THE UNIVERSITY of NEW ORLEANS

"A member of the University of Louisiana System"

ResNet Connection for Windows 8

GENERAL NOTE:

ResNet is provided as a resource for UNO students to access University and Internet based services. As such, the network must be secured to prevent unauthorized usage. The instructions located in this document will guide you in configuring your system to use industry-standard authentication services to access the network.

After your computer system is set up to use the authentication services, Windows 7 will retain your UNO Account credentials and your system will automatically reconnect to the network every time you plug into the network and power up your computer.

This will remain in effect as long as your UNO account is active or until your password changes, at which time you will have to login with the new password.

IMPORTANT CONSIDERATION:

Since your computer will connect using your UNO account credentials, on campus only, anyone borrowing your system will be identified as you.

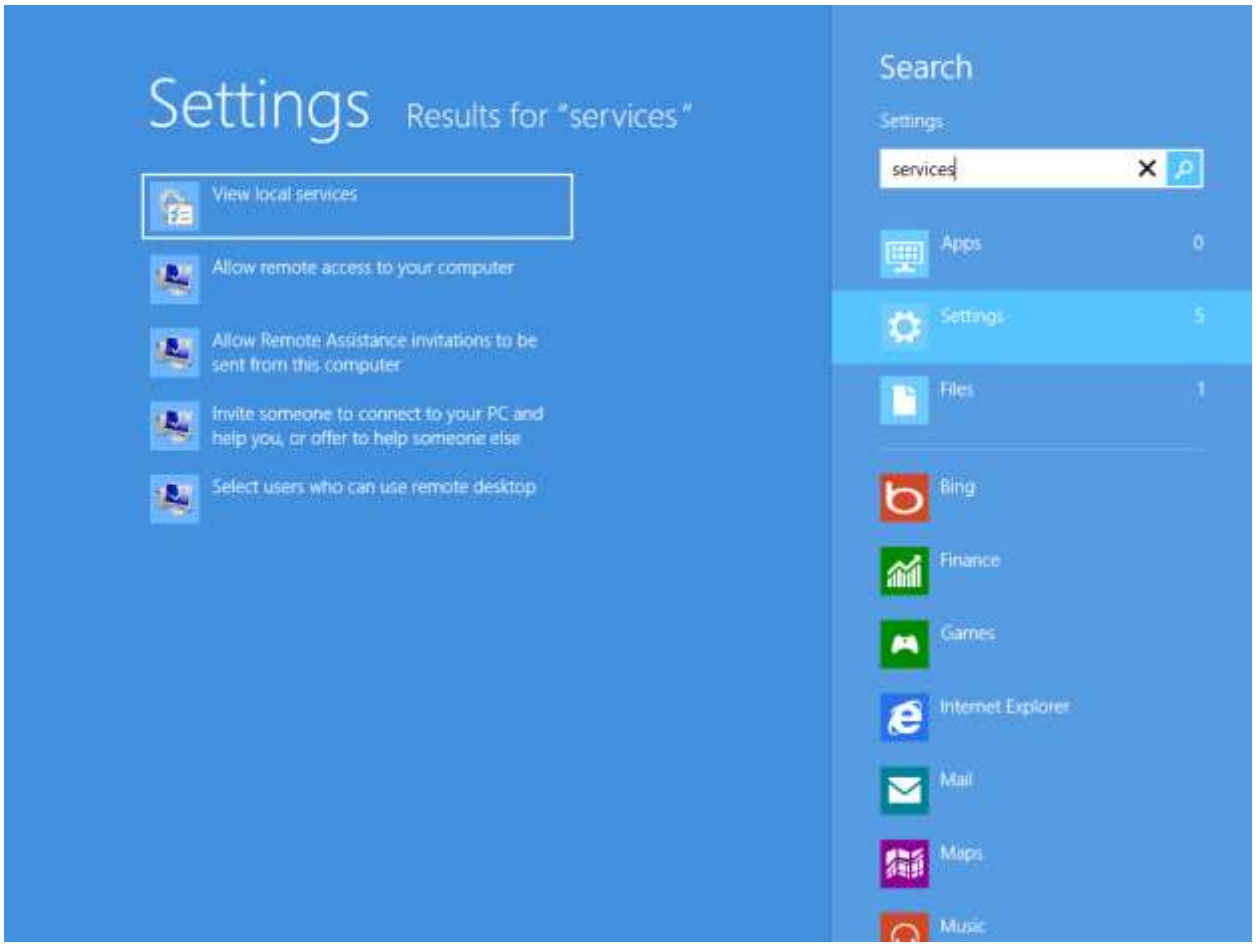
Please note that you are responsible for following all University policies regarding the use of:

- Your personal UNO accounts,
- The UNO network,
- Internet usage, and
- Any other University computer systems that your UNO account may have access to on the campus network.

