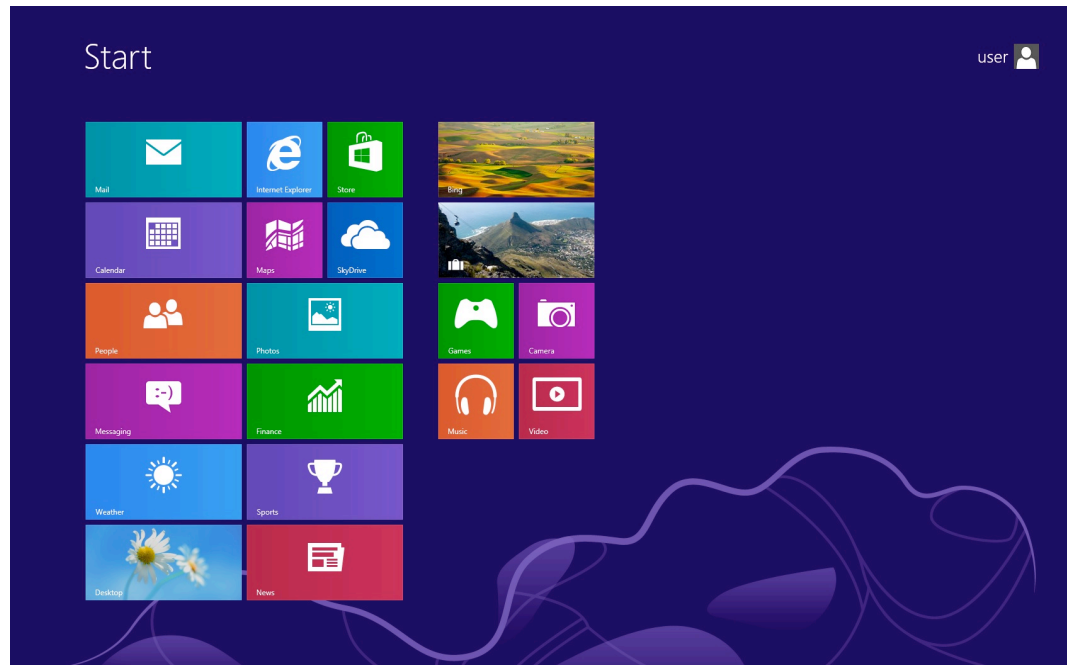
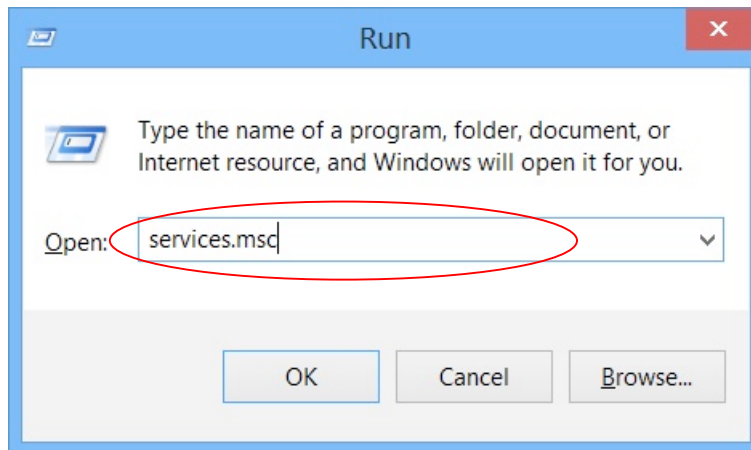


