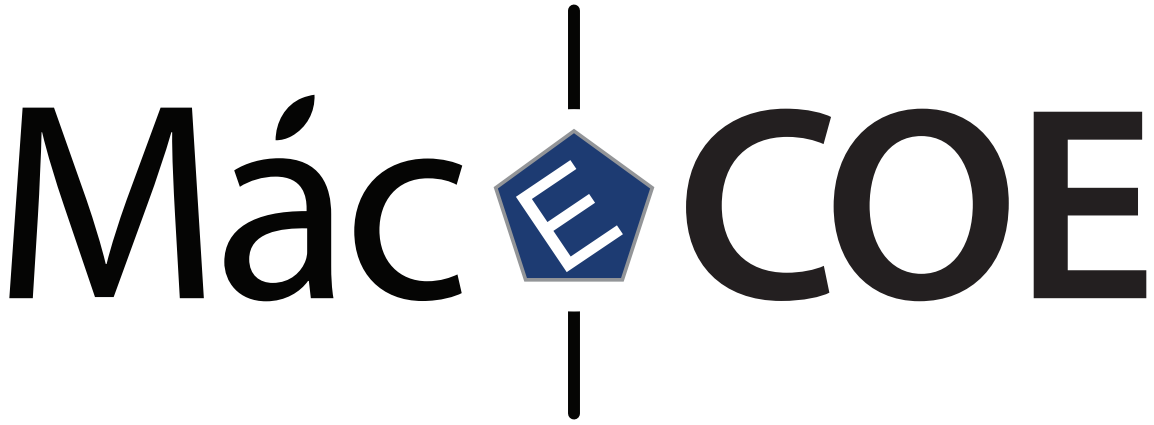


Secure Host Baseline Guide:
OS X El Capitan SHB Image Creation

Version 1.0

Revision History

Version	Date	Revision Description	Revised by
1.0	2015-06-04	Initial version	Daniel Brodjieski, Sr. Macintosh Engineer, Mac COE

Approving Official

_____

Monica Langley
Chief, Information Resource Management,
Office of the Assistant Secretary of Defense – Public Affairs

Table of Contents

1.0 INTRODUCTION

The Joint Service Provider (JSP) Macintosh Center of Excellence (Mac COE) created the OS X El Capitan SHB Image Creation Tools and this accompanying Deployment Guide. The image created is based on the requirements of the Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIG).

The process outlined here is used to create the Secure Host Baseline (SHB) for OS X El Capitan. The end result of this process will be:

- A DMG image file that has the STIG requirements already configured and includes the baseline VirusScan engine from McAfee

This process offers flexibility to agencies that may need to add required software packages and other components. Depending on the environment in which the SHB is to be used, there may be additional configuration that needs to take place before deployment. For example, you will need to provide configuration for CAC support, Active Directory, and HBSS integration, along with any other software that is required in your environment. The goal of the SHB is to make the process as straightforward as possible, so that these configurations are easy to integrate in each environment.

1.1 Purpose

This guide is for Macintosh system administrators and engineers who deploy a secure image in their environment. The guide and packaged scripts are being made available to members of the DoD, and must not be distributed outside of those authorized members.

1.2 STIG Compliance

The SHB has been developed to meet the requirements as outlined in the DISA STIG for OS X 10.11 El Capitan. There are some requirements that are dependent on external factors that must be addressed in each environment. Some of these settings could not be automated, and must be configured manually to ensure compliance.

The following table outlines the STIG requirements that are not met automatically in the SHB.

STIG ID	Description	SHB Notes
AOSX-11-000110	The operating system must automatically remove or disable temporary user accounts after 72 hours.	There are no temporary user accounts included with the SHB. If temporary user accounts are added to the system, they should be automatically removed or disabled according to the STIG requirement.

STIG ID	Description	SHB Notes
AOSX-11-000155	The system firewall must be configured with a default-deny policy.	The built-in firewall does not contain an option for a default-deny policy. HBSS should be leveraged to perform the desktop firewall functions in order to meet this requirement.
AOSX-11-000750	The operating system must issue or obtain public key certificates under an appropriate certificate policy from an approved service provider.	This is a manual check to be sure all trusted certificates are correctly loaded in the keychain.
AOSX-11-000835	The operating system must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where HBSS is used; 30 days, for any additional internal network scans not covered by HBSS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).	While the SHB includes the McAfee antivirus protection, agencies should integrate their system into the HBSS solution for centralized management.
AOSX-11-001145	All **setuid** executables on the system must be vendor-supplied.	The list of files with the **setuid** executable bit set is listed in Appendix A.
AOSX-11-001235	Unused network devices must be disabled.	The default installation should have all unused network devices disabled. This requirement is not automated, and should be validated by manual means on a regular basis.
AOSX-11-001240	System Preferences must be securely configured so IPv6 is turned off if not being used.	The default installation should have IPv6 disabled. This requirement is not automated, and should be validated by manual means on a regular basis.
AOSX-11-002055	All users must use PKI authentication for login and privileged access.	There is no built-in support for smart cards in the SHB. Third-party support is available and should be obtained accordingly.
AOSX-11-002060	The system must be integrated into a directory services infrastructure.	The SHB must be configured to integrate into a local directory service infrastructure (**Active Directory**, **Open Directory**, etc.)
AOSX-11-002106	System log files must be mode 640 or less permissive.	The SHB is configured with all system log files to have the correct permissions. This requirement is not automated, and should be