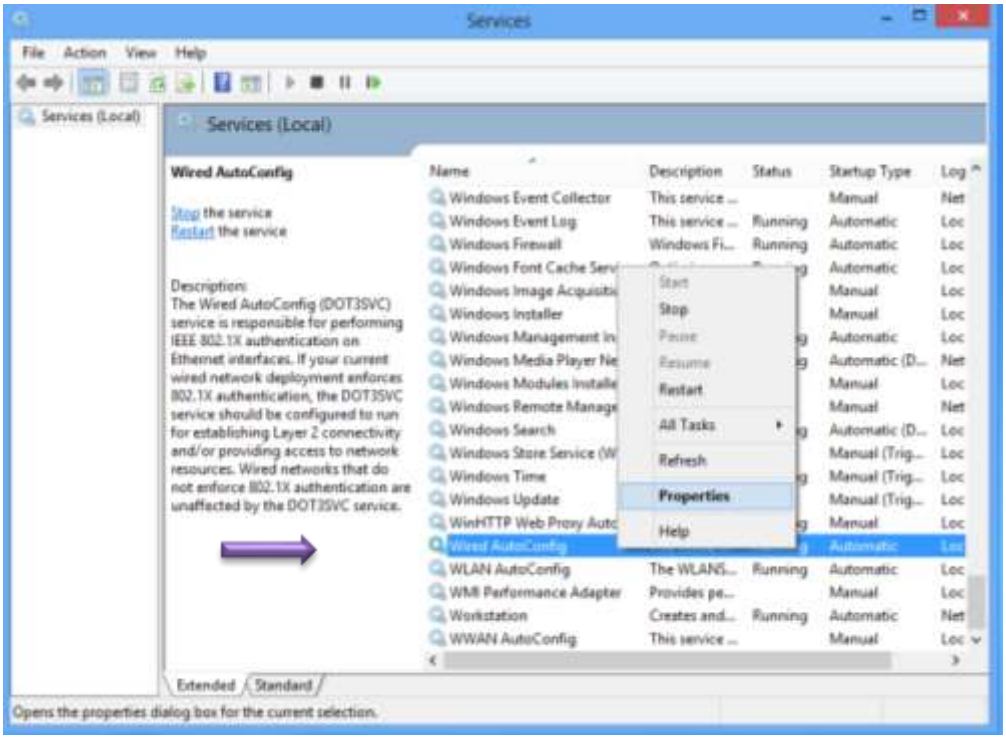
Please consider carefully as you are responsible for all actions taken by your personal login account.

The following instructions are for Windows 8 users. If your computer uses any other operating system, please refer to the other documentation on the UCC page. If you need help call the UCC Help Desk at (504) 280-4357.

