

Connecting to Rovernet 2.0 with Mac OS X 10.3 (Panther)

Rovernet 2.0 is a Michigan Tech WPA Enterprise Solution that allows for greater flexibility and security when accessing the campus wireless network. The “**MichiganTech**” (SSID) is only accessible via WPA Enterprise (PEAP) authentication. Once authenticated, the traffic is encrypted. To obtain access to this encrypted network, wireless clients will be required to configure their devices for WPA/WPA2 authentication.

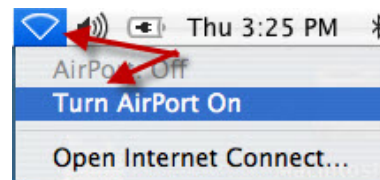
Before you begin this procedure, you need to determine whether your computer supports WPA and/or WPA2.

Minimum System Requirements

- Be within the “**MichiganTech**” SSID wireless coverage areas.
- Be a current Michigan Tech student, faculty, or staff member.
- Have a valid ISO User Name and Password.
- Have installed Mac OS X 10.3 or later.
- Have installed all critical updates and patches to your operating system.
- Have installed and enabled an AirPort card that supports WPA; or an AirPort Extreme card that supports WPA2.
(Note: older, non-Extreme Airport cards do not support WPA2)
- Have installed the AirPort software version 3.3 or later for the AirPort Card (available via Software Update); or the AirPort software version 3.2 or later for the AirPort Extreme Card (available via Software Update).

Adding and Configuring the “MichiganTech” SSID with Mac OS X 10.3 (Panther)

1. Click the **AirPort** icon located at the top right corner of the menu bar.



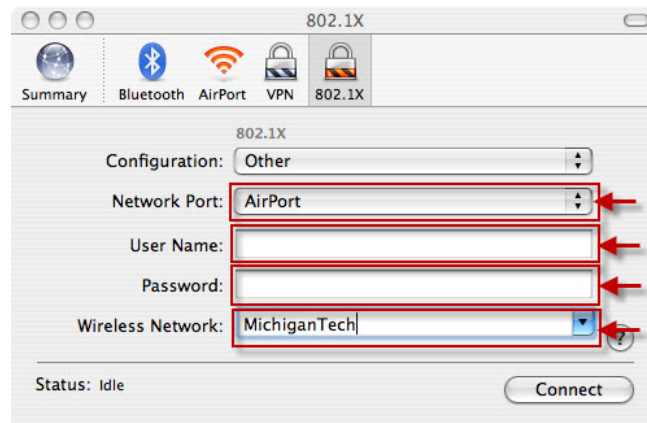
2. Make sure that **AirPort** is turned on. If it is not on, select **Turn AirPort On**.
3. Click the **AirPort** Icon again and then Click **Open Internet Connect**.

4. Select the **802.1X** tab at the top of the **Internet Connect** window.

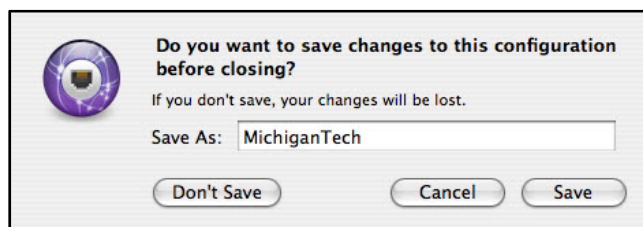


If you don't see the **802.1X** icon, you can display the icon by performing one of the following methods:

- a. Click the minimize/maximize button in the upper right corner of the **Internet Connect Window**, or
 - b. Click on the **File** Menu and then select **New 802.1X Connection**.
5. Specify the **802.1X** Network Details for the "**MichiganTech**" Secured Wireless network:

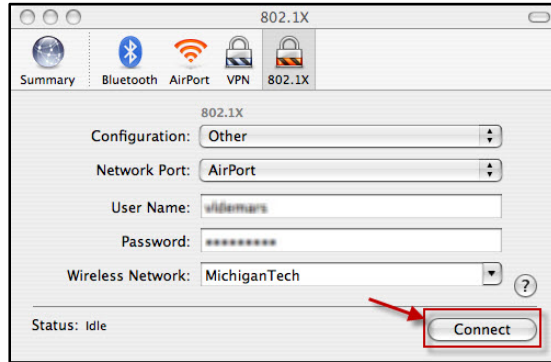


- a. Select **AirPort** for the **Network Port**.
 - b. Enter your **ISO User** name and **password**.
 - c. Enter "**MichiganTech**" for the **Wireless Network**.
 - d. Select **Edit Configurations** from the **Configuration** pull-down menu.
A dialog box will be displayed that asks you to save your configuration.
6. Type "**MichiganTech**" in the **Save As** field.



7. Click **Save**.
A sheet will roll down with the settings that you previously entered, as well as several authentication options to choose from.

8. Choose **PEAP** as the **Authentication** method.
 - a. Uncheck all protocols except **PEAP** in the **Authentication** list.
 - b. Click **OK** to save your changes.
9. Click **Connect** to connect to the “**MichiganTech**” SSID.



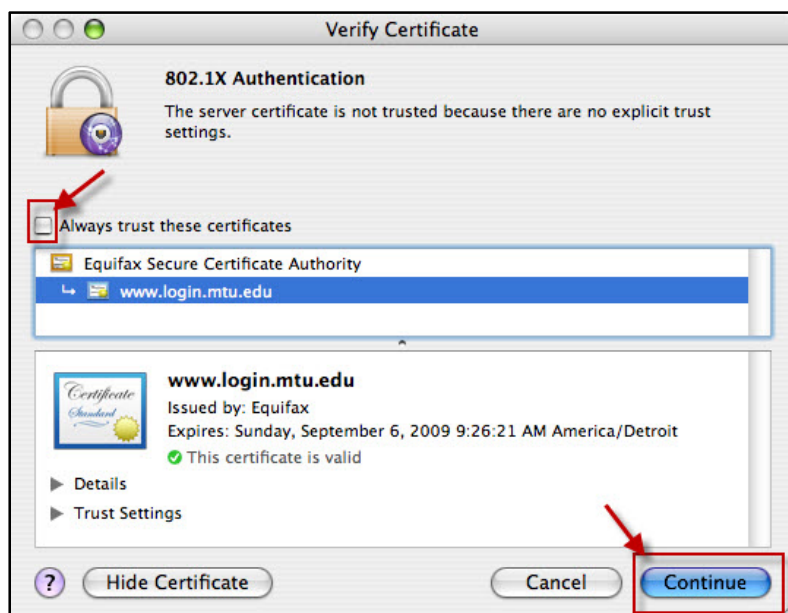
When you connect for the first time, the Server Certificate dialog box is displayed.



10. Click **Show Certificate**.

The **Verify Certificate** dialog box is displayed.

11. Verify the information contained in the **Verify Certificate** dialog box.



12. If the certificate is correct,

- a. Select the Equifax Secure Certificate Authority **www.login.mtu.edu** certificate and check the box to “**Always trust these certificates.**”
- b. Click **Continue**.

You should now be connected to the “MichiganTech” wireless network.

If you are unable to connect, please check to make sure you entered your ISO User name and Password correctly in step 5. Refer to the Initial Sign-On (ISO) Site at www.login.mtu.edu, if you have forgotten your MTU ISO password.