OS X 10.13 CIS Configuration Benchmark Setup Guide

While connected to AC Power and the ORAU network (locally or through VPN).

Part One: Configure the System

Because these changes are system-level (system-wide) changes, they effect *all* users and thus only need to be configured *one* time. Account-level changes will need to be repeated on a per-account basis.

1. Login as itsadmin

If the account doesn't exist, create it now.

*** Verify Computer Name is Property # or change in Sharing/ Computer Name

2. Run the System Setup Script

Run the system_setup.sh script as follows:

1. Open Utilities (Shift+CMD+U)
2. Launch Terminal
3. Using the Finder, click on the script file and drag it to the Terminal window, release it once the cursor is over the window. The path to the script should populate in the appropriate line so that it can be executed.
4. Press Enter to execute the script. You will be asked to Authenticate a number of times.

Manual Configuration Instructions

Note: These tasks can be performed while the system setup script is running in the background by opening another Terminal window. *Be sure not to close the Terminal that is running the script.*

1. Restrict NTP Server to Loopback Interface (CIS 2.2.3)

1. Open Utilities (Shift+CMD+U)
2. Launch Terminal
3. Type sudo vi /etc/ntp-restrict.conf.
4. Type i to enable editing/text insertion.
5. Use the arrow keys to navigate to an empty line below the other lines beginning with "restrict".
6. Type restrict lo interface ignore wildcard interface listen lo.
7. Press the ESC key to disable editing/text insertion.
8. Type ':wq' to Save and Quit.

2. Disable ability to login to another user's active and locked session (CIS 5.11)

1. Open Utilities (Shift+CMD+U)
2. Launch Terminal
3. Type sudo vi /etc/pam.d/screensaver.
4. Type i to enable editing/text insertion.

5. Use the arrow keys to navigate to account required pam_group.so no_warn group=admin,wheel fail_safe.
6. Delete admin *and the trailing comma* from this line.
7. The result should look like this: account required pam_group.so no_warn group=wheel fail_safe
8. Press the ESC key to disable editing/text insertion.
9. Type ':wq' to Save and Quit.

3. Disable the Remote Control Infrared Receiver (CIS 2.9)

If the user **does not have (or is not using)** a remote control for their device, the IR Receiver should be disabled.

1. Open System Preferences
2. Select Security & Privacy
3. Select the General tab
4. Click the "lock" at the bottom-left of the window, to unlock the Advanced section.
5. Select Advanced
6. Check Disable remote control infrared receiver.

If the user *does* have a remote control for their device, it should be paired so that no other remotes can control that device.

1. Holding the remote close to the computer, point the remote at the front of the computer.
2. Pair the Apple Remote.
   - If you have an Apple Remote with seven buttons, press and hold both the Right and Menu buttons on the remote until the paired-remote icon appears on your screen.
   - If you have an Apple Remote with six buttons, press and hold both the Next and Menu buttons on the remote until the paired-remote icon appears on your screen.

4. Ensure users do not enter a password-related hint (CIS 5.14)

1. Using an Administrator account, Open System Preferences
2. Launch Users & Groups
3. Highlight a user account
4. Select Change Password
   - *It may be necessary to first click the 'lock' icon at the bottom left of the window to unlock this option.*
5. Verify that no text is entered in the Password hint box

5. Grant Temporary Admin Rights to All Accounts

1. Using an Administrator account, Open System Preferences
2. Launch Users & Groups
3. Highlight a user account
4. Check Allow user to administer this device (sic).
5. Do this for each of the three accounts on the device.

6. Disable Bluetooth (CIS 2.1.1)

If the user is not using a wireless Bluetooth keyboard, mouse, or other device then Bluetooth connectivity must be disabled.

1. Open System Preferences.
2. Double-click on the Bluetooth icon.
3. By default, there may be a Bluetooth mouse and keyboard listed in the Devices section of this screen. If they are not being utilized by the user, select each device and remove them from the list.
4. Click Turn off Bluetooth.

Part Two: Configure User Accounts

Because these changes are account-level, they will need to be repeated for each account on the system; unlike the system-level changes above.

1. Run the User Setup Script

Run the user_setup.sh script as follows:

1. Open Terminal (Shift+CMD+U to open Utilities then double-click on Terminal to open.)
2. Using the Finder, click on the script file and drag it to the Terminal window, release it once the cursor is over the window. The path to the script should populate in the appropriate line so that it can be executed.
3. Press Enter to execute the script. You will be asked to authenticate a number of times.

