

Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

Preface:

The ISU-OIT-WPA implementation supports either WPA with TKIP or WPA2 with AES. Both support the enterprise DOT1X & CCKM Authentication Key Management features as well. This document is designed to walk a user through setting up a Windows Vista machine using Windows to Manage the Wireless adapter using WPA2 with AES. There are references within the document on how WPA with TKIP would be used. If a program other than Windows is managing the wireless connection, the images and directions will be similar but not exact.

WPA2 is the recommended protocol to use with this configuration as it is the most secure. However some hardware does not support WPA2, therefore WPA can be used.

ISU-OIT-NWEP, ISU-OIT-WEP and ISU-OIT-WPA are CCA managed networks. However, WPA is using Role based authentication. This means that Faculty and Staff users will not be required to run CCA. Students will still be required to run CCA. Faculty and Staff users will receive a 139.102.176.x thru 139.102.183.x address. Students will continue to receive a 10.139.x.x address.

Summary of Wireless Security Levels

Rating	SSID	Notes
WORST	ISU-OIT-NWEP	Open - All traffic is viewable
POOR	ISU-OIT-WEP	Uses a published shared WEP key – Can be decrypted
OKAY	ISU-OIT-LEAP*	Uses CISCO technology to change WEP Keys automatically
GOOD	ISU-OIT-WPA	Using WPA / TKIP
BEST	ISU-OIT-WPA	Using WPA2 / AES

* ISU-OIT-LEAP SSID was discontinued in favor of the WPA / WPA2 configuration. LEAP requires a Network card that supports or emulates CISCO technologies.

Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

Setting up WPA on Windows Vista

Secured wireless access for users with:

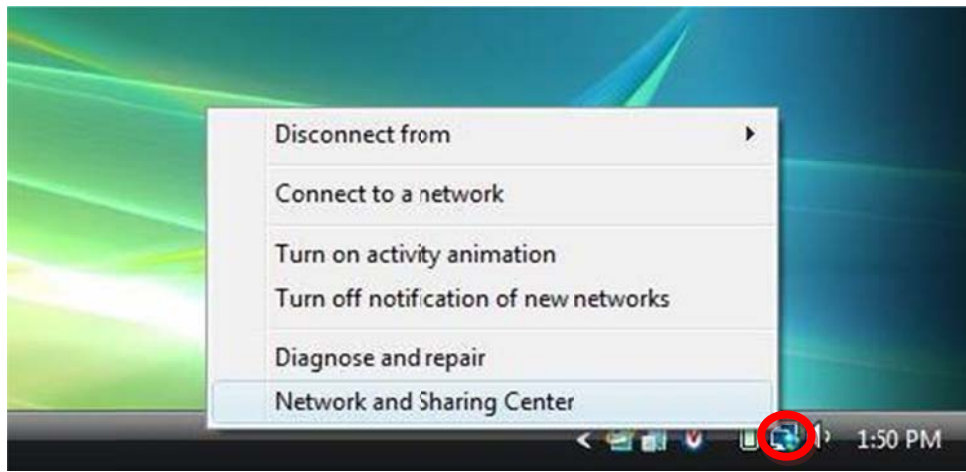
Operating System- Microsoft Windows Vista

Adapter type- Integrated wireless adapter.

