Connecting to the Private HMS Wireless Network Using Mac OS X

Overview: Harvard Medical School (HMS) provides encrypted wireless connection to the World Wide Web through the use of the private HMS wireless network for matriculated HMS/HSDM/HST/DMS predoctoral students.

Special Considerations:

- This document has been tested using Mac OS X Snow Leopard.
- We strongly recommend that you install the latest priority updates for your Macintosh operating system.
- This document assumes that you have never set up the HMS Private Wireless settings on your computer. Follow the steps in order as they appear. If you have set your computer up before or made a mistake in the steps below, jump down to the bottom of this document to Troubleshooting to initialize your Mac for setup.

Step-by-Step Configuration Instructions:

1. Open System Preferences>Network>Airport.
2. Turn Airport Off, if it is on, and enable by checking Show Airport status in menu bar.
3. Click the link, Advanced... in the window.
4. Click on the + (plus sign) under the Preferred Networks: to add a new network.
5. Enter HMS Private in the text field of Network Name:.
7. Enter your MyCourses username and case-sensitive password in Username: and Password:, respectively.
8. Click the button, **Add**. Click the button, **OK**, and then the button, **Apply**.

9. Click on the button, **Turn Airport On**.

10. Click the button, **Show Certificate**, that pops up in the **Verify Certificate** window.

11. Make sure that **Always trust “GeoTrust Global CA”** is enabled with a check mark.

12. Highlight the following text, **GeoTrust Global CA** in the window below, and click the **Trust** information and choose **When using this certificate: Always Trust**.
13. Highlight the next text: **GeoTrust SSL CA**, and click the **Trust** information and choose **When using this certificate**: **Always Trust**.

14. Highlight the **itcascp01.med.harvard.edu** or **itcascp02.med.harvard.edu**, and click the **Trust** information and choose **When using this certificate**: **Always Trust**.

15. Double check each one again to make sure that **Always Trust** is selected.
16. Click the button, Continue.
17. Enter your Mac computer’s password when prompted for changes to Certificate Trust Settings, and click OK. You might be prompted three times.
18. Wait for the Status: Connected in the Network dialog box.
19. Test by launching a web browser and go to any website. You should be all set!

Troubleshooting:
If you are unable to connect, follow the steps below:
1. Navigate to System Preferences>Network and Turn Airport Off.
2. Click on Advanced... and click on the - (the negative sign) for all HMS networks (HMS Private and/or HMS Public) listed under Preferred Networks:

3. Click on the tab 802.1X and remove again all HMS networks from the window. Click OK and then Apply.
4. Navigate to Finder>Applications>Utilities and launch KeyChain Access.
5. Highlight login under Keychains and All Items under Category.
6. Delete GeoTrust Global CA, GeoTrust SSL CA, itcacsp01.med.harvard.edu and itcacsp02.med.harvard.edu. You may be prompted with the following message “Delete Keychain The references to be deleted refer to files on your disk. Do you wish to delete only the references and not the related files?” If so, click on the button, Delete References. If not, then delete each one under the Edit menu when prompted.

7. Keep login under Keychains highlighted and highlight Passwords, Secure Notes, My Certificates, etc. under Category to check if there are any other references to the HMS Private or Public networks. Remove them if they exist.

8. Highlight System under Keychains and parse through the list under Category to remove any references to HMS Private or HMS Public (e.g., something like HMS WPA Private).

9. Now restart your computer.

10. Go back to the directions at the top of this document (Step-by-Step Configuration Instructions) and carefully repeat each step in the order that it was given.