**MAC SETUP PROCEDURE**

* If the MacBook is being reissued, the hard drive will need to be reformatted (see procedure below).

**Formatting and Loading the OS**

* Connect the Mac to the network prior to beginning.
* Hold down Command – R during startup; and once the screen is presented, select “Disk Utility.”
* In the left column, select the SSD and click on the “Erase” tab. Once selected, go to the bottom right corner and choose “Erase.”
* After erasing the drive, close the box and return to the “OS X Utilities” box.
* Choose “Reinstall OS X” and “Continue.” This will take you through the setup process. Take all defaults during setup.
* After reboot, configure basic settings.
* When prompted for the Apple ID setup and registration information, please enter the following information:

User ID: [**premierhca@me.com**](mailto:premierhca@me.com)

Password: **H3!pbg8t**

* Change the Admin username / password to the following:

Username: **dtservice**

Password: **H3!pbg8t**

* Logon as dtservice and begin the basic configuration.

**Enable Root Account**

* Choose System Preferences and **Users & Groups**.
* Click the lock and authenticate as an administrator account.
* Click Login Options....
* Click the "Edit..." or "Join..." button at the bottom right.
* Click the "Open Directory Utility..." button.
* Click the lock in the Directory Utility window.
* Enter an administrator account name and password, then click OK.
* Choose **Enable Root User**from the **Edit** menu on the upper menu bar.
* Enter the root password D3$kt0p in both the Password and Verify fields, then click OK. Click the lock and close.
* Remain in **Users & Groups** for the next step.

**Enable FileVault Master Password**

* While in **Users & Groups**, click on the gearwheel, choose “Set Master Password” and enter the FileVault Master password: **Encrypt10n**
* Remain in **Users & Groups** for the next step.

**Main Settings and Application Setup**

* Disable guest access via System Preferences / Users and Groups. Highlight Guest User and uncheck “Allow Guests to Connect to Shared Folders.” Click the lock to relock the settings.
* Close Users and Groups.
* Update the OS X software by going to the Apple menu and selecting Software Update. After updates complete, reboot if needed and go to the next step.
* Launch Terminal (go to Launchpad / Utilities / Terminal) in Lion. Mountian Lion (go to Laucnpad/Other/Terminal) or on either OSX you can Select Finder and then to GO/Utilities
* At the Terminal window, type the following commands:

**Sudo scutil --set ComputerName *asset#username-m***

(This renames the machine in WINS.)

**Sudo scutil --set HostName *asset#username-m***

(This renames the machine in DNS.)

**Sudo scutil --set LocalHostName *asset#username-m***

(This renames the machine in NetBIOS.)

When prompted for password, use the dtservice password (**H3!pbg8t).**

* Exit and close Terminal.
* Reboot and login as dtservice.
* Go to System Preferences / Network and select the Advanced button.
* Choose the DNS tab and add CORP.premierinc.com. If premierinc.com disappears, please re-add.
* Select “Apply.”
* While in System Preferences, check the system time. Go to Date and Time and uncheck “Set date and time automatically.” This should later populate with the server **c3picorpdc5.corp.premierinc.com**; and adjust the time accordingly. In the meanwhile, if the time and date needs adjustment, please do so. Close Date and Time.
* In System Preferences, go to Sharing; and enable Remote Login and File Sharing. Make sure to allow access for dtservice.

**Centrify Domain Setup**

* **Give IP Address to Roger, Michael Dean or Ed Guy to add the MAC to the Domain**

(System Preferences / Network, choose network interface and note IP address)

After deployment is completed, check Centrify on the Mac (System Preferences / Centrify) to ensure all settings in the Account Configuration reflect the correct computer name.