802.1x Configuration Guide for Windows 8

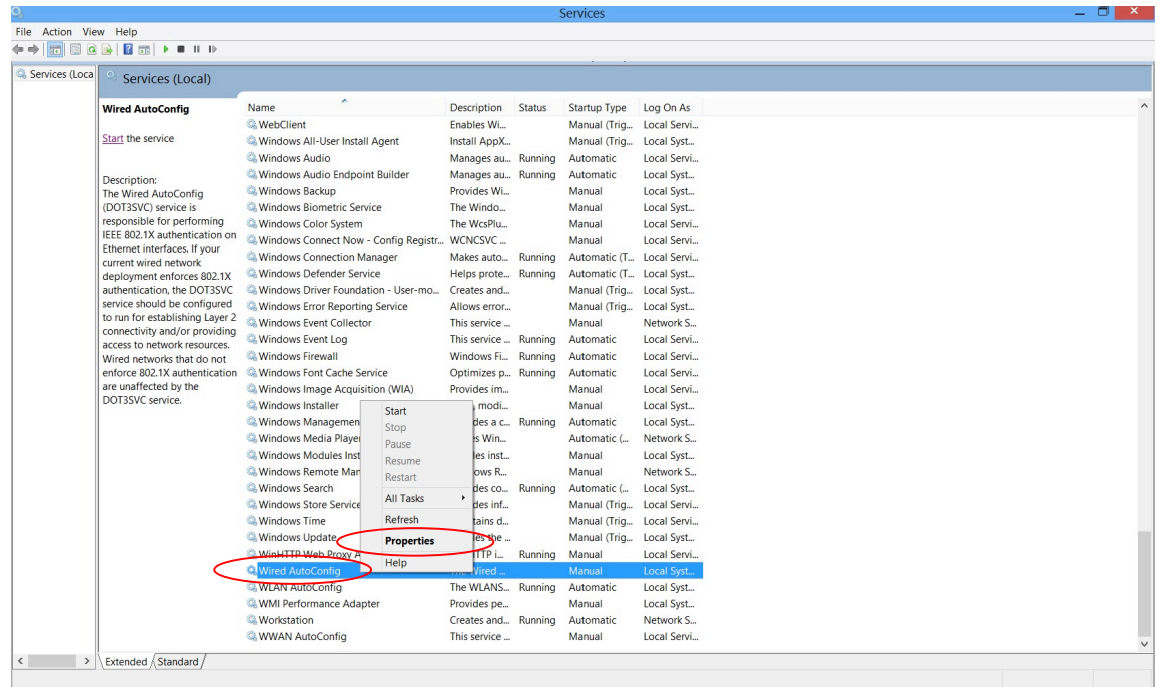
1. Press **Window-key** button  on keyboard to gain access to traditional desktop.



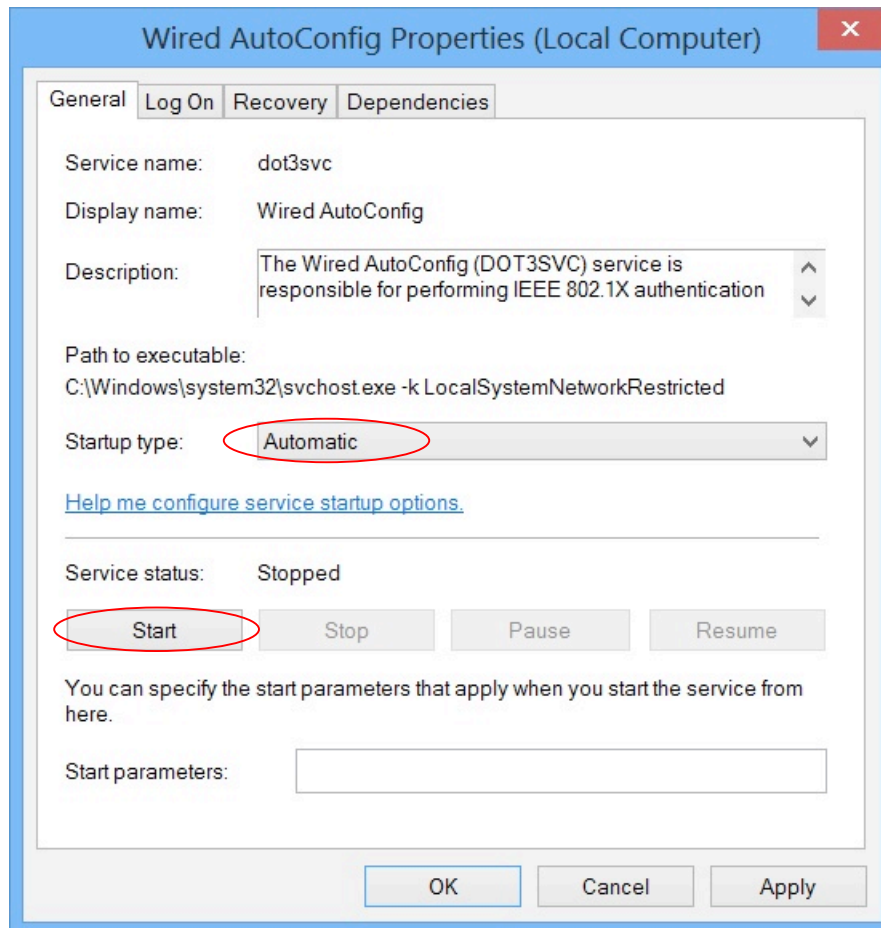
2. Hold **Window-key** button and press **R**, type **services.msc** and then click **OK**.



