

# CIS Apple macOS 11.0 Big Sur Benchmark

v2.0.0 - 11-01-2021

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

## Table of Contents

Terms of Use .....	1
Overview.....	7
Intended Audience .....	7
Consensus Guidance .....	8
Typographical Conventions.....	9
Assessment Status .....	9
Profile Definitions.....	10
Acknowledgements.....	11
Recommendations.....	12
1 Install Updates, Patches and Additional Security Software.....	12
1.1 Verify all Apple-provided software is current (Automated) .....	13
1.2 Ensure Auto Update Is Enabled (Automated) .....	17
1.3 Ensure Download New Updates When Available is Enabled (Automated).....	21
1.4 Ensure Installation of App Update Is Enabled (Automated).....	25
1.5 Ensure System Data Files and Security Updates Are Downloaded Automatically Is Enabled (Automated) .....	29
1.6 Ensure Install of macOS Updates Is Enabled (Automated) .....	33
1.7 Audit Computer Name (Manual).....	37
2 System Preferences .....	39
2.1 Bluetooth.....	40
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated) .....	41
2.1.2 Ensure Show Bluetooth Status in Menu Bar Is Enabled (Automated).....	44
2.2 Date & Time.....	48
2.2.1 Ensure "Set time and date automatically" Is Enabled (Automated) .....	49
2.2.2 Ensure time set is within appropriate limits (Automated) .....	53
2.3 Desktop & Screen Saver.....	57
2.3.1 Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled (Automated) .....	58
2.3.2 Ensure Screen Saver Corners Are Secure (Automated) .....	63
2.3.3 Audit Lock Screen and Start Screen Saver Tools (Manual).....	68

2.4 Sharing .....	73
2.4.1 Ensure Remote Apple Events Is Disabled (Automated).....	74
2.4.2 Ensure Internet Sharing Is Disabled (Automated) .....	76
2.4.3 Ensure Screen Sharing Is Disabled (Automated) .....	80
2.4.4 Ensure Printer Sharing Is Disabled (Automated) .....	82
2.4.5 Ensure Remote Login Is Disabled (Automated) .....	84
2.4.6 Ensure DVD or CD Sharing Is Disabled (Automated) .....	88
2.4.7 Ensure Bluetooth Sharing Is Disabled (Automated).....	90
2.4.8 Ensure File Sharing Is Disabled (Automated) .....	94
2.4.9 Ensure Remote Management Is Disabled (Automated).....	97
2.4.10 Ensure Content Caching Is Disabled (Automated).....	100
2.4.11 Ensure AirDrop Is Disabled (Automated).....	103
2.4.12 Ensure Media Sharing Is Disabled (Automated).....	108
2.5 Security & Privacy .....	113
2.5.1 Encryption.....	114
2.5.1.1 Ensure FileVault Is Enabled (Automated) .....	115
2.5.1.2 Ensure all user storage APFS volumes are encrypted (Manual).....	117
2.5.1.3 Ensure all user storage CoreStorage volumes are encrypted (Manual)...	121
2.5.2 Firewall.....	125
2.5.2.1 Ensure Gatekeeper is Enabled (Automated) .....	125
2.5.2.2 Ensure Firewall Is Enabled (Automated) .....	129
2.5.2.3 Ensure Firewall Stealth Mode Is Enabled (Automated) .....	135
2.5.3 Ensure Location Services Is Enabled (Automated) .....	139
2.5.4 Audit Location Services Access (Manual).....	142
2.5.5 Ensure Sending Diagnostic and Usage Data to Apple Is Disabled (Automated) .....	145
2.5.6 Ensure Limit Ad Tracking Is Enabled (Automated) .....	149
2.5.7 Audit Camera Privacy and Confidentiality (Manual).....	154
2.6 Apple ID .....	157
2.6.1 iCloud .....	158
2.6.1.1 Audit iCloud Configuration (Manual) .....	159

2.6.1.2 Audit iCloud Keychain (Manual).....	164
2.6.1.3 Audit iCloud Drive (Manual) .....	168
2.6.1.4 Ensure iCloud Drive Document and Desktop Sync is Disabled (Automated) .....	171
2.6.2 Audit App Store Password Settings (Manual) .....	175
2.7 Time Machine .....	177
2.7.1 Ensure Backup Up Automatically is Enabled (Automated) .....	179
2.7.2 Ensure Time Machine Volumes Are Encrypted (Automated) .....	184
2.8 Ensure Wake for Network Access Is Disabled (Automated).....	187
2.9 Ensure Power Nap Is Disabled (Automated).....	190
2.10 Ensure Secure Keyboard Entry terminal.app is Enabled (Automated).....	193
2.11 Ensure EFI Version Is Valid and Checked Regularly (Automated).....	197
2.12 Audit Automatic Actions for Optical Media (Manual) .....	199
2.13 Audit Siri Settings (Manual) .....	203
2.14 Audit Sidecar Settings (Manual) .....	209
2.15 Audit Touch ID and Wallet & Apple Pay Settings (Manual).....	213
2.16 Audit Notification System Preference Settings (Manual) .....	215
3 Logging and Auditing.....	217
3.1 Ensure Security Auditing Is Enabled (Automated) .....	218
3.2 Ensure Security Auditing Flags Are Configured Per Local Organizational Requirements (Automated).....	220
3.3 Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated) .....	223
3.4 Ensure Security Auditing Retention Is Enabled (Automated) .....	226
3.5 Ensure Access to Audit Records Is Controlled (Automated) .....	228
3.6 Ensure Firewall Logging Is Enabled and Configured (Automated) .....	231
3.7 Audit Software Inventory (Manual) .....	233
4 Network Configurations.....	236
4.1 Ensure Bonjour Advertising Services Is Disabled (Automated) .....	237
4.2 Ensure Show Wi-Fi status in Menu Bar Is Enabled (Automated) .....	240
4.3 Audit Network Specific Locations (Manual) .....	244

4.4 Ensure HTTP Server Is Disabled (Automated) .....	247
4.5 Ensure NFS Server Is Disabled (Automated) .....	249
4.6 Audit Wi-Fi Settings (Manual) .....	251
5 System Access, Authentication and Authorization .....	254
5.1 File System Permissions and Access Controls .....	255
5.1.1 Ensure Home Folders Are Secure (Automated) .....	256
5.1.2 Ensure System Integrity Protection Status (SIPS) Is Enabled (Automated) .....	259
5.1.3 Ensure Apple Mobile File Integrity Is Enabled (Automated) .....	261
5.1.4 Ensure Library Validation Is Enabled (Automated) .....	263
5.1.5 Ensure Sealed System Volume (SSV) Is Enabled (Automated) .....	267
5.1.6 Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated) .....	270
5.1.7 Ensure No World Writable Files Exist in the System Folder (Automated). 272	
5.1.8 Ensure No World Writable Files Exist in the Library Folder (Automated) 274	
5.2 Password Management .....	276
5.2.1 Ensure Password Account Lockout Threshold Is Configured (Automated) .....	277
5.2.2 Ensure Password Minimum Length Is Configured (Automated) .....	280
5.2.3 Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Manual) .....	283
5.2.4 Ensure Complex Password Must Contain Numeric Character Is Configured (Manual) .....	286
5.2.5 Ensure Complex Password Must Contain Special Character Is Configured (Manual) .....	289
5.2.6 Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Manual) .....	292
5.2.7 Ensure Password Age Is Configured (Automated) .....	294
5.2.8 Ensure Password History Is Configured (Automated) .....	297
5.3 Ensure the Sudo Timeout Period Is Set to Zero (Automated) .....	300
5.4 Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated) .....	303

5.5 Ensure login keychain is locked when the computer sleeps (Manual) .....	305
5.6 Ensure the "root" Account Is Disabled (Automated) .....	308
5.7 Ensure Automatic Login Is Disabled (Automated).....	310
5.8 Ensure a Password is Required to Wake the Computer From Sleep or Screen Saver Is Enabled (Automated).....	313
5.9 Ensure system is set to hibernate (Automated).....	317
5.10 Require an administrator password to access system-wide preferences (Automated) .....	322
5.11 Ensure an administrator account cannot login to another user's active and locked session (Automated) .....	325
5.12 Ensure a Custom Message for the Login Screen Is Enabled (Automated) ...	327
5.13 Create a Login window banner (Automated) .....	330
5.14 Do not enter a password-related hint (Automated) .....	333
5.15 Ensure Fast User Switching Is Disabled (Manual).....	335
6 User Accounts and Environment.....	338
6.1 Accounts Preferences Action Items .....	339
6.1.1 Ensure Login Window Displays as Name and Password Is Enabled (Automated) .....	339
6.1.2 Ensure Show Password Hints Is Disabled (Automated) .....	342
6.1.3 Ensure Guest Account Is Disabled (Automated) .....	345
6.1.4 Ensure Guest Access to Shared Folders Is Disabled (Automated).....	349
6.1.5 Remove Guest home folder (Automated) .....	353
6.2 Ensure Show All Filename Extensions Setting is Enabled (Automated) .....	355
6.3 Ensure Automatic Opening of Safe Files in Safari Is Disabled (Automated)..	358
7 Appendix: Additional Considerations .....	362
7.1 Extensible Firmware Interface (EFI) password (Manual).....	363
7.2 FileVault and Local Account Password Reset using AppleID (Manual).....	365
Appendix: Recommendation Summary Table.....	367
Appendix: Change History .....	372

# Overview

This document, CIS Apple macOS 11.0 Big Sur Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Apple macOS 11.0 Big Sur. This guide was tested against Apple macOS 11.0 Big Sur. To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto:feedback@cisecurity.org).

This Benchmark includes instructions for auditing and remediation that includes three different methods (Graphical User Interface (GUI), Command Line Interface using Terminal (CLI), Configuration Profiles) to evaluate the current configuration status and make changes as desired. In most cases all methods are supported by the Operating System and it is up to organizational implementation personnel on how best to implement. There are some recommendations that can only be managed through one of the methods. Each organization must decide if control management outside their standard process is required if no solution is possible through their organization's specific choice of implementation. It is best practice, for Enterprise managed devices at this time, to use profiles for management, a mix of both profile device management, and command line hardening scripts will be the most comprehensive solution.

More profile information:

<https://developer.apple.com/documentation/devicemanagement>

[https://developer.apple.com/documentation/devicemanagement/configuring\\_multiple\\_devices\\_using\\_profiles](https://developer.apple.com/documentation/devicemanagement/configuring_multiple_devices_using_profiles)

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Apple macOS 11.0.



## Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
< <i>italic font in brackets</i> >	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
<b>Note</b>	Additional information or caveats

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology.

## Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

### **Author**

Ron Colvin

### **Contributor**

William Harrison

Mark Andersen CISSP, GMOB

Ben Montour

Sara Archacki

Hao Shu

Jeffrey Compton

Jorge Escobar

Tim Harrison CISSP, ICP, KMP, Center for Internet Security

Laura Gardner

Mauro Faccenda

Mischa van der Bent

Jason Olsen BSCS, ACSP 10.9, ACMT 2015, Comerica Bank

### **Editor**

Eric Pinnell

Edward Byrd

# Recommendations

## ***1 Install Updates, Patches and Additional Security Software***

Install Updates, Patches and Additional Security Software

## 1.1 Verify all Apple-provided software is current (Automated)

### Profile Applicability:

- Level 1

### Description:

Software vendors release security patches and software updates for their products when security vulnerabilities are discovered. There is no simple way to complete this action without a network connection to an Apple software repository. Please ensure appropriate access for this control. This check is only for what Apple provides through software update.

Software updates should be run at minimum every 30 days. Run the following command to verify when software update was previously run: `$ sudo defaults read`

`/Library/Preferences/com.apple.SoftwareUpdate | grep -e`

`LastFullSuccessfulDate`. The response should be in the last 30 days (*Example*):

`LastFullSuccessfulDate = "2020-07-30 12:45:25 +0000";`

### Rationale:

It is important that these updates be applied in a timely manner to prevent unauthorized persons from exploiting the identified vulnerabilities.

### Impact:

Missing patches can lead to more exploit opportunities.

## Audit:

Perform the following to ensure there are no available software updates:

*Graphical Method:*

1. Open System Preferences
2. Select Software Update
3. Select Automatically check for updates to allow Software Update to check with Apple's servers for any outstanding updates
4. Select Show Updates to verify that there are no software updates available

*Terminal Method:*

Run the following command to verify there are no software updates:

```
$ sudo softwareupdate -l  
  
Software Update Tool  
  
Finding available software  
No new software available.
```

Computers that have installed pre-release software in the past will fail this check if there are pre-release software updates available when audited. In the App Store setting System Preferences the computer may be set to no longer receive pre-release software.

## Remediation:

Perform the following to install all available software updates:

*Graphical Method:*

1. Open System Preferences
2. Select Software Update
3. Select Show Updates
4. Select Update All

*Terminal Method:*

Run the following command to verify what packages need to be installed:

```
$ sudo softwareupdate -l
```

The output will include the following:

Software Update found the following new or updated software:

Run the following command to install all the packages that need to be updated:

```
$ sudo softwareupdate -i -a
```

Or run the following command to install individual packages:

```
$ sudo softwareupdate -i '<package name>'
```

*example:*

```
$ sudo softwareupdate -l
Software Update Tool













Finding available software
Software Update found the following new or updated software:
  * iTunesX-12.8.2
    iTunes (12.8.2), 273614K [recommended]

$ sudo softwareupdate -i 'iTunesX-12.8.2'
Software Update Tool

Downloaded iTunes
Installing iTunes
Done with iTunes
Done.
```



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.3 Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.4 Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b><u>3.5 Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## *1.2 Ensure Auto Update Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Auto Update verifies that your system has the newest security patches and software updates. If "Automatically check for updates" is not selected background updates for new malware definition files from Apple for XProtect and Gatekeeper will not occur.

<http://macops.ca/os-x-admins-your-clients-are-not-getting-background-security-updates/>

<https://derflounder.wordpress.com/2014/12/17/forcing-xprotect-blacklist-updates-on-mavericks-and-yosemite/>

### **Rationale:**

It is important that a system has the newest updates applied so as to prevent unauthorized persons from exploiting identified vulnerabilities.

### **Impact:**

Without automatic update, updates may not be made in a timely manner and the system will be exposed to additional risk.

## Audit:

Perform the following to ensure the system is automatically checking for updates:

*Graphical Method:*

1. Open System Preferences
2. Select Software Update
3. Select Advanced
4. Verify that Check for updates is selected

*Terminal Method:*

Run the following command to verify that software updates are automatically checked:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdateAutomaticCheckEnabled
```

1

**Note:** If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

**or**

Run the following command to verify that a profile is installed that enables software updates to be automatically checked:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'AutomaticCheckEnabled = 1'
```

1

## Remediation:

Perform the following to enable the system to automatically check for updates:

*Graphical Method:*

1. Open System Preferences
2. Select Software Update
3. Select Advanced
4. Select Check for updates

*Terminal Method:*













Run the following command to enable auto update:

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.SoftwareUpdate  
AutomaticCheckEnabled -bool true
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.SoftwareUpdate`
2. Add the key `AutomaticCheckEnabled`
3. Set the key to `<true/>`

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.3 Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.4 Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b><u>3.5 Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

### *1.3 Ensure Download New Updates When Available is Enabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

In the GUI both "Install macOS updates" and "Install app updates from the App Store" are dependent on whether "Download new updates when available" is selected.

**Rationale:**

It is important that a system has the newest updates downloaded so that they can be applied.

**Impact:**

If "Download new updates when available" is not selected, updates may not be made in a timely manner and the system will be exposed to additional risk.

## Audit:

Perform the following to ensure the system is automatically checking for updates:

*Graphical Method:*

1. Open System Preferences
2. Select Software Update
3. Select Advanced
4. Verify that Download new updates when available is selected

*Terminal Method:*

Run the following command to verify that software updates are automatically checked:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate  
AutomaticDownload
```

```
1
```

**Note:** If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

**or**

Run the following command to verify that a profile is installed that enables software updates to be downloaded when available:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'AutomaticDownload =  
1'
```

```
1
```

## Remediation:

Perform the following to enable the system to automatically check for updates:

*Graphical Method:*

1. Open System Preferences
2. Select Software Update
3. Select Advanced
4. Select Download new updates when available

*Terminal Method:*

Run the following command to enable auto update:













```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.SoftwareUpdate  
AutomaticDownload -bool true
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.SoftwareUpdate`
2. Add the key `AutomaticDownload`
3. Set the key to `<true/>`



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.3 Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.4 Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b><u>3.5 Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## *1.4 Ensure Installation of App Update Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Ensure that application updates are installed after they are available from Apple. These updates do not require reboots or admin privileges for end users.

### **Rationale:**

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

### **Impact:**

Unpatched software may be exploited.

## Audit:

Perform the following to ensure that App Store updates install automatically:

*Graphical Method:*

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Verify that Install app updates from the App Store is checked

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Automatically Install App Updates` set to `True`

*Terminal Method:*

Run the following command to verify that App Store updates are auto updating:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.commerce  
AutoUpdate  
1
```

**or**

Run the following command to verify that a profile is installed that enables App Store updates to be automatically installed:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep  
AutomaticallyInstallAppUpdates  
  
AutomaticallyInstallAppUpdates = 1;
```

## Remediation:

Perform the following to enable App Store updates to install automatically:

*Graphical Method:*

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Select Install app updates from the App Store

*Terminal Method:*

Run the following command to turn on App Store auto updating:













```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.commerce  
AutoUpdate -bool TRUE
```

**Note:** This remediation requires a log out and log in to show in the GUI.

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.SoftwareUpdate`
2. Add the key `AutomaticallyInstallAppUpdates`
3. Set the key to `<true/>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.3 Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.4 Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b><u>3.5 Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## *1.5 Ensure System Data Files and Security Updates Are Downloaded Automatically Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Ensure that system and security updates are installed after they are available from Apple. This setting enables definition updates for XProtect and Gatekeeper. With this setting in place new malware and adware that Apple has added to the list of malware or untrusted software will not execute. These updates do not require reboots or end user admin rights.

<http://www.thesafemac.com/tag/xprotect/>

<https://support.apple.com/en-us/HT202491>

### **Rationale:**

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

### **Impact:**

Unpatched software may be exploited.

## Audit:

Perform the following to ensure that system data files and security updates install automatically:

*Graphical Method:*

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Verify that Install system data files and security updates is selected

*Terminal Method:*

Run the following commands to verify that system data files and security updates are automatically checked:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate
ConfigDataInstall
1

$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate
CriticalUpdateInstall
1
```

**Note:** If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

**or**

Run the following commands to verify that a profile is installed that enables system data files and security updates to automatically download:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'ConfigDataInstall =
1'
1

$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep -c
'CriticalUpdateInstall = 1'
1
```

## Remediation:

Perform the following to enable system data files and security updates to install automatically:

### *Graphical Method:*

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Select Install system data files and security updates

### *Terminal Method:*

Run the following commands to enable automatically checking of system data files and security updates:















```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.SoftwareUpdate  
ConfigDataInstall -bool true  
  
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.SoftwareUpdate  
CriticalUpdateInstall -bool true
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.SoftwareUpdate
2. Add the key ConfigDataInstall
3. Set the key to <true/>
4. Add the key CriticalUpdateInstall
5. Set the key to <true/>



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.3 Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.4 Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.7 Remediate Detected Vulnerabilities</u></b> Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.			
v7	<b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b><u>3.5 Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## *1.6 Ensure Install of macOS Updates Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Ensure that macOS updates are installed after they are available from Apple. This setting enables macOS updates to be automatically installed. Some environments will want to approve and test updates before they are delivered. It is best practice to test first where updates can and have caused disruptions to operations. Automatic updates should be turned off where changes are tightly controlled and there are mature testing and approval processes. Automatic updates should not be turned off so the admin can call the users first to let them know it's ok to install. A dependable, repeatable process involving a patch agent or remote management tool should be in place before auto-updates are turned off.

### **Rationale:**

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

### **Impact:**

Unpatched software may be exploited.

## Audit:

Perform the following to ensure that macOS updates are set to auto update:

*Graphical Method:*

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Verify that "Install macOS updates" is selected

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has Automatically Install macOS Updates set to True

*Terminal Method:*

Run the following command to verify that macOS updates are automatically checked and installed:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate  
AutomaticallyInstallMacOSUpdates  
1
```

**Note:** If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

**or**

Run the following command to verify that a profile is installed that enables the installation of macOS updates:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep -c  
'AutomaticallyInstallMacOSUpdates = 1'  
1
```

## Remediation:

Perform the following to enable macOS updates to run automatically:

*Graphical Method:*

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Select Install macOS updates

*Terminal Method:*













Run the following command to to enable automatic checking and installing of macOS updates:

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.SoftwareUpdate  
AutomaticallyInstallMacOSUpdates -bool TRUE
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.SoftwareUpdate
2. Add the key AutomaticallyInstallMacOSUpdates
3. Set the key to <true/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.3 Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b><u>7.4 Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b><u>3.5 Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## *1.7 Audit Computer Name (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

If the computer is used in an organization that assigns host names, it is a good idea to change the computer name to the host name. This is more of a best practice than a security measure. If the host name and the computer name are the same, computer support may be able to track problems down more easily.

Standard naming patterns avoid collisions and mitigate risk for computer users.

With mobile devices using DHCP IP tracking has serious drawbacks; hostname or computer name tracking makes much more sense for those organizations that can implement it. If the computer is using different names for the "Computer Name" DNS and Directory environments it can be difficult to manage Macs in an Enterprise asset inventory.

### **Rationale:**

Part of IT security is having visibility into all of the devices that the organization is responsible for. Without a complete inventory it is impossible to ensure all security controls are met on all organizational devices.

Default macOS naming deconfliction controls can create issues for appropriate management and tracking as well as privacy exposure. By default the name of a macOS computer is derived from the first user created. If the user has multiple computers or an image is used without an appropriate name change there will be multiple computers with names derived from the same user for discovery deconfliction. How many "Ron Colvin's MacBook Pro" should there be, are any missing?

Local network auto renaming to avoid collisions also allows for the enumeration of local computer names. Computers should not be named after their users, especially on untrusted networks. For social engineering purposes the computer name should not provide a full name of the user or an identifiable name that might be used to assist in targeted user attacks.

A documented plan to better enable a complete device inventory without exposing user or organizational information is part of mature security.

## Audit:

Perform the following to verify the computer name:

1. Open System Preferences
2. Select Sharing
3. Verify that Computer Name is set to your organization's parameters

## Remediation:






Perform the following to set the computer name:

1. Open System Preferences
2. Select Sharing
3. Set Computer Name to your organization's parameters

## References:

1. <https://support.apple.com/en-ca/guide/mac-help/mchlp1177/11.0/mac/11.0>
2. <https://uberagent.com/blog/choosing-macos-computer-names-wisely/>
3. <https://support.apple.com/en-ca/guide/mac-help/mchlp2322/11.0/mac/11.0>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>1.1 Establish and Maintain Detailed Enterprise Asset Inventory</u></b></p> <p>Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.</p>			
v7	<p><b><u>9.1 Associate Active Ports, Services and Protocols to Asset Inventory</u></b></p> <p>Associate active ports, services and protocols to the hardware assets in the asset inventory.</p>			

## ***2 System Preferences***

This section contains recommendations related to configurable options in the *System Preferences* panel.



## **2.1 Bluetooth**

Bluetooth is a short-range, low-power wireless technology commonly integrated into portable computing and communication devices and peripherals. Bluetooth is best used in a secure environment where unauthorized users have no physical access near the Mac. If Bluetooth is used, it should be secured properly (see below).

### 2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Bluetooth devices use a wireless communications system that replaces the cables used by other peripherals to connect to a system. It is by design a peer-to-peer network technology and typically lacks centralized administration and security enforcement infrastructure.

#### Rationale:

Bluetooth is particularly susceptible to a diverse set of security vulnerabilities involving identity detection, location tracking, denial of service, unintended control and access of data and voice channels, and unauthorized device control and data access.

#### Impact:

There have been many Bluetooth exploits. While Bluetooth can be hardened, it does create a local wireless network that can be attacked to compromise both devices and information. Apple has emphasized the ease of use in Bluetooth devices so it is generally expected that Bluetooth will be used. Turning off Bluetooth with this control will also disable the Bluetooth sharing capability that is more strongly recommended against in control 2.4.7.

#### Audit:

Perform the following to ensure that Bluetooth is only enabled if there are paired devices:  
Run the following command to verify that Bluetooth is disabled:

```
$ sudo defaults read /Library/Preferences/com.apple.Bluetooth  
ControllerPowerState  
  
0
```

If the value 1 is returned it indicates that Bluetooth is enabled. The computer is compliant only if paired devices exist.

Run the following command to verify if there are paired devices:

```
$ sudo system_profiler SPBluetoothDataType 2>/dev/null | grep -m1 'Paired:  
Yes'  
  
Paired: Yes
```

## Remediation:

Perform the following to disable Bluetooth:

*Graphical Method:*

1. Open System Preferences
2. Select Bluetooth
3. Select Turn Bluetooth Off











*Terminal Method:*

Run the following command to disable Bluetooth

```
$ sudo defaults write /Library/Preferences/com.apple.Bluetooth  
ControllerPowerState -int 0  
  
$ sudo killall -HUP bluetoothd
```

**Note:** When using the terminal method to disable Bluetooth, the prescribed state will not be properly shown in the GUI. Use the terminal method of the audit to verify if Bluetooth is enabled/disabled.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v8	<p><b><u>12.6 Use of Secure Network Management and Communication Protocols</u></b></p> <p>Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).</p>			
v8	<p><b><u>13.9 Deploy Port-Level Access Control</u></b></p> <p>Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			
v7	<p><b><u>15.6 Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients</u></b></p> <p>Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.</p>			
v7	<p><b><u>15.8 Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication</u></b></p> <p>Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.</p>			

### *2.1.2 Ensure Show Bluetooth Status in Menu Bar Is Enabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

By showing the Bluetooth status in the menu bar, a small Bluetooth icon is placed in the menu bar. This icon quickly shows the status of Bluetooth, and can allow the user to quickly turn Bluetooth on or off.

**Rationale:**

Enabling "Show Bluetooth status in menu bar" is a security awareness method that helps understand the current state of Bluetooth, including whether it is enabled, discoverable, what paired devices exist, and what paired devices are currently active.