**System Preference Changes**

* Restart the Mac and login as the user. We will now make several changes in System Preferences.
* First, we will change the Login Options. Once again, go in to System Preferences / Users & Groups and unlock the settings. Then select Login Options and change (if needed) the setting from List of users to Name and password.
* Next, we will grant the user local admin rights. While we are still in System Preferences / Users & Groups, highlight the user’s account and check the box to “Allow users to administer this computer.” At this point, lock the box.
* While still in System Preferences, go to Displays and check (if needed) “Show displays in menu bar” or “Show mirroring options …”
* To setup Hot Corners, go to System Preferences / Mission Control and click the Hot Corners button (bottom, left corner). Click the upper left corner and select “Start Screen Saver.”
* To change the Mac power settings, go to System Preferences / Energy Saver and uncheck “Put hard drive to sleep when possible.”
* Setup requires a password for sleep and the screen saver. To do so, go to System Preferences / Security & Privacy and check “Require password for sleep and screen saver” or “Require password immediately after sleep or screen saver begins.” This setting may already be in effect. After making these changes, relock.
* Lastly, to enable Mac usage on the Premier – Employee wireless network, Desktop needs to generate a Service Desk request to the Networking team. This request should have the wireless adapter’s MAC address (System Preferences / Network / Wi-Fi / Advanced / Hardware tab and note MAC Address).

**SCCM CLIENT INSTALL**

\*Make sure the name of the computer has been finalized. Once the client is installed, a computer name change will be recognized. Copy the MAC Deploy folder from 10.32.39.186/windows7. Everything you’ll need to install will be in that location.

* Copy the **“Tools”** folder to the desktop from this location – mac deploy/sccm tools/.
* In Terminal, Change directory (**cd**) to the **desktop/tools** directory. When prompted for password, use **H3!pbg8t**.
* **sudo ./ccmsetup**
* **Reboot the Mac. After logging in, a GUI will appear.**
* **Enter username: CORP\sccm, password: ASMteam1 and server name: c3pisccm.corp.premierinc.com.**
* **Reboot**
* Open System Preferences and check to see if Configuration Manager is present (bottom area). If not, uninstall / reinstall SCCM client using the above UNIX commands. If Configuration Manager is present, select the “Connect Now” button to test connectivity. If it continually fails, the client may need to be uninstalled / reinstalled. **To Uninstall the SCCM client: cd to desktop/tools and then Sudo ./CMUninstall –c**
* **If Configuration Manager is present, open the System Center 2012 Configuration Manager console on your laptop. If it has not been installed, contact Bob Carthage for the required software.**
* **On the left side, choose “Devices;” and then “Search asset #.”**
* **Once the active asset is found, right click it; and choose “Add Selected Items.” Then take “Add Selected Items to Existing Device Collections.”**
* **In the left column, select Mac OS / Mac Deployment; and then OK.**
* **Again in the left column, choose “Device Collections” / Mac OS X.**
* **In the right column, choose “Mac Deployment.” In the upper menu, select “Update Membership.”**

\*\*SCCM Account is the only account that can enroll the Mac Certificate properly.

\*\*\* Should the SCCM client fail to download the appropriate software (SCEP, Office, Lync, Chrome, FireFox, Remote Desktop and View client), all software can be manually installed from the Mac Deploy folder.

**Cisco AnyConnect VPN Configuration**

**\*\*Install as the User\*\***

* Install the Cisco Anyconnect client (**anyconnect-macosx-i386-3.1.04072-k9.dmg**) located in the Mac Deploy / VPNFile / Anyconnect\_MAC folder. During installation, **uncheck Web Security option**.
* Install the new Java client located in the Mac Deploy / Java folder.
* Once that’s installed do the following in order to get VPN to work. Go to System Preferences / Java / Advance and uncheck “Enable blacklist revocation check”
* The next step is to copy the **com.apple.netauth.plist** file located in the Mac Deploy / VPN File folder to System / Library /LaunchDaemons. The file is required for the network to recognize the Mac as a domain machine over VPN.
* From that same VPN folder. Copy the file **eventlogd** to /opt/likewise/sbin/. The likewise/sbin folders will need to be created. Kyle King will change this location at some point in time.

At this point, disconnect from the wired LAN; and connect wirelessly to the Premier – Guest network. You can then launch and test the Cisco AnyConnect client.

