Mac User Migration Script
By Don Howdeshell

This script will affect all campus OS X users that log in to AD.

This script will be installed on all campus-owned machines that IT can remotely administer. Depending on how the user authenticates, it may not do anything – if the user logs in to a local account, no changes will be made for that user.

The package will be pushed to campus after the IT pilot. The IT pilot will take place on 3/3. If there are any problems with the script then it will be changed and then pushed to the rest of campus.

Why is the User Migration Script needed?

Once a user logs in to a campus build of OS X, it caches that user’s credentials so he can log in while off the campus network. OS X caches the user’s domain, so if the user is moved the cached credentials are no longer valid.

The system does not know this if the user cannot talk to AD, and will allow the user to log in. If the system can talk to AD then it knows that the user’s credentials are wrong and will not allow authentication.

What does the script do?

A lot. The script is being installed via a software package (.pkg). The install package does the following:

- Sets the time service to point at a campus time server
- Configures Software Update to look at our campus SUS server
- Installs a program written by DI to check for updates every Tuesday at 3:15 PM and report the result
- Installs some Perl modules required by the user migration script
- Installs a StartupItem that includes the user migration script

The script will run at startup before the user can log in. It will do the following and write it all to a log file:

1. Check for user accounts on the system that have cached AD credentials in umr.edu.
2. Try to connect to an mst.edu Domain Controller via LDAP. It will try to connect up to 30 times and wait one second between tries. If it cannot connect the script will terminate.
3. Update the time from a mst.edu time server.
4. Check the date. If the date is between 3/24 (3/3 for the IT pilot) and 5/20 it will run the script. If it is before the specified date it will do nothing, if it is after the StartupItem will be removed.

5. Check the domain that the computer thinks it is in. If the computer is not in mst.edu then the script will terminate and uninstall. **The machine will need to be rebuilt if this is the case.**

6. Do an LDAP lookup for the cached user accounts from item 1. If a user is in mst.edu with cached umr.edu credentials then it will delete the cached credentials so the user can log in.

Note: If the user is not in mst.edu or if the user is in mst.edu and has cached mst.edu credentials then the script will do nothing with that user account.

**Note: After the User Migration Script runs at startup, the user may not be able to log in for up to 5 minutes. This is expected behavior. Let the computer sit and finish running all of its scripts and then the user should be able to log in.**

What if the script fails and the user cannot log into the machine?

If the script fails, for whatever reason then the user will need to bring their machine to campus and plug it into the wired network and reboot it. There is a good chance that this will fix the problem by allowing the script to run, but if it still fails to remove the credentials or if the script is not installed then do the following:

1. Install the User Migration Script package (the .pkg) and reboot. This can be done remotely via SSH (see the footnote on SSH). The package is in appdist.
2. Run the following command “sudo dscl . –delete /users/<userid>” where <userid> is the user’s SSO userid. Example: “sudo dscl . –delete /users/dmh4k4”. This can also be done over SSH (see the footnote on SSH).
3. If nothing works:
   a. Double check that the machine is in mst.edu. If it is not, then rebuild the machine.
   b. Double check the wired connection. Can you successfully ping “mst-dc.mst.edu”?
   c. Try to log in as an AD user that has never attempted to log in to that machine before. If that does not work then there is a problem with the DirectoryService settings and the machine will likely need to be rebuilt.
   d. Contact DI. Be sure to provide the hostname, IP address, and userID in question.

Using SSH to fix a broken Mac:

1) Obtain the hostname of the system in question. Be sure it is plugged into the campus network.
2) Using PuTTY or a UNIX-like shell, connect to the system.
3) Log in as either local administrator or the itadmin account using the standard desktop password.
4) Run the commands necessary. To install a package run “sudo installer –pkg /path/to/pkg.pkg –target /”. You may need to mount a network share first if you intend to install over the network.