**Impact:**

Bluetooth is a useful wireless tool that has been widely exploited when configured improperly. The user should have insight into the Bluetooth status.

## Audit:

Perform the following to ensure that Bluetooth status shows in the menu bar:

*Graphical Method:*

1. Open System Preferences
2. Select Dock & Menu Bar
3. Select Bluetooth
4. Verify that Show in Menu Bar is selected

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has Bluetooth set to 18

*Terminal Method:*

For each user, run the following command to verify that the Bluetooth status is enabled to show in the menu bar:

```
$ sudo -u <username> defaults -currentHost read com.apple.controlcenter.plist  
Bluetooth  
18
```

**Note:** If the settings has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

*example:*

```
$ sudo -u firstuser defaults -currentHost read com.apple.controlcenter.plist  
Bluetooth  
18
```

**or**

Run the following command to verify that a profile is installed that enables Bluetooth to be shown in the menu bar:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep 'Bluetooth = 18'  
  
Bluetooth = 18;
```

## Remediation:

Perform the following to enable Bluetooth status in the menu bar:

*Graphical Method:*

1. Open System Preferences
2. Select Dock & Menu Bar
3. Select Bluetooth
4. Select Show in Menu Bar

*Terminal Method:*

For each user, run the following command to enable Bluetooth status in the menu bar:

```
$ sudo -u <username> defaults -currentHost write  
com.apple.controlcenter.plist Bluetooth -int 18
```






*example:*

```
$ sudo -u firstuser defaults -currentHost write com.apple.controlcenter.plist  
Bluetooth -int 18
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of  
com.apple.controlcenter
2. Add the key Bluetooth
3. Set the key to <integer>18</integer>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<b><u>13.9 Deploy Port-Level Access Control</u></b> Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			
v7	<b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			



## ***2.2 Date & Time***

This section contains recommendations related to the configurable items under the *Date & Time* panel.

### 2.2.1 Ensure "Set time and date automatically" Is Enabled (Automated)

#### **Profile Applicability:**

- Level 1

#### **Description:**

Correct date and time settings are required for authentication protocols, file creation, modification dates and log entries.

**Note:** If your organization has internal time servers, enter them here. Enterprise mobile devices may need to use a mix of internal and external time servers. If multiple servers are required use the Date & Time System Preference with each server separated by a space.

#### **Rationale:**

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features.

#### **Impact:**

Apple's automatic time update solution will enable an NTP server that is not controlled by the Application Firewall. Turning on "Set time and date automatically" allows other computers to connect to set their time and allows for exploit attempts against ntpd. It also allows for more accurate network detection and OS fingerprinting

Current testing shows scanners can easily determine the MAC address and the OS vendor. More extensive OS fingerprinting may be possible.

## Audit:

Perform the following to ensure that the system's date and time are set automatically:

*Graphical Method:*

1. Open System Preferences
2. Select Date & Time
3. Verify that Set date and time automatically is selected

*Terminal Method:*

Run the following command to ensure that date and time are automatically set:

```
$ sudo /usr/sbin/systemsetup -getusingnetworktime  
Network Time: On
```

**or**

Run the following command to verify that a profile is installed that enables date and time to be set automatically:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep  
forceAutomaticDateAndTime  
  
forceAutomaticDateAndTime = 1;
```

## Remediation:

Perform the following to enable the date and time to be set automatically:

*Graphical Method:*

1. Open System Preferences
2. Select Date & Time
3. Verify that Set date and time automatically is selected

*Terminal Method:*

Run the following commands to enable the date and time setting automatically:

```
$ sudo /usr/sbin/systemsetup -setnetworktimeserver <your.time.server>
setNetworkTimeServer: <your.time.server>

$ sudo /usr/sbin/systemsetup -setusingnetworktime on
setUsingNetworkTime: On
```

*example:*

```
$ sudo /usr/sbin/systemsetup -setnetworktimeserver time.apple.com
setNetworkTimeServer: time.apple.com

$ sudo /usr/sbin/systemsetup -setusingnetworktime on
setUsingNetworkTime: On
```

Run the following commands if you have not set, or need to set, a new time zone:

```
$ sudo /usr/sbin/systemsetup -listtimezones

$ sudo /usr/sbin/systemsetup -settimezone <selected time zone>
```

*example:*

```
$ sudo /usr/sbin/systemsetup -listtimezones

Time Zones:
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
...
Pacific/Wake
Pacific/Wallis





$ sudo /usr/sbin/systemsetup -settimezone America/New_York

Set TimeZone: America/New_York
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.applicationaccess`
2. Add the key `forceAutomaticDateAndTime`
3. Set the key to `</true>`

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.4 <u>Standardize Time Synchronization</u></b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	<b>6.1 <u>Utilize Three Synchronized Time Sources</u></b> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

## 2.2.2 Ensure time set is within appropriate limits (Automated)

### Profile Applicability:

- Level 1

### Description:

Correct date and time settings are required for authentication protocols, file creation, modification dates and log entries. Ensure that time on the computer is within acceptable limits. Truly accurate time is measured within milliseconds. For this audit, a drift under four and a half minutes passes the control check. Since Kerberos is one of the important features of macOS integration into Directory systems the guidance here is to warn you before there could be an impact to operations. From the perspective of accurate time, this check is not strict, so it may be too great for your organization. Your organization can adjust to a smaller offset value as needed.

**Note:** `ntdate` has been deprecated with 10.14. `sntp` replaces that command.

### Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features. Audit check is for more than 4 minutes and 30 seconds ahead or behind.

### Impact:

Accurate time is required for many computer functions.

## Audit:

Run the following commands to verify the time is set within an appropriate limit:

```
$ sudo systemsetup -getnetworktimeserver
```

The output will include `Network Time Server:` and the name of your time server.

*example:* `Network Time Server: time.apple.com`

```
$ sudo sntp <your.time.server> | grep +/-
```

Ensure that the offset result(s) are between -270.x and 270.x seconds.

*example:*

```
$ sudo systemsetup -getnetworktimeserver
Network Time Server: time.apple.com
$ sudo sntp time.apple.com | grep +/-
2020-10-14 06:42:29.171327 (+0700) +0.51522 +/- 0.343675 time.apple.com
17.253.14.251 s1 no-leap
```

## Remediation:

Run the following commands to ensure your time is set within an appropriate limit:

```
$ sudo systemsetup -getnetworktimeserver
```

The output will include `Network Time Server:` and the name of your time server

*example:* `Network Time Server: time.apple.com.`

```
$ sudo touch /var/db/ntp-kod
$ sudo chown root:wheel /var/db/ntp-kod
$ sudo sntp -sS <your.time.server>
```

*example:*





```
$ sudo systemsetup -getnetworktimeserver
Network Time Server: time.apple.com
$ sudo touch /var/db/ntp-kod
$ sudo chown root:wheel /var/db/ntp-kod
$ sudo sntp -sS time.apple.com
```

## Additional Information:

The associated check will fail if no network connection is available.



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.4 <u>Standardize Time Synchronization</u></b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	<b>6.1 <u>Utilize Three Synchronized Time Sources</u></b> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

## ***2.3 Desktop & Screen Saver***

This section contains recommendations related to the configurable items under the Desktop & Screen Saver panel.

### *2.3.1 Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

A locking screensaver is one of the standard security controls to limit access to a computer and the current user's session when the computer is temporarily unused or unattended. In macOS, the screensaver starts after a value is selected in the drop down menu. 20 minutes or less is an acceptable value. Any value can be selected through the command line or script but a number that is not reflected in the GUI can be problematic. 20 minutes is the default for new accounts.

#### **Rationale:**

Setting an inactivity interval for the screensaver prevents unauthorized persons from viewing a system left unattended for an extensive period of time.

#### **Impact:**

If the screensaver is not set users may leave the computer available for an unauthorized person to access information.

## Audit:

The preferred audit procedure for this control will evaluate every user account on the computer and will report on all users where the value has been set. If the default value of 20 minutes is used and the user has never changed the setting there will not be an audit result on their compliant setting. The time is set in seconds so all outputs will be in that format.

Perform the following to ensure the system is set for the screen saver to activate in 20 minutes of less:

Run this script to verify the idle times for all users:

```
UUID=`ioreg -rd1 -c IOPlatformExpertDevice | grep "IOPlatformUUID" | sed -e 's/^.* "\(.*\)"$/\1/'`

for i in $(find /Users -type d -maxdepth 1)
do
    PREF=$i/Library/Preferences/ByHost/com.apple.screensaver.$UUID
    if [ -e $PREF.plist ]
    then
        echo -n "Checking User: '$i': "
        defaults read $PREF.plist idleTime 2>&1
    fi
done
```

**Note:** If the output of the script includes The domain/default pair of (com.apple.screensaver, idleTime) does not exist for any user, then the setting has not been changed from the default. Follow the remediation instructions to set the idle time to match your organization's policy.

For Macs with a single user:

*Graphical Method:*

1. Open System Preferences
2. Select Desktop & Screen Saver
3. Select Screen Saver
4. Verify that Start after is set for 20 minutes or less ( $\leq 1200$ )

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has Idle Time set to  $\leq 1200$

*Terminal Method:*

Run the following command to verify that the screen saver idle time is set to less than or equal to 20 minutes:

```
$ sudo /usr/bin/defaults -currentHost read com.apple.screensaver idleTime
```

The output should be less than or equal to 20 minutes ( $\leq 1200$ ). *example:* 60, 120, 300, 600, or 1200

**Note:** If the output is The domain/default pair of (com.apple.screensaver, idleTime) does not exist, then the setting has not been changed from the default. Follow the remediation instructions to set the idle time to match your organization's policy.

**or**

Run the following command to verify that a profile is installed that enables a screensaver idle time of less than or equal to 20 minutes:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep idleTime
```

The output should be less than or equal to 20 minutes ( $\leq 1200$ ). *example:* 60, 120, 300, 600, or 1200

## Remediation:

Perform the following to set the screen saver to activate in 20 minutes of less:

### *Graphical Method:*

1. Open System Preferences
2. Select Desktop & Screen Saver
3. Select Screen Saver
4. Select on option for Start after that is 20 minutes or less ( $\leq 1200$ )

### *Terminal Method:*

Run the following command to verify that the idle time of the screen saver is set to 20 minutes of less ( $\leq 1200$ )

```
$ sudo -u <username> /usr/bin/defaults -currentHost write  
com.apple.screensaver idleTime -int <value  $\leq 1200$ >
```

### *example:*

```
$ sudo /usr/bin/defaults -currentHost write com.apple.screensaver idleTime -  
int 600
```

If there are multiple users out of compliance with the prescribed setting, run this command for each user to set their idle time:

```
$ sudo -u <username> /usr/bin/defaults -currentHost write  
com.apple.screensaver idleTime -int <value  $\leq 1200$ >
```

### *example:*







```
$ sudo -u seconduser /usr/bin/defaults -currentHost write  
com.apple.screensaver idleTime -int 600  
  
$ sudo -u seconduser /usr/bin/defaults -currentHost read  
com.apple.screensaver idleTime  
  
600
```

**\*\*Note:\*\***Issues arise if the command line is used to make the setting something other than what is available in the GUI Menu. Choose either 1 (60), 2 (120), 5 (300), 10 (600), or 20 (120) minutes to avoid any issues.

### *Profile Method:*

1. Create or edit a configuration profile with the PayLoadType of `com.apple.screensaver.user`
2. Add the key `idleTime`
3. Set the key to  $\leq 1200$

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.3 Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b><u>16.11 Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

### *2.3.2 Ensure Screen Saver Corners Are Secure (Automated)*

**Profile Applicability:**

- Level 2

**Description:**

Hot Corners can be configured to disable the screen saver by moving the mouse cursor to a corner of the screen.

**Rationale:**

Setting a hot corner to disable the screen saver poses a potential security risk since an unauthorized person could use this to bypass the login screen and gain access to the system.



## Audit:

Perform the following to ensure that a Hot Corner is not set to Disable Screen Saver:

*Graphical Method:*

1. Open System Preferences
2. Select Desktop & Screen Saver
3. Select Screen Saver
4. Select Hot Corners... and verify that Disable Screen Saver is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `<wvous-tl-corner>`, `<wvous-bl-corner>`, `<wvous-tr-corner>`, and `<wvous-br-corner>` not set to 6

*Terminal Method:*

For all users, run the following commands to verify that Disable Screen Saver is not set as a Hot Corner:

```
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-tl-corner
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-bl-corner
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-tr-corner
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-br-corner
```

Verify that the output does not have 6 as a key value. Any other number, or an output that includes `does not exist`, is compliant.

*example:*

```
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-tl-corner
10
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-bl-corner
2020-07-31 14:32:29.018 defaults[39521:1276494]
The domain/default pair of (com.apple.dock, wvous-bl-corner) does not exist

$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-tr-corner
2020-07-31 14:32:32.403 defaults[39523:1276515]
The domain/default pair of (com.apple.dock, wvous-tr-corner) does not exist

$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-br-corner
2020-07-31 14:32:36.045 defaults[39525:1276529]
The domain/default pair of (com.apple.dock, wvous-br-corner) does not exist
```

Run the following command to verify that a profile is installed secures screen saver corners:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-bl-corner
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-br-corner
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-tl-corner
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-tr-corner
```

The output should include wvous-bl-corner, wvous-br-corner, wvous-tl-corner, and wvous-tr-corner are ≠ 6;

## Remediation:

Perform the following to disable a Hot Corner set to Disable Screen Saver:

*Graphical Method:*

1. Open System Preferences
2. Select Desktop & Screen Saver
3. Select Screen Saver
4. Select Hot Corners... and turn off any corner that is set to Disable Screen Saver

*Terminal Method:*

Run the following command to turn off Disable Screen Saver for a Hot Corner:

```
$ sudo -u <username> /usr/bin/defaults write com.apple.dock <corner that is set to '6'> -int 0
```

*example:*







```
$ sudo -u seconduser /usr/bin/defaults write com.apple.dock wvous-tl-corner -int 0  
  
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-tl-corner  
0
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.dock
2. Add the key Forced
3. Set the key to the following:

```
<array>  
  <dict>  
    <key>mcx_preference_settings</key>  
    <dict>  
      <key>wvous-bl-corner</key>  
      <integer><#6></integer>  
      <key>wvous-br-corner</key>  
      <integer><#6></integer>  
      <key>wvous-tl-corner</key>  
      <integer><#6></integer>  
      <key>wvous-tr-corner</key>  
      <integer><#6></integer>  
    </dict>  
  </dict>  
</array>
```

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

### *2.3.3 Audit Lock Screen and Start Screen Saver Tools (Manual)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

In 10.13 Apple added a "Lock Screen" option to the Apple Menu. Prior to this the best quick lock options were to use either a lock screen option with the screen saver or the lock screen option from Keychain Access if status was made available in the menu bar. With 10.13 the menu bar option is no longer available. The intent of this control is to resemble control-alt-delete on Windows Systems as a means of quickly locking the screen. If the user of the system is stepping away from the computer the best practice is to lock the screen and setting a hot corner is an appropriate method.

#### **Rationale:**

Ensuring the user has a quick method to lock their screen may reduce the opportunity for individuals in close physical proximity of the device to see screen contents.

**Audit:**

Perform the following to ensure that a Hot Corner is set to either Start Screen Saver or Put Display to Sleep:

*Graphical Method:*

1. Open System Preferences
2. Select Desktop & Screen Saver
3. Select Screen Saver
4. Select Hot Corners... and verify that Start Screen Saver or Put Display to Sleep is set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has <wvous-tl-corner>, <wvous-bl-corner>, <wvous-tr-corner>, and <wvous-br-corner> set to either 5 or 10

### *Terminal Method:*

For all users, run the following commands to verify that Start Screen Saver or Put Display to Sleep is set as a Hot Corner:

```
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-tl-corner
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-bl-corner
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-tr-corner
$ sudo -u <username> /usr/bin/defaults read com.apple.dock wvous-br-corner
```

For each user, verify at least one of the key values is set to 5 or 10. *example* "wvous-tr-corner" = 5; **or** "wvous-br-corner" = 10;  
*example:*

```
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-tl-corner
0
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-bl-corner
2020-08-03 08:21:08.223 defaults[1115:19336]
The domain/default pair of (com.apple.dock, wvous-bl-corner) does not exist
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-tr-corner
10
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-br-corner
5
```

**Note:** Alert the user on how to use this functionality  
**or**

Run the following command to verify that a profile is installed that enables a screen saver corner that enables either the screen saver or screen lock:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-bl-corner
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-br-corner
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-tl-corner
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep wvous-tr-corner
```

The output should include either wvous-bl-corner, wvous-br-corner, wvous-tl-corner, or wvous-tr-corner are set 5 or 10;

## Remediation:

Perform the following to set a Hot Corner to either Start Screen Saver or Put Display to Sleep:

*Graphical Method:*

1. Open System Preferences
2. Select Desktop & Screen Saver
3. Select Screen Saver
4. Select Hot Corners... and turn on either/both Start Screen Saver or Put Display to Sleep

*Terminal Method:*

For all users, run the following commands to set Start Screen Saver or Put Display to Sleep as a Hot Corner:

```
$ sudo -u <username> /usr/bin/defaults read com.apple.dock <corner> -int <5  
or 10>
```

*example:*

```
$ sudo -u seconduser /usr/bin/defaults write com.apple.dock wvous-tl-corner -  
int 10  
  
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-tl-corner  
10  
  
$ sudo -u seconduser /usr/bin/defaults write com.apple.dock wvous-bl-corner -  
int 5  
  
$ sudo -u seconduser /usr/bin/defaults read com.apple.dock wvous-bl-corner  
10
```









### Profile Method:

1. Create or edit a configuration profile with the PayloadType of `com.apple.dock`
2. Add the key `Forced`
3. Set the key to the following (based on the corner(s) that your organization has selected):

```
<array>
  <dict>
    <key>mcx_preference_settings</key>
    <dict>
      <key>wvous-bl-corner</key>
      <integer><5 or 10></integer>
      <key>wvous-br-corner</key>
      <integer><5 or 10></integer>
      <key>wvous-tl-corner</key>
      <integer><5 or 10></integer>
      <key>wvous-tr-corner</key>
      <integer><5 or 10></integer>
    </dict>
  </dict>
</array>
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## **2.4 *Sharing***

This section contains recommendations related to the configurable items under the *Sharing* panel.

### 2.4.1 Ensure Remote Apple Events Is Disabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on one computer to communicate with a program on a different computer.

#### Rationale:

Disabling Remote Apple Events mitigates the risk of an unauthorized program gaining access to the system.

#### Impact:

With remote Apple events turned on, an AppleScript program running on another Mac can interact with the local computer.

#### Audit:

Perform the following to ensure that Remote Apple Events is not enabled:

##### *Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Remote Apple Events is not set

##### *Terminal Method:*

Run the following commands to verify that Remote Apple Events is not set

```
$ sudo /usr/sbin/systemsetup -getremoteappleevents  
Remote Apple Events: Off
```

## Remediation:

Perform the following to disable Remote Apple Events:

*Graphical Method:*











1. Open System Preferences
2. Select Sharing
3. Verify that Remote Apple Events is not set

*Terminal Method:*

Run the following commands to set Remote Apple Events to Off:

```
$ sudo /usr/sbin/systemsetup -setremoteappleevents off  
setremoteappleevents: Off
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## *2.4.2 Ensure Internet Sharing Is Disabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Internet Sharing uses the open source `natd` process to share an internet connection with other computers and devices on a local network. This allows the Mac to function as a router and share the connection to other, possibly unauthorized, devices.

### **Rationale:**

Disabling Internet Sharing reduces the remote attack surface of the system.

### **Impact:**

Internet Sharing allows the computer to function as a router and other computers to use it for access. This can expose both the computer itself and the networks it is accessing to unacceptable access from unapproved devices.

## Audit:

Perform the following to ensure Internet Sharing is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Internet Sharing is not set

*Terminal Method:*

Run the following commands to verify that Internet Sharing is not set:

```
$ sudo defaults read /Library/Preferences/SystemConfiguration/com.apple.nat |  
grep -i Enabled
```

Verify that the output does not include `Enabled = 1`.

**Note:** If the settings has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

**or**

Run the following command to verify that a profile is installed that automatically disables internet sharing:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep forceInternetSharingOff  
  
forceInternetSharingOff = 1;
```

## Remediation:

Perform the following to disable Internet Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Internet Sharing

*Terminal Method:*

Run the following command to turn off Internet Sharing:

```
$ sudo defaults write /Library/Preferences/SystemConfiguration/com.apple.nat  
NAT -dict Enabled -int 0
```

**Note:** Using the Terminal Method will not uncheck the setting in System Preferences>Sharing but will disable the underlying service.











*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.MCX`
2. Add the key `forceInternetSharingOff`
3. Set the key to `</true>`

## References:

1. STIGID AOSX-12-001270

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			



### 2.4.3 Ensure Screen Sharing Is Disabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Screen Sharing allows a computer to connect to another computer on a network and display the computer's screen. While sharing the computer's screen, the user can control what happens on that computer, such as opening documents or applications, opening, moving, or closing windows, and even shutting down the computer.

#### Rationale:

Disabling Screen Sharing mitigates the risk of remote connections being made without the user of the console knowing that they are sharing the computer.

#### Audit:

Perform the following to ensure Screen Sharing is not enabled:

##### *Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Screen Sharing is not set

##### *Terminal Method:*

Run the following commands to verify that Screen Sharing is not set:

```
$ sudo launchctl print-disabled system | grep -c '"com.apple.screensharing"
=> true'
```

1

**Note:** If the settings has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

## Remediation:

Perform the following to disable Screen Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Screen Sharing

*Terminal Method:*











Run the following command to turn off Screen Sharing:

```
$ sudo launchctl disable system/com.apple.screensharing
```

## References:

1. <http://support.apple.com/kb/ph11151>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 2.4.4 Ensure Printer Sharing Is Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

By enabling Printer Sharing the computer is set up as a print server to accept print jobs from other computers. Dedicated print servers or direct IP printing should be used instead.

### Rationale:

Disabling Printer Sharing mitigates the risk of attackers attempting to exploit the print server to gain access to the system.

### Audit:

Perform the following to ensure that Printer Sharing is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Printer Sharing is not enabled

*Terminal Method:*

Run the following command to verify that Printer Sharing is not enabled:

```
$ sudo cupsctl | grep _share_printers | cut -d'=' -f2  
0
```

**Note:** If the setting has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

## Remediation:

Perform the following to disable Printer Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Printer Sharing

*Terminal Method:*











Run the following command to disable Printer Sharing:

```
$ sudo cupsctl --no-share-printers
```

## References:

1. <http://support.apple.com/kb/PH11450>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

### *2.4.5 Ensure Remote Login Is Disabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Remote Login allows an interactive terminal connection to a computer.

**Rationale:**

Disabling Remote Login mitigates the risk of an unauthorized person gaining access to the system via Secure Shell (SSH). While SSH is an industry standard to connect to posix servers, the scope of the benchmark is for Apple macOS clients, not servers.

macOS does have an IP based firewall available (pf, ipfw has been deprecated) that is not enabled or configured. There are more details and links in section 7.5. macOS no longer has TCP Wrappers support built-in and does not have strong Brute-Force password guessing mitigations, or frequent patching of openssh by Apple. Since most macOS computers are mobile workstations, managing IP-based firewall rules on mobile devices can be very resource-intensive. All of these factors can be parts of running a hardened SSH server.

## Impact:

The SSH server built-in to macOS should not be enabled on a standard user computer, particularly one that changes locations and IP addresses. A standard user that runs local applications including email, web browser and productivity tools should not use the same device as a server. There are Enterprise management tool-sets that do utilize SSH. If they are in use, the computer should be locked down to only respond to known, trusted IP addresses and appropriate admin service accounts.

For macOS computers that are being used for specialized functions there are several options to harden the SSH server to protect against unauthorized access including brute force attacks. There are some basic criteria that need to be considered:

- Do not open an SSH server to the internet without controls in place to mitigate SSH brute force attacks. This is particularly important for systems bound to Directory environments. It is great to have controls in place to protect the system, but if they trigger after the user is already locked out of their account they are not optimal. If authorization happens after authentication directory accounts for users that don't even use the system can be locked out.
- Do not use SSH key pairs when there is no insight to the security on the client system that will authenticate into the server with a private key. If an attacker gets access to the remote system and can find the key they may not need a password or a key logger to access the SSH server.
- Detailed instructions on hardening an SSH server, if needed, are available in the CIS Linux Benchmarks but it is beyond the scope of this benchmark.

## Audit:

Perform the following to ensure that Remote Login is disabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Remote Login is not set

*Terminal Method:*

Run the following command to verify that Remote Login is disabled:

```
$ sudo systemsetup -getremotelogin
```

```
Remote Login: Off
```

## Remediation:

Perform the following to disable Remote Login:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Remote Login

*Terminal Method:*

Run the following command to disable Remote Login:

```
$ sudo systemsetup -setremotelogin off
```











```
Do you really want to turn remote login off? If you do, you will lose this  
connection and can only turn it back on locally at the server (yes/no)?
```

Entering yes will disable remote login.

## Additional Information:

```
man sshd_config
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			



## 2.4.6 Ensure DVD or CD Sharing Is Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

DVD or CD Sharing allows users to remotely access the system's optical drive. While Apple does not ship Macs with built-in optical drives any longer, external optical drives are still recognized when they are connected. In testing the sharing of an external optical drive persists when a drive is reconnected.

### Rationale:

Disabling DVD or CD Sharing minimizes the risk of an attacker using the optical drive as a vector for attack and exposure of sensitive data.

### Impact:

Many Apple devices are now sold without optical drives and drive sharing may be needed for legacy optical media. The media should be explicitly re-shared as needed rather than using a persistent share. Optical drives should not be used for long term storage. To store necessary data from an optical drive it should be copied to another form of external storage. Optionally, an image can be made of the optical drive so that it is stored in it's original form on another form of external storage

### Audit:

Perform the following to ensure that DVD or CD Sharing is disabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that DVD or CD sharing is not set

*Terminal Method:*

Run the following command to verify that DVD or CD Sharing is disabled

```
$ sudo launchctl print-disabled system | grep -c '"com.apple.ODSAgent" => true'
```

```
1
```

## Remediation:

Perform the following to disable DVD or CD Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck DVD or CD sharing











*Terminal Method:*

Run the following command to disable DVD or CD Sharing:

```
$ sudo launchctl disable system/com.apple.ODSAgent
```

**Note:** If using the Terminal method, the GUI will still show the service checked until after a reboot.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

### *2.4.7 Ensure Bluetooth Sharing Is Disabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Bluetooth Sharing allows files to be exchanged with Bluetooth-enabled devices.