Wireless Management- Done by Microsoft Windows

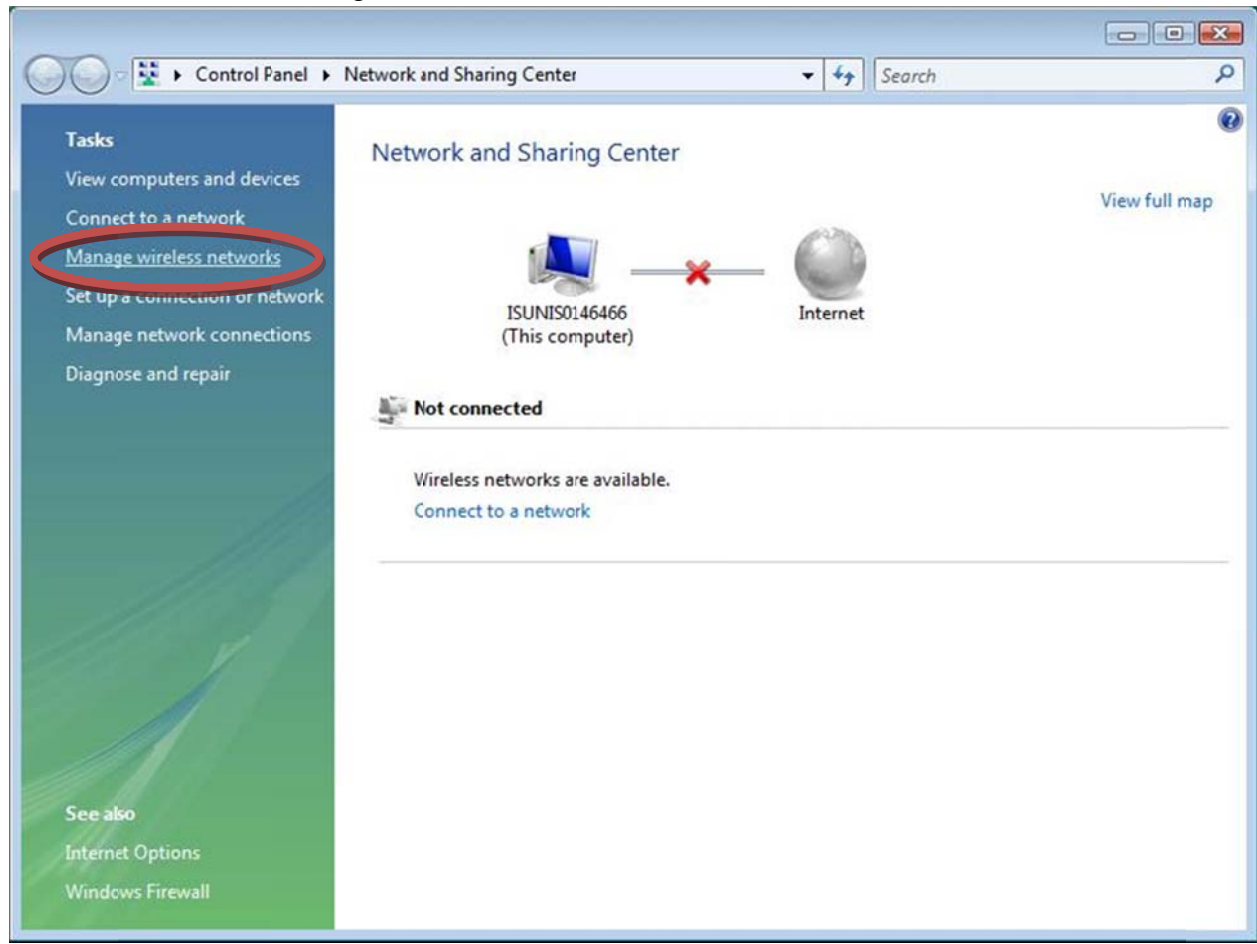
SSID- ISU-OIT-WPA

1.) Click on the **wireless connection icon** in the system tray and click the link to “Open Network and Sharing Center”.