STIG ID	Description	SHB Notes
		validated by manual means on a regular basis.
AOSX-11-002107	ACLs for system log files must be set correctly.	The SHB is configured with all system log files to have the correct ACL settings. This requirement is not automated, and should be validated by manual means on a regular basis.

Please review the entire contents of this guide to better understand the processes involved.

1.3 Contacts

For more information about this document, please contact the following department:

Table 1-1: Contacts

Contact Name	Organization/Role	E-Mail
Daniel Brodjieski	WHS-JSP-Mac COE – Sr. Engineer	daniel.d.brodjieski.ctr@mail.mil

2.0 BACKGROUND

2.1 Installation Prerequisites

Software requirements

1. **AutoSHB**
   Available for download on the DoD SHB website
2. **Install OS X El Capitan.app**
   Available from Apple App Store

Hardware requirements

- You must be running the image creation process on a system with OS X 10.11 El Capitan installed.
- It is advised that you run the latest version available from Apple.

2.2 Third-Party Software

In addition to using this guide to configure an Apple computer in your environment, you may require installers for third-party applications (for example, Firefox, Chrome, Photoshop, etc.). If you or your agency requires third-party applications, your agency is responsible for acquiring, testing, and maintaining them.

The software can be included in the SHB creation process. See step 5 of section 3.3.1 below or use your own post-imaging deployment method.

2.3 References

Apple OS X 10.11 Workstation STIG, Version 1 has been published by DISA. It is available from <**http://iase.disa.mil/stigs/os/mac**>.

3.0 CREATION OF THE STIG IMAGE

3.1 About the Creation of the Image

The Mac COE created a configuration package to provide the settings and environment required to configure the image based on the Apple OS X 10.11 Workstation STIG, Version 1 (2016-04-12).

3.2 mil.osd.STIG-10.11.SHB.pkg

The **mil.osd.STIG-10.11.SHB.pkg** contains the configuration files needed for the image to configure itself on first boot.

This package installs the **/var/shb** folder, configuration files, and a launch daemon. The launch daemon is configured to initiate a first-run script to configure the standard OS X installation to the required settings for STIG compliance.

- Configures no multicast advertisements for Bonjour
- Configures the system to hide accounts with UID less than 500
- Disables unused network devices
  - Disables Thunderbolt bridge
  - Disables Bluetooth DUN
  - Disables Bluetooth PAN
  - Disables FireWire
  - Disables Wi-Fi (except for laptops)
- Disables IPv6 for Ethernet
- Configures user template
  - Disables iCloud setup screen for new accounts
  - Configures the default Dock
- Configures /**etc/sysctl.conf**
  - Disables Kernel core dumps
  - Disables ICMP responses to broadcast traffic
  - Disables source-routed IPv4 packets
  - Disables IPv4 ICMP redirect messages
  - Disables IP forwarding for IPv4
  - Disables ICMP timestamp responses
- Enables the firewall
  - Sets global state to **on**
  - Turns on logging
- Disables USBMUXD
- Configures App Store to not check automatically for updates
- Disables automatic actions for CD/DVDs in user template
    - Copy **/var/shb/com.apple.digihub.plist** to /**System/Library/User\ Template/English.lproj/Library/Preferences/**

- Set the DoD policy banner
    - Copy **/var/shb/PolicyBanner.rtfd** to **/Library/Security/**
- Configure audit logging
    - Copy **/var/shb/audit_control** to **/etc/security/**
- Configure SSH server settings
    - Copy **/var/shb/sshd_config** to **/etc/ssh/**
- Configure SSH client settings
    - Copy **/var/shb/ssh_config** to **/etc/ssh/**
- **C**onfigures sudo to authenticate users on a per-tty basis
    - Copy **/var/shb/sudoers** to **/etc/**