**Rationale:**

Disabling Bluetooth Sharing minimizes the risk of an attacker using Bluetooth to remotely attack the system.

**Impact:**

Control 2.1.1 discusses disabling Bluetooth if no paired devices exist. There is a general expectation that Bluetooth peripherals will be used by most users in Apple's ecosystem. It is possible that sharing is required and Bluetooth peripherals are not. Bluetooth must be enabled if sharing is an acceptable use case.

## Audit:

Perform the following to verify that Bluetooth Sharing is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Bluetooth Sharing is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `PrefKeyServicesEnabled = 0`

*Terminal Method:*

Run the following command to verify that Bluetooth Sharing is disabled:

```
sudo -u <username> /usr/bin/defaults -currentHost read com.apple.Bluetooth
PrefKeyServicesEnabled

0

$ sudo -u firstuser /usr/bin/defaults -currentHost read com.apple.Bluetooth
PrefKeyServicesEnabled

0
```

**or**

Run the following command to verify that a profile is installed that disables Bluetooth sharing:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep
"PrefKeyServicesEnabled"

PrefKeyServicesEnabled = 0;
```

## Remediation:

Perform the following to disable Bluetooth Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Bluetooth Sharing

Run the following command to disable Bluetooth Sharing is disabled:

















```
sudo -u <username> /usr/bin/defaults -currentHost write com.apple.Bluetooth  
PrefKeyServicesEnabled -bool false  
  
$ sudo -u firstuser /usr/bin/defaults -currentHost write com.apple.Bluetooth  
PrefKeyServicesEnabled -bool false
```

*Profile Method:*

1. Create or edit a configuration profile with the key of `com.apple.Bluetooth` under `PayloadContent`
2. Add the following set of keys with the `com.apple.Bluetooth` key:

```
<dict>  
    <key>Forced</key>  
    <array>  
        <dict>  
            <key>mcx_preference_settings</key>  
            <dict>  
                <key>PrefKeyServicesEnabled</key>  
                <false/>  
            </dict>  
        </dict>  
    </array>  
</dict>
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.3 Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>4.8 Log and Alert on Changes to Administrative Group Membership</u></b> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<b><u>14.6 Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## *2.4.8 Ensure File Sharing Is Disabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Server Message Block (SMB), Common Internet File System (CIFS) When Windows (or possibly Linux) computers need to access file shared on a Mac, SMB/CIFS file sharing is commonly used. Apple warns that SMB sharing stores passwords in a less secure fashion than AFP sharing and anyone with system access can gain access to the password for that account. When sharing with SMB, each user that will access the Mac must have SMB enabled.

### **Rationale:**

By disabling File Sharing, the remote attack surface and risk of unauthorized access to files stored on the system is reduced.

### **Impact:**

File Sharing can be used to share documents with other users but hardened servers should be used rather than user endpoints. Turning on File Sharing increases the visibility and attack surface of a system unnecessarily.

## Audit:

Perform the following to ensure that File Sharing is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that File Sharing is not set

*Terminal Method:*

Run the following command to verify that SMB File Sharing is not enabled:

```
$ sudo launchctl print-disabled system | grep -c '"com.apple.smbd" => true'
1
```

**Note:** If the settings have not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

## Remediation:

Perform the following to disable File Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck File Sharing

*Terminal Method:*

Run the following command to disable SMB file sharing:

















```
$ sudo launchctl disable system/com.apple.smbd
```

## Additional Information:

macOS also supported file sharing using Apple File Protocol (AFP) until 10.15 Catalina. AFP was removed in 11.0 Big Sur.



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v8	<p><b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b></p> <p>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>			
v7	<p><b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b></p> <p>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## 2.4.9 Ensure Remote Management Is Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

Remote Management is the client portion of Apple Remote Desktop (ARD). Remote Management can be used by remote administrators to view the current screen, install software, report on, and generally manage client Macs.

The screen sharing options in Remote Management are identical to those in the Screen Sharing section. In fact, only one of the two can be configured. If Remote Management is used, refer to the Screen Sharing section above on issues regard screen sharing.

Remote Management should only be enabled when a Directory is in place to manage the accounts with access. Computers will be available on port 5900 on a macOS System and could accept connections from untrusted hosts depending on the configuration, definitely a concern for mobile systems.

### Rationale:

Remote Management should only be enabled on trusted networks with strong user controls present in a Directory system. Mobile devices without strict controls are vulnerable to exploit and monitoring.

### Impact:

Many organizations utilize ARD for client management.

### Audit:

Perform the following to verify that Remote Management is not enabled:

1. Open System Preferences
2. Select Sharing
3. Verify that Remote Management is not set

Run the following command to verify that Remote Management is not enabled:

```
$ sudo ps -ef | grep -e ARDAgent  
0  9233  8630  0  3:32pm ttys001    0:00.00 grep -e ARDAgent
```

## Remediation:

Perform the following to disable Remote Management:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Remote Management

*Terminal Method:*






Run the following command to disable Remote Management:

```
$ sudo  
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources  
/kickstart -deactivate -stop  
  
Starting...  
Removed preference to start ARD after reboot.  
Done.
```

## Additional Information:

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources  
/kickstart -help
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			
v7	<b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<b><u>14.3 Disable Workstation to Workstation Communication</u></b> Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.			

## 2.4.10 Ensure Content Caching Is Disabled (Automated)

### Profile Applicability:

- Level 2

### Description:

Starting with 10.13 (macOS High Sierra) Apple introduced a service to make it easier to deploy data from Apple, including software updates, where there are bandwidth constraints to the Internet and fewer constraints and greater bandwidth on the local subnet. This capability can be very valuable for organizations that have throttled and possibly metered Internet connections. In heterogeneous enterprise networks with multiple subnets the effectiveness of this capability would be determined on how many Macs were on each subnet at the time new large updates were made available upstream. This capability requires the use of macOS clients as P2P nodes for updated Apple content. Unless there is a business requirement to manage operational Internet connectivity bandwidth user endpoints should not store content and act as a cluster to provision data.

### [Content types supported by Content Caching in macOS](#)

### Rationale:

The main use case for Mac computers is as mobile user endpoints. P2P sharing services should not be enabled on laptops that are using untrusted networks. Content Caching can allow a computer to be a server for local nodes on an untrusted network. While there are certainly logical controls that could be used to mitigate risk, they add to the management complexity. Since the value of the service is in specific use cases organizations with the use case described above can accept risk as necessary.

### Impact:

This setting will adversely affect bandwidth usage between local subnets and the Internet.

## Audit:

Perform the following to ensure that Content Caching is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Content Caching is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `AutoActivation` set to 0
4. Verify that an installed profile has `AllowSharedCaching` set to 0

*Terminal Method:*

Run the following command to verify that Content Caching is not enabled:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.AssetCache.plist
Activated
0
```

**or**

Run the following command to verify that a profile is installed that disables content caching:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep AutoActivation
AutoActivation = 0;

$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep AllowSharedCaching
AllowSharedCaching = 0;
```

## Remediation:

Perform the following to disable Content Caching:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Content Caching

*Terminal Method:*

Run the following command to disable Content Caching:

```
$ sudo /usr/bin/AssetCacheManagerUtil deactivate
```

The output will include Content caching deactivated

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.AssetCache`
2. Add the key `AutoActivation`
3. Set the key to `</false>`
4. Add the key `AllowSharedCaching`
5. Set the key to `</false>`

## References:

1. <https://support.apple.com/guide/mac-help/about-content-caching-mchl9388ba1b/>
2. <https://support.apple.com/guide/mac-help/set-up-content-caching-on-mac-mchl3b6c3720/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

### *2.4.11 Ensure AirDrop Is Disabled (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

AirDrop is Apple's built-in on demand ad hoc file exchange system that is compatible with both macOS and iOS. It uses Bluetooth LE for discovery that limits connectivity to Mac or iOS users that are in close proximity. Depending on the setting it allows everyone or only Contacts to share files when they are nearby to each other.

In many ways this technology is far superior to the alternatives. The file transfer is done over a TLS encrypted session, does not require any open ports that are required for file sharing, does not leave file copies on email servers or within cloud storage, and allows for the service to be mitigated so that only people already trusted and added to contacts can interact with you.

While there are positives to AirDrop, there are privacy concerns that could expose personal information. For that reason, AirDrop should be disabled, and should only be enabled when needed and disabled afterwards.

#### **Rationale:**

AirDrop can allow malicious files to be downloaded from unknown sources. Contacts Only limits may expose personal information to devices in the same area.

#### **Impact:**

Disabling AirDrop can limit the ability to move files quickly over the network without using file shares.



**Audit:**

Perform the following to ensure that AirDrop is disabled:

*Graphical Method:*

1. Open Control Center in the Menu Bar
2. Select AirDrop
3. Verify that AirDrop is not set
4. Open System Preferences
5. Select Dock & Menu Bar
6. Select AirDrop
7. Verify that Show in Menu Bar is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `DisableAirDrop = 1` is set

### *Terminal Method:*

For all users, run the following commands to verify whether AirDrop is disabled:

```
$ sudo -u <username> /usr/bin/defaults read com.apple.NetworkBrowser  
DisableAirDrop  
  
1
```

**Note:** If the setting has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

*example:*

```
$ sudo -u firstuser /usr/bin/defaults read com.apple.NetworkBrowser  
DisableAirDrop  
  
1  
  
$ sudo -u seconduser /usr/bin/defaults read com.apple.NetworkBrowser  
DisableAirDrop  
  
0  
  
$ sudo -u thirduser /usr/bin/defaults read com.apple.NetworkBrowser  
DisableAirDrop  
  
The domain/default pair of (com.apple.NetworkBrowser, DisableAirDrop) does  
not exist
```

**or**

Run the following command to verify that a profile is installed that disabled AirDrop:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep DisableAirDrop  
  
DisableAirDrop = 1;
```

## Remediation:

Perform the following to disable AirDrop:

*Graphical Method:*

1. Open Control Center in the Menu Bar
2. Select AirDrop
3. Set AirDrop to disabled
4. Open System Preferences
5. Select Dock & Menu Bar
6. Select AirDrop
7. Set Show in Menu Bar to Off

*Terminal Method:*

Run the following commands to disable AirDrop:

```
$ sudo -u <username> defaults write com.apple.NetworkBrowser DisableAirDrop -bool true
```

*example:*

```
$ sudo -u seconduser defaults write com.apple.NetworkBrowser DisableAirDrop -bool true
```

*Profile Method:*












1. Create or edit a configuration profile with the PayloadType of com.apple.NetworkBrowser
2. Add the key Forced
3. Set the key to the following:

```
<array>
  <dict>
    <key>mcx_preference_settings</key>
    <dict>
      <key>DisableAirDrop</key>
      <true/>
    </dict>
  </dict>
</array>
```

## References:

1. <https://www.techrepublic.com/article/apple-airdrop-users-reportedly-vulnerable-to-security-flaw/>
2. <https://www.imore.com/how-apple-keeps-your-airdrop-files-private-and-secure>
3. <https://en.wikipedia.org/wiki/AirDrop>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<b><u>6.7 Centralize Access Control</u></b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>15.4 Disable Wireless Access on Devices if Not Required</u></b> Disable wireless access on devices that do not have a business purpose for wireless access.			

## 2.4.12 Ensure Media Sharing Is Disabled (Automated)

### Profile Applicability:

- Level 2

### Description:

Starting with macOS 10.15 Apple has provided a control to allow a user to share Apple downloaded content on all Apple devices that are signed in with the same Apple ID. This allows a user to share downloaded Movies, Music or TV shows with other controlled macOS, iOS and iPadOS devices as well as photos with Apple TVs.

With this capability guest users can also use media downloaded on the computer.

The recommended best practice is not to use the computer as a server but to utilize Apple's cloud storage to download and use content stored there if content stored with Apple is used on multiple devices.

<https://support.apple.com/guide/mac-help/set-up-media-sharing-on-mac-mchlp13371337/mac> This capability requires the use of macOS clients as P2P nodes for updated Apple content. Unless there is a business requirement to manage operational Internet connectivity bandwidth user endpoints should not store content and act as a cluster to provision data.

### [Content types supported by content caching in macOS](#)

### Rationale:

Disabling Media Sharing reduces the remote attack surface of the system.

### Impact:

Media Sharing allows for pre-downloaded content on a Mac to be available to other Apple devices on the same network. Leaving this disabled forces device users to stream or download content from each Apple authorized device. This sharing could even allow unauthorized devices on the same network media access.

**Audit:**

Perform the following to ensure that Media Sharing is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Verify that Media Sharing is not selected

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `homeSharingUIStatus` set to 0
4. Verify that an installed profile has `legacySharingUIStatus` set to 0
5. Verify that an installed profile has `mediaSharingUIStatus` set to 0

### *Terminal Method:*

Run the following command to verify that Media Sharing is not enabled:

```
$ sudo -u <username> defaults read com.apple.amp.mediasharingd home-sharing-enabled  
0
```

*example:*

```
$ sudo -u test defaults read com.apple.amp.mediasharingd home-sharing-enabled  
0  
  
$ sudo -u test2 defaults read com.apple.amp.mediasharingd home-sharing-enabled  
1
```

**or**

Run the following command to verify that a profile is installed that disables Media Sharing:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep homeSharingUIStatus  
homeSharingUIStatus = 0;  
  
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep legacySharingUIStatus  
legacySharingUIStatus = 0;  
  
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep mediaSharingUIStatus  
mediaSharingUIStatus = 0;
```

## Remediation:

Perform the following to disable Media Sharing:

*Graphical Method:*

1. Open System Preferences
2. Select Sharing
3. Uncheck Media Sharing

*Terminal Method:*

Run the following command to disable Media Sharing:

```
$ sudo -u <username> defaults write com.apple.amp.mediasharingd home-sharing-enabled -int 0
```

*example:*











```
$ sudo -u test2 defaults write com.apple.amp.mediasharingd home-sharing-enabled -int 0
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.preferences.sharing.SharingPrefsExtension
2. Add the key homeSharingUIStatus
3. Set the key to <integer>0</integer>
4. Add the key legacySharingUIStatus
5. Set the key to <integer>0</integer>
6. Add the key mediaSharingUIStatus
7. Set the key to <integer>0</integer>



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## **2.5 Security & Privacy**

This section contains recommendations for configurable options under the *Security & Privacy* panel.

[Additional privacy preference information from Apple](#)

### ***2.5.1 Encryption***

Apple has created simple easy to use encryption capabilities built-in to macOS. In order to protect data and privacy, those tools need to be utilized to protect information processed by macOS computers.

### 2.5.1.1 Ensure FileVault Is Enabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

FileVault secures a system's data by automatically encrypting its boot volume and requiring a password or recovery key to access it.

Filevault may also be enabled using command line using the `fdsetup` command. To use this functionality, consult the Der Flounder blog for more details:

<https://derflounder.wordpress.com/2015/02/02/managing-yosemites-filevault-2-with-fdsetup/> <https://derflounder.wordpress.com/2019/01/15/unlock-or-decrypt-your-filevault-encrypted-boot-drive-from-the-command-line-on-macos-mojave/>

#### Rationale:

Encrypting sensitive data minimizes the likelihood of unauthorized users gaining access to it.

#### Impact:

Mounting a FileVaulted volume from an alternate boot source will require a valid password to decrypt it.

#### Audit:

Perform the following to verify that FileVault is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select FileVault
4. Verify that FileVault is on

*Terminal Method:*

Run the following command to verify that FileVault is enabled:

```
$ sudo fdsetup status  
FileVault is On
```

## Remediation:

Perform the following to enable FileVault:










*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select FileVault
4. Select Turn on FileVault

## Additional Information:

FileVault may not be desirable on a virtual OS. As long as the hypervisor and file storage are encrypted the virtual OS does not need to be. Rather than checking if the OS is virtual and passing the control regardless of the encryption of the host system the normal check will be run. Security officials can evaluate the comprehensive controls outside of the OS being tested.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.6 <u>Encrypt Data on End-User Devices</u></b> Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.			
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u></b> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

### *2.5.1.2 Ensure all user storage APFS volumes are encrypted (Manual)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

Apple developed a new file system that was first made available in 10.12 and then became the default in 10.13. The file system is optimized for Flash and Solid State storage and encryption. [https://en.wikipedia.org/wiki/Apple\\_File\\_System](https://en.wikipedia.org/wiki/Apple_File_System) macOS computers generally have several volumes created as part of APFS formatting including Preboot, Recovery and Virtual Memory (VM) as well as traditional user disks.

All APFS volumes that do not have specific roles that do not require encryption should be encrypted. "Role" disks include Preboot, Recovery and VM. User disks are labelled with "(No specific role)" by default.

#### **Rationale:**

In order to protect user data from loss or tampering volumes carrying data should be encrypted.

#### **Impact:**

While FileVault protects the boot volume data may be copied to other attached storage and reduce the protection afforded by FileVault. Ensure all user volumes are encrypted to protect data.

## Audit:

Run the following command to list the APFS Volumes:

```
$ sudo diskutil ap list
```

Ensure all user data disks are encrypted.

*example:*

```
APFS Volume Disk (Role):  disk1s1 (No specific role)
Name:                     Macintosh HD (Case-insensitive)
Mount Point:              /
Capacity Consumed:        188514598912 B (188.5 GB)
FileVault:                Yes (Unlocked)

APFS Containers (2 found)
|
+-- Container disk1 XXXX
|  =====
|  APFS Container Reference:  disk1
|  Size (Capacity Ceiling):  249152200704 B (249.2 GB)
|  Minimum Size:            249152200704 B (249.2 GB)
|  Capacity In Use By Volumes: 195635597312 B (195.6 GB) (78.5% used)
|  Capacity Not Allocated:   53516603392 B (53.5 GB) (21.5% free)
|  |
|  +-< Physical Store disk0s4 XXXXXY
|  |  -----
|  |  APFS Physical Store Disk:  disk0s4
|  |  Size:                      249152200704 B (249.2 GB)
|  |  |
|  +-> Volume disk1s1 XXXXXZ
|  |  -----
|  |  APFS Volume Disk (Role):  disk1s1 (No specific role)
|  |  Name:                     HighSierra (Case-insensitive)
|  |  Mount Point:              /
|  |  Capacity Consumed:        188514598912 B (188.5 GB)
|  |  FileVault:                Yes (Unlocked)
|  |  |
|  +-> Volume disk1s2 XXXXXZZ
|  |  -----
|  |  APFS Volume Disk (Role):  disk1s2 (Preboot)
|  |  Name:                     Preboot (Case-insensitive)
|  |  Mount Point:              Not Mounted
|  |  Capacity Consumed:        23961600 B (24.0 MB)
|  |  FileVault:                No
|  |  |
|  +-> Volume disk1s3 XXXXXYY
|  |  -----
|  |  APFS Volume Disk (Role):  disk1s3 (Recovery)
|  |  Name:                     Recovery (Case-insensitive)
|  |  Mount Point:              Not Mounted
|  |  Capacity Consumed:        518127616 B (518.1 MB)
|  |  FileVault:                No
|  |  |
```

```

|   +-> Volume disk1s4 XXXXXYYYY
|   -----
|   APFS Volume Disk (Role):   disk1s4 (VM)
|   Name:                     VM (Case-insensitive)
|   Mount Point:              /private/var/vm
|   Capacity Consumed:        6442704896 B (6.4 GB)
|   FileVault:                No
|
+-- Container disk4 XXXXXYYYYY
=====
APFS Container Reference:      disk4
Size (Capacity Ceiling):      119824367616 B (119.8 GB)
Minimum Size:                 143192064 B (143.2 MB)
Capacity In Use By Volumes:   126492672 B (126.5 MB) (0.1% used)
Capacity Not Allocated:       119697874944 B (119.7 GB) (99.9% free)
|
+--< Physical Store disk3s2 XXXXXYYYYYYY
|   -----
|   APFS Physical Store Disk:  disk3s2
|   Size:                     119824371200 B (119.8 GB)
|
+-> Volume disk4s1 C4D99580-1FDA-43BF-BB62-B21BF7EE568C
|   -----
|   APFS Volume Disk (Role):   disk4s1 (No specific role)
|   Name:                     Passport (Case-insensitive)
|   Mount Point:              /Volumes/Passport
|   Capacity Consumed:        839680 B (839.7 KB)
|   FileVault:                Yes (Unlocked)

```










## Remediation:

Use Disk Utility to erase a user disk and format as APFS (Encrypted).

**Note:** APFS Encrypted disks will be described as "FileVault" whether they are the boot volume or not in the ap list.



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.6 Encrypt Data on End-User Devices</u></b> Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.			
v8	<b><u>3.11 Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b><u>13.6 Encrypt the Hard Drive of All Mobile Devices.</u></b> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.			
v7	<b><u>14.8 Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

### *2.5.1.3 Ensure all user storage CoreStorage volumes are encrypted (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

Apple introduced CoreStorage with 10.7. It is used as the default for formatting on macOS volumes prior to 10.13.

All HFS and CoreStorage Volumes should be encrypted

**Rationale:**

In order to protect user data from loss or tampering, volumes carrying data should be encrypted

**Impact:**

While FileVault protects the boot volume data may be copied to other attached storage and reduce the protection afforded by FileVault. Ensure all user volumes are encrypted to protect data.

## Audit:

Run the following command to list the CoreStorage Volumes:

```
$ sudo diskutil cs list
```

Ensure all "Logical Volume Family" disks are encrypted

*example:*

```
CoreStorage logical volume groups (2 found)
|
|-- Logical Volume Group XXXXX
|   =====
|   Name:           Macintosh HD
|   Status:         Online
|   Size:           250160967680 B (250.2 GB)
|   Free Space:     6516736 B (6.5 MB)
|   |
|   +-< Physical Volume XXXXXY
|       -----
|       |   Index:      0
|       |   Disk:       disk0s2
|       |   Status:     Online
|       |   Size:       250160967680 B (250.2 GB)
|       |
|       +-> Logical Volume Family XXXXXYY
|           -----
|           Encryption Type:      AES-XTS
|           Encryption Status:    Unlocked
|           Conversion Status:    Complete
|           High Level Queries:   Fully Secure
|           |                     Passphrase Required
|           |                     Accepts New Users
|           |                     Has Visible Users
|           |                     Has Volume Key
|           |
|           +-> Logical Volume XXXXXYYY
|               -----
|               Disk:             disk2
|               Status:           Online
|               Size (Total):     249802129408 B (249.8 GB)
|               Revertible:       Yes (unlock and decryption required)
|               LV Name:         Macintosh HD
|               Volume Name:     Macintosh HD
|               Content Hint:     Apple_HFS
|
```

```









+-- Logical Volume Group XXXXXXXYYY
=====
Name:          Passport
Status:        Online
Size:          119690149888 B (119.7 GB)
Free Space:    1486848 B (1.5 MB)
|
+-< Physical Volume XXXXXXXYYY
|-----
| Index:       0
| Disk:        disk3s2
| Status:      Online
| Size:        119690149888 B (119.7 GB)
|
+-> Logical Volume Family XXXXXXXYYYY
-----
Encryption Type:      AES-XTS
Encryption Status:    Unlocked
Conversion Status:    Complete
High Level Queries:   Fully Secure
|                     Passphrase Required
|                     Accepts New Users
|                     Has Visible Users
|                     Has Volume Key
|
+-> Logical Volume XXXXXXXYYYYY
-----
Disk:                disk4
Status:              Online
Size (Total):        119336337408 B (119.3 GB)
Revertible:          No
LV Name:             Passport
Volume Name:         Passport
Content Hint:        Apple_HFS

```

## Remediation:

Use Disk Utility to erase a disk and format as macOS Extended (Journaled, Encrypted)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.9 Encrypt Data on Removable Media</u></b> Encrypt data on removable media.			
v8	<b><u>3.11 Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b><u>13.6 Encrypt the Hard Drive of All Mobile Devices.</u></b> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.			
v7	<b><u>14.8 Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## 2.5.2 Firewall

macOS has a built-in firewall that has two main configuration aspects. Both the Application Layer Firewall (ALF) and the Packet Filter Firewall (PF) can be used to secure running ports and services on a Mac. The Application Firewall is the one accessible in System Preferences under security. The PF firewall contains many more capabilities than ALF, but also requires a greater understanding of firewall recipes and rule configurations. For standard use cases on a Mac use of the PF firewall is not necessary. macOS may expose server services that are reachable remotely but that is not the primary use case or design. If custom use cases are required the PF firewall can provide additional security. Macs that are used as mobile desktops do not need to use the PF firewall capabilities unless permanently open ports need to be protected with more granular IP access controls.

### Additional information

<https://www.muo.com/tag/mac-really-need-firewall/>

<https://blog.neilsabol.site/post/quickly-easily-adding-pf-packet-filter-firewall-rules-macos-osx/>

<http://marckerr.com/a-simple-guide-to-the-mac-pf-firewall/>

<https://blog.scottlowe.org/2013/05/15/using-pf-on-os-x-mountain-lion/>

### 2.5.2.1 *Ensure Gatekeeper is Enabled (Automated)*

#### Profile Applicability:

- Level 1

#### Description:

Gatekeeper is Apple's application white-listing control that restricts downloaded applications from launching. It functions as a control to limit applications from unverified sources from running without authorization.

#### Rationale:

Disallowing unsigned software will reduce the risk of unauthorized or malicious applications from running on the system.

## Audit:

Perform the following to ensure that Gatekeeper is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select General
4. Verify that Allow apps downloaded from is set to App Store and identified developers

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has Policies set to Enable
4. Verify that an installed profile has Identified Developers set to Allow

*Terminal Method:*

Run the following command to verify that Gatekeeper is enabled:

```
$ sudo /usr/sbin/spctl --status  
assessments enabled
```

**or**

Run the following command to verify that a profile is installed that enables Gatekeeper:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep  
AllowIdentifiedDevelopers  
  
AllowIdentifiedDevelopers = 1;  
  
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep EnableAssessment  
  
EnableAssessment = 1;
```

## Remediation:

Perform the following to enable Gatekeeper:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select General
4. Set Allow apps downloaded from to App Store and identified developers

*Terminal Method:*

Run the following command to enable Gatekeeper to allow applications from App Store and identified developers:















```
$ sudo /usr/sbin/spctl --master-enable
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.systempolicy.control`
2. Add the key `AllowIdentifiedDevelopers`
3. Set the key to `<true/>`
4. Add the key `EnableAssessment`
5. Set the key to `<true/>`



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>10.1 <u>Deploy and Maintain Anti-Malware Software</u></b> Deploy and maintain anti-malware software on all enterprise assets.			
v8	<b>10.2 <u>Configure Automatic Anti-Malware Signature Updates</u></b> Configure automatic updates for anti-malware signature files on all enterprise assets.			
v8	<b>10.5 <u>Enable Anti-Exploitation Features</u></b> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	<b>8.2 <u>Ensure Anti-Malware Software and Signatures are Updated</u></b> Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.			
v7	<b>8.4 <u>Configure Anti-Malware Scanning of Removable Devices</u></b> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.			

### *2.5.2.2 Ensure Firewall Is Enabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

A firewall is a piece of software that blocks unwanted incoming connections to a system. Apple has posted general documentation about the application firewall.

<http://support.apple.com/en-us/HT201642>

**Rationale:**

A firewall minimizes the threat of unauthorized users from gaining access to your system while connected to a network or the Internet.

**Impact:**

The firewall may block legitimate traffic. Applications that are unsigned will require special handling.

## Audit:

Perform the following to ensure the firewall is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Firewall
4. Verify that the firewall is turned on

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Firewall` set to `Enabled`

*Terminal Method:*

Run the following command to verify that the firewall is enabled:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.alf globalstate
```

Verify the output is 1 or 2.

