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 XP 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-WPA is a CCA managed network. 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

<table>
<thead>
<tr>
<th>Rating</th>
<th>SSID</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOOD</td>
<td>ISU-OIT-WPA</td>
<td>Using WPA / TKIP</td>
</tr>
<tr>
<td>BEST</td>
<td>ISU-OIT-WPA</td>
<td>Using WPA2 / AES</td>
</tr>
</tbody>
</table>
Setting up WPA on Windows XP

Secured wireless access for users with:
Operating System- Microsoft Windows XP
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 to open the Wireless Network Connection Status window and click on the Properties button.
2.) Click on the **Wireless Networks** tab.
3.) Click on the **Add** button under Preferred Networks:
4.) **WPA2** is preferred over **WPA** whenever possible. This depends on the model of Network Adapter that you have. 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**”

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**”.
5.) Click on the Authentication tab and set the EAP type to **Protected EAP (PEAP)**. Be sure to uncheck the other 2 boxes on the screen if they are not already unchecked. Once these are set click on the **Properties** Button.
6.) On the Protected EAP Properties page Uncheck the **Validate server certificate** box and check the **Enable Fast Reconnect** Box. Click on the Configure button.

![Protected EAP Properties](image)

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.

![EAP MSCHAPv2 Properties](image)
7.) Click on the Connection Tab and make sure the check box is set to “Connect when this network is in range”. Click OK when complete and then the close out / click OK on any other windows still open.
8.) 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.
9.) 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 (Portal id) in the user name field and enter your password. Do not enter anything in for the Domain. Click **OK**.
CAVEATS

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

   a. When using Windows XP to Manage the Wireless networks. The Username and password are stored in the Windows registry for the WPA login. The username is in clear text but the password is secure. In order to delete the username presently you have to edit the registry and remove the key manually. This is particularly important if machine is given to another user.

      HKEY_CURRENT_USER\Software\Microsoft\Eapol\UserEapInfo
      http://support.microsoft.com/kb/823731

      If you are not using Windows to manage your wireless connections and are using the tools that came with your wireless card, you may have the option to prompt for username and password or be able to change it easily. It was found that the wireless card under test did not use the registry key above when using the other tools to manage the card. A tool is available from OIT Networking to remove only the keys that contains ISU-OIT in the SSID name.

   b. If you change your portal password, you will have to remove the registry key in Windows XP (item B above) 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.

   c. On XP systems using Windows to manage the Wireless networks, it has been found that the WPA profile may be changed after disabling and then re-enabling the adapter from the Hardware Wireless On/Off button of the laptop. For example: The profile will change from WPA2 and AES to OPEN and WEP. Simply change these settings back and it will re-enable the ISU-OIT-WPA profile. The user credentials will be retained. There have been instances that it may take multiple resets of the profile before it will stick as well. On machines using Vendor Specific Wireless Management (such as Intel) this behavior has not been documented as of yet.

   d. 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.

   e. 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.
f. 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.

g. 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.