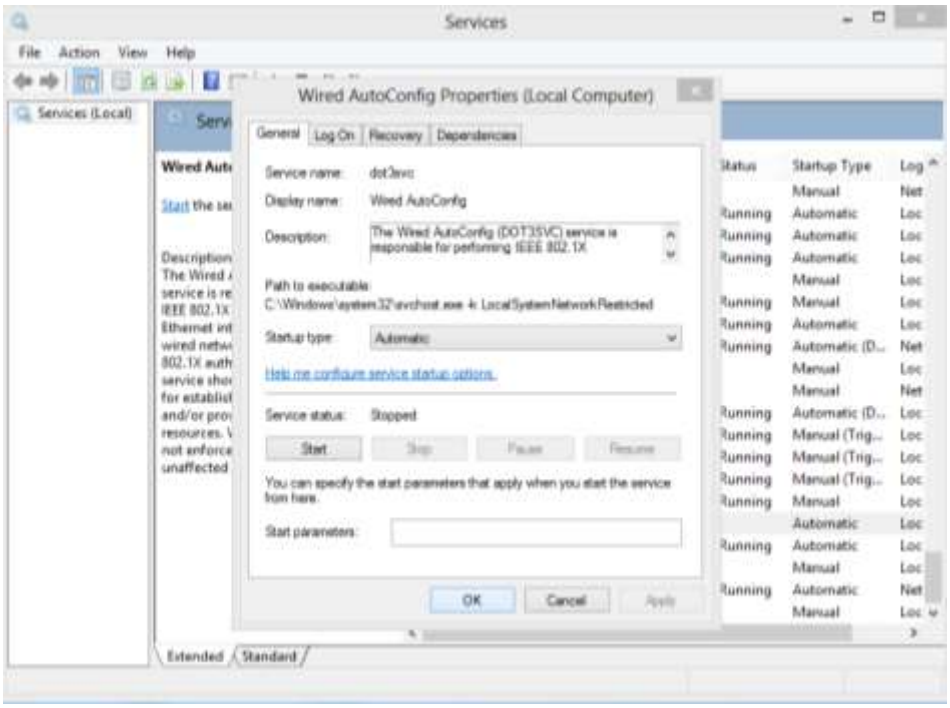
1. At the Windows App Home screen, type **Services**. Windows will automatically start searching for anything named **Services** on the computer.
2. Under the search bar, make sure to select **Settings**.
3. Then on the left hand side of the screen, click on **View Local Services**.



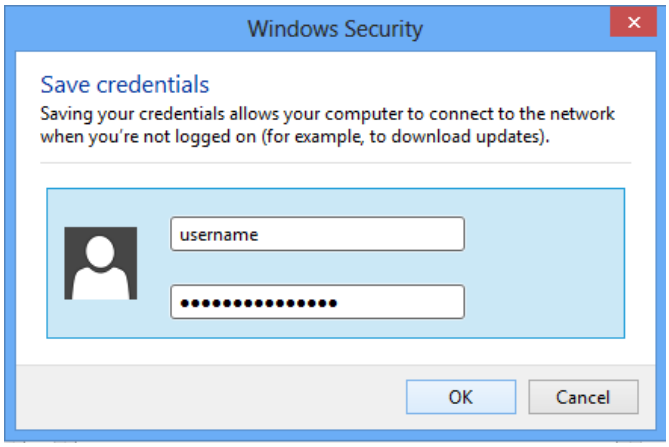
4. Now the **Services** window will open. Scroll down to the bottom of the list of services provided and locate **Wired Autoconfig.** Then, right click on it and select **Properties.**



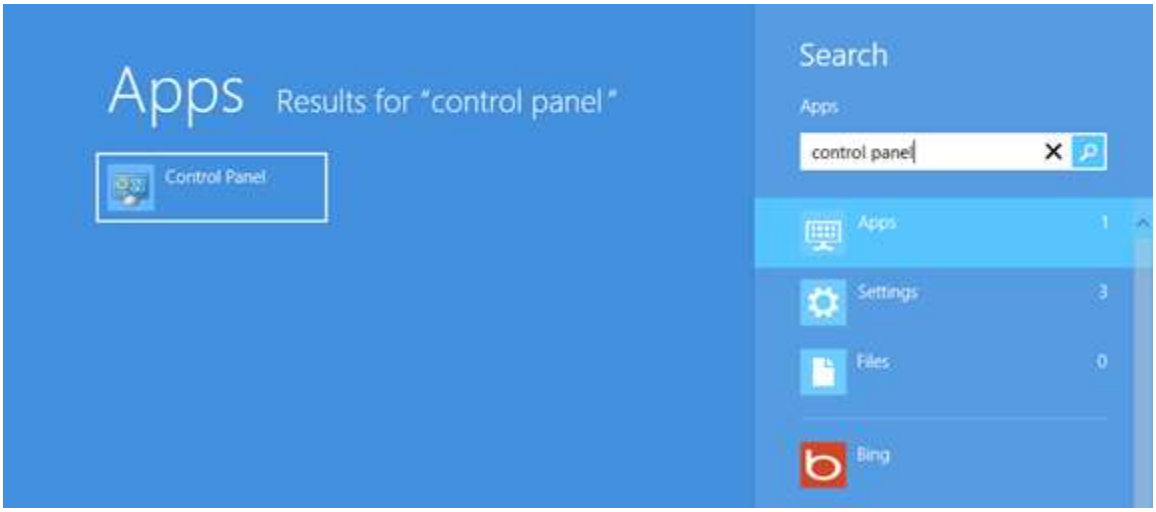
5. A Wired AutoConfig Properties window will appear. For **Startup type** select **Automatic.** Click the **Start** button. A new box with a progress bar will appear. It will automatically go away when the task is finished. Once it is finished, click **OK** to close out the window.