3.3 Image Creation

3.3.1 Download the required files

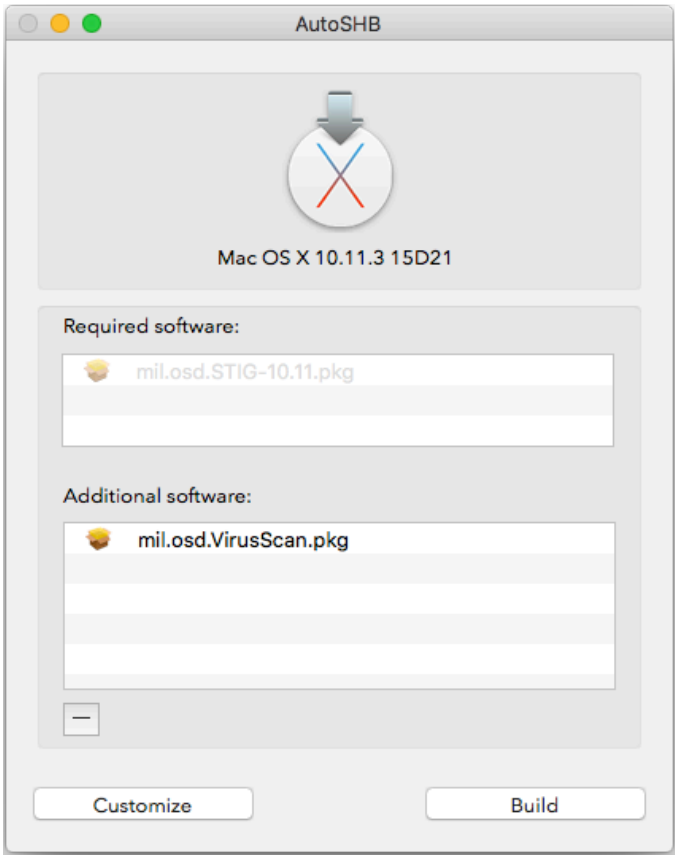
1. Download “AutoSHB.app” from the SHB repository.
2. Download “Install OS X El Capitan.app” from the Mac App Store

3.3.2 Running AutoSHB

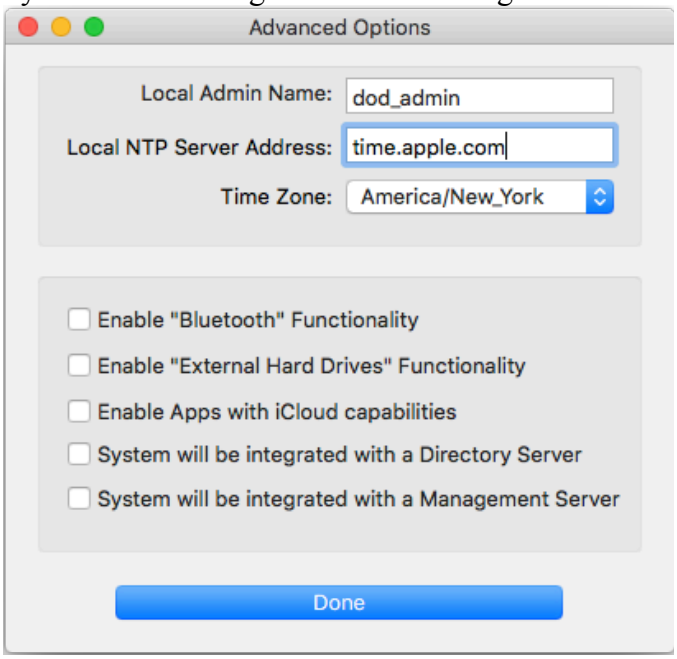
3. Launch AutoSHB.app by double clicking the icon.

4. Drag and drop the Install OS X El Capitan.app file to the upper section of the AutoSHB application window.

5. In the Additional software window, drag and drop any additional software packages you would like to have installed onto the image. By default the McAfee VirusScan engine is added.

