Purple Air and the Mac OS Keychain

There is no one single trick a person can take when trying to repair Purple Air connectivity issues on Mac OS. The easiest thing to do is to completely remove the “Purple Air” stored network profile from a system, and well as the WPA/Purple Air information from within the keychain.

Purple Air utilizes a protocol within the WiFi protected access Enterprise certification software (WPA/WPA2) called the Protected Extensible Authentication Protocol (PEAP), for message exchange during the authentication process. Your login information is stored in the Keychain, and from time to time will have to be purged for various reasons. The main reason we’ve seen is password expiration.

- From the **AirPort menu**, in the upper-right corner of the screen, choose **Turn Airport off**.

  ![AirPort menu](image1)

- From the above menu, choose **Open Network Preferences**.

  ![Network Preferences](image2)
✓ Click Advanced, then the 802.1x tab. You will see one of the screen shots below.

**Case 1: Faulty user Profile**

Case 1: if you encounter more than one user profiles named “WPA: Purple Air”, Delete all except one of them by clicking on the minus (-) symbol in the lower-left corner of the window. Click on the one “WPA: Purple Air” user profile left and put in the correct Williams Webmail username (unix) and password. Click Ok, and then Apply. Then in the Network Preferences window, hit the button to turn Airport on. Select Purple Air from the Network name. (Sometimes this can be enough)

**Case 2: No user profile**

Case 2: However, if you cannot see a user profile under the arrow by User Profiles, click on the Airport tab. You might see nothing under your preferred networks as shown below. In that case, add a preferred network location called Purple Air by clicking on the plus (+) symbol in the lower-left corner of the window. If one already exists then double click on it and proceed to modify it.
✓ Enter *Purple Air* for the **Network name** and click on the drop box next to **Security** and select *WPA2 Enterprise*. Put in your Williams Webmail username (unix) and password. Choose *Automatic* for the drop box by **802.1X** and click on the check box by **Remember this network**.

![Network Configuration Screen](image)

✓ Click **Add**. Click **Ok** in the Airport tab, and then click **Apply** in the Network Preferences window. Click on Turn Airport On. Select Purple Air from the Network name. If you are still not connected after a few seconds and optionally turning the airport off and on again, continue to the following steps.

- Below is a screen shot of a setting that really **should never** be touched, but in very rare cases will be a measure of last resort. Basically, by modifying the “WPA: Purple Air” key to be accessible by any application, in theory removes the operating system’s inability to make changes/updates…i.e. store a new password. With the “All items” Category and “login” under Keychains selected double click on the “WPA: Purlple Air” item and click on the “Access Control” tab. Make sure to allow all applications to access the item as shown below.
• Once you tell your Airport to connect to Purple Air and present it your williams webmail (unix) as username as well as your password, you will see ONCE, a “Verify Certificate” message.

• Our Secure Authentication Server will also present a valid security certificate to Purple Air users.

• After This takes place right after the moment you submit your username and password. This certificate basically say’s, “Hi, I’m ACS and I will be authenticating you today. I am who I say I am, in this certificate.” You should tell OS X to always trust the ACS, otherwise you’ll be prompted every time your connect to Purple Air. You may need to enter in a local Admin username and password to save the “Trust” settings.
If you have an Ethernet connection to the wired network, make sure that your OS is up to date with Apple Patches:

☑️ OS X (10.4.11)
☑️ OS X (10.5.8)
☑️ OS X (10.6.2) Not officially supported by OIT as of yet...That is the first step.

Go to the Apple Menu, in the upper-left corner, and open Software Update. Install the appropriate MAC OS X Update. If you cannot access the wired network using an Ethernet cable, send an email to stchelp@williams.edu or contact the help desk at (413) 597-3088.

- Secondly, for all versions of the above stated OS, it is KEY to ensure file permissions on the hard drive are correct. There are several reasons why file permissions can become problematic on Mac OS X. Use the Disk utility to ensure that there aren’t any write permission errors where the Keychain wants to write and where the WPA wireless username/password has to be stored.
Click on the First Aid tab as in indicated in the above screenshot and among the partitions on your hard drive choose the one currently being used for the Mac OS X operating system that you are using. This is usually the Macintosh HD partition. Click on it and the Repair Disk Permissions and Repair Disk buttons should no longer be grayed out.

- Unfortunately, there is another application that should be run **Keychain First Aid** from time to time, to repair more issues that could cause Keychain problems. This time it is a utility within the Keychain itself. See here:
If you can't find one of these mentioned utilities within your version of Mac OS, then it is possible it doesn't exist, in which case just move to the next step in this guide.

**OS X.4 is different!**

- From the AirPort menu, in the upper-right corner of the screen, choose Open Internet Connect...
- Select the network Purple Air in the dropdown menu of the Airport tab as shown below.

- Type in your Williams Webmail username (unix) and password. Choose Automatic for the 802.1X Configuration and click on the check box for your password to be stored in your keychain.
A window may appear saying that *The server certificate is not trusted because there are no explicit trust settings*. Click on *Show Certificate*, then **check the box** that says *Always trust “acs.williams.edu”* and **click on Continue**. You might be asked for the main password for your keychain. You’re done!