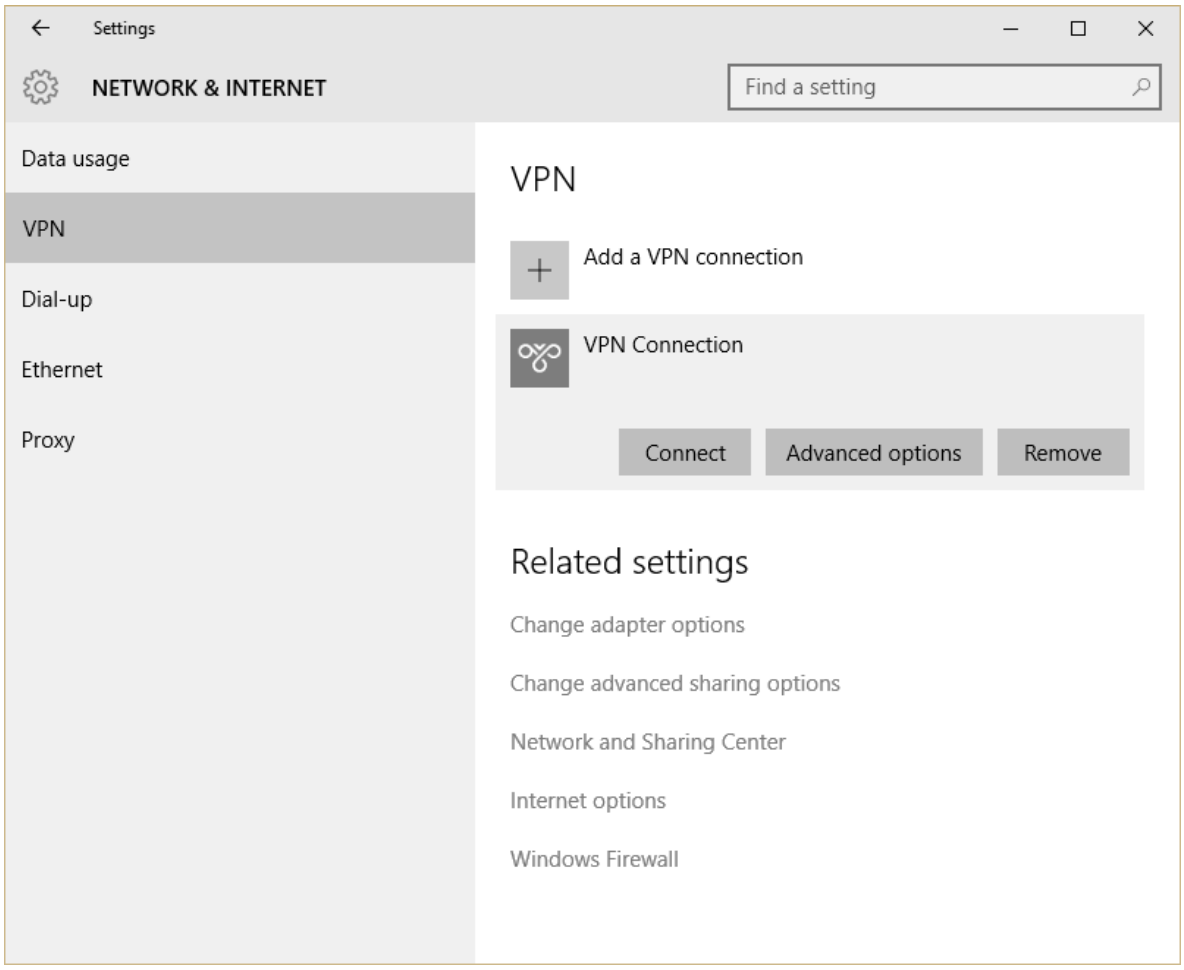
In **Advanced Properties** dialog box, choose "**Use preshared key for authentication**" and enter the pre-shared key that admin created in Security appliance > Configure > Client VPN settings.