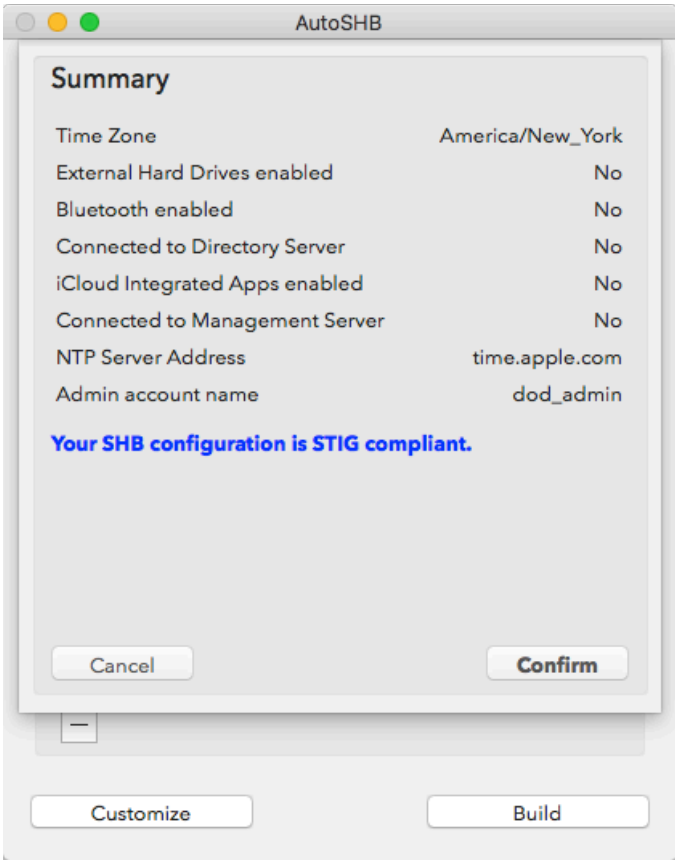


6. Click on 'Customize' to make changes to the default configuration settings.
    a. Type in the name you would like for the local administrator
    b. Enter a NTP server address to use.
    c. Select your local time zone.
    d. Options (these options may alter compliance with the STIG):
        i. Enable Bluetooth Functionality
        ii. Enable External Hard Drive functionality
        iii. Enable Apps with iCloud capabilities
        iv. System will be integrated with a Directory Server
        v. System will be integrated with a Management Server



7. Click **Done** when settings are complete.
8. Click Build to begin creating the image.

9. You will be presented with a summary of your configured settings. Click Confirm.



10. Choose a destination to save the image, and click Save.

4.0 DEPLOYMENT

The image can be deployed using any preferred method of Macintosh image deployment. Examples would be Disk Utility, Filewave, Casper Imaging, or DeployStudio. This document will not cover specific methods, and assumes the audience is well versed in their method of choice.

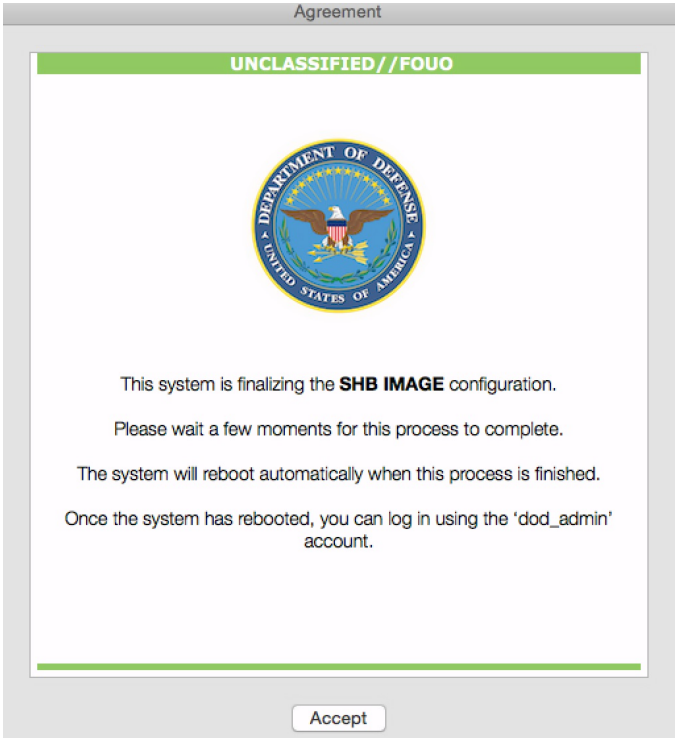
5.0 POST-DEPLOYMENT OPERATIONS

This section provides the additional steps required to make the STIG image fully operational in various environments.

5.1 First Boot

After you boot the STIG image for the first time, a banner will appear to notify you that background processes are still running. Depending on your system, this screen may not appear, as the processing of the first boot script may complete before this screen is available.

Note: At this point, do *not* click **Accept**; please wait while the processes are completed.



After the machine has rebooted and this screen has been replaced by a standard DoD **Agreement** screen, then click **Accept**.

Log in using the administrator account you created during the SHB creation; the default account is **'dod_admin'**. There is no initial password for this account so you will be prompted to create one of your choosing. Be sure the password meets the STIG requirements for acceptable complexity.

After you have implemented the above configurations, you can then make other appropriate configuration changes for your environment. Be sure to get approval from your AO for an exception to deviate from the STIG.