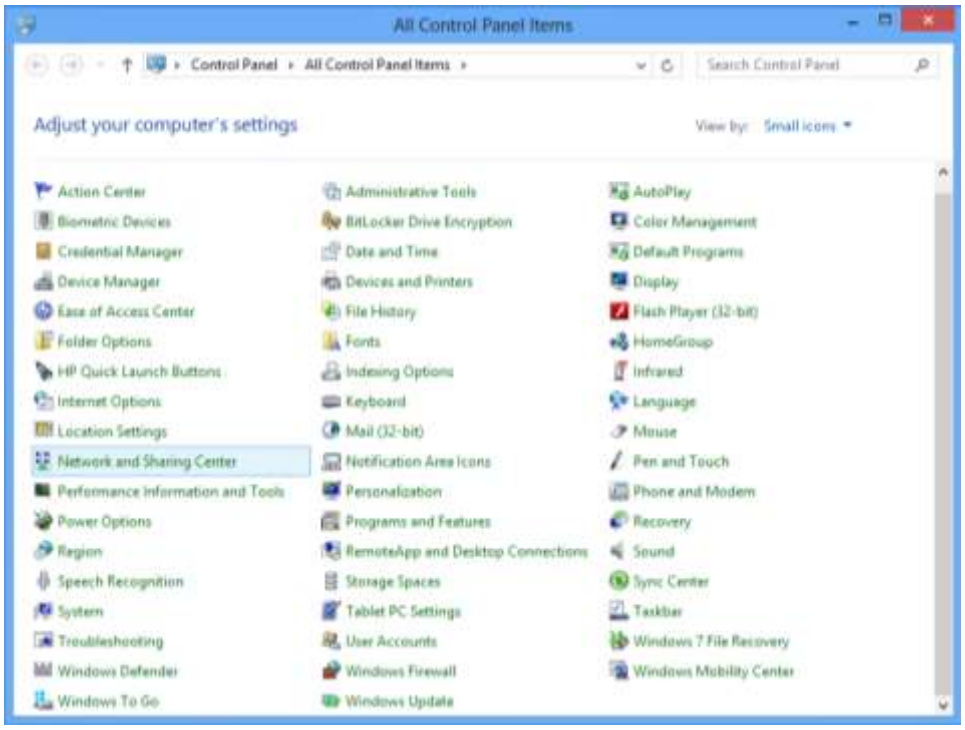
If a **Network Security Alert** appears like the one below, skip to step 17.



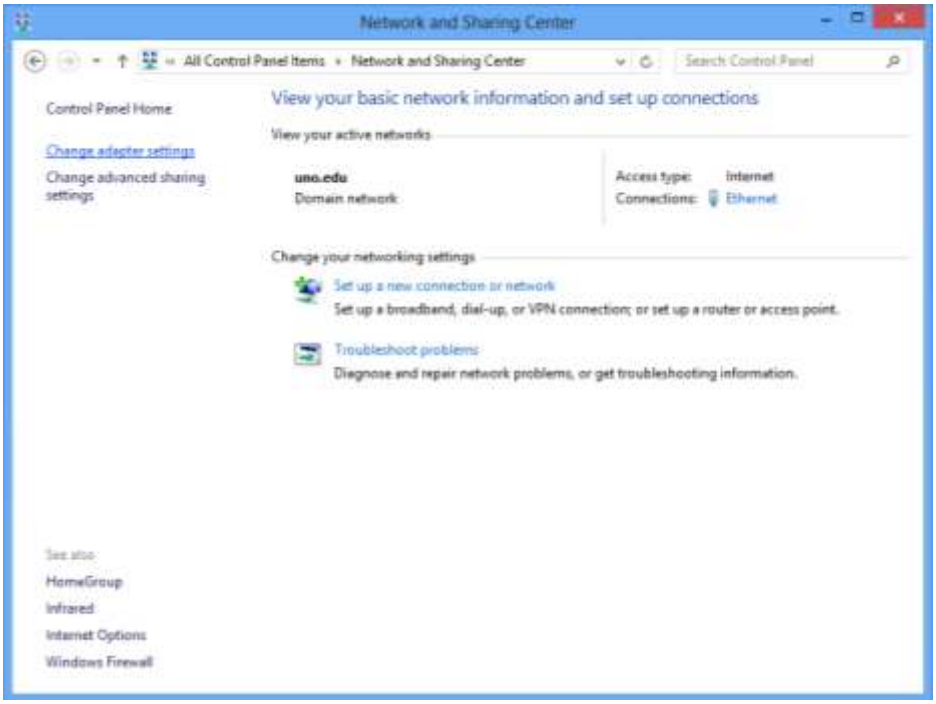
6. Click the **Windows Key** to return to the app home screen. From there, type **Control Panel** and click the option on the left of the page.