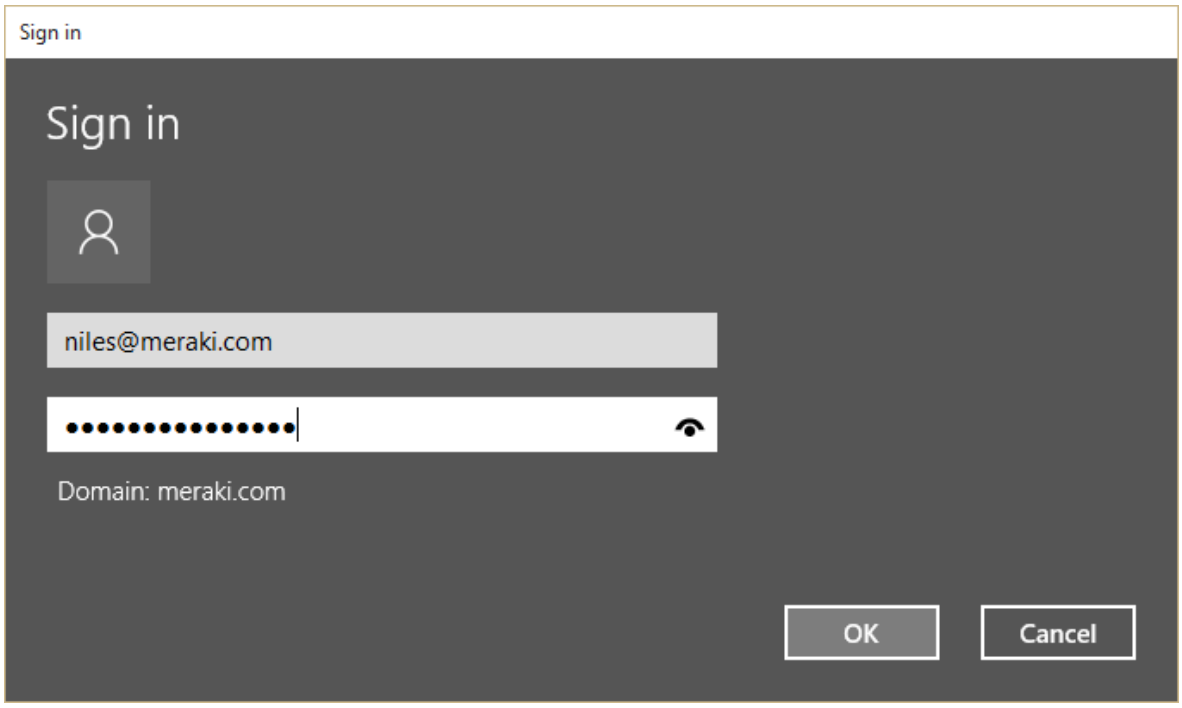
Back at the **Network Connections** window, right-click on the **VPN connection** and click **Connect / Disconnect**.



Find your VPN profile and click **Connect**.