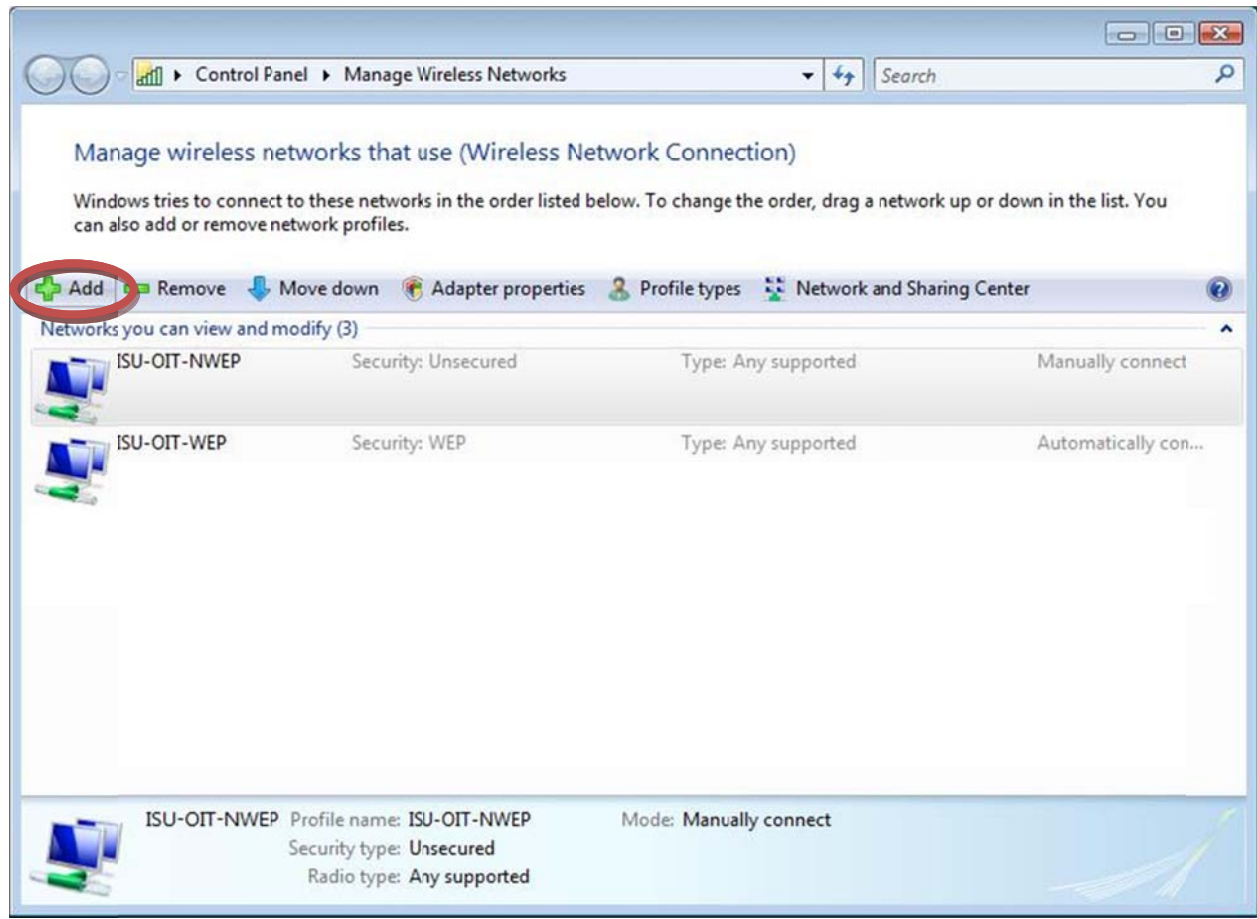
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

2.) Click the link to “Manage wireless networks”.



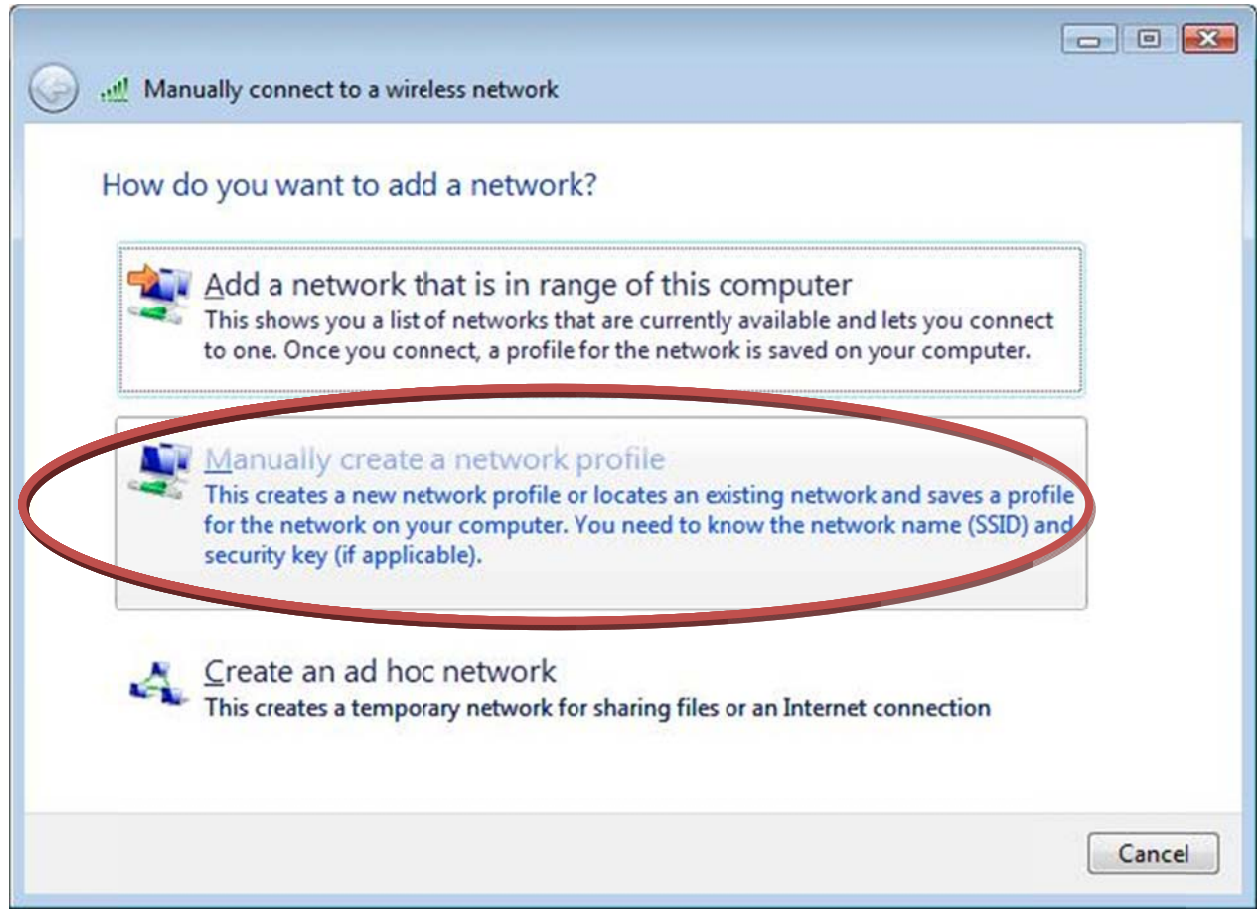
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