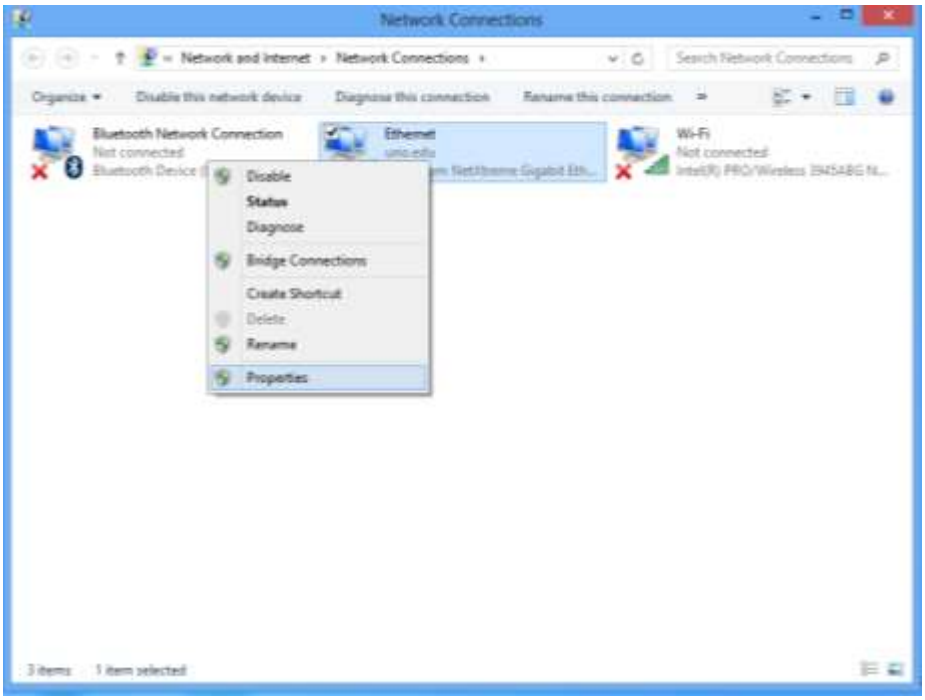
7. Inside the Control Panel, change the **View by:** setting to **Small icons.** Then, click on **Network and Sharing Center.**



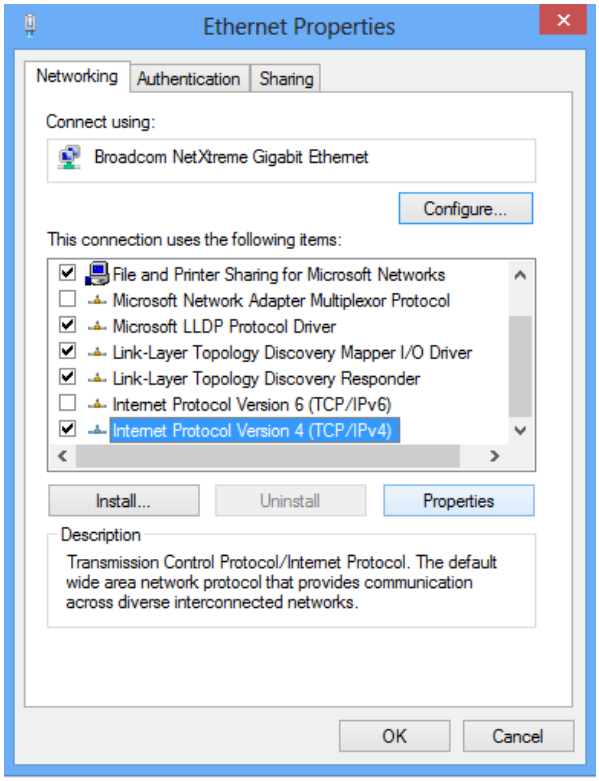
8. The Network and Sharing Center window will now appear. Click the **Change adapter settings** option located in the left column of the window.