5.2 About the .mobileconfig files

The STIG image includes default Configuration Profiles that are applied during the First Boot process. The profile provides a number of settings that are outlined in the STIG. The Configuration Profiles can be altered as needed for your individual environment. Either the default or custom profile should be applied in accordance with the STIG. The default configuration profiles can be found here:

```
/var/shb/Configuration Profiles/
   U_Apple_OS_X_10-11_V1R1_STIG_Application_Restrictions_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Bluetooth_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Custom_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Disable_iCloud_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Login_Window_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Passcode_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Restrictions_Policy.mobileconfig
   U_Apple_OS_X_10-11_V1R1_STIG_Security_and_Privacy_Policy.mobileconfig
```

6.0 CONTENTS OF MIL.OSD.STIG-10.11.PKG

File/Directory	Description	Use
/Library/LaunchDaemons/mil.osd.SHB-FirstRun.plist	LaunchDaemon to start the STIG-10.11.sh script.	This will only run during the first run, and will be removed automatically to prevent it from running again.
/Library/Security/PolicyBanner.rtfd	This is the initial banner that indicates that there are background processes running.	Once the system finishes the first run setup, this file is replaced by the DOD acceptable use banner.
/var/shb/	This is the folder containing setup files and configurations needed for the STIG image.	See the table in section 6.0 for further information.

7.0 CONTENTS OF /VAR/SHB

This folder contains a number of files for use with the SHB image.

File/Directory	Description	Use
audit_control	Configuration file for the BSM auditing service	This file is copied to /**etc/security**/ during the STIG image first run.
com.apple.digihub.plist	Configuration file for CD/DVD actions, with settings from STIG	This file is copied to the user template folder during the STIG image first run.
com.apple.dock.plist	Configuration file for user's initial dock to account for removed applications	This file is copied to the user template folder during the STIG image first run.
Configuration Profiles	This folder contains the DISA-provided **.mobileconfig** files.	
U_Apple_OS_X_10-11_V1R1_STIG_Application_Restrictions_Policy.mobileconfig	Configuration profile containing the Application Restriction settings	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Bluetooth_Policy.mobileconfig	Configuration profile containing the Bluetooth settings	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Login_Window_Policy.mobileconfig	Configuration profile containing the Login Window settings	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Custom_Policy.mobilconfig	Configuration profile containing the Custom settings	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Disable_iCloud_Policy.mobileconfig	Configuration profile containing the policy to disable the iCloud prompts.	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Passcode_Policy.mobileconfig	Configuration profile containing the passcode settings	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Restrictions_Policy.mobileconfig	Configuration profile containing the restrictions settings	This profile can be modified accordingly and applied to the system.
U_Apple_OS_X_10-11_V1R1_STIG_Security_and_Privacy_Policy.mobileconfig	Configuration profile containing the Security and Privacy settings	This profile can be modified accordingly and applied to the system.
STIG-10.11.sh	Script for securing the STIG image	This script is run as part of the first boot process.

File/Directory	Description	Use
ssh_config	Configuration file for SSH client, with settings from STIG	This file is copied to /etc/ssh/ during the STIG image first run.
sshd_config	Configuration file for SSH server, with settings from STIG	This file is copied to /etc/ssh/ during the STIG image first run.
sudoers	Configuration for ‘sudo’	This file is copied to /etc/ during the STIG image first run.