**or**

Run the following command to verify that a profile is installed that enables the firewall:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep EnableFirewall  
  
EnableFirewall = 1;
```

## Remediation:

Perform the following to turn the firewall on:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Firewall
4. Select Turn On Firewall

*Terminal Method:*

Run the following command to enable the firewall:

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.alf globalstate -int <value>
```

For the <value>, use either 1, specific services, or 2, essential services only.

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.firewall
2. Add the key EnableFirewall
3. Set the key to <true/>

## References:

1. <http://docs.info.apple.com/article.html?artnum=306938>

### **Additional Information:**

Your organization might want to verify and limit specific applications that allow incoming connectivity.

To verify those applications:

Perform the following to ensure the system is configured as prescribed:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Firewall Options
4. Verify that your organizations necessary rules are set

*Terminal Method:*

Run the following command to verify the what applications are allowing incoming connections:

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --listapps
```

The output will show any applications, and their path, and their associated rule.

*example:*

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --listapps
ALF: total number of apps = 3

1 :  /System/Library/CoreServices/RemoteManagement/ARDAgent.app
    ( Allow incoming connections )

2 :  /Applications/Chess.app
    ( Allow incoming connections )

3 :  /Applications/Contacts.app
    ( Block incoming connections )
```

Perform the following to remove unnecessary firewall rules:

1. Open System Preferences
2. Select Security & Privacy
3. Select Firewall Options
4. Select unneeded rule(s)
5. Select the minus sign below to delete them

*Terminal Method:*

Run the following command to remove specific applications:
















```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove  
</path/application name>  
  
Application at path ( </path/application name> ) removed from firewall
```

The </path/application name> is the one to be removed from the previous listing.

*example:*

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --listapps  
ALF: total number of apps = 3  
  
1 : /System/Library/CoreServices/RemoteManagement/ARDAgent.app  
    ( Allow incoming connections )  
  
2 : /Applications/Chess.app  
    ( Allow incoming connections )  
  
3 : /Applications/Contacts.app  
    ( Block incoming connections )  
  
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove  
/Applications/Chess.app  
  
Application at path ( /Applications/Chess.app ) removed from firewall
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.5 Implement and Manage a Firewall on End-User Devices</u></b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	<b><u>13.1 Centralize Security Event Alerting</u></b> Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>9.4 Apply Host-based Firewalls or Port Filtering</u></b> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	<b><u>9.5 Implement Application Firewalls</u></b> Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			

### *2.5.2.3 Ensure Firewall Stealth Mode Is Enabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

While in Stealth mode the computer will not respond to unsolicited probes, dropping that traffic.

<http://support.apple.com/en-us/HT201642>

**Rationale:**

Stealth mode on the firewall minimizes the threat of system discovery tools while connected to a network or the Internet.

**Impact:**

Traditional network discovery tools like ping will not succeed. Other network tools that measure activity and approved applications will work as expected.

This control aligns with the primary macOS use case of a laptop that is often connected to untrusted networks where host segregation may be non-existent. In that use case hiding from the other inmates is likely more than desirable. In use cases where use is only on trusted LANs with static IP addresses stealth mode may not be desirable.



## Audit:

Perform the following to verify the firewall has stealth mode enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Firewall Options
4. Verify that Enable stealth mode is set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Stealth mode` set to `Enabled`

*Terminal Method:*

Run the following command to verify that stealth mode is enabled:

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --getstealthmode  
Stealth mode enabled
```

**or**

Run the following command to verify that a profile is installed that enables firewall stealth mode:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep EnableStealthMode  
EnableStealthMode = 1;
```

## Remediation:

Perform the following to enable stealth mode:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Firewall Options
4. Turn on Enable stealth mode

*Terminal Method:*

Run the following command to enable stealth mode:

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setstealthmode on  
Stealth mode enabled
```

*Profile Method:*















1. Edit a configuration profile with the PayloadType of `com.apple.security.firewall`
2. Add the key `EnableStealthMode`
3. Set the key to `<true/>`

**Note:** This key must be set in the same configuration profile with `EnableFirewall` set to `<true/>`. If it is set in it's own configuration profile, it will fail.

## Additional Information:

<http://docs.info.apple.com/article.html?artnum=306938>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.5 Implement and Manage a Firewall on End-User Devices</u></b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>9.4 Apply Host-based Firewalls or Port Filtering</u></b> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

### *2.5.3 Ensure Location Services Is Enabled (Automated)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

macOS uses location information gathered through local Wi-Fi networks to enable applications to supply relevant information to users. With the operating system verifying the location, users do not need to change the time or the time zone. The computer will change them based on the user's location. They do not need to specify their location for weather or travel times and even get alerts on travel times to meetings and appointment where location information is supplied.

Location Services simplify some processes, for the purpose of asset management and time and log management, with mobile computers.

There are some use cases where it is important that the computer not be able to report its exact location. While the general use case is to enable Location Services, it should not be allowed if the physical location of the computer and the user should not be public knowledge.

<https://support.apple.com/en-us/HT204690>

#### **Rationale:**

Location Services are helpful in most use cases and can simplify log and time management where computers change time zones.

## Audit:

Perform the following to ensure that Location Services is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Verify Location Services is enabled

*Terminal Method:*

Run the following command to verify that Location Services are enabled:

```
$ sudo launchctl list | grep -c com.apple.locationd  
1
```

## Remediation:

Perform the following to enable Location Services:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Enable Location Services









*Terminal Method:*

Run the following command to enable Location Services

```
$ sudo launchctl load -w  
/System/Library/LaunchDaemons/com.apple.locationd.plist
```

**Note:** In some use cases organizations may not want Location Services running. To disable Location Services, System Integrity Protection must be disabled.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## *2.5.4 Audit Location Services Access (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

macOS uses location information gathered through local Wi-Fi networks to enable applications to supply relevant information to users. While Location Services may be very useful, it may not be desirable to allow all applications that can use Location Services to use your location for Internet queries to provide tailored content based on your current location.

Ensure that the applications that can use Location Services are authorized to use that information and provide that information where the application interacts with external systems. Apple provides feedback within System Preferences and may be enabled to provide information on the menu bar when Location Services are used.

Safari can deny access from websites or prompt for access.

Applications that support Location Services can be individually controlled in the Privacy tab in Security & Privacy under System Preferences.

Access should be evaluated to ensure that privacy controls are as expected.

### **Rationale:**

Privacy controls should be monitored for appropriate settings.

### **Impact:**

Many macOS services rely on Location Services for tailored services. Users expect their time zone and weather to be relevant to where they are without manual intervention. Find my Mac does need to know where your Mac actually is. Where possible the tolerance between location privacy and convenience may be best left to the user when the location itself is not sensitive. If facility locations are not public location information should be tightly controlled.

## **Audit:**

Perform the following to verify what applications are enabled for Location Services:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Location Services
5. Verify what applications are set for Location Service information

Perform the following to verify what websites are enabled to ask for access to Location Services:

*Graphical Method:*

1. Open Safari
2. Select Safari from the menu bar
3. Select Preferences
4. Select Websites
5. Select Location
6. Verify that When visiting other websites is set to Ask or Deny

*Terminal Method:*

Run the following command to evaluate the applications that are enabled to use Location Services:

```
$ sudo /usr/bin/defaults read /var/db/locationd/clients.plist
```

Ensure that all applications listed have been authorized to access location information.



## Remediation:













Perform the following to disable unnecessary applications from accessing Location Services:

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Location Services
5. Uncheck applications that are not approved for access to Location Service information

Perform the following to set websites to ask for permission to access Location Services:

1. Open Safari
2. Select Safari from the menu bar
3. Select Preferences
4. Select Websites
5. Select Location
6. Set When visiting other websites to Ask or Deny

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.3 Address Unauthorized Software</u></b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>2.6 Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### *2.5.5 Ensure Sending Diagnostic and Usage Data to Apple Is Disabled (Automated)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Apple provides a mechanism to send diagnostic and analytics data back to Apple to help them improve the platform. Information sent to Apple may contain internal organizational information that should be controlled and not available for processing by Apple. Turn off all Analytics and Improvements sharing.

Share Mac Analytics (Share with App Developers dependent on Mac Analytic sharing)

- Includes diagnostics, usage and location data

Share iCloud Analytics

- Includes iCloud data and usage information

[Share analytics information from your Mac with Apple](#)

#### **Rationale:**

Organizations should have knowledge of what is shared with the vendor and the setting automatically forwards information to Apple.

## Audit:

Perform the following to verify that diagnostic data is not being send to Apple:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Analytics & Improvements
5. Verify that "Share Mac Analytics" is not selected
6. Verify that "Share with App Developers" is not selected

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has Allow Diagnostic Submission set to False

*Terminal Method:*

Run the following command to disable sending diagnostic and usage data to Apple:

```
$ sudo /usr/bin/defaults read /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist AutoSubmit
0
```

**or**

Run the following command to verify that a profile is installed that disables sending diagnostic and usage data to Apple:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep
allowDiagnosticSubmission

allowDiagnosticSubmission = 0;
```

## Remediation:

Perform the following to disable diagnostic data being sent to Apple:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Analytics & Improvements
5. Uncheck "Share Mac Analytics"
6. Uncheck "Share with App Developers"

*Terminal Method:*

```
$ sudo /usr/bin/defaults write /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist AutoSubmit -bool false











$ sudo /bin/chmod 644 /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist

$ sudo /usr/sbin/chgrp admin /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.applicationaccess`
2. Add the key `allowDiagnosticSubmission`
3. Set the key to `</false>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## *2.5.6 Ensure Limit Ad Tracking Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Apple provides a framework that allows advertisers to target Apple users and end-users with advertisements. While many people prefer that when they see advertising it is relevant to them and their interests, the detailed information that is data mining collected, correlated, and available to advertisers in repositories is often disconcerting. This information is valuable to both advertisers and attackers and has been used with other metadata to reveal users' identities.

Organizations should manage advertising settings on computers rather than allow users to configure the settings.

### [Apple Information](#)

Ad tracking should be limited on 10.15 and prior.

### **Rationale:**

Organizations should manage user privacy settings on managed devices to align with organizational policies and user data protection requirements.

### **Impact:**

Users will see generic advertising rather than targeted advertising. Apple warns that this will reduce the number of relevant ads.

**Audit:**

Perform the following to verify that limited ad tracking is set:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Apple Advertising
5. Verify that Personalized Ads is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `forceLimitAdTracking` set to 1
4. Verify that an installed profile has `allowApplePersonalizedAdvertising` set to 0

### *Terminal Method:*

For each user, run the following command to verify that ad tracking is limited:

```
$ sudo -u <username> defaults -currentHost read  
/Users/<username>/Library/Preferences/com.apple.AdLib.plist  
allowApplePersonalizedAdvertising  
  
0
```

### *example:*

```
$ sudo -u firstuser defaults -currentHost read  
/Users/firstuser/Library/Preferences/com.apple.AdLib.plist  
allowApplePersonalizedAdvertising  
  
0  
  
$ sudo -u seconduser defaults -currentHost read  
/Users/seconduser/Library/Preferences/com.apple.AdLib.plist  
allowApplePersonalizedAdvertising  
  
1
```

In this example, firstuser is compliant and seconduser is not.

**or**

Run the following command to verify that a profile is installed that enables Limit Ad Tracking:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep forceLimitAdTracking  
  
forceLimitAdTracking = 1;  
  
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep forceLimitAdTracking  
  
allowApplePersonalizedAdvertising = 0;
```



## Remediation:

Perform the following to set limited ad tracking:

1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Apple Advertising
5. Uncheck Personalized Ads

### *Terminal Method:*

For each needed user, run the following command to enable limited ad tracking:

```
$ sudo -u <username> defaults -currentHost write  
/Users/<username>/Library/Preferences/com.apple.Adlib.plist  
allowApplePersonalizedAdvertising -bool false
```











### *example:*

```
$ sudo -u seconduser defaults -currentHost write  
/Users/seconduser/Library/Preferences/com.apple.Adlib.plist  
forceLimitAdTracking -bool true
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.AdLib`
2. Add the key `forceLimitAdTracking`
3. Set the key to `</true>`
4. Add the key `allowApplePersonalizedAdvertising`
5. Set the key to `</false>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## *2.5.7 Audit Camera Privacy and Confidentiality (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

If the computer is present in an area where there are privacy concerns or sensitive images or actions are taking place the camera should be covered at those times. A permanent cover or alteration may be required when the computer is always located in a confidential area.

Malware is continuously discovered that circumvents the privacy controls of the built-in camera. No computer has perfect security and it seems likely that even if all the drivers are disabled or removed that working drivers can be re-introduced by a determined attacker.

### **Rationale:**

At this point video chatting and other uses of the built-in camera are standard uses for a computer. In cases where the camera is not allowed to be used at all or when the computer is located in private areas additional precautions are warranted. OS components used for the built-in video camera can also be used for other connected cameras, whether USB or Bluetooth. Removed OS components that enable a camera may be re-installed or re-enabled.

The General rule should be that if the camera can capture images that could cause embarrassment or an adverse impact the camera should be covered until it is appropriate to use.

## Audit:

Perform the following to verify if any camera is enabled/connected:

*Graphical Method:*

1. Open /Applications/Utilities/System Information
2. Select Camera
3. Verify that any camera is set to your organization's preference

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Disallow Camera Devices` set to your organization's preference

*Terminal Method:*

Run the following command to verify that a profile is installed that sets connected cameras to your organization's setting:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep allowCamera
```

`allowCamera = 0`; disables the ability to use any connected cameras and `allowCamera = 1`; enables the ability to use any connected cameras.

## Remediation:

Perform the following to set the camera settings to your organization's requirements:

*Profile Method:*







1. Create or edit a configuration profile with the `PayloadType` of `com.apple.applicationaccess`
2. Add the key `allowCamera`
3. Set the key to `</true>` or `</false>` based on your organization's preference

**\*\*Note:\*\***There is no supported method from Apple to enable/disable the built-in FaceTime camera through the GUI or the command line. Remove any external cameras based on your organization's policies.

## Additional Information:

There should be no hardware modifications done to the computers to remove any built-in FaceTime cameras.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 2.6 Apple ID

Apple is a hardware manufacturer that develops operating systems for the hardware it creates. Apple is also a cloud service provider and those services include applications, music, books, television, cloud storage etc. Apple simplifies the process to ensure that all user devices are entitled to content where the user has purchased access, or is part of an Apple basic level of entitlement (BLE) for purchasing an Apple device. The use of an Apple ID allows for a consistent access and experience across all Apple devices. An Apple ID functions as Single-Sign-On access to all Apple provided services. It is critical that each user's account is protected appropriately so that unauthorized access risk is heavily mitigated.

<https://support.apple.com/en-us/HT203993>

[https://en.wikipedia.org/wiki/Apple\\_ID](https://en.wikipedia.org/wiki/Apple_ID)

<https://www.lifewire.com/what-is-an-apple-id-1994330>

<https://support.apple.com/en-us/HT201303>

### **2.6.1 iCloud**

iCloud is Apple's service for synchronizing, storing and backing up data from Apple applications in both macOS and iOS.

macOS controls for iCloud are part of the Apple ID settings in macOS. The configuration options in macOS resemble the options in iOS.

### *2.6.1.1 Audit iCloud Configuration (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Apple's iCloud is a consumer-oriented service that allows a user to store data as well as find, control and backup devices that are associated with their Apple ID (Apple account). The use of iCloud on Enterprise devices should align with the acceptable use policy for devices that are managed as well as confidentiality requirements for data handled by the user. If iCloud is allowed the data that is copied to Apple servers will likely be duplicated on both personal as well as Enterprise devices.

For many users the Enterprise email system may replace many of the available features in iCloud. If using either an Exchange or Google environment email, calendars, notes and contacts can sync to the official Enterprise repository and be available through multiple devices.

Depending on workplace requirements it may not be appropriate to intermingle Enterprise and personal bookmarks, photos and documents. Since the service allows every device associated with the user's ID to synchronize and have access to the cloud storage the concern is not just about having sensitive data on Apple's servers but having that same data on the phone of the teenage son or daughter of an employee. The use of family sharing options can reduce the risk.

Apple's iCloud is just one of many cloud-based solutions being used for data synchronization across multiple platforms and it should be controlled consistently with other cloud services in your environment. Work with your employees and configure the access to best enable data protection for your mission.

#### **Rationale:**

Organizations must make a risk decision on how their computers will interact with public cloud services.

#### **Impact:**

iCloud services are integrated deeply into macOS and in many cases are expected to be used by Mac users. iCloud is a public cloud and is not covered by an organizational security plan. In many cases synchronizing user data from an organizational computer to an uncontrolled location, no matter who is the data owner, is unacceptable.



## Audit:

Perform the following to verify enabled iCloud services:

*Graphical Method:*

1. Open System Preferences
2. Select Apple ID
3. Select iCloud
4. Verify the settings are within your organization's parameters

*Terminal Method:*

For each user, run this command to review enabled iCloud services:

```
$ sudo -u <username> defaults read  
/Users/<username>/Library/Preferences/MobileMeAccounts
```

The output will include all settings for the user's iCloud account.

*example:*

```
$ sudo -u seconduser defaults read  
/Users/seconduser/Library/Preferences/MobileMeAccounts  
  
{  
    Accounts = (  
        {  
            AccountAlternateDSID = "000000-00-00a0aa00-0a00-0000-a000-  
0aa0a0a0a000";  
            AccountDSID = 0000000000;  
            AccountDescription = iCloud;  
            AccountID = "user@domain.domain";  
            DisplayName = "Second User";  
            LoggedIn = 1;  
            Services = (  
                {  
                    Name = CLOUDDESKTOP;  
                    ServiceID = "com.apple.Dataclass.CloudDesktop";  
                    status = active;  
                },  
                {  
                    Name = FAMILY;  
                    ServiceID = "com.apple.Dataclass.Family";  
                    showManageFamily = 1;  
                },  
                {  
                    Enabled = 1;  
                    Name = "MOBILE_DOCUMENTS";  
                    ServiceID = "com.apple.Dataclass.Ubiquity";  
                    apsEnv = production;  
                    authMechanism = token;  
                    url = "https://p13-ubiquity.icloud.com:443";  
                    wsUrl = "https://p13-ubiquityws.icloud.com:443";  
                },  
            )  
        },  
    )  
}
```

```

        {
            Enabled = 1;
            Name = "PHOTO_STREAM";
            ServiceID = "com.apple.Dataclass.Photos";
        },
        {
            Name = "MAIL_AND_NOTES";
            ServiceID = "com.apple.Dataclass.Mail";
        },
        {
            Enabled = 1;
            Name = CONTACTS;
            ServiceID = "com.apple.Dataclass.Contacts";
            authMechanism = token;
            beta = 0;
            protocol = dav;
            url = "https://p13-contacts.icloud.com:443";
        },
        {
            Enabled = 1;
            Name = CALENDAR;
            ServiceID = "com.apple.Dataclass.Calendars";
            authMechanism = token;
            beta = 0;
            protocol = dav;
            url = "https://p13-caldav.icloud.com:443";
        },
        {
            Enabled = 1;
            Name = REMINDERS;
            ServiceID = "com.apple.Dataclass.Reminders";
            authMechanism = token;
            beta = 0;
            protocol = dav;
            url = "https://p13-caldav.icloud.com:443";
        },
        {
            Enabled = 1;
            Name = BOOKMARKS;
            ServiceID = "com.apple.Dataclass.Bookmarks";
            apsEnv = production;
            authMechanism = token;
            beta = 0;
            protocol = dav;
            url = "https://p13-bookmarks.icloud.com:443";
        },
        {
            Enabled = 1;
            Name = NOTES;
            ServiceID = "com.apple.Dataclass.Notes";
        },
    },

```

```

        {
            Name = SIRI;
            ServiceID = "com.apple.Dataclass.Siri";
        },
        {
            Enabled = 0;
            Name = "KEYCHAIN_SYNC";
            ServiceID = "com.apple.Dataclass.KeychainSync";
            authMechanism = token;
            escrowProxyUrl = "https://p13-escrowproxy.icloud.com:443";
        },
        {
            Name = "SHARED_STREAMS";
            ServiceID = "com.apple.Dataclass.SharedStreams";
            apsEnv = production;
            authMechanism = token;
            beta = 0;
            url = "https://p13-sharedstreams.icloud.com:443";
        },
        {
            Enabled = 1;
            Name = "FIND_MY_MAC";
            ServiceID = "com.apple.Dataclass.DeviceLocator";
            apsEnv = Production;
            authMechanism = token;
            hostname = "p13-fmip.icloud.com";
            url = "https://p13-fmip.icloud.com:443";
        }
    );
    beta = 0;
    firstName = Second;
    isManagedAppleID = 0;
    lastName = User;
    primaryEmailVerified = 1;
}
);
}

```














## Remediation:

Perform the following to disable unapproved services:

1. Open System Preferences
2. Select Apple ID
3. Select iCloud
4. Uncheck any services that are not allowed for your organization

Use a profile to disable services where organizationally required.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.3 Address Unauthorized Software</u></b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>15.3 Classify Service Providers</u></b> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>13.4 Only Allow Access to Authorized Cloud Storage or Email Providers</u></b> Only allow access to authorized cloud storage or email providers.			

### *2.6.1.2 Audit iCloud Keychain (Manual)*

**Profile Applicability:**

- Level 2

**Description:**

The iCloud keychain is Apple's password manager that works with macOS and iOS. The capability allows users to store passwords in either iOS or macOS for use in Safari on both platforms and other iOS-integrated applications. The most pervasive use is driven by iOS use rather than macOS. The passwords stored in a macOS keychain on an Enterprise-managed computer could be stored in Apple's cloud and then be available on a personal computer using the same account. The stored passwords could be for organizational as well as for personal accounts.

If passwords are no longer being used as organizational tokens they are not in scope for iCloud keychain storage.

**Rationale:**

Ensure that the iCloud keychain is used consistently with organizational requirements.

## Audit:

Perform the following to verify the iCloud keychain sync service:

*Graphical Method:*

1. Open System Preferences
2. Select iCloud
3. Verify that Keychain is set to your organization's requirements

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Disallow iCloud Keychain Sync` is set to your organization's requirements

*Terminal Method:*

For each user, run this command to verify the iCloud keychain sync services:

```
$ sudo -u <username> /usr/bin/defaults read  
/Users/<username>/Library/Preferences/MobileMeAccounts | grep -B 1  
KEYCHAIN_SYNC  
  
Enabled = <0,1>;  
Name = "KEYCHAIN_SYNC";
```

The output will be either a 0, disabled, or 1, enabled. Verify if the setting meets your organizations requirements

*example:*

```
$ sudo -u seconduser /usr/bin/defaults read  
/Users/seconduser/Library/Preferences/MobileMeAccounts | grep -B 1  
KEYCHAIN_SYNC  
  
Enabled = 0;  
Name = "KEYCHAIN_SYNC";
```

**or**

Run the following command to verify that a profile is installed that sets iCloud Keychain sync to your organizations settings:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep allowCloudKeychainSync
```

`allowCloudKeychainSync = 0;` disables iCloud Keychain Sync and  
`allowCloudKeychainSync = 1;` enables iCloud Keychain sync.

**Remediation:**

Perform the following to set iCloud keychain sync based on your organization's requirements:

*Graphical Method:*













1. Open System Preferences
2. Select iCloud
3. Uncheck (or check) Keychain to meet your organization's requirements

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.applicationaccess`
2. Add the key `allowCloudKeychainSync`
3. Set the key to your organization's requirements

**Note:** iCloud Keychain and iCloud Drive must be set in a single configuration profile.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v8	<p><b><u>15.3 Classify Service Providers</u></b></p> <p>Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			



### *2.6.1.3 Audit iCloud Drive (Manual)*

**Profile Applicability:**

- Level 2

**Description:**

iCloud Drive is Apple's storage solution for applications on both macOS and iOS to use the same files that are resident in Apple's cloud storage. The iCloud Drive folder is available much like Dropbox, Microsoft OneDrive or Google Drive.

One of the concerns in public cloud storage is that proprietary data may be inappropriately stored in an end user's personal repository. Organizations that need specific controls on information should ensure that this service is turned off or the user knows what information must be stored on services that are approved for storage of controlled information.

**Rationale:**

Organizations should review third party storage solutions pertaining to existing data confidentiality and integrity requirements.

**Impact:**

Users will not be able to use continuity on macOS to resume the use of newly composed but unsaved files

## Audit:

Perform the following to verify if iCloud Drive is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Apple ID
3. Select iCloud
4. Verify that iCloud Drive is set within your organization's requirements

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Disallow iCloud Drive` is set to your organization's requirements

*Terminal Method:*

Run the following command to verify that iCloud Drive is set to your organizations specifications:

```
$ sudo -u <username> /usr/bin/defaults read  
/Users/<username>/Library/Preferences/MobileMeAccounts | /usr/bin/grep -B 1  
MOBILE_DOCUMENTS
```

The output will include `Enabled =` and iCloud Drive is either enabled, 1, or disabled, 0.  
Verify that the service is set to your organization's requirements.

*example:*

```
$ sudo -u seconduser /usr/bin/defaults read  
/Users/seconduser/Library/Preferences/MobileMeAccounts | /usr/bin/grep -B 1  
MOBILE_DOCUMENTS  
  
Enabled = 0;  
Name = "MOBILE_DOCUMENTS";
```

**or**

Run the following command to verify that a profile is installed that sets iCloud Drive sync to your organizations settings:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep allowCloudDocumentSync
```

`allowCloudDocumentSync = 0;` disables iCloud Drive Sync and `allowCloudDocumentSync = 1;` enables iCloud Drive sync.

