Apple 10.12 and 10.14 AD Join and JAMF

I recently had to process 2 fairly new Macbook Pro’s for new users and decided to document the method on the 2nd computer to maybe help others avoid the pitfalls I ran into on the 1st.

I.T. does not require Macs to be joined to Active Directory. There are some benefits to do so, drive share access, One Drive and maybe SSO. But, I.T. will, in the near future, require all Mac’s to be encrypted and one of the steps in joining AD will facilitate encryption via JAMF on 10.12 Sierra and 10.14 Mojave.

You will need an administrative local account, a valid Apple ID, Ethernet connectivity, and DHCP. With the newer laptops, this may require you to have a [3-Port USB 3.0 Hub with Ethernet](https://example.com). Wireless access will not be adequate.

**Update OS:** Log-in as admin and update system to the latest 10.14.x via the Apple Store Update tab. Download will require a valid Apple ID. Since my computers are being repurposed, I deleted all local accounts except my local admin. This will recover disk space and help simplify the eventual login screen.

-Click on Apple/About this Mac in the upper left. On the resulting tab will tell you what OS you have along with an Update button. Alternately, open the App Store and go to the update tab.

**Joining Active Directory:**

-Open System Preferences/Users and Groups
-Click on the lock and authenticate to allow editing
-Select Login Options and you will see this →
  -Note some green highlighted options
-Select Network Account Server “Edit…”

![Image of System Preferences](image-url)
There are a gratuitous number of dialog boxes in this process. Once joined, there is really only one “change” that need to be made from the default settings.

Edit results in this box. Select Open Directory Utility

-Unlock dialog box
-Select “Active Directory”
-Select the Edit Pencil above the lock

-Select “Show Options“
-Add ☑ to “Create mobile account at login”
  Note: This is the step required for JAMF encryption

-You can try to add Admin access to SIU dawg tags via the Administrative tab. I’ve found it more effective to assign admin access to network accounts after first login via Users and Groups.
Close all windows and you should have a green light next to AD in Users and Groups

Adding Network Users

You may need the end user handy especially if you want to grant them Admin access to the Mac.

-Just like Windows, the Mac has to be networked for the first network account login. There may be a way but I could not establish a wireless connection at the login prompt. I had to use the adapter described above and DHCP to have a connection at the login screen. BTW, the wireless icon suggests a connection...nope. Once connected, that annoying red dot disappears.

Adding that one checkmark in Directory Utility allows the OS to cache the network login credentials, creating an account on the Mac based on your dawg tag/password. It adds that login to Users and Groups as a “Managed Account” and also adds an icon on the login screen if you have “List of Users” checked here →

After the first login, subsequent access to that managed account doesn’t require a network connection.

Also, according to Jay Spolarich, this setting also allows the Apple OS to create a “Token” that will then be used in the File Vault encryption process to allow the encryption key to be backed up in JAMF. I hope I got that part right...

So, you have added the Mac to AD. You have made the requisite change in the Directory Utility. You are networked via Ethernet and booted to the login screen.

For 1st login, if you use the List of User setting above, select “Other User” and login in with siu dawg tag and network password.
For 1st login, if you use the Name and Password option above, simply login in with siu dawg tag and network password.

Note: If there’s a red dot as pictured to the right and you have logged into the Mac in the past, you will have a successful login. If it’s your first login...nope.

If you want to grant an active directory account admin privileges, have them log-in the first time. Then, log in with your admin account, open System Preferences/Users and Groups, select the account and put a ☑ next to “Allow user to administer this computer”. Note, my siu account has my name, not my Dawg Tag and is labeled Admin, Managed, Mobile.

One other idiosyncrasy I noted...if I wanted to perform an admin function needing name/password while in my network account, say like unlocking Users and Groups, the dialog box would come up with “Harbert, Tom W” in the ID. You need to change the name to your dawg tag or the authentication will fail.