8.0 CONTENTS OF STIG-10.11.SH

```
#!/bin/bash

######### Set Environment
PATH=/usr/libexec:$PATH

######### Global Variables
shbRootDir=/private/var/shb

logContext="OS X STIG"
hwModel=$(system_profiler SPHardwareDataType | grep "Model Identifier" | awk '{print
        $3}' | cut -f1 -d ",")

userTemplateDir="/System/Library/User Template/English.lproj"
preferencesDir="/Library/Preferences"
setupAssistantPreferences="${userTemplateDir}${preferencesDir}/com.apple.SetupAssistant"

configProfilesDir="${shbRootDir}/Configuration Profiles"

# Determine OS version
sw_vers=$(sw_vers -productVersion)

# Determine OS build number

sw_build=$(sw_vers -buildVersion)

# Determin HW UUID
HWUUID=$(/usr/sbin/system_profiler SPHardwareDataType 2> /dev/null | /usr/bin/grep
        "Hardware UUID" | /usr/bin/cut -c22-57)

# Determine if this is run at first boot
[[ -f /Library/LaunchDaemons/mil.osd.SHB-FirstRun.plist ]] && firstRun=1

######### Get SHB customized settings from /var/shb/imageinfo.plist
ntp_server=$(PlistBuddy -c "print LocalSettings:ntpAddress"
        ${shbRootDir}/imageinfo.plist)
time_zone=$(PlistBuddy -c "print LocalSettings:timeZone" ${shbRootDir}/imageinfo.plist)
connected_to_DS=$(PlistBuddy -c "print LocalSettings:connectedToDS"
        ${shbRootDir}/imageinfo.plist)
connected_to_MS=$(PlistBuddy -c "print LocalSettings:connectedToMS"
        ${shbRootDir}/imageinfo.plist)
admin_account=$(PlistBuddy -c "print LocalSettings:adminAccountName"
        ${shbRootDir}/imageinfo.plist)
shbVersion=$(PlistBuddy -c "print LocalSettings:SHBVersion"
        ${shbRootDir}/imageinfo.plist)
ImageCreationTime=$(PlistBuddy -c "print LocalSettings:ImageCreationTime"
        ${shbRootDir}/imageinfo.plist)
enableBluetooth=$(PlistBuddy -c "print LocalSettings:enableBluetooth"
        ${shbRootDir}/imageinfo.plist)
enableCDBurning=$(PlistBuddy -c "print LocalSettings:enableCDBurning"
        ${shbRootDir}/imageinfo.plist)
```

```
enableExternalHD=$(PlistBuddy -c "print LocalSettings:enableExternalHD"
       ${shbRootDir}/imageinfo.plist)
allowiCloudApps=$(PlistBuddy -c "print LocalSettings:allowiCloudApps"
       ${shbRootDir}/imageinfo.plist)

######### Various Functions

disableUnusedNetworkServices(){
oIFS=$IFS
IFS=$'\n'

enabledNetworkServices=($(networksetup -listallnetworkservices | grep -v "\*"))

hwModel=$(system_profiler SPHardwareDataType | grep "Model Identifier" | awk '{print
       $3}' | cut -f1 -d ",")

if [[ $hwModel == *Book* ]]; then
       logger "$logContext - Disabling all network services except Ethernet or Wi-
       Fi..."

       for i in ${enabledNetworkServices[@]}; do
          if [[ ! $i == *Ethernet* ]] && [[ ! $i == *Wi-Fi* ]]; then
                 logger "$logContext - Disabling $i"
                 networksetup -setnetworkserviceenabled "$i" off
          fi
       done
else
       echo "$logContext - Disabling all network services except Ethernet"
       for i in ${enabledNetworkServices[@]}; do
          if [[ ! $i == *Ethernet* ]]; then
                 logger "$logContext - Disabling $i"
                 networksetup -setnetworkserviceenabled "$i" off
          fi
       done
fi

IFS="$oIFS"
}

disableIPV6(){

oIFS="$IFS"
IFS=$'\n'

enabledNetworkservices=( $(networksetup -listallnetworkservices | grep -v "\*") )


##  Disable ipv6 for all services.
for i in "${enabledNetworkservices[@]}"; do
    logger "$logContext - Disabling IPv6 for enabled network services..."
    networksetup -setv6off "$i"
done

IFS="$oIFS"
```

```
}


######## Apply the STIG configuration

## Set the Time Zone
[[ ! -z "$time_zone" ]] && systemsetup -settimezone "$time_zone"

## Set and enable network time server
if [[ ! -z "$ntp_server" ]]; then
        systemsetup -setnetworktimeserver "$ntp_server"
        systemsetup -setusingnetworktime on
fi

## configure the overrides

logger "$logContext - Configuring the overrides ..."

launchctl disable system/com.apple.telnetd
launchctl disable system/com.apple.AppleFileServer
launchctl disable system/com.apple.nfsd
launchctl disable system/com.apple.lockd
launchctl disable system/com.apple.statd.notify
launchctl disable system/com.apple.racoon
launchctl disable system/com.apple.findmymacd
launchctl disable system/com.apple.findmymacmessenger
launchctl disable system/com.apple.NetworkSharing
launchctl disable system/com.apple.fingerd
launchctl disable system/com.apple.screensharing
launchctl disable system/com.apple.uucp
launchctl disable system/com.apple.AEServer
launchctl disable system/com.apple.ODSAgent
launchctl disable system/com.apple.rexecd
launchctl disable system/com.apple.rshd