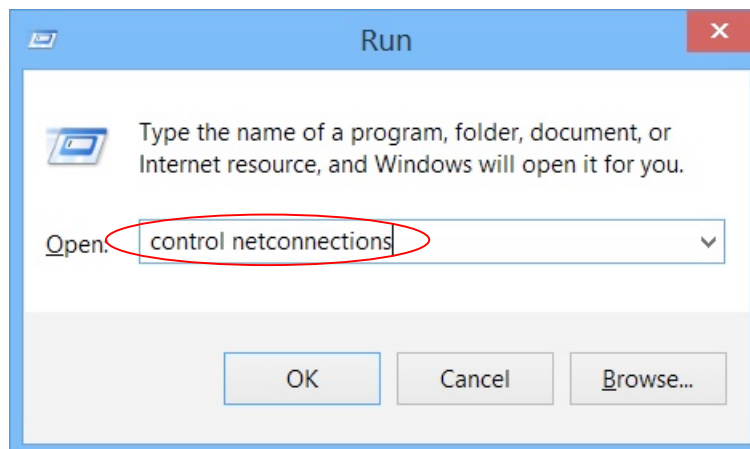
3. Right click on **Wired AutoConfig**. Choose **Properties** from the pop up menu.



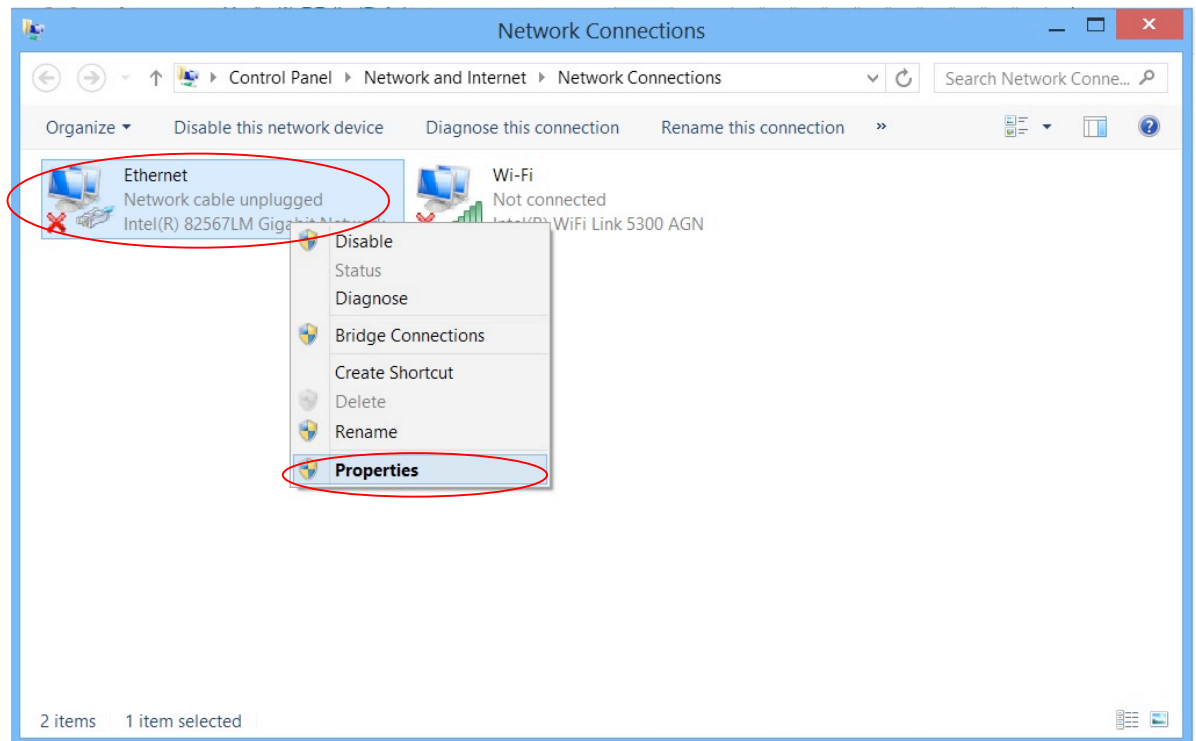
4. Change **Startup type** to **Automatic** and click **Start**. Follow by clicking **OK**



