This document provides step-by-step instructions for troubleshooting common connection issues seen with Mac OS X computers connecting to SU-secure. After completing each numbered section, attempt to connect to SU-secure again. If you are unsuccessful in connecting, continue on to the next numbered section.

Steps for Service Desk Members
1. Verify the account is not locked out
   a. Open Active Directory Users and Computers
   b. Search for the account username and double click on the account
   c. Click on the ‘Account’ tab
   d. Validate that there is no ‘This account is locked’ message
   e. If the account is locked, unlock it and have the user attempt to log back in
   f. If repeated lockouts are seen, escalate the request to Technical Operations to identify which device is locking the user out

2. Verify the account has the correct group membership
   a. Open Active Directory Users and Computers
   b. Search for the username and double click on the account
   c. Click on the ‘Member of’ tab
   d. Verify the account is a member of one of the following Active Directory groups: ALL-STAFF, ALL-FACULTY, ALL-STUDENT, ALL-NMA, ALL-ADJUNCT, VENDOR_SUsecure, or Jesuits.

Steps for end-users
3. Verify Username/Password
   a. If you can successfully login at https://webadvisor.seattleu.edu/ then your credentials are working correctly.
   b. If you are unable to login at https://webadvisor.seattleu.edu/ please follow the instructions at https://www.seattleu.edu/its/support/support-articles/reset-your-su-password.html to reset your password.
   c. If you are still unable to authenticate to SU-secure after resetting your password proceed to the troubleshooting steps below.

4. Verify there are no static IP or DNS server settings
   a. Press the wifi icon in the status menu and select ‘Open Network Preferences’
   b. On the ‘Network’ menu, select your Wi-Fi network and click on ‘Advanced…’
   c. Click on the ‘TCP/IP’ tab and verify ‘Configure IPv4’ is set to ‘Using DHCP’
   d. Click on the ‘DNS’ tab and verify the DNS servers listed are 172.17.72.xx and 172.17.61.26. Remove any other entries. If there are no DNS servers in the list, do NOT manually add any DNS servers. Press ‘OK’ when completed.
5. Verify if a wireless profile has an outdated security certificate
You will be unable to authenticate to SU-secure if your Mac computer contains an expired security certificate in the SU-secure wireless profile. The former certificate expired Sep 1 2019. Follow the steps below to verify if your Mac has the wireless profile and if so the expiration date of the stored certificate.

a. From the Apple menu select System Preferences
b. Select Profiles as shown below

![Profiles selection](image)

If Profiles is not present there are no profiles configured; this is normal as not all Macs will have it. Skip the remaining steps and exit System Preferences.

c. Click the SU-secure profile in the left frame. If the Expired date is prior to today's date, such as the example of Sep 1 2019 below, the expired certificate is used. The wireless profile must be deleted.

![Profile details](image)

d. Click the minus sign at the lower left of the window to remove the profile. If prompted enter the username and password of the authorized user to remove the profile.

e. Agree to any remaining prompts to remove the profile.
f. Close the open windows

You should now be able to re-connect to SU-secure and successfully authenticate. Proceed with the remaining steps only if you cannot authenticate to SU-secure and access external web pages.

6. Forget the SU-secure network
   a. Press the wifi icon in the status menu and select ‘Open Network Preferences’
   b. On the ‘Network’ menu, select your Wi-Fi network and click on ‘Advanced…’
   c. In the ‘Wi-Fi’ tab, select SU-secure, click on the minus button to remove the network, and then click ‘OK’
   d. Click the ‘Apply’ button on the Network menu to apply the settings.
   e. Re-connect to SU-secure following the configuration guide for your device at https://www.seattleu.edu/its/support/support-articles/wireless-network-connect-to-su-secure.html

7. Check for Applications Known to Impact SU-secure Functionality
   a. Avast Antivirus forces your Mac to use external DNS servers. Such DNS use is blocked by the SeattleU firewall. Open Avast, select Settings, select Components, set Secure DNS to off.
   b. Some versions of Cisco AnyConnect Secure Mobility Client prevent internet access while connected to SU-secure. Don’t use this application while connected to SU-secure.
8. Verify the operating system is up to date
   a. Click the Apple button and select ‘About This Mac’
   b. On the ‘Overview’ tab, select ‘Software Update…’ and install any updates

9. If you are still unable to connect
You can contact the Service Desk for assistance either via helpdesk@seattleu.edu or via phone at 206-296-5571. Service Desk hours can be found at https://www.seattleu.edu/its/support/service-desk/.

When opening a support ticket with the Help Desk, please provide the following information:
- Your account username (i.e. ‘doe’).
- The brand and model of the device you are attempting to connect to SU-secure.
- The operating system version of the device you are attempting to connect to SU-secure.
- What location (building, room) you are attempting to connect in.
- A description of the error message or problem you are seeing.