launchctl disable system/org.apache.httpd
launchctl disable system/com.apple.smbd


## disable bonjour multicastadvertisements

logger "$logContext - Disabling bonjour multicast advertisements ..."

/usr/bin/defaults write /Library/Preferences/com.apple.mDNSResponder.plist
        NoMulticastAdvertisements -bool true

## Hide admin accounts

logger "$logContext - Hiding admin accounts ..."

defaults write /Library/Preferences/com.apple.loginwindow Hide500Users -bool yes

## Disable unused network services

logger "$logContext - Disabling unused network services ..."
```

```
disableUnusedNetworkServices

## Disable ipv6 for network services

logger "$logContext - Disabling IPv6 for network services ..."

disableIPV6

## user template configuration

logger "$logContext - Configuring user template ..."

for USER_TEMPLATE in "/System/Library/User Template"/*
  do
    cp "${shbRootDir}/com.apple.dock.plist" "${USER_TEMPLATE}${preferencesDir}"
    cp "${shbRootDir}/com.apple.digihub.plist" "${USER_TEMPLATE}${preferencesDir}"

done

## create the /etc/sysctl.conf file, re-write if it exists

if [ -f "/etc/sysctl.conf" ]; then
       rm -f /etc/sysctl.conf
fi

echo "kern.coredump=0" >> /etc/sysctl.conf
echo "net.inet.icmp.bmcastecho=1" >> /etc/sysctl.conf
echo "net.inet.ip.accept_sourceroute=0" >> /etc/sysctl.conf
echo "net.inet.icmp.drop_redirect=1" >> /etc/sysctl.conf
echo "net.inet.ip.forwarding=0" >> /etc/sysctl.conf
echo "net.inet.ip.redirect=0" >> /etc/sysctl.conf
echo "net.inet.ip.sourceroute=0" >> /etc/sysctl.conf
echo "net.inet.icmp.timestamp=0" >> /etc/sysctl.conf
echo "net.inet6.ip6.forwarding=0" >> /etc/sysctl.conf
echo "net.inet6.ip6.redirect=0" >> /etc/sysctl.conf


## Configure ssh and sshd

logger "$logContext - Configuring ssh and sshd ..."

cp ${shbRootDir}/ssh_config /etc/ssh/
cp ${shbRootDir}/sshd_config /etc/ssh/

## Configure auditing

logger "$logContext - Configuring the auditing system ..."

cp ${shbRootDir}/audit_control /etc/security/


## set the logging correctly for audit_warn
sudo sed -i '' 's/logger -p/logger -s -p/' /etc/security/audit_warn; sudo audit -s
```

```
## Configure sudoers file

logger "$logContext - Configuring the sudoers file ..."

cp ${shbRootDir}/sudoers /etc/

## enable the firewall

logger "$logContext - Enabling the firewall ..."

/usr/libexec/ApplicationFirewall/socketfilterfw --setglobalstate on
/usr/libexec/ApplicationFirewall/socketfilterfw --setloggingmode on


## Disable USBMUXD

logger "$logContext - Disabling USBMUXD ..."

#launchctl unload -w /System/Library/LaunchDaemons/com.apple.usbmuxd.plist
/bin/launchctl disable system/com.apple.usbmuxd

## Disable IR support

logger "$logContext - Disabling IR support ..."

defaults write /Library/Preferences/com.apple.driver.AppleIRController DeviceEnabled -
       bool FALSE

## Disable automatic software updates

logger "$logContext - Disabling automatic software updates ..."

defaults write /Library/Preferences/com.apple.SoftwareUpdate AutomaticCheckEnabled -bool
       FALSE

## Add the DOD certificates to the keychain
security list-keychains -d common -s
       /System/Library/Keychains/SystemCACertificates.keychain

## Remove ACLs from log files
find /var/log/ -acl -exec chmod -N {} \;

## if this is run during initial boot create admin user and set password to change on
       next login, currently is blank
if [[ $firstRun == 1 ]]; then
       logger "$logContext - Creating local admin account ${admin_account}..."
       dscl . -create "/Users/${admin_account}" UniqueID 499
       dscl . -create "/Users/${admin_account}" PrimaryGroupID 20
       dscl . -create "/Users/${admin_account}" NFSHomeDirectory
       "/var/${admin_account}"
       dscl . -create "/Users/${admin_account}" UserShell /bin/bash
       dscl . -create "/Users/${admin_account}" RealName "SHB Administrator"
```

```
        dscl . -create "/Users/${admin_account}" Picture
        "/Library/Security/PolicyBanner.rtfd/Department-of-Defense_140px.png"
        dscl . append /Groups/admin GroupMembership ${admin_account}
        dscl . -passwd "/Users/${admin_account}" ""
        pwpolicy -u ${admin_account} -setpolicy "newPasswordRequired=1"
        touch /var/db/.AppleSetupDone
fi

## Apply the baseline DISA mobileconfig if applicable

## check to see if external hard drives should be enabled, and if so, modify the
        Restrictions mobilconfig accordingly
if [[ "$enableExternalHD" == "1" ]]; then
    sed -i.bak -e '/harddisk-external/{N;N;N;N;d;}' "${configProfilesDir}/10.11 -
        STIG_Restrictions_Policy.mobileconfig"
fi

if [[ "$allowiCloudApps" == "0" ]]; then                          # if system should allow
