

# Old Dominion University's Information Technology Services MAC OS X Workstation Hardening Guide

---

The purpose of this guide is to assist self-administrated MAC OS X Workstation users secure their systems.

You know how to install and configure MAC OS X

You follow the MAC OS X best practices as set down by Apple

You are using a anti-virus protection suite for MAC. You can get McAfee from here:

- o <http://www.odu.edu/ts/software-services/mcafee-win>

- 1) Disable Bonjour's multicast advertisements with the following command and reboot:
  - a. `sudo defaults write /System/Library/ LaunchDaemons/com.apple.mDNSResponder ProgramArguments -array-add "-NoMulticastAdvertisements"`
- 2) Disable Automatic Login and User List:
  - a. Click on "Login Options." Set "Automatic login" to "Off." Set "Display login window as" to "Name and password."
- 3) Disable guest account and sharing:
  - a. Select the Guest Account and then disable it by unchecking "Allow Guest to log in to this computer." Uncheck "Allow guests to connect to shared folders."
- 4) Open the Security pane in System Preferences. In the General tab, ensure that the following are checked:
  - a. Require password "5 seconds" after sleep or screen saver begins
  - b. Disable automatic login
  - c. Use secure virtual memory
  - d. Disable Location Services (if present)
  - e. Disable remote control infrared receiver (if present)
- 5) Turning On File Extensions
  - a. Open Finder.
  - b. From the Finder menu, select Preferences.
  - c.