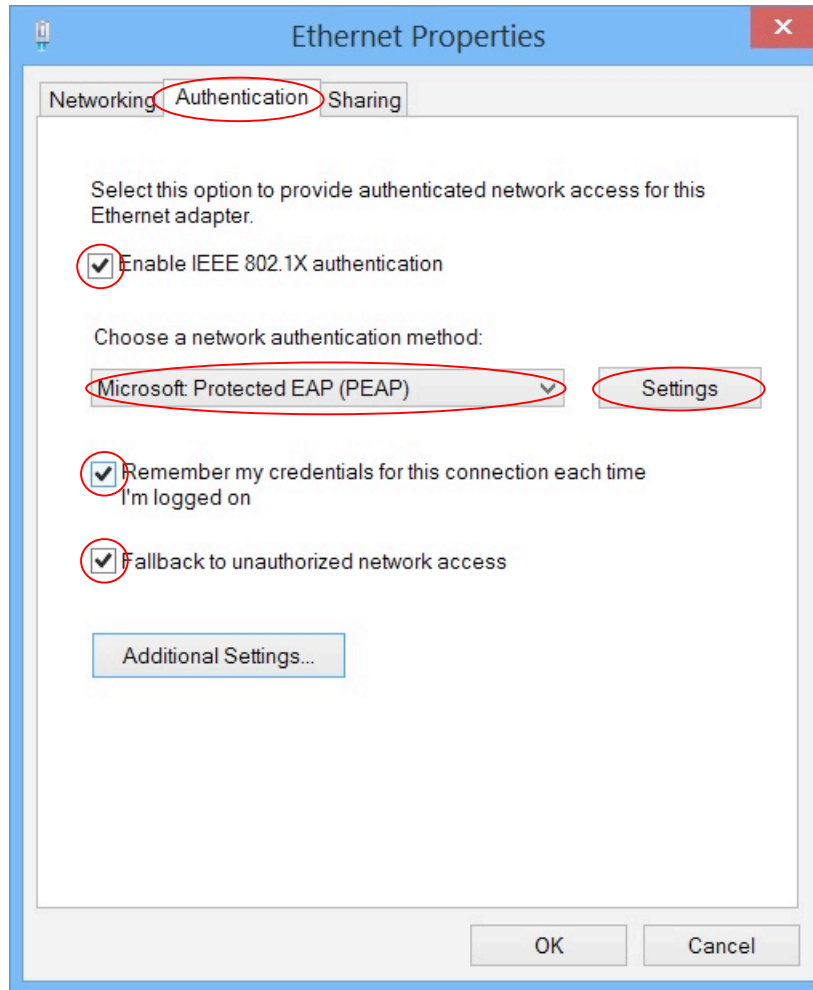
5. Hold **Window-key** button and press **R**, Type **control netconnections** and click **OK**.



6. Right click on **Local Area Connection (Ethernet)**. Choose **Properties** from the pop up menu.



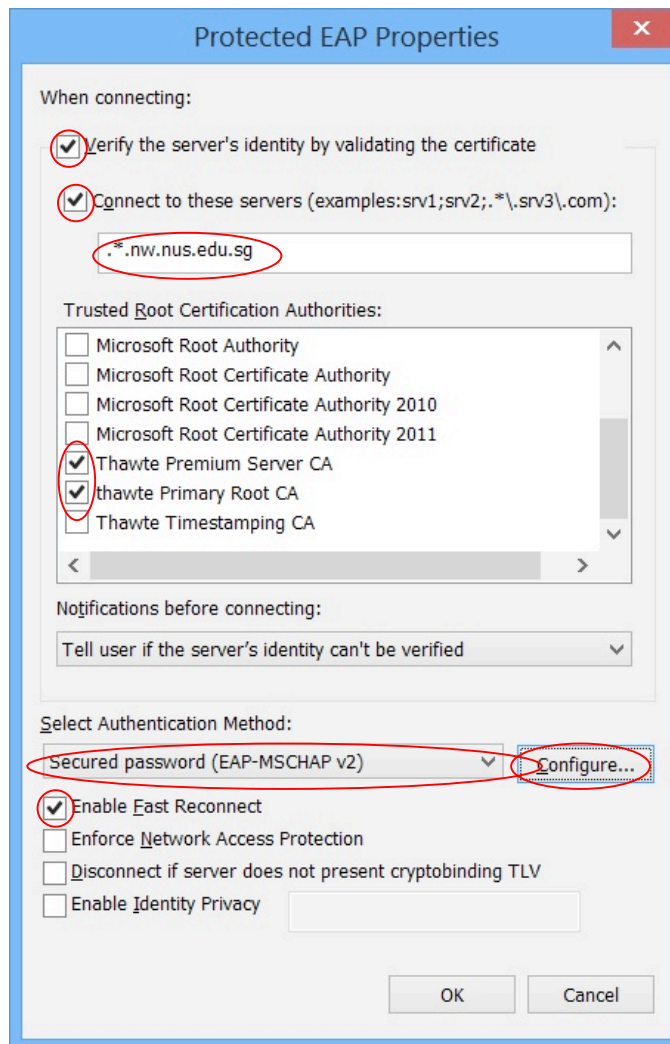
7. Click on **Authentication** tab. Check **Enable IEEE 802.1X authentication**. Check *“Remember my credentials for this connection each time I’m logged on”*. Check *Fallback to unauthorized network access*. Choose **Microsoft Protected EAP (PEAP)** as network authentication method. Then click on **Settings**.



8. Check option “*Verify the server’s identity by validating the certificate*” and “*Connect to these servers*”. Enter **.*.nw.nus.edu.sg** at the field box. Check **Thawte Premium Server CA** and **thawte Primary Root CA**. Check “*Enable Fast Reconnect*”.

Uncheck option “*Enforce Network Access Protection*”, “*Disconnect if server does not present cryptobinding TLV*” & “*Enable Identity Privacy*”

Choose **Secured password (EAP-MSCHAP v2)** as Authentication Method. Then click **Configure**.