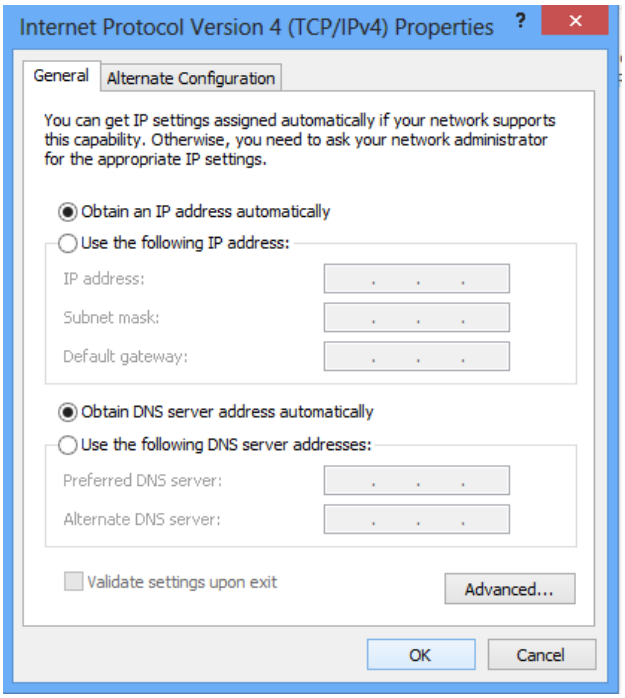
9. Right click the **Ethernet** icon and click **Properties**.



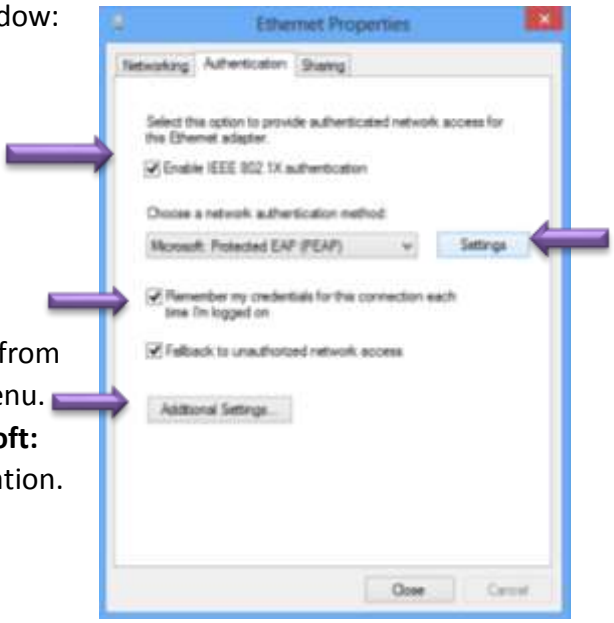
10. In the **Ethernet** window:
    a. Be sure that **Internet Protocol Version 6 (TCP/IPv6)** is **NOT** selected. If it is, then uncheck this selection box.
    b. Click **Internet Protocol Version 4 (TCP/IPv6)** and then click the **Properties** button.



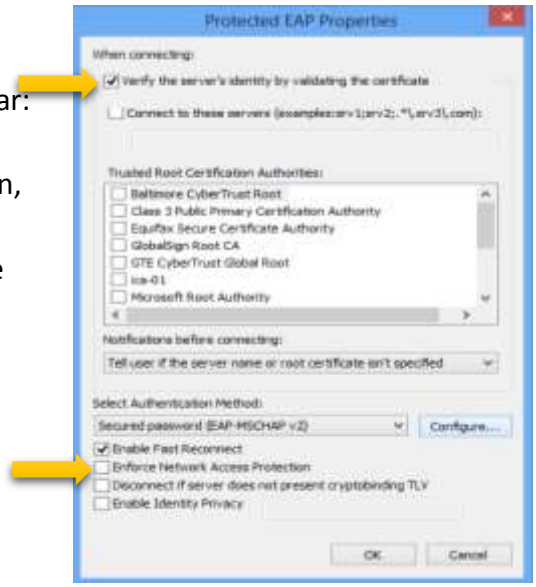
11. Verify the following are selected:
    a. **Obtain an IP address automatically**
    b. **Obtain DNS server address automatically**
    c. Click **OK** to close this window.