Enter your user name and password.
Click **OK.**



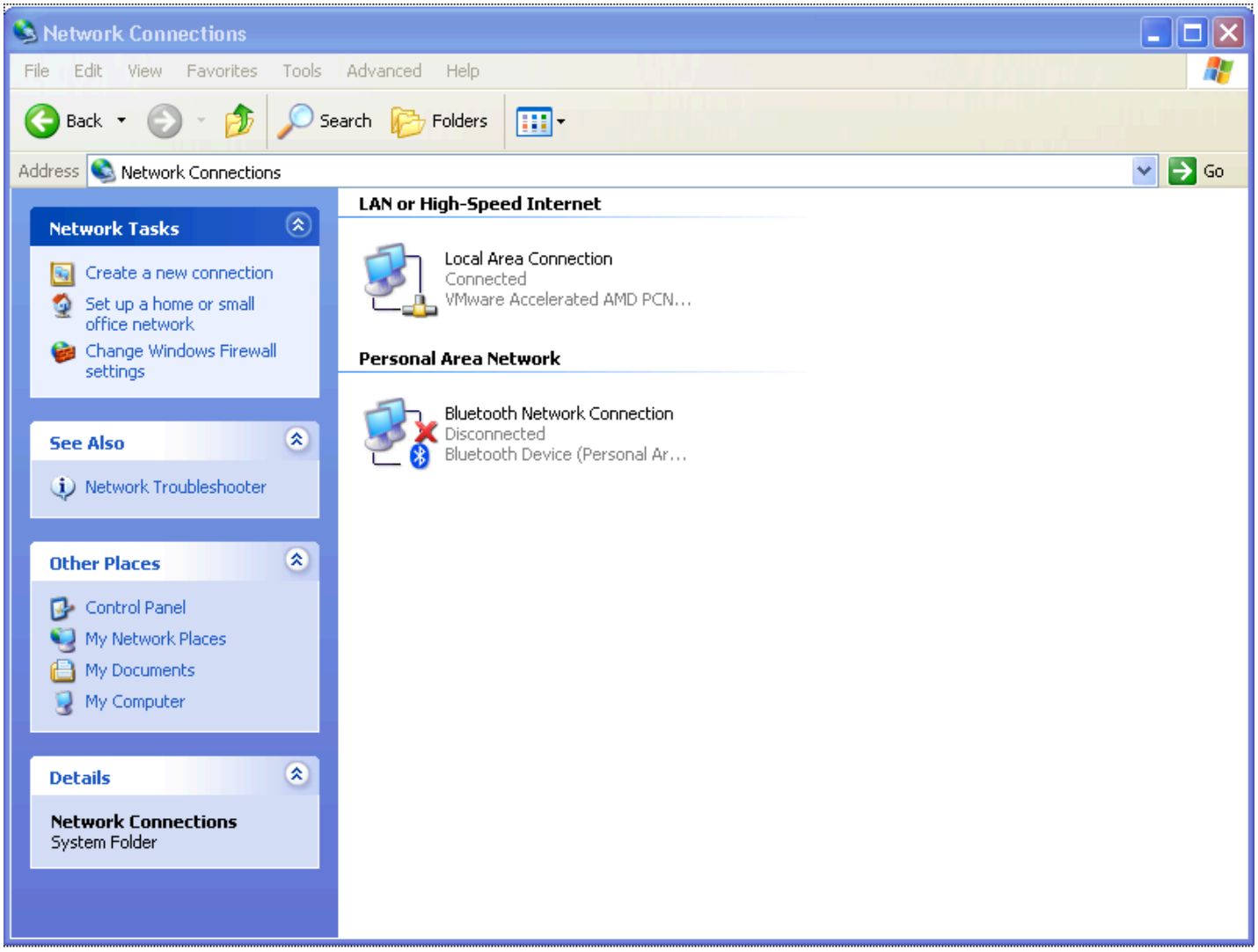
Windows XP

Currently only the following authentication mechanisms are supported:

- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

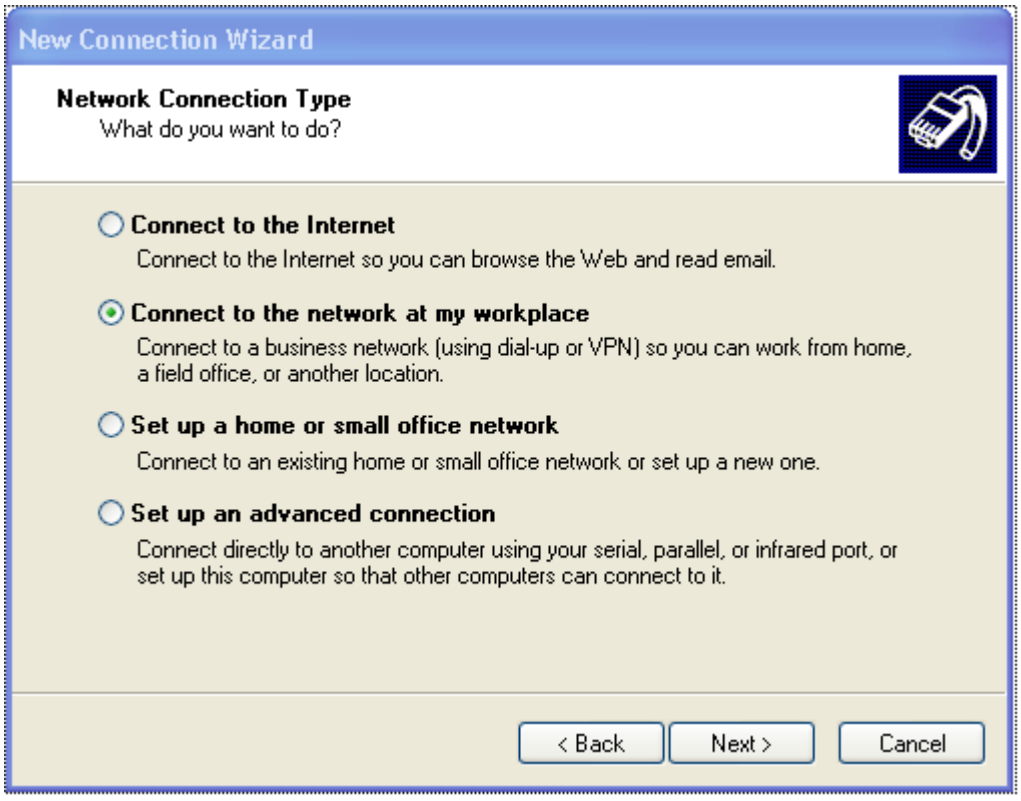
When using Meraki hosted authentication, **use the email address** for VPN account / user name.