The image shows the "Protected EAP Properties" dialog box. It has a blue title bar with a close button. The main area is divided into several sections. The "When connecting:" section has two checked checkboxes: "Verify the server's identity by validating the certificate" and "Connect to these servers (examples: srv1; srv2; *.srv3\,com):". Below the second checkbox is a text box containing ".*.nw.nus.edu.sg". The "Trusted Root Certification Authorities:" section is a list box with several entries, including "Thawte Premium Server CA" and "thawte Primary Root CA", both of which are checked. Below this is a "Notifications before connecting:" section with a dropdown menu set to "Tell user if the server's identity can't be verified". The "Select Authentication Method:" section has a dropdown menu set to "Secured password (EAP-MSCHAP v2)" and a "Configure..." button. Below this are four checkboxes: "Enable Fast Reconnect" (checked), "Enforce Network Access Protection" (unchecked), "Disconnect if server does not present cryptobinding TLV" (unchecked), and "Enable Identity Privacy" (unchecked). At the bottom are "OK" and "Cancel" buttons.

Protected EAP Properties

When connecting:

- ☒ Verify the server's identity by validating the certificate
- ☒ Connect to these servers (examples: srv1; srv2; *.srv3\,com):
.*.nw.nus.edu.sg

Trusted Root Certification Authorities:

- ☐ Microsoft Root Authority
- ☐ Microsoft Root Certificate Authority
- ☐ Microsoft Root Certificate Authority 2010
- ☐ Microsoft Root Certificate Authority 2011
- ☒ Thawte Premium Server CA
- ☒ thawte Primary Root CA
- ☐ Thawte Timestamping CA

Notifications before connecting:

Tell user if the server's identity can't be verified

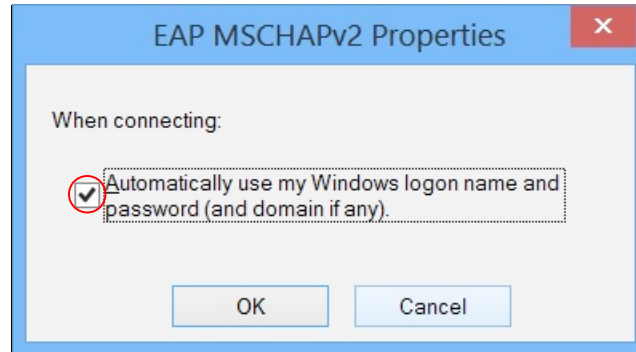
Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

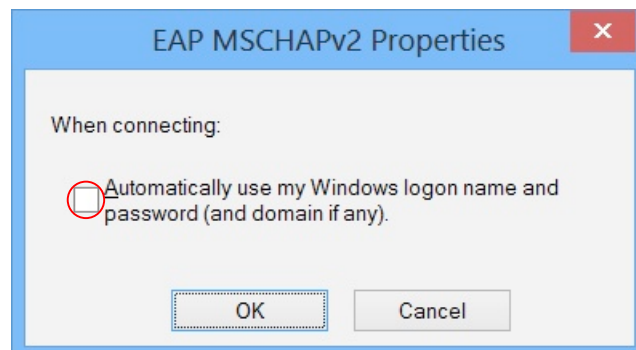
- ☒ Enable Fast Reconnect
- ☐ Enforce Network Access Protection
- ☐ Disconnect if server does not present cryptobinding TLV
- ☐ Enable Identity Privacy

OK Cancel

9. If this is a Domain Computer, check option “*Automatically use my Windows logon name and password (and domain if any)*”.