3.) Click on the **Add** button:



Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

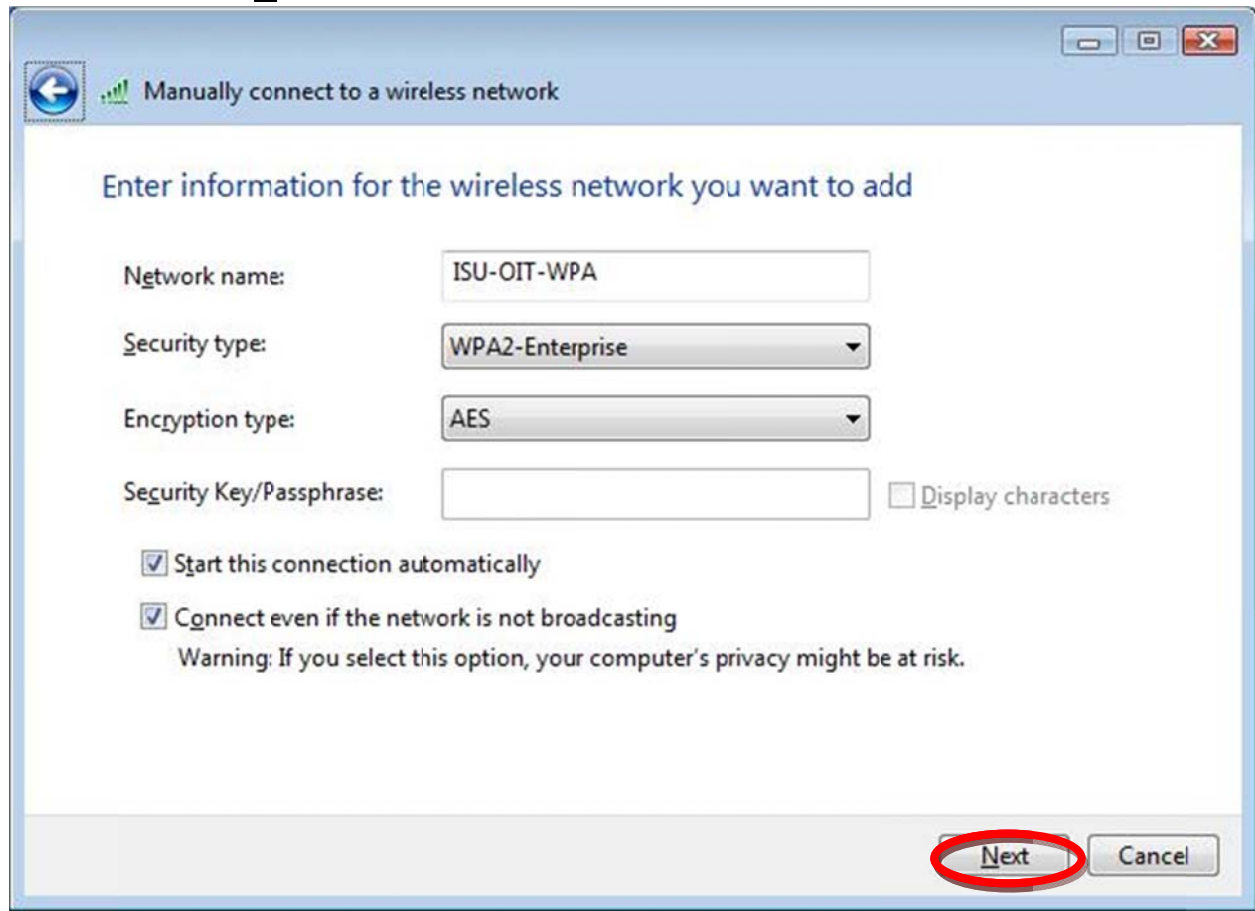
4.) Click the link to “Manually create a network profile” in the **Manually connect to a wireless network** window



Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

5.) Depending on the model of Network Adapter that you have it may support **WPA2**. **WPA2** is preferred over **WPA** whenever possible. Additionally you may need to download a patch from Microsoft KB917021 (Formally KB893357) to enable **WPA2** on your machine. If you are not using Windows to manage your wireless connections and are using the tools that came with your wireless card, you may not need to down load this patch. Some systems may report several **WPA2** types available instead of just **WPA2**. The desired type should be “**WPA2-Enterprise**” over the non-desired type of “**WPA2-Personal**”

Be sure to uncheck the other 2 boxes on the screen if they are not already unchecked. Once these are set click on the **Next** Button.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ISU-OIT-WPA

Security type: WPA2-Enterprise

Encryption type: AES

Security Key/Passphrase: Display characters

Start this connection automatically

Connect even if the network is not broadcasting

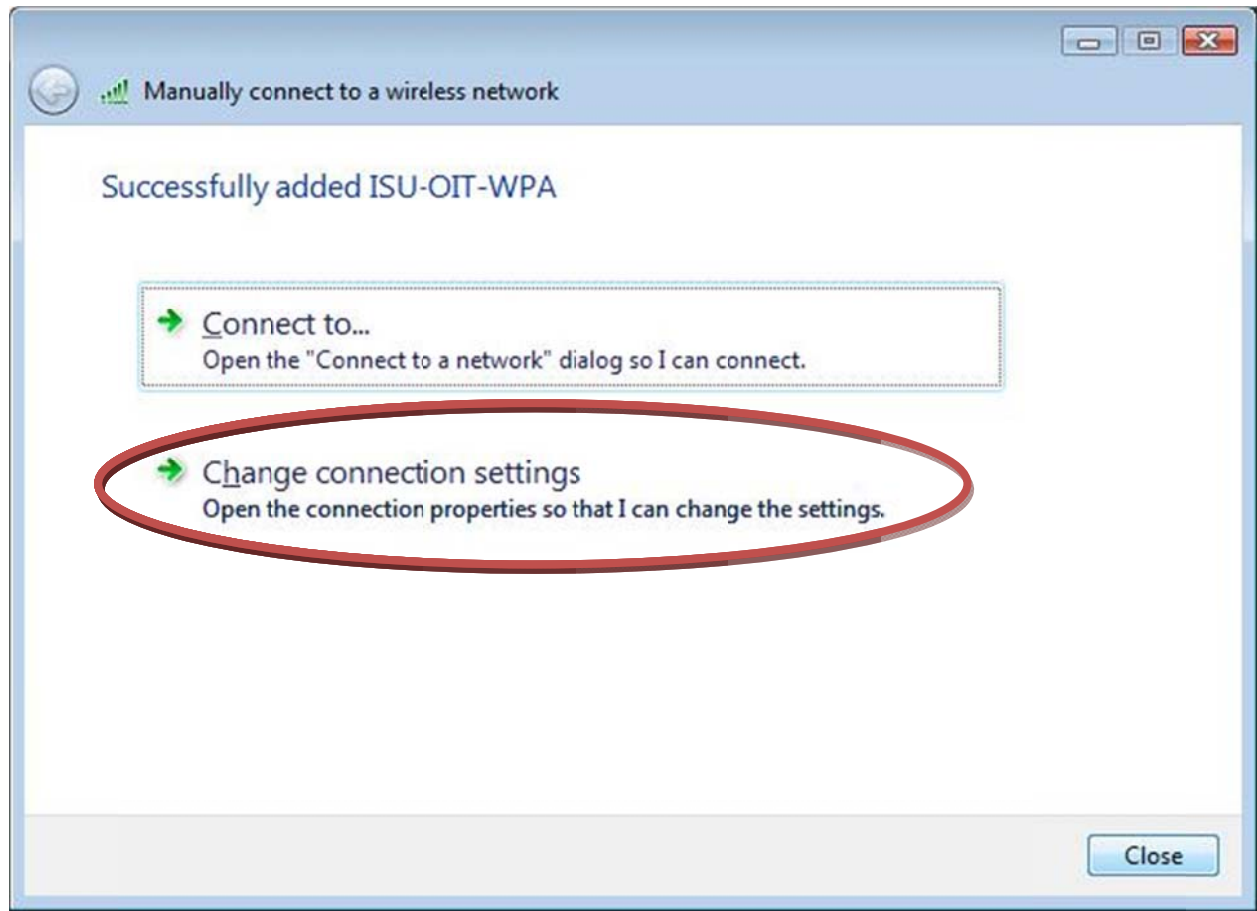
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