Open **Start Menu > Control Panel**, click on **Network Connections.**



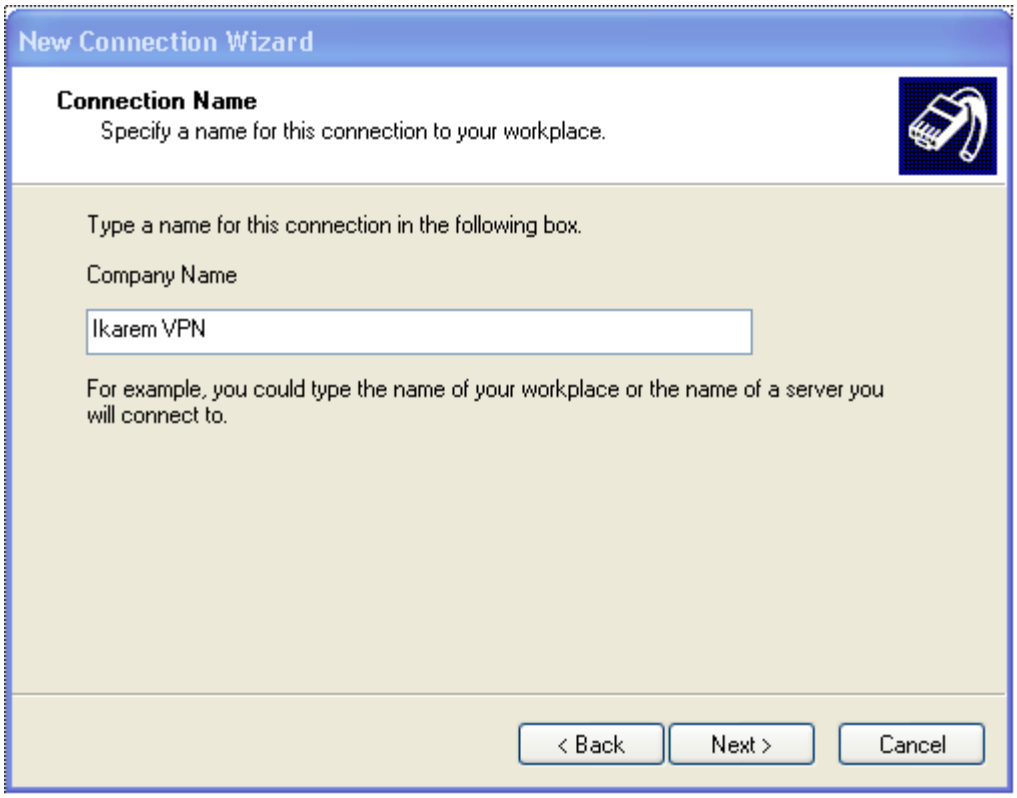
In the **Network Tasks section**, click on **Create a new connection**.

Choose **Connect to the network at my workplace**, in the **New Connection Wizard** window.

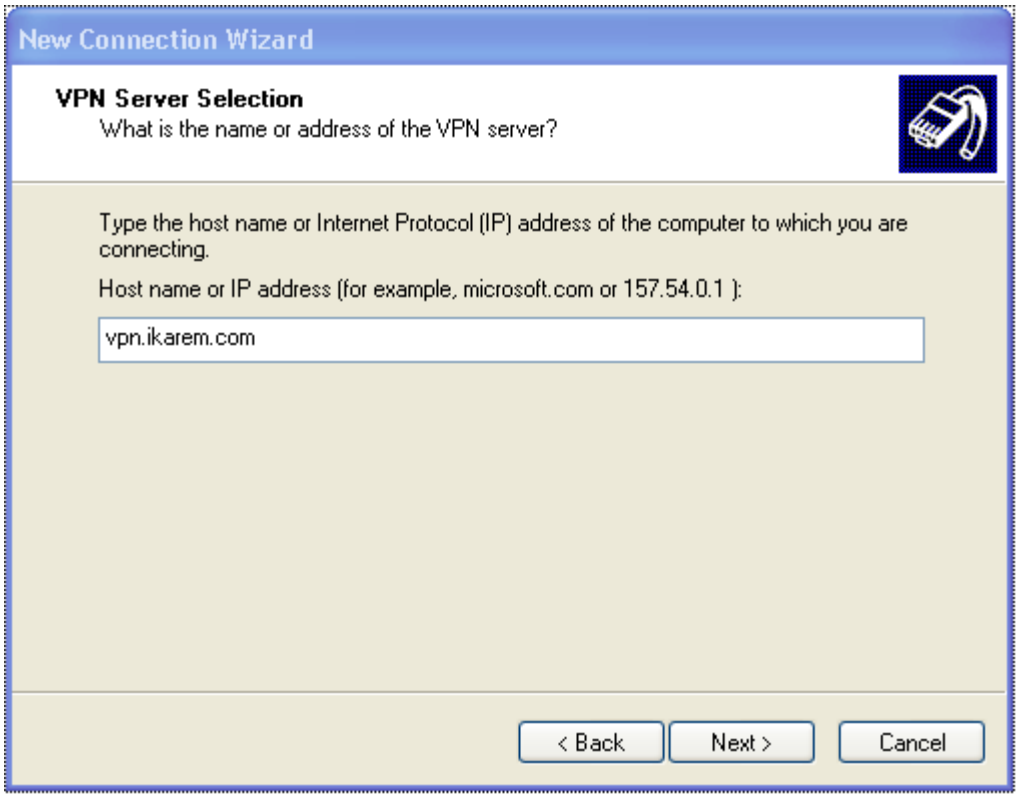


Choose **Virtual Private Network connection** in the next section.

Then, give a name for this connection. This can be anything you want to name this connection, for example, "Work VPN."