After the Cisco client completes connecting, right – click on icon on dock, choose Options / Keep in Dock.

**Remote Desktop Connection**

* Install Microsoft RDC for Mac (RDC\_2.1.1\_ALL.dmg). It is located in the Mac Deploy / RemoteDesktop folder.
* Copy vmware-view.rdp located in MacDeploy / RemoteDesktop to Applications / Remote Desktop Connection / Contents / Resources. To accomplish this, right – click Remote Desktop Connection and choose Show Package Contents. Open the Contents folder and navigate to the Resources folder. Paste the file in this location.
* Right – click on the vmware-view.rdp file, choose Get Info, and under Sharing & Permissions, change everyone’s permission to Read Only. Be sure to unlock prior to changing permissions. Relock after completing.

**Xerox and Equitrac Installations /Configurations**

This currently does not work.

* Install the Xerox Colorqube Printer driver. Go to MAC DEPLOY\Xerox\Xerox Print Drivers 2.32.0.mpkg. When prompted to select a printer, continue without making a selection.
* Next, go to System Preferences / Printers and Scanners ; and click the + in the lower left corner to “Add Printer or Scanner.”
* Select IP at the top menu; and enter the following information:

Address: C3PIPRINT1

Name: C3-COLORQUBE-92XX

Use: Drop down and choose “Select Software.” Then from the Printer Software box, choose Xerox ColorQube 9202, 2.32.0.

* Click Add. If you receive an error message, click repair.
* When the option to make changes to printer options comes up, don’t change any settings.

**Enable FileVault 2**

* While still logged in as the user, create a mobile account. To do so, go to System Preferences / Users and Groups.
* Unlock the box and choose the user’s profile; and create a mobile account. Take all defaults. At this point, you will be directed to “Enter the password to create a mobile account.” After entering the password, the user will be logged off.
* Log into the system with the *DTService* account
* Open *System Preferences* and select *Security and Privacy*.
* Click on the lock and enter the admin password
* Select *FileVault* and then click *Turn On FileVault.*
* When prompted, enable both the End User and DTservice accounts.
* You’ll be given a Recovery Key, copy (**Command – Shift – 4**) it to the desktop; and rename it to the computer’s name. To rename, right click the file, Get Info / Name and Extension / and change to machine name. After renaming , move to smb://10.32.39.186/Windows7/FileVault Recovery Key.
* Do not store the recovery key with Apple.
* System will restart and begin the drive encryption

**Note: Any user not configured in FileVault will not be able to logon to the system.**

**Data Migration**

* If the user is moving from a PC to a Mac, the data files, pst’s, IE Favorites, etc. will need to be migrated. In order for this to happen, the following steps will need to occur.
* The user’s IE Favorites will need to be exported to the PC’s desktop. This export can be done by going into IE / click the Favorites button / Add to Favorites drop down selection / Import and Export / select Export to a file / select Favorites and Cookies / Next / select the user’s desktop as the file location for both Favorites and Cookies / choose Export. The file is then created and can be moved when the other desktop files are copied. If applicable, do the same with the FireFox and Chrome bookmarks.
* Upload the user’s My Documents, Desktop files, C: root files, etc. to a pre-created folder in the smb:[//10.32.39.186/windows7/usmt\_data](\\\\10.32.39.186\\windows7\\usmt_data) directory; or use the admin share method by going to Finder / Go / Connect to Server and mapping a drive to the PC (smb://*computer name*/c$ ).
* After all files have been copied by either method, they then need to be copied to the Mac’s hard drive (***asset#username-m)*** / Users / *user’s profile* / Documents. These contents can be copied by selecting CMD – A (same as CLT – A in Windows) and copy.
* To add the previously created IE bookmark.htm file to Safari, open Safari / Safari menu bar select File / Import Bookmarks / and choose the bookmark.htm file. The same would apply to adding the FireFox and Chrome bookmarks to their respective browsers.
* While in Safari, enable Safari attachment protection by opening Safari / Preferences / General tab and uncheck “Open safe files after downloading.” Also, to set inside.premierinc.com as the homepage, go to Safari / Preferences and select inside.premierinc.com as homepage. Choose “New Windows open with:” to homepage. While logged in as the user, login to inside.premierinc.com; and if prompted for user credentials, login as CORP\*username* and check the keychain box.
* After several login boxes (inside.premierinc.com, home.premierinc.com, share.premierinc.com) have appeared and the credentials entered, open Keychain / login and find each of the above entries.
* Double-click each entry; and select Access Control tab. Check to ensure Safari is listed.
* Select “Allow all applications to access this item.” Save Changes.
* When “Do you want to trust the website ‘inside.premierinc.com’ “ appears, choose “Trust.”
* Close Safari and reopen, checking to see if any further login boxes appear.