If you are unable to select **WPA2** from your list of available Network Authentications, use **WPA**. This will also require you to set your Data Encryption to **TKIP** for **WPA**. As with **WPA2**, some systems may refer to **WPA** as “**WPA-Enterprise**”.

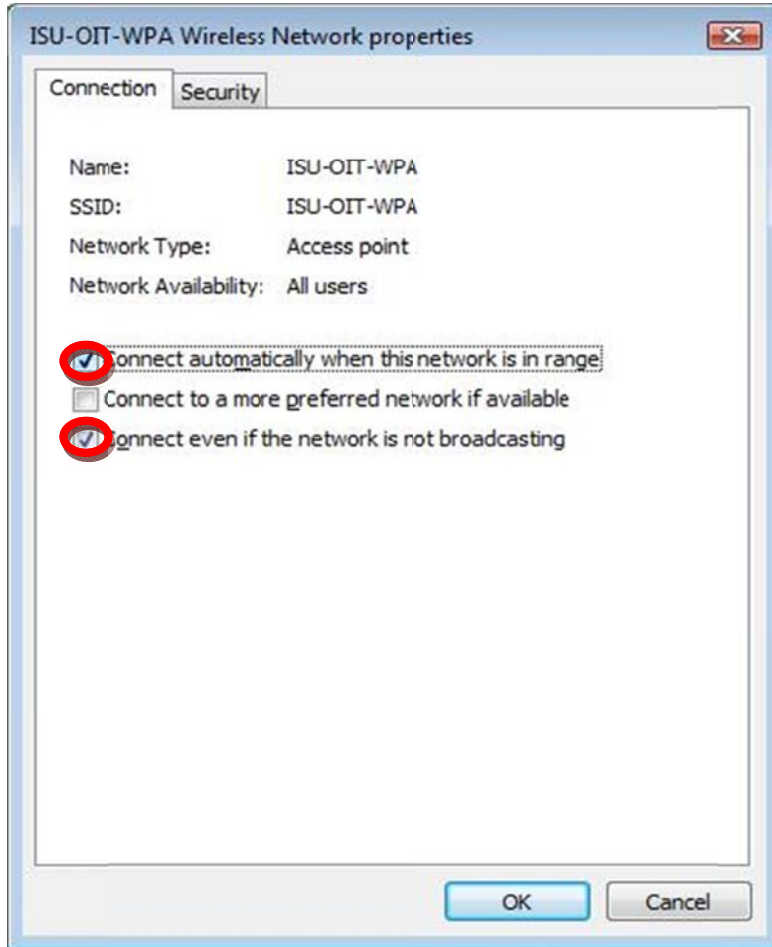
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

6.) Click the link to “Change connection settings” in the **Manually connect to a wireless network** window.