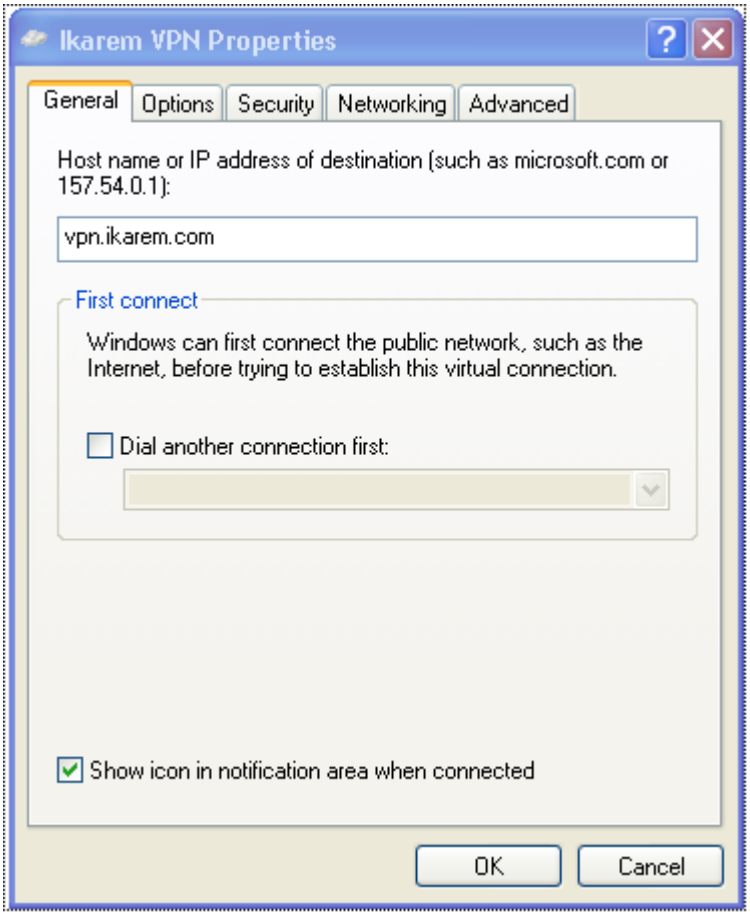


Enter the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.