**Mozy**

To install the Mozy client, perform the following steps:

* Open the Mozy console (mozy.com).
* Select (L side), “Add New User.”
* Choose the applicable group from the dropdown.
* Define a profile. From the “What type of user” dropdown, select “Desktop.” Don’t set a storage limit.
* Enter the user’s information and uncheck “Send user instructions email.”
* Select “Add Users.” After the user is added, select (L side) and choose “Search / List Users.” Search for the newly added employee (ex. Nolan\_sanders) and once found, select.
* Once the account is found, select “Change User Password” and change the password to **Premier1a**. Confirm the password and select “Save Changes.”
* Next, select (L side) “Download MozyPro Client.” Choose the “Current Release (Recommended)” for the Mac. Once downloaded, open the client and choose “MozyPro Installer.” Take all the defaults and install.
* A MozyPro box will appear. Provide the requested information and choose “Next.” Select “Preferences” and a file scan should occur. At this point, lock the box and close.

**Final Steps**

* To Create multiple desktops windows, use 3 fingers to swipe up and click on the + sign in the upper, right corner. You can also move between workspaces by using 4 fingers horizontally. To add additional desktops, use the + sign in the upper, right corner.
* For those employees who will be using the View client, download the View Client for Mac OS from <https://view.premierinc.com>. Expand and move this to the Applications folder. As mentioned previously, this **requires a license**. Once created, View should be opened in the Desktop 2 window; and pinned to the dock for ease of use.
* If the user had previously mapped drives on their PC, go to Finder / Go / Connect to Server. In the Server Address box, type in the path, preceded by smb:// (ex. smb://10.32.39.186/windows7). Once you have designated the path, select the + sign to the right. This will add it to the “Favorite Servers” box. This will be the equivalent of a mapped drive.
* Under Finder / Preferences / Sidebar / Favorites list, check the user’s folder (house symbol); and under Devices, check the the computer’s name. In the same area, choose the General tab, and select “Connected servers.”
* In the RSA console or on the user’s previous PC / Mac, check to see what type of VPN token (physical or soft) is being used. If a soft token is being used, you can find the software (RSASecurIDMac412.dmg) in the MacDeploy / RSA\_SecureID\_Client – FOR MAC /MacOSX folder.
* Open Outlook and manually configure for the user’s Exchange account. Once it has connected and synchronized, import the [client’s pst’s](http://support.microsoft.com/kb/2413370) and setup the [signature file](http://support.microsoft.com/kb/2455171). If the signature file was copied from the previous PC, it can be copied and added using the previous link. To add any Outlook pst files, open Outlook / File / Import / select Outlook Data File / Outlook for Windows Data File / locate the file, choose Import and select Done. In addition, should there be a need to add a shared mailbox, please follow the instructions in this [link](http://www.tr.txstate.edu/get-connected/computerservices/e-mail-setup/outlook2011-mac-shared.html).
* Install the StarTech dongle software (AX88179.dmg). It can be found in the MacDeploy / Startech\_USB\_Dongle / ASIX\_AX88179 / Mac /OSX 10.9 folder. Insert the StarTech dongle, reboot the Mac and test for connectivity.
* Remove any folder’s (i.e. MacDeploy) from the user’s desktop and empty the Trash.