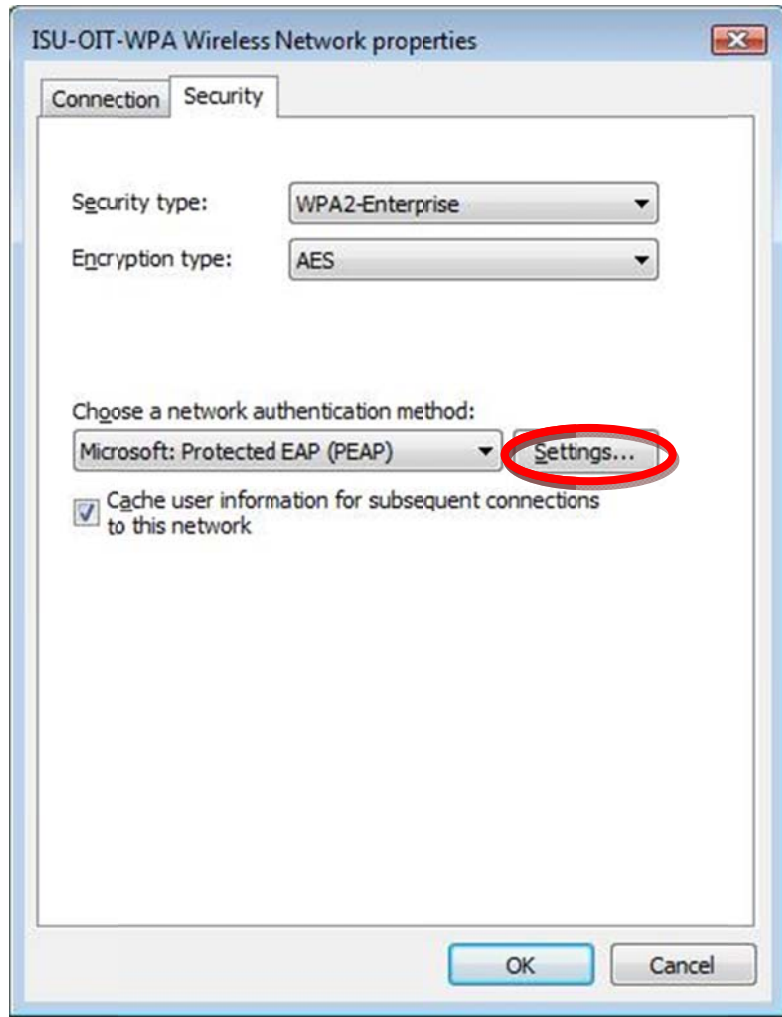
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

7.) Click on the Connection Tab and make sure the check boxes are set to “Connect automatically when this network is in range” and “Connect even if the network is not broadcasting”. Make sure “Connect to a more preferred network if available” is unchecked.



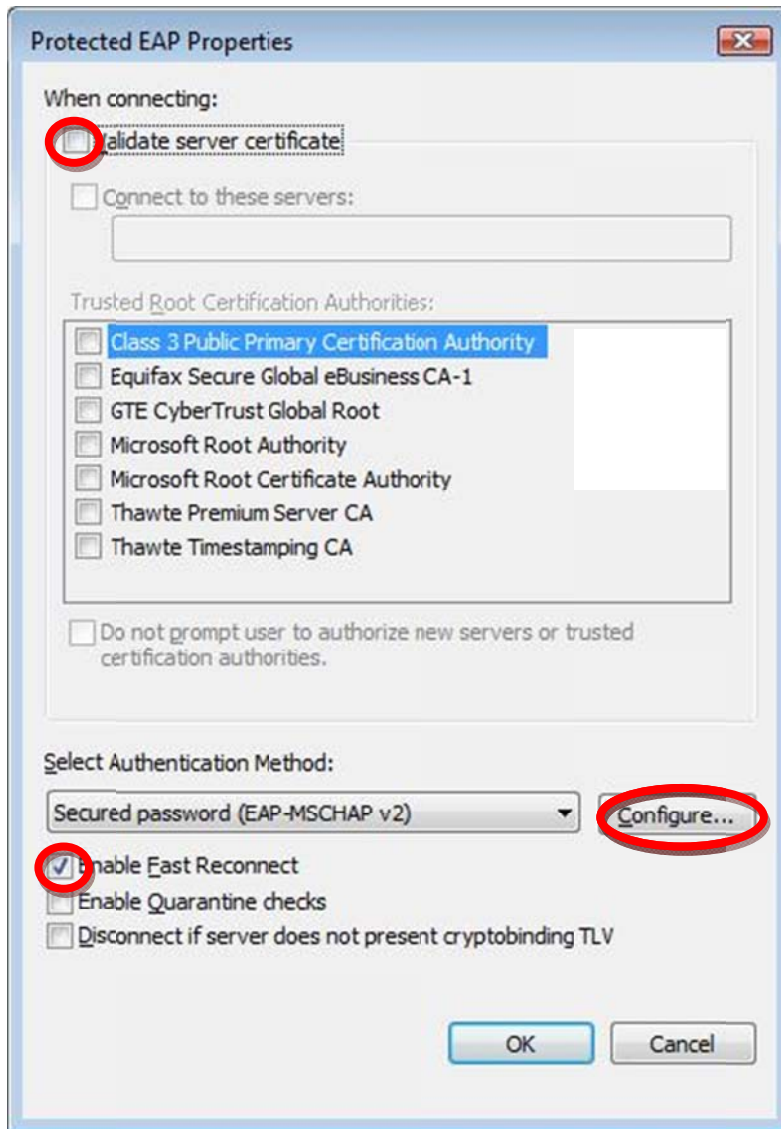
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

8.) Click on the Security Tab and make sure the check box is checked to “Cache user information for subsequent connections to this network” and set the EAP type to **Microsoft: Protected EAP (PEAP)** and click the **Settings** Button.