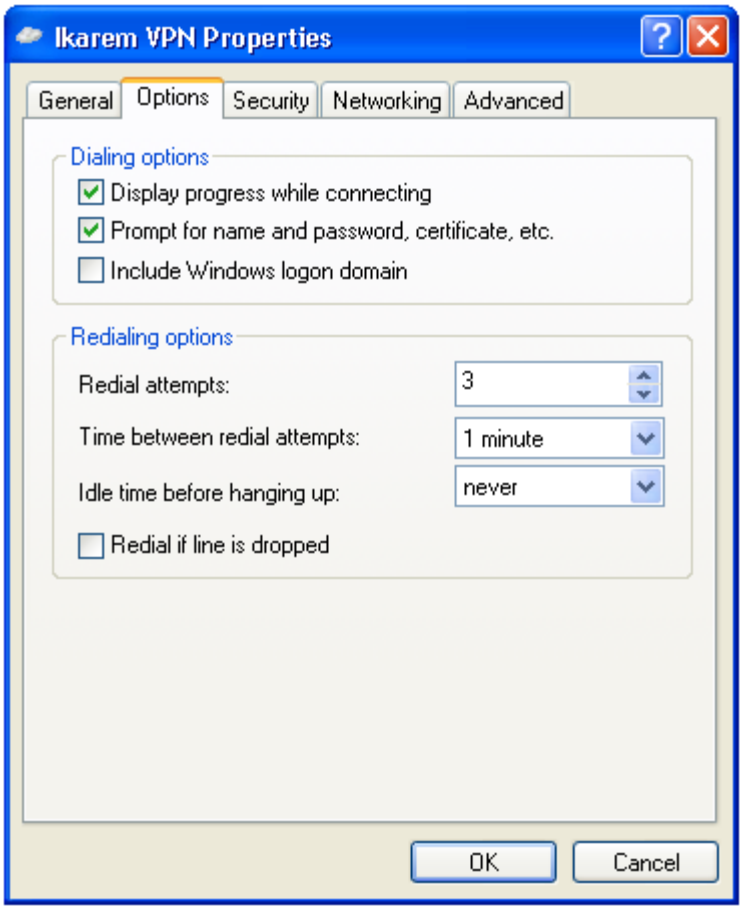


In the **Connect <Connection Name>** box, click on **Properties**

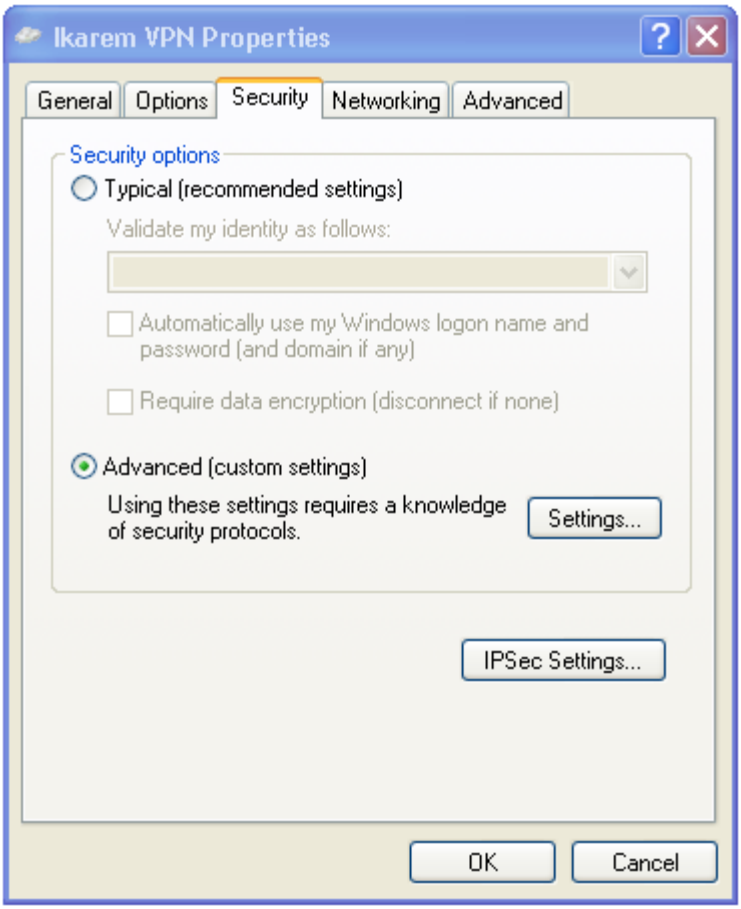
In the **General** tab, verify the **hostname** (e.g. .com) or the **active WAN IP** (e.g. XXX.XXX.XXX)**.** Hostname is encouraged instead of active WAN IP because it is more reliable in cases of WAN failover. Admin can find them in Dashboard, under Security appliance > Monitor > Appliance status.



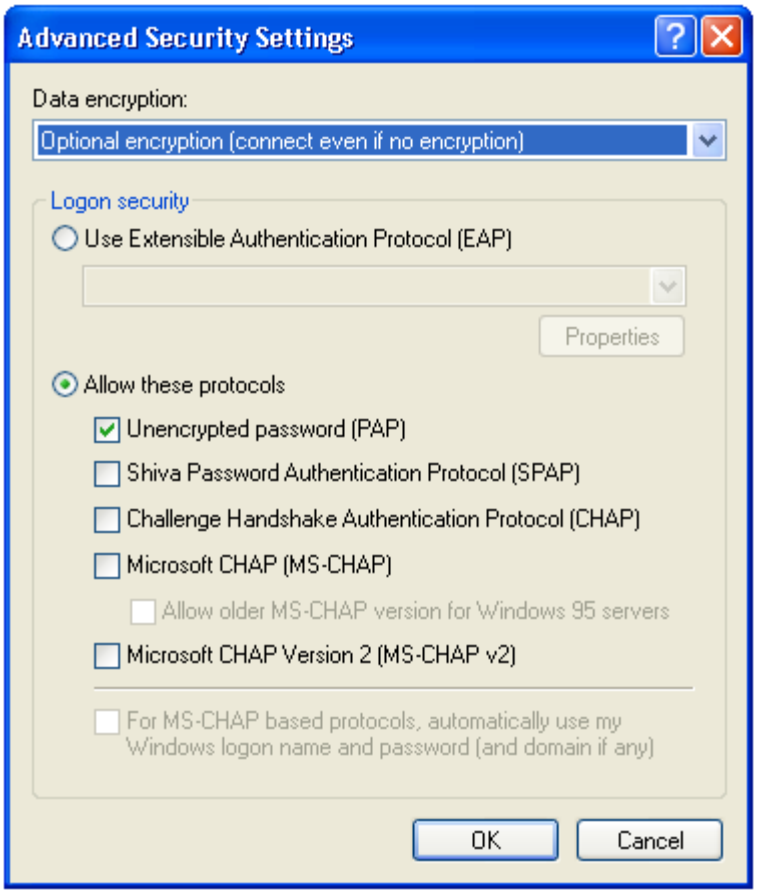
In the **Options** tab, uncheck "**Include Windows logon domain**"



In the **Security** tab, choose **Advanced (custom settings)**.
Click **Settings**