## Remediation:

Perform the following to set iCloud Drive to your organization's requirements:

### Graphical Method:











1. Open System Preferences
2. Select Apple ID
3. Select iCloud
4. Uncheck iCloud Drive if cloud storage is not allowed for your organization

### Profile Method:

1. Create or edit a configuration profile with the PayLoadType of `com.apple.applicationaccess`
2. Add the key `allowCloudDocumentSync`
3. Set the key to `</true>` or `</false>` based on your organization's requirements

**Note:** iCloud Keychain and iCloud Drive must be set in a single configuration profile.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<b>15.3 Classify Service Providers</b> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

#### *2.6.1.4 Ensure iCloud Drive Document and Desktop Sync is Disabled (Automated)*

##### **Profile Applicability:**

- Level 2

##### **Description:**

With macOS 10.12 Apple introduced the capability to have a user's Desktop and Documents folders automatically synchronize to the user's iCloud Drive, provided they have enough room purchased through Apple on their iCloud drive. This capability mirrors what Microsoft is doing with the use of OneDrive and Office 365. There are concerns with using this capability.

The storage space that Apple provides for free is used by users with iCloud mail, all of a user's Photo Library created with the ever larger Multi-Pixel iPhone cameras and all of the iOS Backups. Adding a synchronization capability for users who have files going back a decade or more and storage may be tight without much larger Apple charges than the free 5GB. Users with multiple computers running 10.12 and above with unique content on each will have issues as well.

Enterprise users may not be allowed to store Enterprise information in a third-party public cloud. In previous implementations iCloud Drive or even DropBox the user selected what files were synchronized even if there were no other controls. The new feature synchronizes all files in a folder widely used to put working files.

The automatic synchronization of all files in a user's Desktop and Documents folders should be disabled.

<https://derflounder.wordpress.com/2016/09/23/icloud-desktop-and-documents-in-macos-sierra-the-good-the-bad-and-the-ugly/>

##### **Rationale:**

Automated Document synchronization should be planned and controlled to approved storage.

##### **Impact:**

Users will not be able to use iCloud for the automatic sync of the Desktop and Documents folders.

**Audit:**

Perform the following to verify if Desktop and Documents in iCloud Drive is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Apple ID
3. Select iCloud
4. Verify that iCloud Drive is not set
5. If iCloud Drive is set, select Options
6. Verify that Desktop & Documents Folders is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Disallow iCloud Desktop & Documents Sync` is set to `True`

### *Terminal Method:*

For each user, run the following command to verify that the Documents and Desktop folders are not syncing to iCloud:

```
$ sudo -u <username> /bin/ls -l /Users/<username>/Library/Mobile\
Documents/com~apple~CloudDocs/Documents/ | /usr/bin/grep total

$ sudo -u <username> /bin/ls -l /Users/<username>/Library/Mobile\
Documents/com~apple~CloudDocs/Desktop/ | /usr/bin/grep total
```

### *example:*

```
$ sudo -u seconduser /bin/ls -l /Users/seconduser/Library/Mobile\
Documents/com~apple~CloudDocs/Documents/ | /usr/bin/grep total

$ sudo -u seconduser /bin/ls -l /Users/seconduser/Library/Mobile\
Documents/com~apple~CloudDocs/Desktop/ | /usr/bin/grep total

total 8
```

In the above example, there is an output so the machine is not compliant.

**or**

Run the following command to verify that a profile is installed that disables iCloud Document and Desktop Sync:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep
allowCloudDesktopAndDocuments

allowCloudDesktopAndDocuments = 0;
```

## Remediation:

Perform the following to disable iCloud Desktop and Document syncing:











### *Graphical Method:*

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

### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.applicationaccess`
2. Add the key `allowCloudDesktopAndDocuments`
3. Set the key to `</false>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<b>15.3 Classify Service Providers</b> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 2.6.2 Audit App Store Password Settings (Manual)

### **Profile Applicability:**

- Level 2

### **Description:**

With OS X 10.11 Apple added settings for password storage for the App Store in macOS. These settings parallel the settings in iOS. As with iOS the choices are a requirement to provide a password after every purchase or to have a 15-minute grace period, and whether to require a password for free purchases. The response to this setting is stored in a cookie and processed by iCloud.

There is plenty of risk information on the wisdom of this setting for parents with children buying games on iPhones and iPads. The most relevant information here is the likelihood that users that are not authorized to download software may have physical access to an unlocked computer where someone who is authorized recently made a purchase. If that is a concern a password should be required at all times for App Store access in the Password Settings controls.

### **Rationale:**

### **Audit:**

Perform the following to verify that App Store Passwords are set to your organization's requirements:

#### *Graphical Method:*

1. Open System Preferences
2. Select Apple ID
3. Select Media & Purchases
4. Verify that Free Downloads is set to your organization's requirements
5. Verify that Purchases and In-App Purchases is set to your organization's requirements











## Remediation:

Perform the following to set App Store Passwords to your organization's requirements:

*Graphical Method:*

1. Open System Preferences
2. Select Apple ID
3. Select Media & Purchases
4. Select the setting for Free Downloads that are withing your organization's requirements
5. Select the setting for Purchases and In-App Purchases that are within your organization's requirements

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## ***2.7 Time Machine***

One of the most important IT Operational concerns is to ensure that information is protected against loss or tampering. The purpose of the IT devices is to process the data after all. At one time the cost of IT equipment and the volume of the data might make the protection of the equipment itself more important. At this point the vast size of data archives, and the lower cost of end-user equipment, makes data protection central to operational planning. Backup strategies are generally focused on ensuring that there are multiple copies of relevant versions of user files. The plan is that no single hardware or software loss or failure will result in major data loss.

Apple does not provide a native remote logging capability that encrypts data in transit (DIT). If no third party tool or agent is installed on organizational managed Macs it is even more important to ensure that backup processes are implemented with log backups as part of the architecture.

In recent years the criticality of information backup, protection of data and data backups has become even more important with the rise of cybercriminals that not only commit denial-of-service attacks using ransomware to encrypt your working data to make it inaccessible, they also will encrypt the backups if reachable. Newer threats include blackmail to compromise data confidentiality. A comprehensive plan to protect data from compromise is even more vital with current threats. The Time Machine controls are only recommended best practices to assist in ease of frequent backups and the encryption of backup volumes.

Apple introduced Time Machine in 2007 as a simple-to-use built-in mechanism for users to ensure that their machine was backed up and if there was a mistake or loss, information could be easily recovered. There are other solutions to ensure information is protected including several Enterprise solutions and simple drive or directory cloning.

The controls in this section are specifically about Time Machine. The general ideas are applicable to any data backup solution. These controls are only pertinent to organizations already using Time Machine as part of their backup solutions to ensure the included Apple backup solution is being used effectively. We are not endorsing that Time Machine should be used exclusively or as part of the Enterprise backup solution. The controls first check that Time Machine is actually enabled.

To enable Time Machine, follow the instructions here: <https://support.apple.com/en-us/HT201250>

For more details on Time Machine:

- <https://eclecticlight.co/tag/time-machine/>
- <https://www.pcmag.com/how-to/how-to-back-up-your-mac-with-time-machine>

### *2.7.1 Ensure Backup Up Automatically is Enabled (Automated)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Backup solutions are only effective if the backups run on a regular basis. The time to check for backups is before the hard drive fails or the computer goes missing. In order to simplify the user experience so that backups are more likely to occur Time Machine should be on and set to Back Up Automatically whenever the target volume is available.

Operational staff should ensure that backups complete on a regular basis and the backups are tested to ensure that file restoration from backup is possible when needed.

Backup dates are available even when the target volume is not available in the Time Machine plist.

```
SnapshotDates = (  
"2012-08-20 12:10:22 +0000",  
"2013-02-03 23:43:22 +0000",  
"2014-02-19 21:37:21 +0000",  
"2015-02-22 13:07:25 +0000",  
"2016-08-20 14:07:14 +0000"
```

When the backup volume is connected to the computer more extensive information is available through `tmutil`. See `man tmutil`

#### **Rationale:**

Backups should automatically run whenever the backup drive is available.

#### **Impact:**

The backup will run periodically in the background and could have user impact while running.

## Audit:

Perform the following to ensure that automatic backups are set if Time Machine is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Time Machine
3. Verify that Back Up Automatically is set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `AutoBackup=1`

*Terminal Method:*

Run the following command to verify that Time Machine is set to automatically backup if Time Machine is enabled:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.TimeMachine.plist AutoBackup  
1
```

If Time Machine has never been used, and is not configured there will not be an AutoBackup flag to check. If so, the machine will be in compliance.

Run the following command to check the snapshot dates to verify that the dates meet your organization's approved backup frequency:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.TimeMachine.plist
```

The output will contain all the Time Machine backups in the format "YYYY-MM-DD HH:MM:SS +0000"

*example:*

```
$ sudo /usr/bin/defaults read
/Library/Preferences/com.apple.TimeMachine.plist AutoBackup

1

$ sudo /usr/bin/defaults read
/Library/Preferences/com.apple.TimeMachine.plist

{
    AutoBackup = 1;
    BackupAlias = {length = 270, bytes = 0x00000000 010e0002 00010654
65737454 ... 74544d00 ffff0000 };
    Destinations = (
        {
            BackupAlias = {length = 270, bytes = 0x00000000 010e0002 00010654
65737454 ... 74544d00 ffff0000 };
            BytesAvailable = 450998374400;
            BytesUsed = 48765513728;
            ConsistencyScanDate = "2020-08-07 12:23:26 +0000";
            DestinationID = "C751EDAD-4E5F-4FA9-AF1B-AF34A00FF97F";
            DestinationUUIDs = (
                "24C6B473-A3C5-391F-8191-244A78D40E3C"
            );
            LastKnownEncryptionState = NotEncrypted;
            RESULT = 0;
            ReferenceLocalSnapshotDate = "2020-08-07 12:21:04 +0000";
            RootVolumeUUID = "95953248-32FE-4B24-B546-91ED69B33A47";
            SnapshotDates = (
                "2020-08-06 19:54:13 +0000",
                "2020-08-07 00:10:57 +0000",
                "2020-08-07 10:45:58 +0000",
                "2020-08-07 12:02:01 +0000",
                "2020-08-07 12:03:00 +0000",
                "2020-08-07 12:03:58 +0000",
                "2020-08-07 12:06:22 +0000",
                "2020-08-07 12:08:45 +0000",
                "2020-08-07 12:09:42 +0000",
                "2020-08-07 12:10:56 +0000",
                "2020-08-07 12:11:56 +0000",
                "2020-08-07 12:12:48 +0000",
                "2020-08-07 12:13:41 +0000",
                "2020-08-07 12:14:59 +0000",
                "2020-08-07 12:16:27 +0000",
                "2020-08-07 12:23:26 +0000"
            );
            UnencryptedBackupWarningDate = "2020-08-06 19:38:11 +0000";
        }
    );
    HostUUIDs = (
        "996981ED-1690-55E3-9486-1DD27D9E52D3"
    );
};
```

```
LastConfigurationTraceDate = "2020-08-06 19:31:30 +0000";
LastDestinationID = "C751EDAD-4E5F-4FA9-AF1B-AF34A00FF97F";
LocalizedDiskImageVolumeName = "Time Machine Backups";
PreferencesVersion = 4;
SkipPaths = (
    "~administrator/Applications",
);
SkipSystemFiles = 1;
SuspendHelperActivityTimeStamp = 618498798;
}
```

**or**

Run the following command to verify that a profile is installed that enables auto backup if Time Machine enabled:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "AutoBackup"

AutoBackup = 1;
```

**Remediation:**

Perform the following to enable Time Machine:

*Graphical Method:*

- 1. Open System Preferences
- 2. Select Time Machine
- 3. Verify that Time Machine is enabled
- 4. Select Back Up Automatically

*Terminal Method:*

Run the following command to enable automatic backups if Time Machine is enabled:







```
$ sudo /usr/bin/defaults write
/Library/Preferences/com.apple.TimeMachine.plist AutoBackup -bool true
```

### Profile Method:

1. Create or edit a configuration profile with the key of `com.apple.TimeMachine` under PayloadContent
2. Add the key `Forced`
3. Set the key to the following:

```
<array>
  <dict>
    <key>mcx_preference_settings</key>
    <dict>
      <key>AutoBackup</key>
      <true/>
    </dict>
  </dict>
</array>
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>11.2 <u>Perform Automated Backups</u></b> Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.			
v7	<b>10.1 <u>Ensure Regular Automated Back Ups</u></b> Ensure that all system data is automatically backed up on regular basis.			



## *2.7.2 Ensure Time Machine Volumes Are Encrypted (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

One of the most important security tools for data protection on macOS is FileVault. With encryption in place it makes it difficult for an outside party to access your data if they get physical possession of the computer. One very large weakness in data protection with FileVault is the level of protection on backup volumes. If the internal drive is encrypted but the external backup volume that goes home in the same laptop bag is not it is self-defeating. Apple tries to make this mistake easily avoided by providing a checkbox to enable encryption when setting-up a Time Machine backup. Using this option does require some password management, particularly if a large drive is used with multiple computers. A unique complex password to unlock the drive can be stored in keychains on multiple systems for ease of use.

While some portable drives may contain non-sensitive data and encryption may make interoperability with other systems difficult backup volumes should be protected just like boot volumes.

### **Rationale:**

Backup volumes need to be encrypted.

## Audit:

Perform the following to ensure the drive used for Time Machine is encrypted:

### *Graphical Method:*

1. Open System Preferences
2. Select Time Machine
3. Select Backup Disk...
4. Select the Time Machine backup drive
5. Verify that Encrypt backups is set

### *Terminal Method:*

Run the following command to verify if the Time Machine disk encryption is enabled:

```
$ sudo /usr/bin/tmutil destinationinfo | grep -i NAME
```

The output will be formatted as: 'Name : '. If there are more than one TimeMachine backup disk the command will list all the disks.

```
$ sudo /usr/sbin/diskutil info <volumename> | grep -i Encrypted
```

```
Encrypted:                Yes
```

### *example:*

```
$ sudo /usr/bin/tmutil destinationinfo | grep -i NAME
```

```
Name          : TMbackup1
```

```
Name          : TMbackup2
```

```
$ sudo /usr/sbin/diskutil info TMbackup1 | grep -i Encrypted
```

```
Encrypted:                Yes
```

```
$ sudo /usr/sbin/diskutil info TMbackup2 | grep -i Encrypted
```

```
Encrypted:                Yes
```

## Remediation:
















Perform the following to enable encryption on the Time Machine drive:

*Graphical Method:*

1. Open System Preferences
2. Select Time Machine
3. Select Backup Disk...
4. Select the existing Time Machine backup drive from the Available Drive list
5. Set Encrypt backups
6. Select Use Disk

**Note:** You can set encryption through Disk Utility or `diskutil` in terminal.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.6 <u>Encrypt Data on End-User Devices</u></b> Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.			
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	<b>11.3 <u>Protect Recovery Data</u></b> Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.			
v7	<b>10.4 <u>Ensure Protection of Backups</u></b> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			
v7	<b>13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u></b> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## *2.8 Ensure Wake for Network Access Is Disabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

This feature allows the computer to take action when the user is not present and the computer is in energy saving mode. These tools require FileVault to remain unlocked and fully rejoin known networks. This macOS feature is meant to allow the computer to resume activity as needed regardless of physical security controls.

This feature allows other users to be able to access your computer's shared resources, such as shared printers or iTunes playlists, even when your computer is in sleep mode. In a closed network when only authorized devices could wake a computer it could be valuable to wake computers in order to do management push activity. Where mobile workstations and agents exist the device will more likely check in to receive updates when already awake. Mobile devices should not be listening for signals on any unmanaged network or where untrusted devices exist that could send wake signals.

### **Rationale:**

Disabling this feature mitigates the risk of an attacker remotely waking the system and gaining access.

### **Impact:**

Management programs like Apple Remote Desktop Administrator use wake-on-LAN to connect with computers. If turned off, such management programs will not be able to wake a computer over the LAN. If the wake-on-LAN feature is needed, do not turn off this feature.

The control to prevent computer sleep has been retired for this version of the Benchmark. Forcing the computer to stay on and use energy in case a management push is needed is contrary to most current management processes. Only keep computers unslept if after hours pushes are required on closed LANs.

## Audit:

Perform the following to verify that Wake for network access or Power Nap are disabled:

*Graphical Method:*

1. Open System Preferences
2. Select Energy Saver
3. Verify that Wake for network access is not set

*Terminal Method:*

Run the following command verify if Wake for network access is not enabled:

```
$ sudo pmset -g | grep -e womp  
womp 0
```

## Remediation:

Perform the following disable Wake for network access or Power Nap:

*Graphical Method:*

1. Open System Preferences
2. Select Energy Saver
3. Uncheck Wake for network access

*Terminal Method:*





Run the following command to disable Wake for network access:

```
$ sudo pmset -a womp 0
```

## Additional Information:

man pmset

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## *2.9 Ensure Power Nap Is Disabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

This feature allows the computer to take action when the user is not present and the computer is in energy saving mode. These tools require FileVault to remain unlocked and fully rejoin known networks. This macOS feature is meant to allow the computer to resume activity as needed regardless of physical security controls.

Power Nap allows the system to stay in low power mode, especially while on battery power and periodically connect to previously named networks with stored credentials for user applications to phone home and get updates. This capability requires FileVault to remain unlocked and the use of previously joined networks to be risk accepted based on the SSID without user input.

This control has been updated to check the status on both battery and AC Power. The presence of an electrical outlet does not completely correlate with logical and physical security of the device or available networks.

### **Rationale:**

Disabling this feature mitigates the risk of an attacker remotely waking the system and gaining access.

The use of Power Nap adds to the risk of compromised physical and logical security. The user should be able to decrypt FileVault and have the applications download what is required when the computer is actively used.

The control to prevent computer sleep has been retired for this version of the Benchmark. Forcing the computer to stay on and use energy in case a management push is needed is contrary to most current management processes. Only keep computers unslept if after hours pushes are required on closed LANs.

### **Impact:**

Power Nap exists for unattended user application updates like email and social media clients. With Power Nap disabled the computer will not wake and reconnect to known wireless SSIDs intermittently when slept.

## Audit:

Perform the following to verify that Wake for network access or Power Nap are disabled:

*Graphical Method:*

1. Open System Preferences
2. Select Energy Saver
3. Verify that Power Nap is not set

*Terminal Method:*

Run the following command to verify if Power Nap is not enabled:

```
$ sudo pmset -g everything | grep -c 'powernap' 1  
0
```

## Remediation:

Perform the following to disable Wake for network access or Power Nap:

*Graphical Method:*

1. Open System Preferences
2. Select Energy Saver
3. Uncheck Enable Power Nap

*Terminal Method:*

Run the following command to disable Power Nap:











```
$ sudo pmset -a powernap 0
```

## Additional Information:

man pmset



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## *2.10 Ensure Secure Keyboard Entry terminal.app is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Secure Keyboard Entry prevents other applications on the system and/or network from detecting and recording what is typed into Terminal.

### **Rationale:**

Enabling Secure Keyboard Entry minimizes the risk of a key logger from detecting what is entered in Terminal.

## Audit:

Perform the following to ensure that keyboard entries are secure in Terminal:

*Graphical Method:*

1. Open Terminal
2. Select Terminal in the Menu Bar
3. Verify that Secure Keyboard Entry is set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `SecureKeyboardEntry` is set to 1

*Terminal Method:*

For each user, run the following command to verify that keyboard entries in Terminal are secured:

```
$ sudo -u <username> /usr/bin/defaults read -app Terminal SecureKeyboardEntry
1
```

*example:*

```
$ sudo -u firstuser /usr/bin/defaults read -app Terminal SecureKeyboardEntry
0
$ sudo -u seconduser /usr/bin/defaults read -app Terminal SecureKeyboardEntry
1
```

In the above example the user `seconduser` is compliant, and the user `firstuser` is not compliant.

**or**

Run the following command to verify that a profile is installed that enables secure keyboard entry in Terminal:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep SecureKeyboardEntry
SecureKeyboardEntry = 1;
```

## Remediation:

Perform the following to enable secure keyboard entries in Terminal:

*Graphical Method:*

1. Open Terminal
2. Select Terminal
3. Select Secure Keyboard Entry

*Terminal Method:*

```
$ sudo -u <username> /usr/bin/defaults write -app Terminal  
SecureKeyboardEntry -bool true
```

*example:*

```
$ sudo -u firstuser /usr/bin/defaults write -app Terminal SecureKeyboardEntry  
-bool true
```










*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.Terminal`
2. Add the key `SecureKeyboardEntry`
3. Set the key to `<true/>`

## References:

1. <https://support.apple.com/en-ca/guide/terminal/trml109/2.11>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>4.1 Maintain Inventory of Administrative Accounts</u></b></p> <p>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## 2.11 Ensure EFI Version Is Valid and Checked Regularly (Automated)

### Profile Applicability:

- Level 1

### Description:

In order to mitigate firmware attacks Apple has created an automated Firmware check to ensure that the EFI version running is a known good version from Apple. There is also an automated process to check it every seven days.

### Rationale:

If the Firmware of a computer has been compromised the Operating System that the Firmware loads cannot be trusted either.

### Audit:

Verify that the computer has up-to-date firmware:

```
$ sudo /usr/libexec/firmwarecheckers/eficheck/eficheck --integrity-check
```

The output should include Primary allowlist version match found. No changes detected in primary hashes. as well as the model and version in this format MBP133.xxx.xxxx.xxx.xxxxxxxxxx.

If an Apple T2 Security Chip is present, the output will be:

```
ReadBinaryFromKernel: No matching services found. Either this system is not supported by eficheck, or you need to re-load the kext IntegrityCheck: couldn't get EFI contents from kext
```

Run this command to verify that the machine does have an Apple T2 Security Chip:

```
$ sudo system_profiler SPiBridgeDataType | grep "T2"
```

```
Model Name: Apple T2 Security Chip
```

Either state is compliant.

Run this command to verify that the efi check system daemon is running (including machines with the T2 chip):







```
$ sudo launchctl list | grep com.apple.driver.eficheck
```

```
Result: -      0      com.apple.driver.eficheck
```

## Remediation:

If EFI does not pass the integrity check you may send a report to Apple. Backing up files and clean installing a known good Operating System and Firmware is recommended.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.2 Ensure Authorized Software is Currently Supported</u></b> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	<b><u>2.2 Ensure Software is Supported by Vendor</u></b> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

## *2.12 Audit Automatic Actions for Optical Media (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Managing automatic actions, while useful in very few situations, is unlikely to increase security on the computer and does complicate the user experience and add additional complexity to the configuration. These settings are user controlled and can be changed without Administrator privileges unless controlled through MCX settings or Parental Controls. Unlike Windows, the Auto-run the optical media is accessed through Operating System applications. Those same applications can open and access the media directly. If optical media is not allowed in the environment the optical media drive should be disabled in hardware and software.

### **Rationale:**

Setting automatic actions for optical media can mitigate malicious code from running automatically when optical media is inserted.



## Audit:

Perform the following to verify the optical media settings:

*Graphical Method:*

1. Open System Preferences
2. Select CDs & DVDs
3. Verify that each option is set to your organization's requirements

*Terminal Method:*

For all users, run the following commands to verify the optical media actions:

```
$ sudo -u <username> defaults read com.apple.digihub
```

The output will give the action.

Examples of the actions are:

The action Ask what to do is `action = 2`

The action Ignore is `action = 1`

The action to Open Music is `action = 101`

*example:*

```
$ sudo -u seconduser defaults read  
/Users/seconduser/Library/Preferences/com.apple.digihub  
  
{  
  "com.apple.digihub.blank.cd.appeared" =      {  
    action = 1;  
  };  
  "com.apple.digihub.blank.dvd.appeared" =      {  
    action = 100;  
  };  
  "com.apple.digihub.cd.music.appeared" =      {  
    action = 101;  
  };  
  "com.apple.digihub.cd.picture.appeared" =     {  
    action = 107;  
  };  
  "com.apple.digihub.dvd.video.appeared" =      {  
    action = 105;  
  };  
}
```

## Remediation:

Perform the following to set the optical media action setting:

*Graphical Method:*

1. Open System Preferences
2. Select CDs & DVDs
3. Set each option to meet your organization's requirements

*Terminal Method:*

Run the following command to set the optical media action:












```
$ sudo -u <username> defaults write  
/Users/<username>/Library/Preferences/com.apple.digihub <what type of media>  
-dict action <preferred action>
```

*example:*

```
$ sudo -u seconduser defaults write  
/Users/seconduser/Library/Preferences/com.apple.digihub  
com.apple.digihub.blank.dvd.appeared -dict action 1
```

The five media types are `com.apple.digihub.blank.cd.appeared`(blank cd),  
`com.apple.digihub.blank.dvd.appeared` (blank dvd),  
`com.apple.digihub.cd.music.appeared` (music cd),  
`com.apple.digihub.cd.picture.appeared` (picture cd), and  
`com.apple.digihub.dvd.video.appeared` (DVD movie).