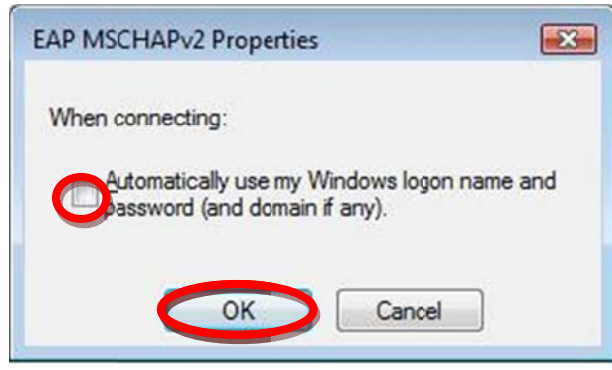
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

9.) On the Protected EAP Properties page **Uncheck** the **Validate server certificate** box and check the **Enable Fast Reconnect** Box. Click on the Configure button.



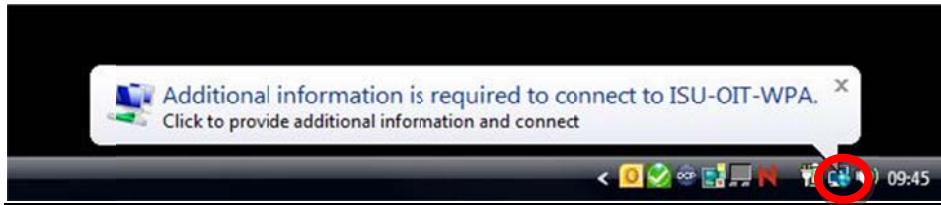
Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

10.) If your user name and password for your machine do not match your ISU Sycamore Login then you must Uncheck the box to “Automatically use my Windows Logon name and password (and domain if any).” Click OK when complete and you will return to the previous screen. Then OK again to return to the Wireless Network Properties Screen.



Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

11.) Once you have saved the configuration you should see the wireless adapter attempt to connect to the SSID of ISU-OIT-WPA and if it is successful you will get a Balloon that is requesting your credentials to login. Click on this balloon.



12.) For the final step you will be presented with a screen to enter your Credentials to login to the network. Put your ISU Sycamore Login (Portalid) in the user name field and enter your password. Do not enter anything in for the Domain. Click OK.



Setting up Windows Vista for WPA Wireless Access (ISU-OIT-WPA)

CAVEATS

1). At the time of this document the following known issues have been found:

a. If you change your portal password, you will have to change the properties in your wireless adaptor if you are using windows for your wireless management. Then when you reconnect enter your new password. Other vendor's tools will have to address this separately to enter the new password.

b. Some devices such as Windows CE devices may list WPA as a supported protocol. However it is WPA-PSK (Pre-Shared Key) protocol and not the WPA Enterprise protocol that is used at ISU.

c. When you have multiple profiles setup and active on a machine. The machine will not necessarily always connect to the preferred net first. The nature of Wireless is that the SSIDs are broadcast as set intervals. Depending on where your machine is in the search process it may hear a non-preferred network first and connect to it. Either delete unwanted profiles, i.e. ISU-OIT-WEP and ISU-OIT-NWEP, or set them to manually connect.

d. When using the computer that has wireless and it is physically connected to the network, the metrics of network performance come into play. Even though the computer may be physically plugged in or docked to the campus network. If the wireless card is still active it can take precedence over the wired connection. This is because the metrics of the network will use the fastest connection. If the wired connection is only 10Mb and the wireless is connected at 56Mb it will use wireless connection. Conversely if you are connected to a 100Mb or faster connection on the wired connection, it will always use the wired connection. To see what network connection is being used you can issue a simple command from the DOS command prompt. "**ROUTE PRINT**" will show you the cost of each interface in your computer. The lower the number the higher the priority / speed of the connection. Additionally at the bottom of the report it will list your "Default Gateway", this will help in determining which interface is being used as the priority metric. It is not recommended to manually set the metrics of interfaces to get the one you desire to work as the priority. Rather, simply disable the undesired interface, i.e. disable your wireless card when on the wired network. This will make sure that when the computer moves to a faster line or another location the metrics will determine the best path for the computer to use.

e. After setup on Windows Vista and Windows 7 it has been found that sometimes the machine has to be restarted for the connection to begin working.

f. Windows based hand held devices will require a "personal" certificate to be installed on the device in order to connect under WPA. Check with the device vendor for information on how import a certificate for you device.