12. You will return to the **Ethernet Properties** window:
    a. Click the **Authentication** tab.
    b. Make sure the **Enable IEEE 802.1X authentication** box is checked.
    c. Select **Remember my credentials for this connection each time I'm logged on.**
    d. Select **Fallback to unauthorized network access.**
    e. Choose **Microsoft: Protected EAP (PEAP)** from the authentication methods pull down menu.
    f. Next, click the **Settings** button for **Microsoft: Protected EAP (PEAP)** network authentication.

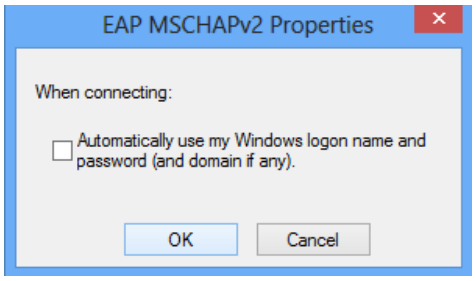


13. The **Protected EAP Properties** window will appear:
    a. Check **Validate server certificate**
    b. In the **Select Authentication Method** section, use the pull down menu to choose **Secured password (EAP-MSCHAP v2)**. Then, click the **Configure** button.

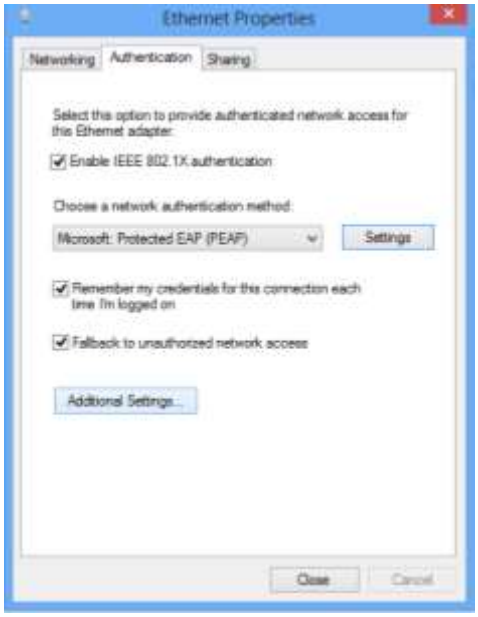


14. The **EAP MSCHAPv2 Properties** window will appear:
    a. Make sure the **Automatically use my Windows logon name and password (and domain if any)** box is **NOT** checked. Then click **OK**.

b. You will return to the **Protected EAP Properties** window. Click **OK** to return to the **Ethernet Properties** dialogue box.

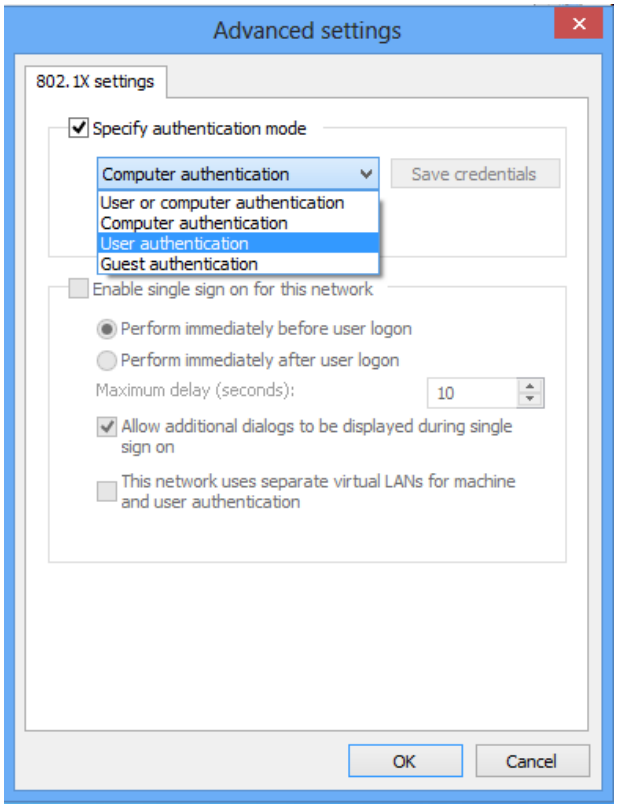


15. Next, click the **Additional Settings** button to get to the Advance Settings.



16. Next, select the following **Advanced Settings** settings:
    a. Select **Specify authentication mode**
    b. Under this setting, choose **User authentication** from the drop down menu.
    c. To complete this setup, select **Save credentials**.