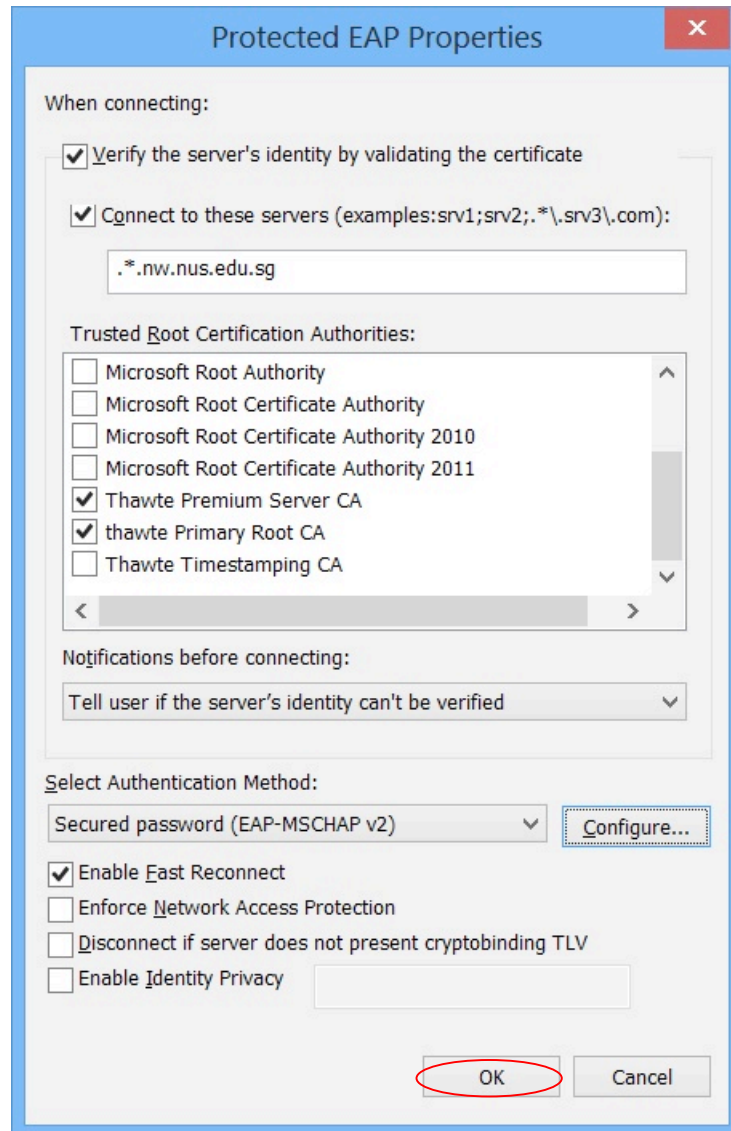


Or else uncheck option.



Then click **OK**.

10. Upon returning to the “*Protected EAP Properties*” menu, click **OK**.

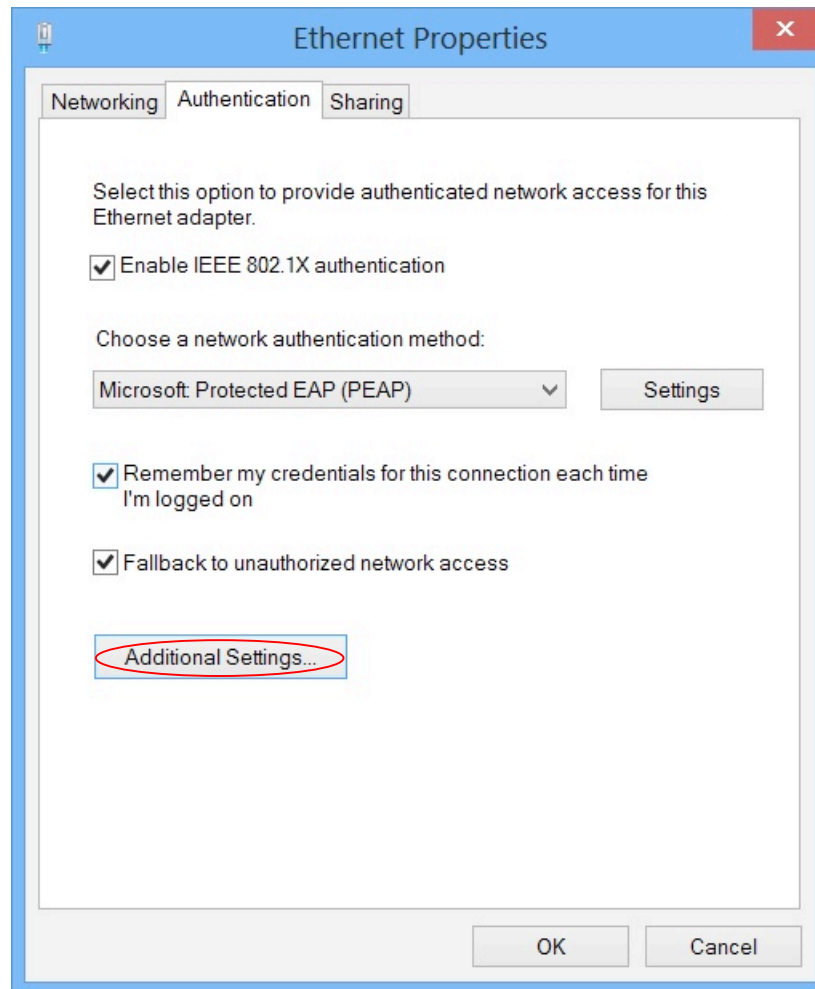


The image shows the "Protected EAP Properties" dialog box. It has a blue title bar with a close button (X) in the top right corner. The main content area is white and contains several sections:

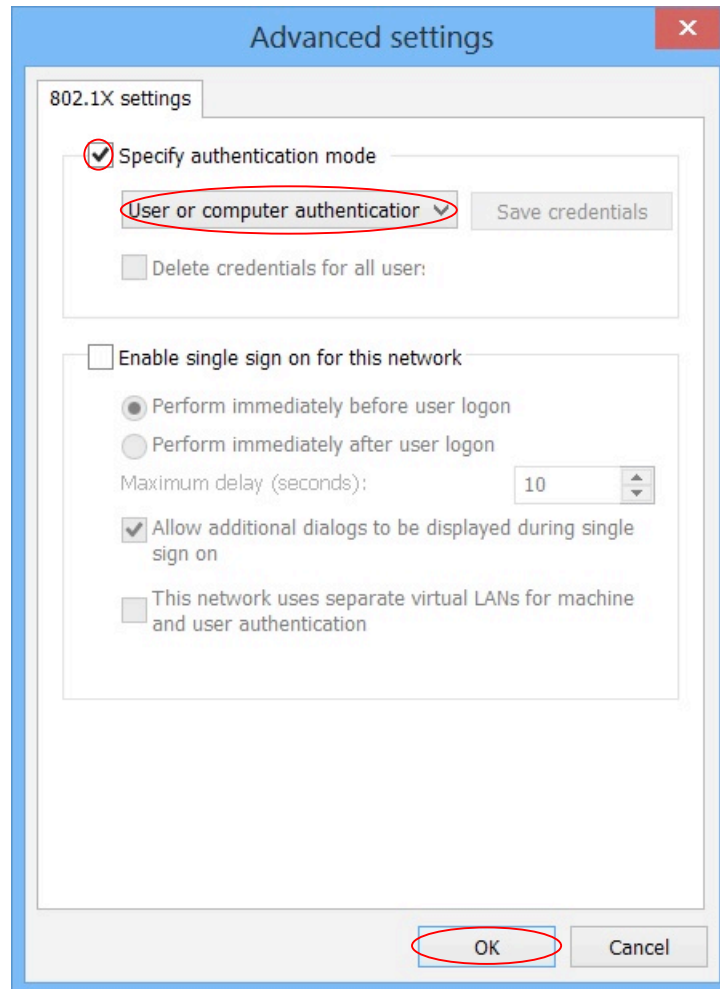
- When connecting:**
 - ☒ **Verify the server's identity by validating the certificate**
 - ☒ **Connect to these servers (examples: srv1; srv2; *.srv3.com):**
Below this is a text box containing the text: `.*.nw.nus.edu.sg`
 - Trusted Root Certification Authorities:**
A list box containing the following items:
 - ☐ Microsoft Root Authority
 - ☐ Microsoft Root Certificate Authority
 - ☐ Microsoft Root Certificate Authority 2010
 - ☐ Microsoft Root Certificate Authority 2011
 - ☒ Thawte Premium Server CA
 - ☒ thawte Primary Root CA
 - ☐ Thawte Timestamping CA
- Notifications before connecting:**
A dropdown menu showing "Tell user if the server's identity can't be verified".
- Select Authentication Method:**
A dropdown menu showing "Secured password (EAP-MSCHAP v2)". To the right of this dropdown is a "Configure..." button.
- Below the authentication method, there are four checkboxes:
 - ☒ **Enable Fast Reconnect**
 - ☐ **Enforce Network Access Protection**
 - ☐ **Disconnect if server does not present cryptobinding TLV**
 - ☐ **Enable Identity Privacy**

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel". The "OK" button is circled in red.

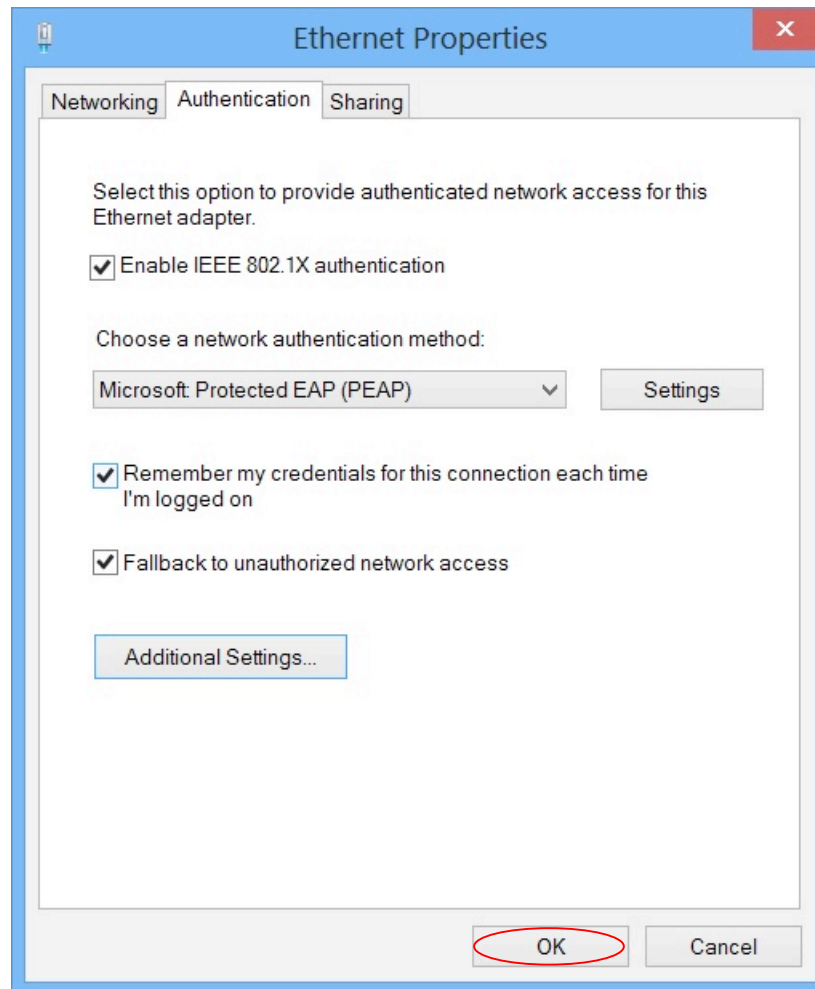
11. Click on **Additional Settings**.