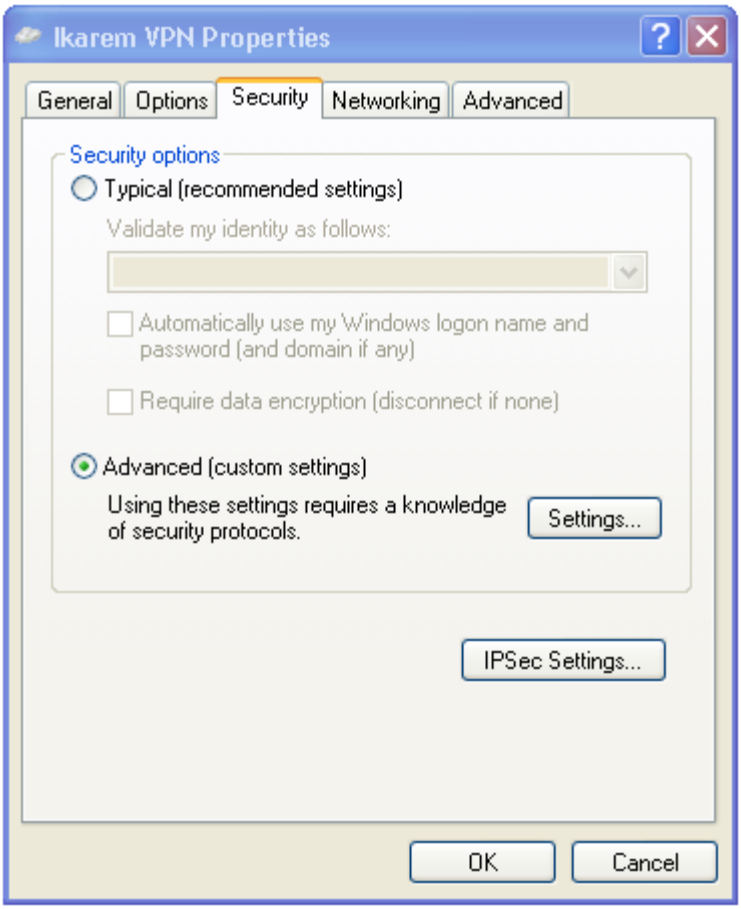


In **Advanced Security Settings** page, select **Optional encryption**from the **Data encryption** pull-down menu. Choose **Unencrypted password (PAP)** from the **Allow these protocols** options and uncheck everything else.

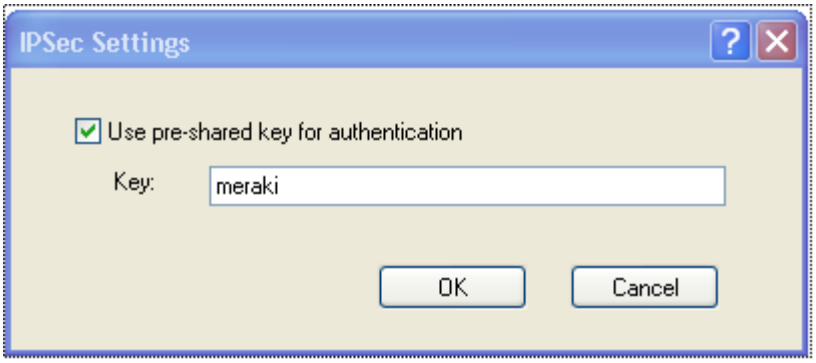


Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.

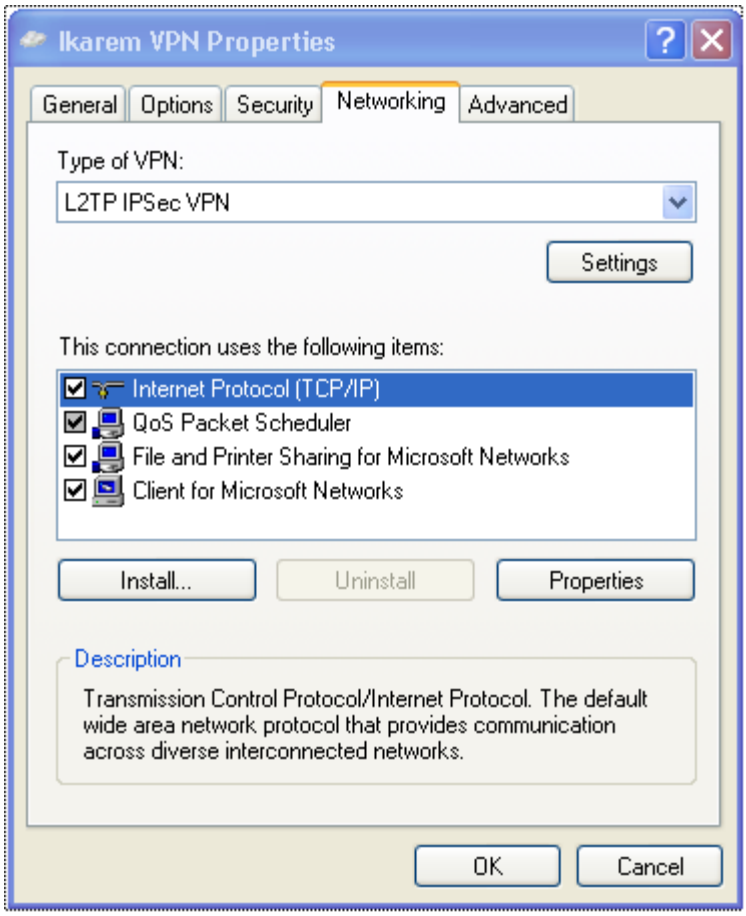
Back on the **Security** tab, click **IPSec Settings...**