2. Disable iCloud Drive Document and Desktop Sync (CIS 2.7.4 and 2.7.5)

If the user has an active iCloud account, Drive Document Sync **must** be disabled. *This may only be necessary for the main user account as the local admin and ITSAdmin accounts shouldn't have iCloud activated at all.*

1. Open System Preferences
2. Launch iCloud
3. Select iCloud Drive
4. Select Options next to iCloud Drive
5. Uncheck Desktop & Documents Folders

3. Enable Secure Keyboard Entry in Terminal (CIS 2.10)

1. Open Utilities (Shift+CMD+U)
2. Launch Terminal
3. Click Terminal in the menu bar at the top of the screen
4. Select Secure Keyboard Entry.

4. Automatically lock the 'login' keychain for inactivity or sleep (CIS 5.7 and 5.8)

1. Open Utilities (Shift+CMD+U)
2. Launch Keychain Access

3. Select the login keychain.
4. Select Edit (from the menu bar at the top of the screen)
5. Select Change Settings for keychain 'login'
6. Authenticate, if requested.
7. Change the Lock after # minutes of inactivity setting for the Login Keychain to 360.
8. Select 'Lock when sleeping' setting

5. Repeat 'Part Two' for each remaining account on the system.

6. Restart the Device

Part Three

Perform the audit on each of the 3 accounts on the sytem.

Performing the CIS Security Benchmark Audit:

1. Open Utilities (Shift+CMD+U)
2. Launch Terminal
3. Open Finder (click the blue 'Mac' logo on the far left of the bottom bar.)
4. Run the audit.sh script by dragging the script from its location in the finder window to the Terminal window.
5. The path and file name of the audit script should now be populated in the Terminal console.
6. Following the path to the audit script, type:
    - > $HOME/Documents/audit_results_{accountname}.html
        - where {accountname} is the name of the current active account.
        - example: /Volumes/MyThumbDrive/audit.sh > $HOME/Documents/audit_results_username.html
        - The resulting file can be found in the Documents folder belonging to the current account.
    - Alternatively, you can choose a different path instead; perhaps to your thumbdrive:
        - > /Volumes/{drivename}/audit_results_{accountname}.html
        - Where {drivename} is the name of the drive as listed in the Finder window/desktop.
    - This enables the audit script to output its results to an easy-to-read, HTML formatted document.
7. **Note**: Expect items 2.6.1 and 5.3 to be Non-compliant until the final audit is performed. They are very time-consuming processes.
8. Open the resulting HTML audit results document and take note of any items other than the above which are marked Non-compliant and verify that those tagged as "Manual" meet the indicated measure of compliance.
9. Perform any suggested remediation steps for the non-compliant items (excluding 2.6.1 and 5.3).
10. Once the audit results are as expected, switch to another account and repeat the audit. * No need to run ITSAdmin since running as Final.

Part Four

Final Remediation Steps - System Level

As ITSAdmin, perform the following tasks in the following order:

1. Reduce the sudo timeout period (CIS 5.3)

1. Open Utilities (Shift+CMD+U)
2. Launch Terminal
3. Type sudo visudo
4. Type i to enable editing/text insertion.
5. Use the arrow keys to navigate to an empty line below the section header labeled # Override built-in defaults.
6. Type Defaults timestamp_timeout=0 (press enter to insert a new line if needed)
7. Press the ESC key to disable editing/text insertion.
8. Type ':wq' to Save and Quit.

2. Enable FileVault (CIS 2.6.1)

1. Open System Preferences
2. Launch Security & Privacy
3. Select FileVault
4. Select Turn on FileVault
5. Enable all 3 listed accounts to unlock the drive at startup[1].

3. Turn off Share Mac Analytics (CIS 2.6.8)

1. Open System Preferences
2. Launch Security & Privacy
3. Select Privacy
4. Select Analytics
5. Ensure that 'Share Mac Analytics' is not selected

1: I don't think we have an established, explicit rule for this, though. At a minimum, the ITSAdmin and standard user account should be able to unlock the drive.

Part Six

Final Audit

Using the ITSAdmin account run the audit.sh script as indicated above, this time adding _final just before the file extension like so; audit_results_{accountname}_final.html. This will ensure that the previous results are not overwritten and to differentiate our results.

You'll notice that you are prompted to Authenticate **far more often** than previous audits. This is an effect of enabling 5.3 and is to be expected.

Ensure that all items are marked Compliant (where applicable) and manually verify those tagged as "Manual" meet compliance standards. **All** items should now be Compliant.

Remove Temporary Admin Rights from User Account

1. Using an Administrator account, Open System Preferences
2. Launch Users & Groups
3. Highlight/select the standard user account
4. Uncheck Allow user to administer this device (sic).

You may now change the account passwords, if necessary, and return the device to its owner.

Install Symantec and update

Install Nessus Agent. Run sudo command after install in nessus.txt file. Verify running.

NOTES:

2.4.2 - Per Craig, script is only looking for one network interface. Results may have multiple networks.

5.1.1 - Per Craig's setup document, 'drwx' is an acceptable result