A window will now open (**Windows Security**) that will allow you to put in your UNO account login information.

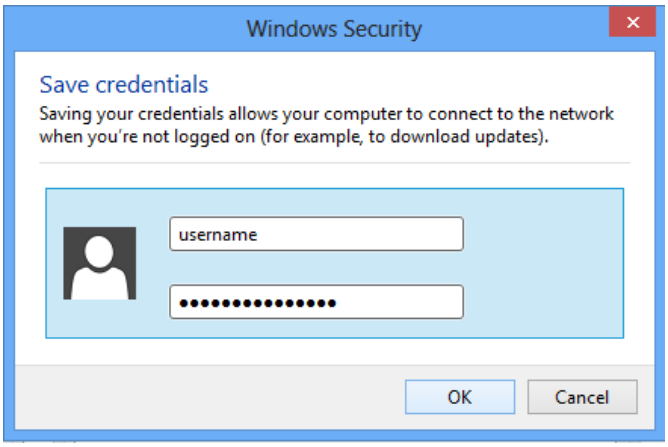


17. Enter your **UNO username** and **password** here – click **OK.**

    Your credentials will be saved here, allowing you to directly connect in the future without having to retype this information every time you connect to the UNO network.

    The only exception will be when your password expires or if you mistyped your password. If this occurs, you will get a login window asking you to input the correct or update credentials when connecting to the network.

    a. At this point, you can close the **Advanced Settings** window by selecting **OK.**
    b. Close the **Ethernet Properties** by selecting **OK**.



18. Then a **Network Security Alert** window will appear. Click **Connect** and you should now be connected and ready to use the network.

ResNet Copyright Infringement Policy:

In accordance with federal legislation, specifically the Digital Millennium Copyright Act of 1998, ResNet Internet Service will undertake very specific action when formal notifications of copyright infringement by ResNet users have been received from copyright holders or their representatives. The ResNet Support Group will certify that positive contact with the user has taken place and that the user has either ceased the infringing activity or that ResNet Support has taken action on its own with the result of ceasing the infringing activity when the activity originates from within the ResNet network.

In response to this legislation, the ResNet Support Group has developed the following procedures. Compliance with applicable law is the ultimate goal. Much of the activity occurring in violation of copyright laws is the result of peer-to-peer file sharing software usage by users who are, as often as not, unaware that certain uses of this software violates copyright laws. Consequently, user education is a necessary component of required compliance efforts. ResNet staff will maintain sufficiently detailed records reflecting infringement notices received and responses thereto. The following are the procedural steps to be taken in response to formal notifications of copyright infringement:

1. University Computing & Communications receives notice that a user may be violating copyright laws. 2. Upon determination that the user is connected to ResNet based on the IP address given in the complaint, the complaint is routed to the ResNet Support Group. 3. ResNet staff will search records and determine the identity of the user. 4. ResNet staff will search records to determine whether the user is a repeat offender. If it is clear that the user is a repeat offender, the complaint will be handled as described under "Repeat Offenders" below. If this complaint is a first offense, the "First Offense" procedure will be followed.

First Offense

1. ResNet Support will immediately suspend network service. 2. ResNet Support issues an e-mail notice to the user explaining the reason for suspension. The infringement notice will be included as an enclosure to the e-mail notice. 3. ResNet Support will reactivate service after contacting the ResNet user.

Repeat Offenders

1. ResNet Support will immediately terminate network service. 2. ResNet Support will send an e-mail notice to the user explaining that a second or subsequent complaint of infringing activity has been received and that the user's network service has been terminated. 3. ResNet Support will notify the University Office of Judicial & Student Assistance that a second offence has occurred and will forward all pertinent information for review.

Failure to adhere to UNO Acceptable Use Policies may result in loss of privileges as well as disciplinary or legal action.

If you encounter any trouble, feel free to contact the Help Desk at (504) 280-4357 or by email at helpdesk@uno.edu. You may also stop by the Help Desk, located in the UCC Room 101.