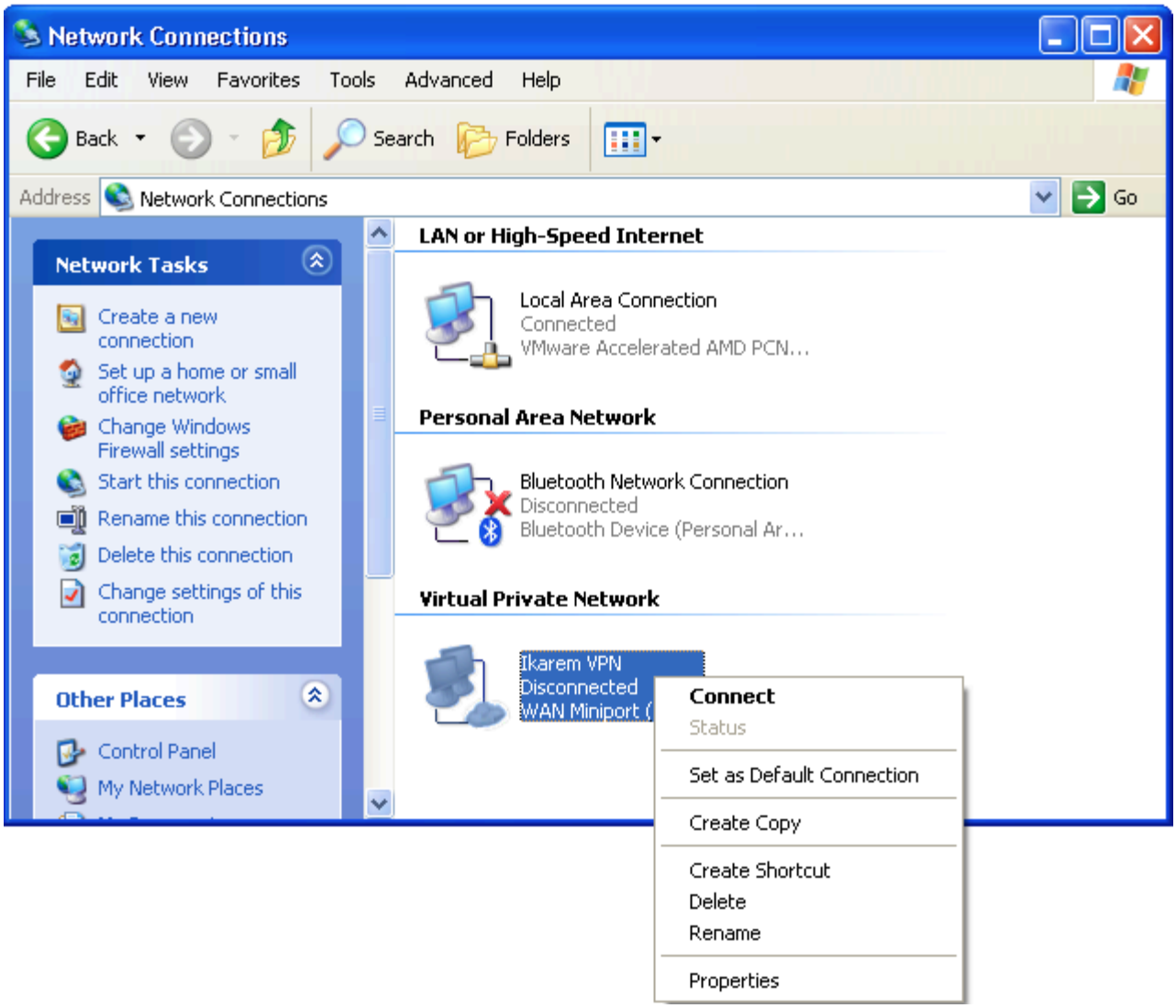
Check "**Use pre-shared key for authentication**" and enter the pre-shared key that admin created in Security appliance > Configure > Client VPN settings.
Click OK.



In **Networking** tab, choose **L2TP IPSec VPN** from the **Type of VPN** options.



Back at the **Network Connections** window, right-click on the **VPN connection** and click **Connect**



Verify your user name and click **Connect**


Connect Ikarem VPN
User name:
niles@meraki.com
Password:
[To change the saved password, click here]
Save this user name and password for the following users:
Me only
Anyone who uses this computer
Connect
Cancel
Properties
Help