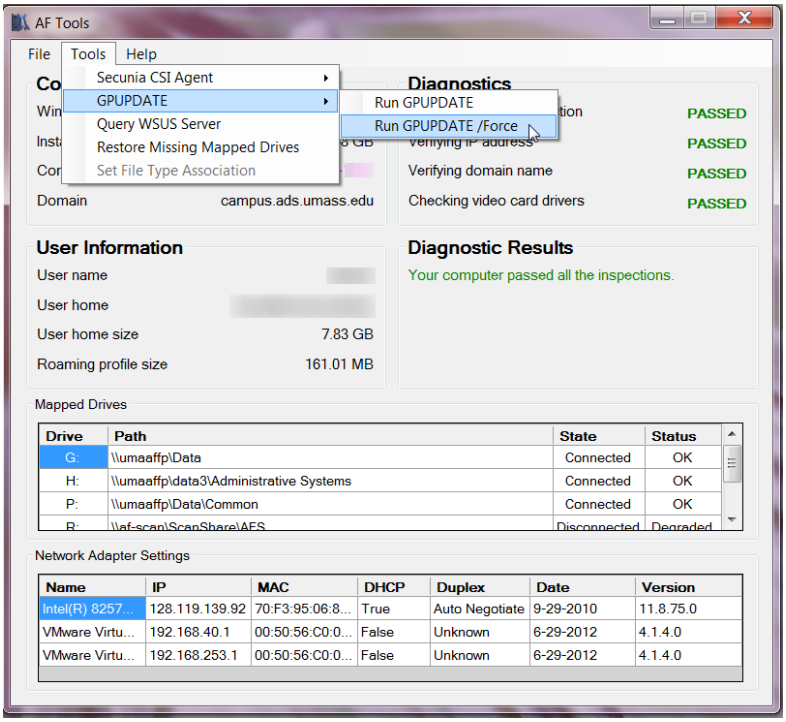
What to Do When You Have a Computer Problem

Don't Panic!!!

1. Check the Ethernet (CAT-5/CAT-6) cable connecting the computer to the wall jack.
2. Check the power cords for both the computer and monitor are plugged in, and the power strip (if applicable) is turned on.
3. Check the monitor is connected to the computer with the appropriate cable.
4. Check the keyboard is connected to the computer.
5. Check the mouse is connected to the computer.
6. Launch the AF Tools icon and choose Tools, GPUPDATE, Run GPUPDATE /force.



7. Reboot the computer.
8. Call AFS Help Desk at 413-545-1956 or send an email to: afssupport@admin.umass.edu (Our office hours are M-F, 8:30-5:00)
9. What if you think you have a virus?
    a. Keep detailed notes. Depending on the severity of the incident, you may be asked to provide details about the incident (i.e. if sensitive University data has been compromised).
    b. STOP using the device. If your computer is exhibiting signs of malware infection, you should keep the system intact for investigative purposes. Do not turn off the device, run anti-virus software, or attempt to back up data.
    c. Contact AFS Help Desk at 413-545-1956 between the hours of M-F, 8:30-5:00.
10. If your university computing device (laptop, cell phone, PDA, USB drive, etc.) is lost or stolen, ESPECIALLY if it contains sensitive or confidential data, you should take the following actions:
    a. Contact the UMass Police Department at 413-545-2121. (Registering your device using Project Protect http://www.umass.edu/umpd/projectprotect/ increases the odds it will be recovered.)
    b. For University-owned devices, contact the UMass Procurement Department at 413-545-0361.

c. Fill out the Lost or Stolen University-Owned Computing Device form: http://www.oit.umass.edu/security/report-a-lost-or-stolen-university-owned-computing-device
d. Change your passwords. Be sure to change your OIT Account password in SPIRE, and any other passwords that may have been exposed.
e. If it is a mobile device such as a smartphone, contact your service provider and request that the contents of your device be wiped remotely.