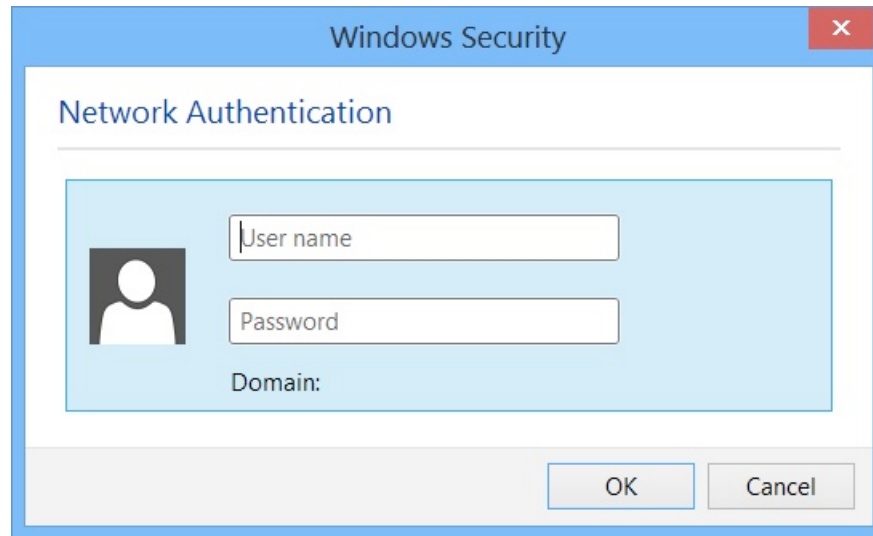
12. Check **Specify authentication mode**, Select **User or computer authentication** from the drop down menu and then click **OK**.



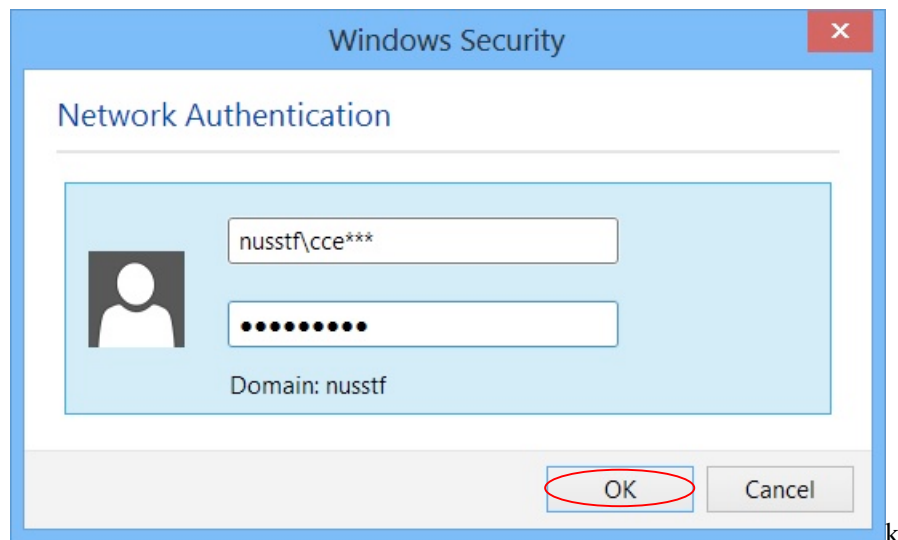
13. Click **OK**.



14. Once connected to the wired port, you will be able to get Network Authentication window.



15. Enter Username and Password and then click on **OK**.
- **Username** : (Enter your “Domain\Username”)
(E.g. of Domain: NUSSTF/NUSSTU/NUSEXT)
 - **Password** : (Enter your Password)



16. Upon authentication, user will be successfully connected to the NUS network.