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>10.3 Disable Autorun and Autoplay for Removable Media</u></b> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 2.13 Audit Siri Settings (Manual)

### **Profile Applicability:**

- Level 1

### **Description:**

With macOS 10.12 Sierra Apple has introduced Siri from iOS to macOS. While there are data spillage concerns with the use of data gathering personal assistant software, the risk here does not seem greater in sending queries to Apple through Siri than in sending search terms in a browser to Google or Microsoft. While it is possible that Siri will be used for local actions rather than Internet searches, Siri could, in theory, tell Apple about confidential Programs and Projects that should not be revealed. This appears to be a usage edge case.

In cases where sensitive and protected data is processed and Siri could help a user navigate their machine and expose that information it should be disabled. Siri does need to phone home to Apple so it should not be available from air-gapped networks as part of its requirements.

Most of the use case data published has shown that Siri is a tremendous time saver on iOS where multiple screens and menus need to be navigated through. Information like sports scores, weather, movie times and simple to-do items on existing calendars can be easily found with Siri. None of the standard use cases should be more risky than already approved activity.

For information on Apple's privacy policy for Siri, [click here](#).

### **Rationale:**

Where "normal" user activity is already limited, Siri use should be controlled as well.

## Audit:

Perform the following to verify Siri settings:

*Graphical Method:*

1. Open System Preferences
2. Select Siri
3. Verify the settings are within your organization's parameters

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Allow Assistant` is within your organization's parameters

*Terminal Method:*

Run the following commands to verify the Siri settings:

```
$ sudo -u <username> /usr/bin/defaults read com.apple.assistant.support.plist  
'Assistant Enabled'
```

The output will be either 0, Siri is disabled, or 1, Siri is enabled.

```
$ sudo -u <username> /usr/bin/defaults read com.apple.Siri.plist
```

The output will be either 0, disabled, or 1 for the following Siri options:

1. LockscreenEnabled - Is Siri enabled when the system is locked?
2. StatusMenuVisible - Is Siri visible in the menu bar?
3. VoiceTriggerUserEnabled - Is "Hey Siri" enabled?

*example:*

```
$ sudo -u firstuser /usr/bin/defaults read com.apple.assistant.support.plist
'Assistant Enabled'

0

$ sudo -u firstuser /usr/bin/defaults read com.apple.Siri.plist

{
    LockscreenEnabled = 0;
    StatusMenuVisible = 0;
    VoiceTriggerUserEnabled = 0;
}

$ sudo -u seconduser /usr/bin/defaults read com.apple.assistant.support.plist
'Assistant Enabled'

1

$ sudo -u seconduser /usr/bin/defaults read com.apple.Siri.plist

{
    LockscreenEnabled = 0;
    StatusMenuVisible = 1;
    VoiceTriggerUserEnabled = 1;
}

$ sudo -u thirduser /usr/bin/defaults read com.apple.assistant.support.plist
'Assistant Enabled'

1

$ sudo -u thirduser /usr/bin/defaults read com.apple.Siri.plist

{
    LockscreenEnabled = 1;
    StatusMenuVisible = 0;
    VoiceTriggerUserEnabled = 1;
}
```

**or**

Run the following command to verify that a profile is installed that sets Siri to your organization's setting:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "allowAssistant"

allowAssistant = 0;
```

**Note:** Siri can only be enabled or disabled through configuration profiles. Any additional settings need to be set through the GUI or CLI

## Remediation:

Perform the following to set Siri to your organization's parameters:

*Graphical Method:*

1. Open System Preferences
2. Select Siri
3. Select the settings that are within your organization's requirements

*Terminal Method:*

Run the following commands to enable or disable Siri settings:

```
$ sudo -u <username> /usr/bin/defaults write  
com.apple.assistant.support.plist 'Assistant Enabled' -bool <true/false>  
  
$ sudo -u <username> /usr/bin/defaults write com.apple.Siri.plist  
LockscreenEnabled -bool <true/false>  
  
$ sudo -u <username> /usr/bin/defaults write com.apple.Siri.plist  
StatusMenuVisible -bool <true/false>  
  
$ sudo -u <username> /usr/bin/defaults write com.apple.Siri.plist  
VoiceTriggerUserEnabled -bool <true/false>
```

After running the default writes, the Windows Server needs to be restarted and the caches cleared. Run the following commands to perform that action:

```
$ sudo /usr/bin/killall -HUP cfprefsd  
  
$ sudo /usr/bin/killall SystemUIServer
```

*example:*

```
$ sudo -u firstuser /usr/bin/defaults write com.apple.assistant.support.plist  
'Assistant Enabled' -bool true  
  
$ sudo -u firstuser /usr/bin/defaults write com.apple.Siri.plist  
StatusMenuVisible -bool true  
  
$ sudo -u firstuser /usr/bin/defaults write com.apple.Siri.plist  
LockscreenEnabled -bool false  
  
$ sudo /usr/bin/killall -HUP cfprefsd  
  
$ sudo /usr/bin/killall SystemUIServer  
  
$ sudo -u seconduser /usr/bin/defaults write  
com.apple.assistant.support.plist 'Assistant Enabled' -bool false  
  
$ sudo /usr/bin/killall -HUP cfprefsd  
  
$ sudo /usr/bin/killall SystemUIServer  
  
$ sudo -u thirduser /usr/bin/defaults write com.apple.Siri.plist  
VoiceTriggerUserEnabled -bool false  
  
$ sudo /usr/bin/killall -HUP cfprefsd  
  
$ sudo /usr/bin/killall SystemUIServer
```

#### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.applicationaccess
2. Add the key allowAssistant
3. Set the key to </true> or </false> based on your organization's requirements











**Note:** Siri can only be enabled or disabled through configuration profiles. Any additional settings need to be set through the GUI of CLI

#### **References:**

1. <https://support.apple.com/en-us/HT210657>



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## 2.14 Audit Sidecar Settings (Manual)

### Profile Applicability:

- Level 1

### Description:

Apple introduced a technology called Sidecar with the release of macOS 10.15 "Catalina" that allows the use of an Apple iPad as an additional screen. There are no known security issues with the use of Sidecar at the time of the publication of this Benchmark. There are security concerns with some of the underlying technology that allows this feature to work. The Apple support article below has the additional requirements that are reproduced below. So while Sidecar may not have an explicit security concern some organizations may have requirements that block the use of the features required to allow Sidecar to work.

<https://support.apple.com/en-afri/HT210380>

#### Additional requirements

- Both devices must be signed in to iCloud with the same Apple ID using two-factor authentication.
- To use Sidecar wirelessly, both devices must be within 10 meters (30 feet) of each other and have Bluetooth, Wi-Fi, and Handoff turned on. Also make sure that the iPad is not sharing its cellular connection and the Mac is not sharing its Internet connection.
- To use Sidecar over USB, make sure that your iPad is set to trust your Mac.

Organizations that do not allow the use of iCloud and more specifically Handoff will not be able to use Sidecar.

Some organizations may not allow the use of mixed ownership for P2P wireless or USB connections so that unless the organization controls both the Mac and the iPad connections may not be approved and the use of a single Apple ID for distinctly managed devices may be prohibited.

### Rationale:

Organizations need to have an understanding of integration of organizational and personal inventory in the work environment.

## Audit:

Perform the following to verify Sidecar's setting:

*Graphical Method:*

1. Open System Preferences
2. Select Sidecar
3. Verify the settings are within your organization's parameters

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `AllowAllDevices` to your organization's parameters
4. Verify that an installed profile has `hasShownPref` to your organization's parameters

*Terminal Method:*

Run the following commands to verify if Sidecar is enabled:

```
$ sudo /usr/bin/defaults read com.apple.sidecar.display AllowAllDevices
```

The output will be either 0, Sidecar is disabled, or 1, Sidecar is enabled.

**Note:** If the output is The domain/default pair of (com.apple.sidecar.display, AllowAllDevices) does not exist, then the setting has not been changed from the default.

**or**

Run the following command to verify that a profile is installed that SideCar is set to your organization's parameters:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "AllowAllDevices"
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "hasShownPref"
```

`AllowAllDevices = 0; and hasShownPref = 0; disables AirDrop and AllowAllDevices = 1; and hasShownPref = 1; enables AirDrop.`

## Remediation:

Perform the following to set Sidecar to your organization's parameters:

*Graphical Method:*

1. Open System Preferences
2. Select Sidecar
3. Select the settings that are within your organization's parameters

*Terminal Method:*

Run the following to enable or disable Sidecar settings:

```
$ sudo /usr/bin/defaults write com.apple.sidecar.display AllowAllDevices
<true/false>

$ sudo /usr/bin/defaults write com.apple.sidecar.display hasShownPref
<true/false>
```

*Profile Method:*

1. Create or edit a configuration profile with the key of `com.apple.sidecar.display` under PayloadContent
2. Add the following set of keys with the `com.apple.Bluetooth` key:











```
<dict>
  <key>Forced</key>
  <array>
    <dict>
      <key>mcx_preference_settings</key>
      <dict>
        <key>AllowAllDevices</key>
        <<true/false>/>
        <key>hasShownPref</key>
        <<true/false>/>
      </dict>
    </dict>
  </array>
</dict>
```

**Note:** Using the Terminal and Profile Methods will not display in System Preferences, but will disable the underlying service.

## References:

1. [https://www.apple.com/macOS/catalina/docs/Sidecar\\_Tech\\_Brief\\_Oct\\_2019.pdf](https://www.apple.com/macOS/catalina/docs/Sidecar_Tech_Brief_Oct_2019.pdf)
2. <https://www.pocket-lint.com/laptops/news/apple/148262-apple-sidecar-macos-ipados-features-explained>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b></p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b><u>5.1 Establish Secure Configurations</u></b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			
v7	<p><b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

## 2.15 Audit Touch ID and Wallet & Apple Pay Settings (Manual)

### **Profile Applicability:**

- Level 1

### **Description:**

Apple has integrated Touch ID with macOS and allows fingerprint use for many common operations. All use of Touch ID requires the presence of a password and the use of that password after every reboot or where it has been more than 48 hours since the device was last unlocked.

Touch ID is a pre-requisite for using Apple Pay and Wallet on macOS. Apple Pay allows an Apple account holder to enroll their credit cards in Apple Pay and pay enrolled vendors without using the physical card or number. Apple's service eliminates the requirement to send the credit card number itself to the vendor. Apple Pay on a Mac allows the use of credit cards the user has already enrolled and reduces user risk for credit card purchases.

### **Rationale:**

Touch ID allows for an account enrolled fingerprint to access a key that uses a previously provided password.

Some environments may have rules around purchases from organizationally managed computers and may want to discourage shopping from them. It is difficult to block access to websites that allow purchases and Apple Pay has additional controls for user protection than the manually entry of credit card information

### **Impact:**

Touch ID is more convenient for use with aggressive screen lock controls.

### **Audit:**

Perform the following to verify Touch ID settings:

*Graphical Method:*

1. Open System Preferences
2. Select Touch ID
3. Verify the Touch ID settings match your organization's settings
4. Open System Preferences
5. Select Wallet & Apple Pay
6. Verify the Wallet & Apple Pay settings match your organization's settings

## Remediation:

Perform the following to set Touch ID to your organization's settings:












*Graphical Method:*

1. Open System Preferences
2. Select Touch ID
3. Select the Touch ID settings match your organization's settings
4. Open System Preferences
5. Select Wallet & Apple Pay
6. Select the Wallet & Apple Pay settings match your organization's settings

## References:

1. <https://support.apple.com/guide/mac-help/use-wallet-apple-pay-on-mac-mchl4773988b/mac>
2. <https://www.apple.com/apple-pay/>
3. <https://support.apple.com/guide/mac-help/touch-id-mchl16fbf90a/mac>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## *2.16 Audit Notification System Preference Settings (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Notification capabilities are designed to allow users to receive updates from applications that are not currently in use, these can be background applications or even notices from processes running on a computer that is not currently being actively used. Where the screen of a computer is visible to others other than the logged-in user due to shared working spaces or public spaces consideration should be made on the exposure of sensitive data in notifications. Applications that use the system-wide application service may be individually managed and applications that might expose confidential information to unauthorized users should not expose notifications except to the current user, especially on the locked screen when the computer may be unattended.

### **Rationale:**

Some work environments will handle sensitive or confidential information with applications that can provide notifications to anyone that can see the computer screen. Organizations must review the likelihood that information may be exposed inappropriately and suppress notifications where risk is not organizationally accepted.

### **Impact:**

Computer users are often juggling too much information through too many applications that want their attention and are often designed to get attention and not ever let it go. Notifications are a mechanism that can be used to cut through the deluge and allow important issues to be resolved in a timely way. Global controls on limiting user notifications, even for certain applications, could impact productivity and the timely remediation of issues.



**Audit:**

Perform the following to verify that Notifications are set to your organization's requirements:

*Graphical Method:*

1. Open System Preferences
2. Select Notifications
3. Verify that Show previews is set to your organization's requirements

**Note:** If the exposure of controlled information or data leakage is possible with application notifications the acceptable notification level should be established through a risk analysis of what unauthorized leaks may occur.

**Remediation:**

Perform the following to set Notifications to your organization's requirements:

*Graphical Method:*

1. Open System Preferences
2. Select Notifications
3. Select the setting for Show previews that are withing your organization's requirements
4. Turn off or mute notifications that may expose information to unauthorized people that might be able to view screens of organizational computers.

### ***3 Logging and Auditing***

This section provide guidance on configuring the logging and auditing facilities available in macOS. Starting with macOS 10.12 Apple introduced unified logging. This capability replaces the previous logging methodology with centralized system wide common controls. A full explanation of macOS logging behavior is beyond the scope of this Benchmark. These changes impact previous logging controls from macOS Benchmarks. At this point many of the syslog controls have been or are being removed since the old logging methods have been deprecated. Controls that still appear useful will be retained. Some legacy controls have been removed for this release.

More info <https://developer.apple.com/documentation/os/logging>  
<https://eclecticlight.co/2018/03/19/macos-unified-log-1-why-what-and-how/>

### 3.1 Ensure Security Auditing Is Enabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

macOS's audit facility, `auditd`, receives notifications from the kernel when certain system calls, such as `open`, `fork`, and `exit`, are made. These notifications are captured and written to an audit log.

#### Rationale:

Logs generated by `auditd` may be useful when investigating a security incident as they may help reveal the vulnerable application and the actions taken by a malicious actor.

#### Audit:

Perform the following to verify that security auditing is enabled:

Run the following command to verify `auditd`:

```
$ sudo launchctl list | grep -i auditd  
-      0      com.apple.auditd
```











#### Remediation:

Perform the following to enable security auditing:

Run the following command to load `auditd`:

```
$ sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

### *3.2 Ensure Security Auditing Flags Are Configured Per Local Organizational Requirements (Automated)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Auditing is the capture and maintenance of information about security-related events. Auditable events often depend on differing organizational requirements.

#### **Rationale:**

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises or attacks that have occurred, have begun, or are about to begin. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised.

Depending on the governing authority, organizations can have vastly different auditing requirements. In this control we have selected a minimal set of audit flags that should be a part of any organizational requirements. The flags selected below may not adequately meet organizational requirements for users of this benchmark. The auditing checks for the flags proposed here will not impact additional flags that are selected.

## Audit:

Historical audit flags are listed below as preliminary guidance.

Perform the following to ensure the enabled Security Auditing Flags:

Run the following command to verify the Security Auditing Flags that are enabled:

```
$ sudo grep -e "^flags:" /etc/security/audit_control
```

The output should include the following flags:

- `fm` - audit successful/failed file attribute modification events
- `ad` - audit successful/failed administrative events
- `-ex` - audit failed program execution
- `aa` - audit all authorization and authentication events
- `-fr` - audit all failed read actions where enforcement stops a read of a file
- `lo` - audit successful/failed login/logout events
- `-fw` - audit all failed write actions where enforcement stopped a file write

The `-all` flag will capture all failed events across all audit classes and can be used to supersede the individual flags for failed events.

**Note:** excluding potentially noisy audit events may be ideal, depending on your use-case.

## Remediation:

Perform the following to set the require Security Auditing Flags:

Edit the `/etc/security/audit_control` file and add `fm`, `ad`, `-ex`, `aa`, `-fr`, `lo`, and `-fw` flags or add `-all` to flags.

## References:

1. <https://derflounder.wordpress.com/2012/01/30/openbsm-auditing-on-mac-os-x/>
2. <https://csrc.nist.gov/CSRC/media/Publications/sp/800-179/rev-1/draft/documents/sp800-179r1-draft.pdf>
3. <https://meliot.me/2017/07/02/mac-os-real-time-auditing/>
4. <https://www.scip.ch/en/?labs.20150108>
5. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>
6. <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf>

## Additional Information:

Flag settings are currently based on the guidance provided by the NIST through the macOS Security guidance they are providing in there GitHub repository. You can find that guidance [here](#).

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.14 <u>Log Sensitive Data Access</u></b> Log sensitive data access, including modification and disposal.			●
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u></b> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

### 3.3 Ensure *install.log* Is Retained for 365 or More Days and No Maximum Size (Automated)

#### Profile Applicability:

- Level 1

#### Description:

macOS writes information pertaining to system-related events to the file `/var/log/install.log` and has a configurable retention policy for this file. The default logging setting limits the file size of the logs and the maximum size for all logs. The default allows for an errant application to fill the log files and does not enforce sufficient log retention. The Benchmark recommends a value based on standard use cases. The value should align with local requirements within the organization.

The default value has an "all\_max" file limitation, no reference to a minimum retention and a less precise rotation argument.

The all\_max flag control will remove old log entries based only on the size of the log files. Log size can vary widely depending on how verbose installing applications are in their log entries. The decision here is to ensure that logs go back a year and depending on the applications a size restriction could compromise the ability to store a full year.

While this Benchmark is not scoring for a rotation flag the default rotation is sequential rather than using a timestamp. Auditors may prefer timestamps in order to simply review specific dates where event information is desired.

Please review the File Rotation section in the man page for more information.

```
man asl.conf
```

- The maximum file size limitation string should be removed "all\_max="
- An organization appropriate retention should be added "ttl="
- The rotation should be set with timestamps "rotate=utc" or "rotate=local"

#### Rationale:

Archiving and retaining `install.log` for at least a year is beneficial in the event of an incident as it will allow the user to view the various changes to the system along with the date and time they occurred.



**Impact:**

Without log files system maintenance and security forensics cannot be properly performed.

**Audit:**

Perform the following to ensure that the install logs are retained for at least 365 days with no maximum size:

Run the following command to verify how long install log files are retained and if there is a maximum size:

```
$ sudo grep -i ttl /etc/asl/com.apple.install
```

The output must include `ttl≥365`

```
$ sudo grep -i all_max= /etc/asl/com.apple.install
```










No results should be returned.

**Remediation:**

Perform the following to ensure that install logs are retained for at least 365 days:

Edit the `/etc/asl/com.apple.install` file and add or modify the `ttl` value to 365 or greater on the `file` line. Also, remove the `all_max=` setting and value from the `file` line.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.1 <u>Establish and Maintain an Audit Log Management Process</u></b> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.			
v7	<b>6.7 <u>Regularly Review Logs</u></b> On a regular basis, review logs to identify anomalies or abnormal events.			

### 3.4 Ensure Security Auditing Retention Is Enabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

The macOS audit capability contains important information to investigate security or operational issues. This resource is only completely useful if it is retained long enough to allow technical staff to find the root cause of anomalies in the records.

Retention can be set to respect both size and longevity. To retain as much as possible under a certain size the recommendation is to use the following:

expire-after:60d OR 1G

More info in the man page `man audit_control`

#### Rationale:

The audit records need to be retained long enough to be reviewed as necessary.

#### Impact:

The recommendation is that at least 60 days or 1 gigabyte of audit records are retained. Systems that have very little remaining disk space may have issues retaining sufficient data.

#### Audit:

Run the following command to verify audit retention:

```
$ sudo grep -e "^expire-after" /etc/security/audit_control
```










The output value for `expire-after:` should be  $\geq$  60d OR 1G

#### Remediation:

Perform the following to set the audit retention length:

Edit the `/etc/security/audit_control` file so that `expire-after:` is at least 60d OR 1G

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.1 <u>Establish and Maintain an Audit Log Management Process</u></b> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.			
v7	<b>6.7 <u>Regularly Review Logs</u></b> On a regular basis, review logs to identify anomalies or abnormal events.			

### *3.5 Ensure Access to Audit Records Is Controlled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

The audit system on macOS writes important operational and security information that can be both useful for an attacker and a place for an attacker to attempt to obfuscate unwanted changes that were recorded. As part of defense-in-depth the `/etc/security/audit_control` configuration and the files in `/var/audit` should be owned only by root with group wheel with read-only rights and no other access allowed. macOS ACLs should not be used for these files.

**Rationale:**

Audit records should never be changed except by the system daemon posting events. Records may be viewed or extracts manipulated, but the authoritative files should be protected from unauthorized changes.

**Impact:**

This control is only checking the default configuration to ensure that unwanted access to audit records is not available.

## Audit:

Run the following commands to check file access rights:

```
$ sudo ls -le /etc/security/audit_control
```

The output should include the owner is `root` and the group is `wheel` or `root` and should not be readable or writable by Other. Ex: `-r--r-----` not `-r--r--r--` or `-r--r---w-`

```
$ sudo ls -le /var/audit/
```

The output should include the owner is `root` and the group is `wheel` or `root` and all entries should not be readable or writable by Other (excluding the final current line). Ex: `-r--r-----` not `-r--r--r--` or `-r--r---w-`

*example:*

```
$ sudo ls -le /etc/security/audit_control
-r----- 1 root wheel 369 27 Jul 15:56 /etc/security/audit_control
$ sudo ls -le /var/audit/
-r--r----- 1 root wheel 1328341 10 Aug 09:08 20200810120444.crash_recovery
-r--r----- 1 root wheel 2718979 10 Aug 09:16 20200810131220.20200810131641
-r--r----- 1 root wheel 2102184 10 Aug 09:16 20200810131641.20200810131658
-r--r----- 1 root wheel 2103140 10 Aug 09:18 20200810131658.20200810131810
-r--r----- 1 root wheel 2097751 10 Aug 10:40 20200810131810.20200810144036
-r--r----- 1 root wheel 1481487 10 Aug 11:39 20200810144036.not_terminated
lrwxr-xr-x 1 root wheel 40 10 Aug 10:40 current ->
/var/audit/20200810144036.not_terminated
```

## Remediation:

Run the following to commands to set the audit records to the root user and wheel group:

```
$ sudo chown -R root:wheel /etc/security/audit_control
$ sudo chmod -R -o-rw /etc/security/audit_control
$ sudo chown -R root:wheel /var/audit/
$ sudo chmod -R -o-rw /var/audit/
```

**Note:** It is recommended to do a thorough verification process on why the audit logs have been changed before following the remediation steps. If the system has different access controls on the audit logs, and the changes cannot be traced, a new install may be prudent. Check for signs of file tampering as well as unapproved OS changes.

## Additional Information:

From ls man page







```
-e      Print the Access Control List (ACL) associated with the file, if  
       present, in long (-l) output.
```

More info:

<https://www.techrepublic.com/blog/apple-in-the-enterprise/introduction-to-os-x-access-control-lists-acls/>

<http://ahaack.net/technology/OS-X-Access-Control-Lists-ACL.html>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### *3.6 Ensure Firewall Logging Is Enabled and Configured (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

The socketfilter firewall is what is used when the firewall is turned on in the Security Preference Pane. In order to appropriately monitor what access is allowed and denied logging must be enabled. The logging level must be set to "detailed" to be useful in monitoring connection attempts that the firewall detects. Throttled log is not sufficient for examine firewall connection attempts.

#### **Rationale:**

In order to troubleshoot the successes and failures of a firewall, logging should be enabled.

#### **Impact:**

Detailed logging may result in excessive storage.

#### **Audit:**

Run the following command to verify that the firewall log is enabled:

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --getloggingmode
Log mode is on

$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --getloggingopt
Log Option is detail
```

#### **Remediation:**

Run the following command to enable logging of the firewall:

```
$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setloggingmode on
Turning on log mode
















$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setloggingopt detail
Setting detail log option
```



## Additional Information:

More info <http://krypted.com/tag/socketfilterfw/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

### *3.7 Audit Software Inventory (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

With the introduction of Mac OS X 10.6.6, Apple added a new application, App Store, which resides in the Applications directory. This application allows a user with admin privileges and an Apple ID to browse Apple's online App Store, purchase (including no cost purchases), and install new applications, bypassing Enterprise software inventory controls. Any admin user can install software in the /Applications directory whether from internet downloads, thumb drives, optical media, cloud storage or even binaries through email. Even standard users can run executables downloaded to their home folder by default. The source of the software is not nearly as important as a consistent audit of all installed software for patch compliance and appropriateness.

A single user desktop where the user, administrator and the person approving software are all the same person probably does not need to audit software inventory to this extent. It is helpful in the case of stability problems or malware however.

Scan systems on a monthly basis and determine the number of unauthorized pieces of software that are installed. Verify that if an unauthorized piece of software is found one month, it is removed from the system the next.

Export System Information through the built-in System Information Application or other third-party tools on an organizationally defined timetable.

#### **Rationale:**

Part of comprehensive IT security involves device management and ensuring that all software is authorized and patched. Checking for macOS updates and app updates are relatively simple for the end user and can even be updated with minimal privileges from trusted sources if enabled. Remote monitoring of the patch status for software maintained through Apple is very well supported by management applications. Neither Apple capabilities nor third-party patch management solutions will cover all mission necessary software for most organizations. Full visibility into software present on the system enables vulnerability and risk management.

PS Don't forget about browser plugins/extensions for all installed software.

## **Audit:**

Perform the following to access System Information through the GUI or the command line:

*Graphical Mode:*

1. Select the Apple icon
2. Select About this Mac
3. Select System Report
4. Select File
5. Select Save
6. Choose the name of the file and location to save the file to

*Terminal Method:*

Run the following command to view all System Profiler details

```
$ sudo system_profiler
```

To find more detailed instructions on the use of the system\_profiler command, run the following:

```
$ sudo man system_profiler
```

## **Remediation:**







Delete any unnecessary applications from the system.