        iCloud enabled applications
         logger "$logContext - Applying the DISA STIG Application Restrictions Policy
        configuration profile..."
         profiles -I -F "${configProfilesDir}/10.11 -
        STIG_Application_Restrictions_Policy.mobileconfig"
else
         logger "$logContext - DISA Application Restriction Policy Configuration Profile
        will not be installed, application restrictions should be enforced by your MDM"
fi

if [[ "$connected_to_MS" == "0" ]]; then                                # if system is
        not to be managed by a MDM
        logger "$logContext - Applying the DISA STIG configuration profiles..."
        profiles -I -F "${configProfilesDir}/10.11 - STIG_Custom_Policy.mobileconfig"
        profiles -I -F "${configProfilesDir}/10.11 -
        STIG_Login_Window_Policy.mobileconfig"
        profiles -I -F "${configProfilesDir}/10.11 -
        STIG_Security_Privacy_Policy.mobileconfig"
    profiles -I -F "${configProfilesDir}/10.11 - STIG_Restrictions_Policy.mobileconfig"

else
        logger "$logContext - DISA baseline STIG Configuration Profile will not be
        installed, these settings should be enforced by your MDM"
fi

if [[ "$connected_to_DS" == "0" ]]; then                        # if system is not to be
        bound to a directory server
        logger "$logContext - Applying the DISA STIG Passcode Policy configuration
        profile..."
        profiles -I -F "${configProfilesDir}/10.11 - STIG_Passcode_Policy.mobileconfig"
else
        logger "$logContext - DISA Password Policy Configuration Profile will not be
        installed, password policies should be enforced by directory server"
fi
```

```
if [[ "$enableBluetooth" == "0" ]]; then                    # if system is not to be
       bound to a directory server
    logger "$logContext - Applying the DISA STIG Bluetooth Policy configuration
       profile..."
    profiles -I -F "${configProfilesDir}/10.11 - STIG_Bluetooth_Policy.mobileconfig"
else
    logger "$logContext - DISA Bluetooth Policy Configuration Profile will not be
       installed, ensuring other Bluetooth requirements are met."
    for USER_TEMPLATE in "/System/Library/User Template"/*
        do
        /usr/bin/defaults write
       "${USER_TEMPLATE}"/Library/Preferences/ByHost/com.apple.Bluetooth.${HWUUID}.plis
       t RemoteWakeEnabled 0
        /usr/bin/defaults write
       "${USER_TEMPLATE}"/Library/Preferences/ByHost/com.apple.Bluetooth.${HWUUID}.plis
       t PrefKeyServicesEnabled 0
    done

fi

## Install configuration profile for iCloud prompt

logger "$logContext - Applying configuration profile to disable iCloud signin prompt
       ..."

profiles -I -F "${configProfilesDir}/10.11 - STIG_Disable_iCloud_policy.mobileconfig"


## If virusscan package is ready and this is the initial boot, install it and brand the
       SHB for HBSS
if [[ -f ${shbRootDir}/VSM980-RTW-1791.pkg ]] && [[ $firstRun == 1 ]]; then
       installer -pkg ${shbRootDir}/VSM980-RTW-1791.pkg -target /
       /Library/McAfee/cma/bin/msaconfig -CustomProps1 "$shbVersion"
fi

## If McAfee VirusScan hotfix HF1088931 is available, install it
if [[ -f ${shbRootDir}/VSM980-2584-HF1088931.pkg ]] && [[ $firstRun == 1 ]]; then
       installer -pkg ${shbRootDir}/VSM980-2584-HF1088931.pkg -target /
fi



## Copy PolicyBanner into place
cp -Rp ${shbRootDir}/PolicyBanner.rtfd /Library/Security/
cp -Rp ${shbRootDir}/banner /etc/

## Clean up STIG-First Run so it doesn't run again

logger "$logContext - Cleaning up SHB First Run ..."

rm -f /Library/LaunchDaemons/mil.osd.SHB-FirstRun.plist


logger "$logContext - Configuration complete, rebooting the system..."
```

```
shutdown -r now
```

9.0 ACRONYMS

Acronym/Term	Definition
AO	Authorizing Official
BSM	Basic Security Module
CD	Compact Disc
DISA	Defense Information Systems Agency
DMG	Apple Disk Image
DoD	Department of Defense
DVD	Digital Versatile Disk
FOUO	For Official Use Only
Mac COE	Macintosh Center of Excellence
OS X	Macintosh Operating System
SHB	Secure Host Baseline
SSH	Secure Shell
STIG	Security Technical Implementation Guidelines

APPENDIX A: SETUID FILES

/bin/ps
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent
/System/Library/PrivateFrameworks/SystemAdministration.framework/Versions/A/Resources/readconfig
/usr/bin/at
/usr/bin/atq
/usr/bin/atrm
/usr/bin/batch
/usr/bin/crontab
/usr/bin/login
/usr/bin/newgrp
/usr/bin/quota
/usr/bin/su
/usr/bin/sudo
/usr/bin/top
/usr/lib/sa/sadc
/usr/libexec/authopen
/usr/libexec/security_authtrampoline
/usr/sbin/traceroute
/usr/sbin/traceroute6