## **Additional Information:**

[About System Information on your Mac](#)

[Inventory and Control of Software Assets](#)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.1 Establish and Maintain a Software Inventory</u></b> Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.			
v7	<b><u>2.1 Maintain Inventory of Authorized Software</u></b> Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.			

## ***4 Network Configurations***

This section contains guidance on configuring the networking-related aspects of macOS.

## *4.1 Ensure Bonjour Advertising Services Is Disabled (Automated)*

### **Profile Applicability:**

- Level 2

### **Description:**

Bonjour is an auto-discovery mechanism for TCP/IP devices which enumerate devices and services within a local subnet. DNS on macOS is integrated with Bonjour and should not be turned off, but the Bonjour advertising service can be disabled.

### **Rationale:**

Bonjour can simplify device discovery from an internal rogue or compromised host. An attacker could use Bonjour's multicast DNS feature to discover a vulnerable or poorly-configured service or additional information to aid a targeted attack. Implementing this control disables the continuous broadcasting of "I'm here!" messages. Typical end-user endpoints should not have to advertise services to other computers. This setting does not stop the computer from sending out service discovery messages when looking for services on an internal subnet, if the computer is looking for a printer or server and using service discovery. To block all Bonjour traffic except to approved devices the pf or other firewall would be needed.

### **Impact:**

Some applications, like Final Cut Studio and AirPort Base Station management, may not operate properly if the `mDNSResponder` is turned off.

## Audit:

Perform the following to ensure that Bonjour Advertising is disabled:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `NoMulticastAdvertisements` set to 1

*Terminal Method:*

Run the following command to verify that Bonjour Advertising is not enabled:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.mDNSResponder.plist NoMulticastAdvertisements  
1
```

**Note:** If the settings has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

**or**

Run the following command to verify that a profile is installed that disables Bonjour Advertising:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep  
"NoMulticastAdvertisements"  
  
NoMulticastAdvertisements = 1;
```

## Remediation:

Perform the following to disable Bonjour Advertising:

*Terminal Method:*

Run the following command to disable Bonjour Advertising services:

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











*Profile Method:*

1. Create or edit a configuration profile with the `PayloadType` of `com.apple.mDNSResponder`
2. Add the key `NoMulticastAdvertisements`
3. Set the key to `true`

## Additional Information:

Anything Bonjour discovers is already available on the network and probably discoverable with network scanning tools. The security benefit of disabling Bonjour for that reason is minimal.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			



## *4.2 Ensure Show Wi-Fi status in Menu Bar Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

The Wi-Fi status in the menu bar indicates if the system's wireless internet capabilities are enabled. If so, the system will scan for available wireless networks to connect to. At the time of this revision all computers Apple builds have wireless network capability, which has not always been the case. This control only pertains to systems that have a wireless NIC available. Operating systems running in a virtual environment may not score as expected either.

### **Rationale:**

Enabling "Show Wi-Fi status in menu bar" is a security awareness method that helps mitigate public area wireless exploits by making the user aware of their wireless connectivity status.

### **Impact:**

The user of the system should have a quick check on their wireless network status available.

## Audit:

Perform the following to verify that the Wi-Fi status shows in the menu bar:

*Graphical Method:*

1. Open System Preferences
2. Select Dock & Menu Bar
3. Select Wi-Fi
4. Verify that Show in Menu Bar is set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `WiFi` set to `18`

*Terminal Method:*

For each user, run the following command to verify that Wi-Fi status is enabled in the menu bar:

```
$ sudo -u <username> defaults -currentHost read com.apple.controlcenter.plist  
WiFi  
18
```

**Note:** If the settings has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

*example:*

```
$ sudo -u firstuser defaults -currentHost read com.apple.controlcenter.plist  
WiFi  
18
```

**or**

Run the following command to verify that a profile is installed that enables Bluetooth to be shown in the menu bar:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep 'WiFi = 18'  
  
WiFi = 18;
```

## Remediation:

Perform the following to enable Wi-Fi status in the menu bar:

*Graphical Method:*

1. Open System Preferences
2. Select Dock & Menu Bar
3. Select Wi-Fi
4. Set Show in Menu Bar

*Terminal Method:*

For each user, run the following to turn the Wi-Fi status on in the menu bar

```
$ sudo -u <username> defaults -currentHost write  
com.apple.controlcenter.plist WiFi -int 18
```

*example:*

```
$ sudo -u firstuser defaults -currentHost write com.apple.controlcenter.plist  
WiFi -int 18
```







*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of  
com.apple.controlcenter
2. Add the key WiFi
3. Set the key to <integer>18</integer>

## Additional Information:

AirPort is Apple's marketing name for its 802.11b, g, and n wireless interfaces.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v8	<p><b><u>12.6 Use of Secure Network Management and Communication Protocols</u></b></p> <p>Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).</p>			
v7	<p><b><u>15.4 Disable Wireless Access on Devices if Not Required</u></b></p> <p>Disable wireless access on devices that do not have a business purpose for wireless access.</p>			
v7	<p><b><u>15.5 Limit Wireless Access on Client Devices</u></b></p> <p>Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.</p>			

## 4.3 Audit Network Specific Locations (Manual)

### Profile Applicability:

- Level 2

### Description:

The network location feature of the Mac is a very powerful tool to manage network security. By creating different network locations, a user can easily (and without administrative privileges) change the network settings on the Mac. By only using the network interfaces needed at any specific time, exposure to network attacks is limited.

A little understanding of how the Network System Preferences pane works is required.

### Rationale:

Network locations allow the computer to have specific configurations ready for network access when required. Locations can be used to manage which network interfaces are available for specialized network access.

### Impact:

Unneeded network interfaces increase the attack surface and could lead to a successful exploit.

### Audit:

Perform the following to verify that all network locations meet your organization's requirements:

1. Open System Preferences
2. Select Network
3. Select Location
4. Verify that each available network location and the associated network interfaces meet your organization's requirements

**Remediation:**

Perform the following actions to create and edit multiple network locations as needed:












1. Open System Preferences
2. Select Network
3. Select Location
4. Select Edit Locations from the Locations popup menu
5. Select any unneeded network locations
6. Click the minus button for any unneeded locations
7. Select Done
8. Select any remaining network locations
9. Select any unneeded network interfaces
10. Select the minus button to remove them

**Note:** Delete the Automatic location for any device that does not use multiple network services set for DHCP or dynamic addressing. If network services like FireWire, VPN, AirPort or Ethernet are not used by a specific device class those services should be deleted.

**Additional Information:**

Deleting the Automatic location cannot be undone.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>12.2 Establish and Maintain a Secure Network Architecture</u></b> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>15.10 Create Separate Wireless Network for Personal and Untrusted Devices</u></b> Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.			

## 4.4 Ensure HTTP Server Is Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

macOS used to have a graphical front-end to the embedded Apache web server in the Operating System. Personal web sharing could be enabled to allow someone on another computer to download files or information from the user's computer. Personal web sharing from a user endpoint has long been considered questionable, and Apple has removed that capability from the GUI. Apache however is still part of the Operating System and can be easily turned on to share files and provide remote connectivity to an end-user computer. Web sharing should only be done through hardened web servers and appropriate cloud services.

### Rationale:

Web serving should not be done from a user desktop. Dedicated webservers or appropriate cloud storage should be used. Open ports make it easier to exploit the computer.

### Impact:

The web server is both a point of attack for the system and a means for unauthorized file transfers.

### Audit:

Run the following command to verify that the http server services are not currently enabled. This check does not reflect any auto-start settings, only whether the web server is currently enabled:

```
$ sudo launchctl print-disabled system | /usr/bin/grep -c '"org.apache.httpd"
=> true'
```

1

**Note:** If the setting has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.



## Remediation:











Run the following command to disable the http server services:

```
$ sudo systemctl disable system/org.apache.httpd
```

## References:

1. STIGID AOSX-12-001275

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 4.5 Ensure NFS Server Is Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

macOS can act as an NFS fileserver. NFS sharing could be enabled to allow someone on another computer to mount shares and gain access to information from the user's computer. File sharing from a user endpoint has long been considered questionable, and Apple has removed that capability from the GUI. NFSD is still part of the Operating System and can be easily turned on to export shares and provide remote connectivity to an end-user computer.

### Rationale:

File serving should not be done from a user desktop. Dedicated servers should be used. Open ports make it easier to exploit the computer.

### Impact:

The nfs server is both a point of attack for the system and a means for unauthorized file transfers.

### Audit:

Run the following commands to verify that the NFS fileserver service is not enabled:

```
$ sudo launchctl print-disabled system | grep -c '"com.apple.nfsd" => true'
1
```

**Note:** If the setting has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

```
$ sudo cat /etc/exports
cat: /etc/exports: No such file or directory
```

## Remediation:











Run the following command to disable the nfsd fileserver services:

```
$ sudo launchctl disable system/com.apple.nfsd
```

Remove the exported Directory listing.

```
$ sudo rm /etc/exports
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 4.6 Audit Wi-Fi Settings (Manual)

### **Profile Applicability:**

- Level 2

### **Description:**

Some organizations have comprehensive rules that cover the use of wireless technologies in order to implement operational security. There are specific policies governing the use of both Bluetooth and Wi-Fi (802.11) that often include disabling the wireless capability in either software or hardware or both.

Wireless access is part of the feature set required for mobile computers and is considered essential for most users.

### **Rationale:**

The general use case for macOS is to use wireless connectivity. In the current hardware offering very few computers made by Apple provide a built-in wired network capability. While it is possible to get an ethernet adapter for wired connectivity it is not the default. The almost exclusive Apple use case is to support mobile connectivity for users of their devices through wireless connections. For use cases that wireless connectivity is not allowed an Apple model with built-in ethernet is the best option. Wireless can be turned off in those situations in the network system preference pane.

## Audit:

Perform the following to verify the Airport Settings:

*Graphical Method:*

1. Open System Preferences
2. Select Network
3. Select Wi-Fi
4. Verify that Status is set within your organization's parameters

*Terminal Method:*

Run the following commands to verify the Airport settings:

```
$ sudo networksetup -listallhardwareports | grep -A 1 'Hardware Port: Wi-Fi'
```

The output will include `Device:` and the network device number. *ex:* `Device: en0`

```
$ sudo networksetup -getairportpower <network device number>
```

The output will state whether wireless is enabled or disabled.

*Example:*

Wireless enabled:

```
$ sudo networksetup -listallhardwareports | grep -A 1 'Hardware Port: Wi-Fi'

Hardware Port: Wi-Fi
Device: en1

$ sudo networksetup -getairportpower en1

Wi-Fi Power (en1): On
```

Wireless disabled:

```
$ sudo networksetup -listallhardwareports | grep -A 1 'Hardware Port: Wi-Fi'

Hardware Port: Wi-Fi
Device: en1

$ sudo networksetup -getairportpower en1

Wi-Fi Power (en1): Off
```

## Remediation:

Perform the following to set Airport to the correct status:

*Graphical Method:*

1. Open System Preferences
2. Select Network
3. Select Wi-Fi
4. Set Status to your organization's parameters

*Terminal Method:*







Run the following command to set Airport to the correct status:

```
$ sudo networksetup -setairportpower <network device number> <on/off>
```

*Example:*

```
$ sudo networksetup -setairportpower en1 on
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<b>12.6 <u>Use of Secure Network Management and Communication Protocols</u></b> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			
v7	<b>15.4 <u>Disable Wireless Access on Devices if Not Required</u></b> Disable wireless access on devices that do not have a business purpose for wireless access.			
v7	<b>15.5 <u>Limit Wireless Access on Client Devices</u></b> Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			

## ***5 System Access, Authentication and Authorization***

The controls in this section are a combination of hardening controls that are not specifically in a System Preference pane. Many of these controls are only accessible using the Command Line or a Device Profile and not available in the Graphical User Interface. The Benchmark does contain simple, easy to follow instructions for technical staff to audit and implement recommended controls.

## ***5.1 File System Permissions and Access Controls***

File system permissions have always been part of computer security. There are several principles that are part of best practices for a POSIX-based system that are contained in this section. This section does not contain a complete list of every permission on a macOS System that might be problematic. Developers and use cases differ and what some admins long in the profession might consider a travesty a risk assessor steeped in BYOD trends may not give a second glance at. We are documenting here controls that should point out truly bad practices or anomalies that should be looked at and considered closely. Many of the controls are to mitigate the risk of privilege escalation attacks and data exposure to unauthorized parties.



### *5.1.1 Ensure Home Folders Are Secure (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

By default, macOS allows all valid users into the top level of every other user's home folder and restricts access to the Apple default folders within. Another user on the same system can see you have a "Documents" folder but cannot see inside it. This configuration does work for personal file sharing but can expose user files to standard accounts on the system.

The best parallel for Enterprise environments is that everyone who has a Dropbox account can see everything that is at the top level but can't see your pictures. Similarly with macOS, users can see into every new Directory that is created because of the default permissions.

Home folders should be restricted to access only by the user. Sharing should be used on dedicated servers or cloud instances that are managing access controls. Some environments may encounter problems if execute rights are removed as well as read and write. Either no access or execute only for group or others is acceptable.

#### **Rationale:**

Allowing all users to view the top level of all networked users' home folder may not be desirable since it may lead to the revelation of sensitive information.

#### **Impact:**

If implemented, users will not be able to use the "Public" folders in other users' home folders. "Public" folders with appropriate permissions would need to be set up in the /Shared folder.

## Audit:

Run the following command to ensure that all home folders are secure:

```
$ sudo /bin/ls -l /Users/
```

The output for each home folder should be either `drwx-----` or `drwx--x--x`  
*example:*

```
$ sudo /bin/ls -l /Users/

total 0
drwxr-xr-x+ 12 Guest      _guest  384 24 Jul 13:42 Guest
drwxrwxrwt   4 root       wheel   128 22 Jul 11:00 Shared
drwx--x--x+ 18 firstuser  staff   576 10 Aug 14:36 firstuser
drwx--x--x+ 15 seconduser staff   480 10 Aug 09:16 seconduser
drwxrwxrwx+ 11 thirduser  staff   352 10 Aug 14:53 thirduser
drwxrw-rw-+ 11 fourthuser staff   352 10 Aug 14:53 fourthuser
```

## Remediation:

For each user, run the following command to secure all home folders:

```
$ sudo /bin/chmod -R og-rwx /Users/<username>
```

Alternately, run the following command if there needs to be executable access for a home folder:







```
$ sudo /bin/chmod -R og-rw /Users/<username>
```

*example:*

```
$ sudo /bin/chmod -R og-rw /Users/thirduser/
$ sudo /bin/chmod -R og-rwx /Users/fourthuser/
# /bin/ls -l /Users/

total 0
drwxr-xr-x+ 12 Guest      _guest  384 24 Jul 13:42 Guest
drwxrwxrwt   4 root       wheel   128 22 Jul 11:00 Shared
drwx--x--x+ 18 firstuser  staff   576 10 Aug 14:36 firstuser
drwx--x--x+ 15 seconduser staff   480 10 Aug 09:16 seconduser
drwx--x--x+ 11 thirduser  staff   352 10 Aug 14:53 thirduser
drwx-----+ 11 fourthuser staff   352 10 Aug 14:53 fourthuser
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.3 Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b><u>14.6 Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 5.1.2 Ensure System Integrity Protection Status (SIPS) Is Enabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

System Integrity Protection is a security feature introduced in OS X 10.11 El Capitan. System Integrity Protection restricts access to System domain locations and restricts runtime attachment to system processes. Any attempt to inspect or attach to a system process will fail. Kernel Extensions are now restricted to `/Library/Extensions` and are required to be signed with a Developer ID.

#### Rationale:

Running without System Integrity Protection on a production system runs the risk of the modification of system binaries or code injection of system processes that would otherwise be protected by SIP.

#### Impact:

System binaries and processes could become compromised.

#### Audit:

Run the following command to verify that System Integrity Protection is enabled:

```
$ sudo /usr/bin/csrutil status
`System Integrity Protection status: enabled.`
```

## Remediation:

Perform the following to enable System Integrity Protection:

1. Reboot into the Recovery Partition (reboot and hold down Command (⌘) + R)
2. Select Utilities
3. Select Terminal
4. Run the following command:

```
$ sudo /usr/bin/csrutil enable
```

Successfully enabled System Integrity Protection. Please restart the machine for the changes to take effect.

5. Reboot the computer

**Note:** You cannot enable System Integrity Protection from the booted operating system. If the remediation is attempted in the booted OS and not the Recovery Partition the output will give the error `csrutil: failed to modify system integrity configuration`. This tool needs to be executed from the Recovery OS.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.3 <u>Address Unauthorized Software</u></b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	<b>2.6 <u>Allowlist Authorized Libraries</u></b> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
v8	<b>10.5 <u>Enable Anti-Exploitation Features</u></b> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

### 5.1.3 Ensure Apple Mobile File Integrity Is Enabled (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Apple Mobile File Integrity was first released in macOS 10.12, the daemon and service block attempts to run unsigned code. AMFI uses lanchd, code signatures, certificates, entitlements, and provisioning profiles to create a filtered entitlement dictionary for an app. AMFI is the macOS kernel module that enforces code-signing and library validation.

#### Rationale:

Apple Mobile File Integrity (AMFI) validates that application code is validated.

#### Impact:

Applications could be compromised with malicious code.

#### Audit:

Run the following command to verify that Apple Mobile File Integrity is enabled:

```
$ sudo /usr/sbin/nvram -p | /usr/bin/grep -c "amfi_get_out_of_my_way=1"
0
```

#### Remediation:









Run the following command to enable the Apple Mobile File Integrity service:

```
$ sudo /usr/sbin/nvram boot-args=""
```

#### References:

1. <https://eclecticlight.co/2018/12/29/amfi-checking-file-integrity-on-your-mac/>
2. [https://github.com/usnistgov/macos\\_security/issues/39](https://github.com/usnistgov/macos_security/issues/39)
3. [https://github.com/usnistgov/macos\\_security/issues/40](https://github.com/usnistgov/macos_security/issues/40)
4. <https://www.naut.ca/blog/2020/11/13/forbidden-commands-to-liberate-macos/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.3 Address Unauthorized Software</u></b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<b><u>2.6 Allowlist Authorized Libraries</u></b> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v7	<b><u>2.6 Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

### *5.1.4 Ensure Library Validation Is Enabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Library Validation is a security feature introduced in macOS 10.10 Yosemite. Library Validation protects processes from loading arbitrary libraries. This stops root from loading arbitrary libraries into any process (depending on SIP status), and keeps root from becoming more powerful. Security is strengthened, because some user processes can no longer be fooled to run additional code without root's explicit request, which may grant access to daemons that depend on Library Validation for secure validation of code identity.

**Rationale:**

Running without Library Validation on a production system runs the risk of the modification of system binaries or code injection of system processes that would otherwise be protected by Library Validation.

**Impact:**

System binaries and processes could load arbitrary libraries.



## Audit:

Perform the following to ensure that library validation is enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `DisableLibraryValidation = 0` is set

*Terminal Method:*

Run the following command to verify that library validation is set:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.security.libraryvalidation.plist  
DisableLibraryValidation  
  
0
```

**Note:** If the settings has not been changed from the default, then this audit will fail on the command line. Follow the remediation instructions to verify that it is set to a disabled status.

**or**

Run the following command to verify that a profile is installed that enables library validation:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep  
DisableLibraryValidation  
  
DisableLibraryValidation = 0;
```

## Remediation:

Perform the following to enable library validation:

### *Terminal Method:*

Run the following command to set library validation:

```
$ sudo /usr/bin/defaults write  
/Library/Preferences/com.apple.security.libraryvalidation.plist  
DisableLibraryValidation -bool false
```

### *Profile Method:*









1. Create or edit a configuration profile with the PayloadType of com.apple.security.libraryvalidation
2. Add the key Forced
3. Set the key to the following:

```
<array>  
  <dict>  
    <key>mcx_preference_settings</key>  
    <dict>  
      <key>DisableLibraryValidation</key>  
      <false/>  
    </dict>  
  </dict>  
</array>
```

## References:

1. <https://github.com/Automattic/wp-desktop/issues/790>
2. <https://www.naut.ca/blog/2020/11/13/forbidden-commands-to-liberate-macos/>
3. <http://www.newosxbook.com/articles/CodeSigning.pdf>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.3 Address Unauthorized Software</u></b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<b><u>2.6 Allowlist Authorized Libraries</u></b> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v7	<b><u>2.6 Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

### 5.1.5 Ensure Sealed System Volume (SSV) Is Enabled (Automated)

#### **Profile Applicability:**

- Level 1

#### **Description:**

Sealed System Volume is a security feature introduced in macOS 11.0 Big Sur.

During system installation, a SHA-256 cryptographic hash is calculated for all immutable system files and stored in a Merkle tree which itself is hashed as the Seal. Both are stored in the metadata of the snapshot created of the System volume.

The seal is verified by the boot loader at startup. macOS will not boot if system files have been tampered with. If validation fails, the user will be instructed to reinstall the operating system.

During read operations for files located in the Sealed System Volume, a hash is calculated and compared to the value stored in the Merkle tree.

#### **Rationale:**

Running without Sealed System Volume on a production system could run the risk of Apple software, that integrates directly with macOS, being modified.

#### **Impact:**

Apple Software that integrates with the operating system could become compromised.

#### **Audit:**

Run the following command to verify that Sealed System Volume is enabled:

```
$ sudo /usr/bin/csrutil authenticated-root status  
Authenticated Root status: enabled
```

## Remediation:

Perform the following to enable System Integrity Protection:

1. Reboot into the Recovery Partition (reboot and hold down Command (⌘) + R)
2. Select an administrator's account and enter that account's password
3. Select Utilities
4. Select Terminal
5. Run the following command:

```
$ sudo /usr/bin/csrutil enable authenticated-root
```

Successfully enabled System authenticated root.  
Restart the machine for the changes to take effect.










6. Reboot the computer

**Note:** You cannot enable Sealed System Volume from the booted operating system. If the remediation is attempted in the booted OS and not the Recovery Partition the output will give the error `csrutil: This tool needs to be executed from Recovery OS`.

## References:

1. <https://developer.apple.com/news/?id=3xpv8r2m>
2. <https://eclecticlight.co/2020/11/30/is-big-surs-system-volume-sealed/>
3. <https://eclecticlight.co/2020/06/25/big-surs-signed-system-volume-added-security-protection/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.6 Encrypt Data on End-User Devices</u></b> Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.			
v8	<b><u>3.11 Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b><u>13.6 Encrypt the Hard Drive of All Mobile Devices.</u></b> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.			
v7	<b><u>14.8 Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## 5.1.6 Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated)

### Profile Applicability:

- Level 1

### Description:

Applications in the System Applications Directory (/Applications) should be world executable since that is their reason to be on the system. They should not be world-writable and allow any process or user to alter them for other processes or users to then execute modified versions.

### Rationale:

Unauthorized modifications of applications could lead to the execution of malicious code.

### Impact:

Applications changed will no longer be world-writable.

### Audit:

Run the following command to verify that all applications have the correct permissions:

```
$ sudo /usr/bin/find /Applications -iname "*.app" -type d -perm -2 -ls
```

If there is any output, the that application is not in compliance.

*example:*

```
$ sudo /usr/bin/find /Applications -iname "*.app" -type d -perm -2 -ls
921804      0 drwxr-xrwx    3 seconduser      admin           96  8
Aug 04:32 /Applications/Google Chrome.app
922602      0 drwxr-xrwx    3 seconduser      admin           96  8
Aug 04:32 /Applications/Google Chrome copy.app
```

## Remediation:







Run the following command to change the permissions for each application that does not meet the requirements:

```
$ sudo /bin/chmod -R o-w /Applications/<applicationname>
```

*example:*

```
$ sudo /bin/chmod -R o-w /Applications/Google\ Chrome.app/
$ sudo /usr/bin/find /Applications -iname "*.app" -type d -perm -2 -ls
922602          0 drwxr-xrwx    3 seconduser      admin              96   8
Aug 04:32 /Applications/Google Chrome copy.app
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			



## 5.1.7 Ensure No World Writable Files Exist in the System Folder (Automated)

### Profile Applicability:

- Level 1

### Description:

Software sometimes insists on being installed in the `/System/Volumes/Data/System` Directory and have inappropriate world-writable permissions.

### Rationale:

Folders in `/System/Volumes/Data/System` should not be world-writable. The audit check excludes the "Drop Box" folder that is part of Apple's default user template.

### Audit:

Run the following command to check for directories in the `/System` folder that are world-writable:

```
$ sudo /usr/sbin/find /System/Volumes/Data/System -type d -perm -2 -ls
```

If there is no output then it is complaint.

*example:*

```
$ sudo /usr/sbin/find /System/Volumes/Data/System -type d -perm -2 -ls
640774      0 drwx-wx-wx   3 root          wheel              96
Aug  9  2020 /System/Volumes/Data/System/Library/baddir
```

### Remediation:







Run the following command to set permissions so that folders are not world-writable in the `/System` folder:

```
$ sudo /bin/chmod -R o-w /Path/<baddir>
```

*example:*

```
$ sudo /bin/chmod -R o-w /System/Volumes/Data/System/Library/baddir
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.3 Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b><u>14.6 Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 5.1.8 Ensure No World Writable Files Exist in the Library Folder (Automated)

#### Profile Applicability:

- Level 2

#### Description:

Software sometimes insists on being installed in the `/Library` Directory and have inappropriate world-writable permissions.

#### Rationale:

Folders in `/System/Volumes/Data/Library` should not be world-writable. The audit check excludes the `/System/Volumes/Data/Library/Caches` and `/System/Volumes/Data/Library/Preferences/Audio/Data` folders where the sticky bit is set.

#### Audit:

Run the following to verify that no directories in the `/System/Volumes/Data/Library` folder are world-writable:

```
$ sudo /usr/sbin/find /System/Volumes/Data/Library -type d -perm -2 -ls |  
/usr/bin/grep -v Caches | grep -v Audio
```

*example:*

```
$ sudo /usr/sbin/find /System/Volumes/Data/Library -type d -perm -2 -ls |  
/usr/bin/grep -v Caches | grep -v Audio  
  
929686          0 drwxr-xrwx    2 root          wheel          64  
Aug 11 09:49 /System/Volumes/Data/Library/baddir
```

#### Remediation:







Run the following command to set permissions so that folders are not world-writable in the `/System/Volumes/Data/Library` folder:

```
$ sudo /bin/chmod -R o-w /System/Volumes/Data/Library/<baddir>
```

*example:*

```
$ sudo /bin/chmod -R o-w /System/Volumes/Data/Library/baddir
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.3 Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b><u>14.6 Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 5.2 Password Management

Password security is an important part of general IT security where passwords are in use. For macOS passwords are still much more widely used than other methods for account access. While there are other authentication and authorization methods for access from a macOS computer to organizational services, console access to the Mac is probably done using a password. This section contains password controls.

Recent updates based on research by NIST in SP800-63 call in to question traditional password complexity and rotation requirements. Sticky notes are not a password management program and password vault APIs are under increasing attack. Ideally the user will remember their important passwords. The new understanding has informed changes to the previous password recommendations.

Length, threshold, and a yearly rotation requirement are the only scored controls below. Other controls will remain as unscored options. Passwords used for macOS are likely to also function as encryption keys for FileVault. Depending on the information confidentiality on FileVault volumes, stronger passwords may be required than are necessary to pass the controls in this Benchmark.

Apple supported solutions for managing local passwords on macOS are to use either an XML file that contains password rules that are imported with pwpolicy or through the use of a profile. In either case, the controls in this section can be implemented with an organizationally-approved password policy.

Content is available where security hardening content is available and is native to Management suites and MDM tools.

Content also available here: <https://github.com/ronc-LAemigre/macOS-sec-config>

NIST guidance on passwords starting at 5.1.1.1

<https://pages.nist.gov/800-63-3/sp800-63b.html>

### *5.2.1 Ensure Password Account Lockout Threshold Is Configured (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

The account lockout threshold specifies the amount of times a user can enter an incorrect password before a lockout will occur.

Ensure that a lockout threshold is part of the password policy on the computer.

**Rationale:**

The account lockout feature mitigates brute-force password attacks on the system.

**Impact:**

The number of incorrect log on attempts should be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user log on.

The locked account will auto-unlock after a few minutes when bad password attempts stop. The computer will accept the still-valid password if remembered or recovered.

## Audit:

Perform the following to ensure that the Password Account Threshold is set to less than or equal to 5:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Max Failed Attempts` set to  $\leq 5$

*Terminal Method:*

Run the following command to verify that the number of failed attempts is less than or equal to 5:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A 1  
'policyAttributeMaximumFailedAuthentications' | /usr/bin/tail -1 |  
/usr/bin/cut -d'>' -f2 | /usr/bin/cut -d'<' -f1
```

The output should be  $\leq 5$

**or**

Run the following command to verify that a profile is installed that configures account lockout threshold set to less than or equal to 5:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "maxFailedAttempts"
```

The output should include `maxFailedAttempts`  $\leq 5$ ;

## Remediation:

Perform the following to enable Password Account Thresholds to less than or equal to 5:

### *Terminal Method:*

Run the following command to set the maximum number of failed login attempts to less than or equal to 5:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"maxFailedLoginAttempts=<value≤5>"
```

### *example:*

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"maxFailedLoginAttempts=5"
```






### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `maxFailedAttempts`
3. Set the key to `<value≤5>`

## References:

1. CIS Password Policy - <https://workbench.cisecurity.org/communities/113>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.2 <u>Establish an Access Revoking Process</u></b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<b>16.7 <u>Establish Process for Revoking Access</u></b> Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			



### *5.2.2 Ensure Password Minimum Length Is Configured (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

A minimum password length is the fewest number of characters a password can contain to meet a system's requirements.

Ensure that a minimum of a 15-character password is part of the password policy on the computer.

Where the confidentiality of encrypted information in FileVault is more of a concern requiring a longer password or passphrase may be sufficient rather than imposing additional complexity requirements that may be self-defeating.

**Rationale:**

Information systems that are not protected with strong password schemes including passwords of minimum length provide a greater opportunity for attackers to crack the password and gain access to the system.

**Impact:**

Short passwords can be easily attacked.

## Audit:

Perform the following to ensure that the Password Account Threshold is set to greater than or equal to 15:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Min Password Length` set to  $\geq 15$

*Terminal Method:*

Run the following command to verify that the password length is greater than or equal to 15:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
minimumLength | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 | /usr/bin/cut -d  
'<' -f1
```

The output value should be  $\geq 15$

**or**

Run the following command to verify that a profile is installed that configures the minimum password length set to greater than or equal to 15:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "minLength"
```

The output should include `minLength  $\geq 15$` ;

## Remediation:

Perform the following to enable passwords of a minimum length of 15:

### *Terminal Method:*

Run the following command to set the password length to greater than or equal to 15:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy "minChars=<value≥15>"
```






### *example:*

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy "minChars=15"
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayLoadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `minLength`
3. Set the key to `<integer><value≥15></integer>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 <u>Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### *5.2.3 Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Manual)*

**Profile Applicability:**

- Level 2

**Description:**

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that an Alphabetic character is part of the password policy on the computer

**Rationale:**

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

**Impact:**

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

## Audit:

Perform the following to ensure that the passwords must contain at least 1 alphabetic characters:

### *Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Requires Alphanumeric` set to `True`

### *Terminal Method:*

Run the following command to verify that the password requires at least one letter:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
minimumLetters | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 | /usr/bin/cut -d  
'<' -f1
```

The output should be  $\geq 1$

**or**

Run the following command to verify that a profile is installed that requires passwords to require at least 1 alphabetic characters:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "requireAlphanumeric"
```

The output should include `requireAlphanumeric  $\geq 1$` ;

## Remediation:

Perform the following to enable passwords to require at least 1 alphabetical characters:

### *Terminal Method:*

Run the following command to set the that passwords must contain at least one letter:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -  
setaccountpolicies "requiresAlpha=<value≤5>"
```

### *example:*






```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy "requiresAlpha=1"
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayLoadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `requireAlphanumeric`
3. Set the key to `<integer><value≥1></integer>`

**Note:** This profile requires both an alphabetical and numeric characters.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

#### *5.2.4 Ensure Complex Password Must Contain Numeric Character Is Configured (Manual)*

**Profile Applicability:**

- Level 2

**Description:**

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that a number or numeric value is part of the password policy on the computer.

**Rationale:**

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

**Impact:**

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

## Audit:

Perform the following to ensure that the passwords must contain at least 1 numeric characters:

### *Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Requires Alphanumeric` set to `True`

### *Terminal Method:*

Run the following command to verify that passwords require at least one number:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
minimumNumericCharacters | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 |  
/usr/bin/cut -d'<' -f1
```

The output should be  $\geq 1$

**or**

Run the following command to verify that a profile is installed that requires passwords to require at least 1 numeric characters:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "requireAlphanumeric"
```

The output should include `requireAlphanumeric  $\geq 1$` ;



## Remediation:

Perform the following to enable passwords to require at least 1 numeric characters:

### *Terminal Method:*

Run the following command to set passwords to require at least one number:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -  
setaccountpolicies "requiresNumeric=<value≥1>"
```

### *example:*






```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"requiresNumeric=2"
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayLoadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `requireAlphanumeric`
3. Set the key to `<integer><value≥1></integer>`

**Note:** This profile requires both an alphabetical and numeric characters.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 <u>Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### *5.2.5 Ensure Complex Password Must Contain Special Character Is Configured (Manual)*

**Profile Applicability:**

- Level 2

**Description:**

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Ensure that a special character is part of the password policy on the computer.

**Rationale:**

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

**Impact:**

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

## Audit:

Perform the following to ensure that the passwords must contain at least 1 special characters:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Min Complex Length` set to  $\geq 1$

*Terminal Method:*

Run the following command to set verify that the password requires at least one special character:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
minimumSymbols | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 | /usr/bin/cut -d  
'<' -f1
```

The output value should be  $\geq 1$

**or**

Run the following command to verify that a profile is installed that requires passwords to require at least 1 special character:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "minComplexChars"
```

The output should include `minComplexChars  $\geq 1$` ;

## Remediation:

Perform the following to enable passwords to require at least 1 special characters:

### *Terminal Method:*

Run the following command to set passwords to require at least one special character:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -  
setaccountpolicies "requiresSymbol=<value≥1>"
```






### *example:*

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"requiresSymbol=1"
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayLoadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `minComplexChars`
3. Set the key to `<integer><value≥1></integer>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 <u>Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

## 5.2.6 Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Manual)

### Profile Applicability:

- Level 2

### Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that both uppercase and lowercase letters are part of the password policy on the computer.

### Rationale:

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

### Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

### Audit:

Run the following command to set verify that the password requires at upper and lower case letter:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
minimumMixedCaseCharacters | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 |  
/usr/bin/cut -d '<' -f1
```

The output should be  $\geq 1$

## Remediation:






Run the following command to set passwords to require at upper and lower case letter:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"requiresMixedCase=<value>1>"
```

*example:*

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"requiresMixedCase=1"
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 <u>Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### *5.2.7 Ensure Password Age Is Configured (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Over time passwords can be captured by third-parties through mistakes, phishing attacks, third party breaches or merely brute force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed) users should reset passwords periodically. This control uses 365 days as the acceptable value. Some organizations may be more or less restrictive. This control mainly exists to mitigate against password reuse of the macOS account password in other realms that may be more prone to compromise. Attackers take advantage of exposed information to attack other accounts.

**Rationale:**

Passwords should be changed periodically to reduce exposure.

**Impact:**

Required password changes will lead to some locked computers requiring admin assistance.

## Audit:

Perform the following to ensure that the passwords expire after at most 365 days:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Max Age (days)` set to  $\leq 365$

*Terminal Method:*

Run the following command to verify that the password expires after at most 365 days:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
policyAttributeDaysUntilExpiration | /usr/bin/tail -1 | /usr/bin/cut -d'>' -  
f2 | /usr/bin/cut -d'<' -f1
```

The output should be  $\leq 365$

**or**

Run the following command to verify that a profile is installed that requires passwords to expire less than or equal to 365 days:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "maxPINAgeInDays"
```

The output should include `maxPINAgeInDays  $\leq 365$` ;

## Remediation:

Perform the following to enable passwords expiring at no greater than 365 days:

*Terminal Method:*

Run the following command to require that passwords expire after at most 365 days:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"maxMinutesUntilChangePassword=<value $\leq 525600$ >"
```

*example:*







```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy  
"maxMinutesUntilChangePassword=43200"
```

*Profile Method:*

1. Create or edit a configuration profile with the `PayLoadType` of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `maxPINAgeInDays`
3. Set the key to `<integer><value $\leq 365$ ></integer>`



**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.3 <u>Disable Dormant Accounts</u></b> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			
v7	<b>16.9 <u>Disable Dormant Accounts</u></b> Automatically disable dormant accounts after a set period of inactivity.			

## 5.2.8 Ensure Password History Is Configured (Automated)

### **Profile Applicability:**

- Level 1

### **Description:**

Over time passwords can be captured by third-parties through mistakes, phishing attacks, third party breaches or merely brute force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed) users must reset passwords periodically. This control ensures that previous passwords are not reused immediately by keeping a history of previous password hashes. Ensure that password history checks are part of the password policy on the computer. This control checks whether a new password is different than the previous 15. The latest NIST guidance based on exploit research referenced in this section details how one of the greatest risks is password exposure rather than password cracking. Passwords should be changed to a new unique value whenever a password might have been exposed to anyone other than the account holder. Attackers have maintained persistent control based on predictable password change patterns and substantially different patterns should be used in case of a leak.

### **Rationale:**

Old passwords should not be reused.

### **Impact:**

Required password changes will lead to some locked computers requiring admin assistance.

## Audit:

Perform the following to ensure that the password is not the same as at least the last 15 passwords:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Max History Kept` set to  $\geq 15$

*Terminal Method:*

Run the following command to verify that the password is required to be different from at least the last 15 passwords:

```
$ sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -A1  
policyAttributePasswordHistoryDepth | /usr/bin/tail -1 | /usr/bin/cut -d'>' -  
f2 | /usr/bin/cut -d '<' -f1
```

The output should be  $\geq 15$

**or**

Run the following command to verify that a profile is installed that requires passwords history of at least the previous 15 passwords:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "pinHistory"
```

The output should include `pinHistory  $\geq 15$` ;

## Remediation:

Perform the following to enable new passwords to be different than at least the last 15 passwords:

### *Terminal Method:*

Run the following command to require that the password must to be different from at least the last 15 passwords:

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy "usingHistory=<value>15"
```






*example:*

```
$ sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy "usingHistory=15"
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `pinHistory`
3. Set the key to `<integer><value>15</integer>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 <u>Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

## 5.3 Ensure the Sudo Timeout Period Is Set to Zero (Automated)

### Profile Applicability:

- Level 1

### Description:

The `sudo` command allows the user to run programs as the root user. Working as the root user allows the user an extremely high level of configurability within the system. This control along with the control to use a separate timestamp for each tty limits the window where an unauthorized user, process or attacker could utilize legitimate credentials that are valid for longer than required.

### Rationale:

The `sudo` command stays logged in as the root user for five minutes before timing out and re-requesting a password. This five-minute window should be eliminated since it leaves the system extremely vulnerable. This is especially true if an exploit were to gain access to the system, since they would be able to make changes as a root user.

### Impact:

This control has a serious impact where users often have to use `sudo`. It is even more of an impact where users have to use `sudo` multiple times in quick succession as part of normal work processes. Organizations with that common use case will likely find this control too onerous and are better to accept the risk of not requiring a 0 grace period.

In some ways the use of `sudo -s`, which is undesirable, is better than a long grace period since that use does change the hash to show that it is a root shell rather than a normal shell where `sudo` commands will be implemented without a password.

### Audit:

Perform the following to verify the `sudo` timeout period:

```
$ sudo /usr/bin/grep -e "timestamp" /etc/sudoers  
Defaults timestamp_timeout=0
```

## Remediation:

Run the following command to edit the sudo settings:

```
$ sudo /usr/sbin/visudo
```

Add the line `Defaults timestamp_timeout=0` in the Override built-in defaults section.

## Additional Information:

```
#
# Sample /etc/sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
##
# Override built-in defaults
##
Defaults      env_reset
Defaults      env_keep += "BLOCKSIZE"
Defaults      env_keep += "COLORFGBG COLORTERM"
Defaults      env_keep += "__CF_USER_TEXT_ENCODING"
Defaults      env_keep += "CHARSET LANG LANGUAGE LC_ALL LC_COLLATE
LC_CTYPE"
Defaults      env_keep += "LC_MESSAGES LC_MONETARY LC_NUMERIC LC_TIME"
Defaults      env_keep += "LINES COLUMNS"
Defaults      env_keep += "LSCOLORS"
Defaults      env_keep += "SSH_AUTH_SOCK"
Defaults      env_keep += "TZ"
Defaults      env_keep += "DISPLAY XAUTHORIZATION XAUTHORITY"
Defaults      env_keep += "EDITOR VISUAL"
Defaults      env_keep += "HOME MAIL"

Defaults      lecture_file = "/etc/sudo_lecture"
Defaults timestamp_timeout=0

##
# User alias specification
##
# User_Alias   FULLTIMERS = millert, mikef, dowdy

##
# Runas alias specification
##
# Runas_Alias  OP = root, operator
```

```
##
# Host alias specification
##
# Host_Alias    CUNETS = 128.138.0.0/255.255.0.0
# Host_Alias    CSNETS = 128.138.243.0, 128.138.204.0/24, 128.138.242.0
# Host_Alias    SERVERS = master, mail, www, ns
# Host_Alias    CDROM = orion, perseus, hercules







##
# Cmnd alias specification
##
# Cmnd_Alias    PAGERS = /usr/bin/more, /usr/bin/pg, /usr/bin/less

##
# User specification
##

# root and users in group wheel can run anything on any machine as any user
root            ALL = (ALL) ALL
%admin          ALL = (ALL) ALL

## Read drop-in files from /private/etc/sudoers.d
## (the '#' here does not indicate a comment)
#includedir /private/etc/sudoers.d
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## 5.4 Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated)

### Profile Applicability:

- Level 1

### Description:

Using tty tickets ensures that a user must enter the sudo password in each Terminal session.

With sudo versions 1.8 and higher, introduced in 10.12, the default value is to have tty tickets for each interface so that root access is limited to a specific terminal. The default configuration can be overwritten or not configured correctly on earlier versions of macOS.

### Rationale:

In combination with removing the sudo timeout grace period, a further mitigation should be in place to reduce the possibility of a background process using elevated rights when a user elevates to root in an explicit context or tty.

Additional mitigation should be in place to reduce the risk of privilege escalation of background processes.

### Impact:

This control should have no user impact. Developers or installers may have issues if background processes are spawned with different interfaces than where sudo was executed.

### Audit:

Run the following commands to verify that the default sudoers controls are in place with explicit tickets per tty:

```
$ sudo /usr/bin/grep -E -s '!tty_tickets' /etc/sudoers /etc/sudoers.d/*
```

Nothing should be returned.

```
$ sudo /usr/bin/grep -E -s 'timestamp_type' /etc/sudoers /etc/sudoers.d/*
```

Ensure that nothing is returned or that the output does not include `timestamp_type=ppid` or `timestamp_type=global`



## Remediation:

Edit the `/etc/sudoers` file with `visudo` and remove `!tty_tickets` from any Defaults line. If there is a Default line of `timestamp_type=` with a value other than `tty`, change the value to `tty`

If there is a file in the `/etc/sudoers.d/` folder that contains `Defaults !tty_tickets`, edit the file and remove `!tty_tickets` from any Defaults line. If there is a file `/etc/sudoers.d/` folder that contains a Default line of `timestamp_type=` with a value other than `tty`, change the value to `tty`







## Default Value:

If no value is set, the default value of `tty_tickets` enabled will be used.

## Additional Information:

<https://github.com/jorangreef/sudo-prompt/issues/33>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## *5.5 Ensure login keychain is locked when the computer sleeps (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

The login keychain is a secure database store for passwords and certificates and is created for each user account on macOS. The system software itself uses keychains for secure storage. Anyone with physical access to an unlocked keychain where the screen is also unlocked can copy all passwords in that keychain. The approach recommended here is that the login keychain be set to lock when the computer sleeps to reduce the risk of password exposure. Organizations that use Firefox and Thunderbird will have a much different tolerance than those organizations using keychain aware applications extensively.

In previous versions of the Benchmark there were recommendations for inactivity timeouts and maintaining individual keychains. The user experience with a short inactivity timeout is difficult. Users will be unlocking the keychain often to all keychain aware applications access. This benchmark lengthened the inactivity timeout substantially in the past to keep the inactivity control. At this time it has been dropped. The compensating controls of a screen lock, lock when sleeping, and the built-in keychain encryption make the control allows for a small residual risk.

Early guidance, including in this Benchmark, recommended the use of additional keychains as needed to separate confidentiality levels or separate user domains (work, school, volunteer groups...) At this point, particularly with the availability of iCloud Keychain key segregation is a niche use case. Recent recommendations on distinct keychains is very rare.

### **Rationale:**

While logged in, the keychain does not prompt the user for passwords for various systems and/or programs. This can be exploited by unauthorized users to gain access to password-protected programs and/or systems in the absence of the user.

### **Impact:**

The user may experience multiple prompts to unlock the keychain when waking from sleep.

## Audit:

Perform the following to verify that the keychain locks when the computer sleeps:

### *Graphical Method:*

1. Open Keychain Access
2. Select the login keychain
3. Select Edit
4. Select Change Settings for keychain `login`
5. Verify that Lock when sleeping is set

### *Terminal Method:*

For each user, run the following command to unlock the keychain and verify it locks on sleep:

```
$ sudo -u <username> security unlock-keychain  
/Users/<username>/Library/Keychains/login.keychain  
  
$ sudo -u <username> security show-keychain-info  
/Users/<username>/Library/Keychains/login.keychain
```

The output should contain `lock-on-sleep`.

### *example:*

```
$ sudo -u firstuser security unlock-keychain  
/Users/firstuser/Library/Keychains/login.keychain  
  
password to unlock /Users/firstuser/Library/Keychains/login.keychain:  
  
$ sudo -u firstuser security show-keychain-info  
/Users/firstuser/Library/Keychains/login.keychain  
  
Keychain "/Users/firstuser/Library/Keychains/login.keychain" lock-on-sleep  
timeout=21600s
```

## Remediation:

Perform the following to set the login keychain to lock on sleep:

*Graphical Method:*

1. Open Keychain Access
2. Select the login keychain
3. Select Edit
4. Select Change Settings for keychain `login`
5. Set Lock when sleeping

*Terminal Method:*







For each user, run the following command to set the login keychain to sleep on lock:

```
$ sudo -u <username> security set-keychain-settings -l  
/Users/<username>/Library/Keychains/login.keychain
```

*example:*

```
$ sudo -u firstuser security set-keychain-settings -l  
/Users/firstuser/Library/Keychains/login.keychain
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## 5.6 Ensure the "root" Account Is Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

The root account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. With some Linux distros the system administrator may commonly use the root account to perform administrative functions.

### Rationale:

Enabling and using the root account puts the system at risk since any successful exploit or mistake while the root account is in use could have unlimited access privileges within the system. Using the `sudo` command allows users to perform functions as a root user while limiting and password protecting the access privileges. By default the root account is not enabled on a macOS computer. An administrator can escalate privileges using the `sudo` command (use `-s` or `-i` to get a root shell).

### Impact:

Some legacy POSIX software might expect an available root account.

### Audit:

Perform the following to ensure that the root user is not enabled:

*Graphical Method:*

1. Open `/System/Library/CoreServices/Applications/Directory Utility`
2. Click the lock icon to unlock the service
3. Click Edit
4. Verify that the menu shows Enable Root User, not Disable Root User

*Terminal Method:*

Run the following command to verify the the root user has not been enabled:

```
$ sudo /usr/bin/dscl . -read /Users/root AuthenticationAuthority  
  
No such key: AuthenticationAuthority
```

## Remediation:

Perform the following to ensure that the root user is disabled:

*Graphical Method:*







1. Open /System/Library/CoreServices/Applications/Directory Utility
2. Click the lock icon to unlock the service
3. Click Edit
4. Click Disable Root User

*Terminal Method:*

Run the following command to disable the root user:

```
$ sudo /usr/sbin/dsenableroot -d  
  
username = root  
user password:
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<b>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

## *5.7 Ensure Automatic Login Is Disabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

The automatic login feature saves a user's system access credentials and bypasses the login screen. Instead, the system automatically loads to the user's desktop screen.

### **Rationale:**

Disabling automatic login decreases the likelihood of an unauthorized person gaining access to a system.

### **Impact:**

If automatic login is not disabled an unauthorized user could gain access to the system without supplying any credentials.

## Audit:

Perform the following to ensure that automatic login is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Click the lock to authenticate
4. Select Login Options
5. Verify that Automatic login is set to Off

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `DisableAutoLoginClient = 1` is set

*Terminal Method:*

Run the following command to verify that automatic login has not been enabled:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.loginwindow  
autoLoginUser
```

No output should be returned.

**or**

Run the following command to verify that a profile is installed that disables automatic login:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep  
"com.apple.login.mcx.DisableAutoLoginClient"  
  
com.apple.login.mcx.DisableAutoLoginClient = 1;
```



## Remediation:

Perform the following to set automatic login to off:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Click the lock to authenticate
4. Select Login Options
5. Select Automatic login and set it to Off

*Terminal Method:*







Run the following command to disable automatic login:

```
$ sudo /usr/bin/defaults delete /Library/Preferences/com.apple.loginwindow autoLoginUser
```

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.loginwindow
2. Add the key com.apple.login.mcx.DisableAutoLoginClient
3. Set the key to <true/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.7 <u>Manage Default Accounts on Enterprise Assets and Software</u></b> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<b>4.2 <u>Change Default Passwords</u></b> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			

## *5.8 Ensure a Password is Required to Wake the Computer From Sleep or Screen Saver Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Sleep and screensaver modes are low power modes that reduce electrical consumption while the system is not in use.

### **Rationale:**

Prompting for a password when waking from sleep or screensaver mode mitigates the threat of an unauthorized person gaining access to a system in the user's absence.

### **Impact:**

Without a screenlock in place anyone with physical access to the computer would be logged in and able to use the active user's session.

## Audit:

Perform the following to verify that a password is required to wake from sleep or screen saver:

### *Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select General
4. Verify that Require password after or screensaver begins is set with `immediately` or `'5 seconds'`

### **or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Ask For Password` set to `True`
4. Verify that the same installed profile has `Ask For Password Delay` set to `<0,5>`

### *Terminal Method:*

Run the following command to verify that a profile is installed that requires a password to wake the computer from sleep or from the screen saver:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep askForPassword  
  
askForPassword = 1;  
askForPasswordDelay = <0,5>;
```

## Remediation:

Perform the following to enable a password for unlock after a screen saver begins or after sleep:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select General
4. Set Require password after or screensaver begins with a time of `immediately` or `'5 seconds'`

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.screensaver`
2. Add the key `askForPassword`
3. Set the key to `</true>`
4. Add the key `askForPasswordDelay`
5. Set the key to `<integer><0,5></integer>`

## Additional Information:

This only protects the system when the screen saver is running.







**Note:** The command line check in previous versions of the Benchmark does not work as expected here. The use of a profile is recommended for both implementation and auditing on a 10.13 system.

Issue <https://blog.kolide.com/screensaver-security-on-macos-10-13-is-broken-a385726e2ae2>

Profile to control screensaver

<https://github.com/rtrouton/profiles/blob/master/SetDefaultScreensaver/SetDefaultScreensaver.mobileconfig>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></b> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<b><u>4.2 Change Default Passwords</u></b> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			

## 5.9 Ensure system is set to hibernate (Automated)

### Profile Applicability:

- Level 2

### Description:

In order to use a computer with Full Disk Encryption (FDE) macOS must keep encryption keys in memory to allow the use of the disk that has been FileVault protected. The storage volume has been unlocked and acts as if it was not encrypted. When the system is not in use the volume is protected through encryption. When the system is sleeping and available to quickly resume the encryption keys remain in memory.

If an unauthorized party has possession of the computer and the computer is only slept there are known attack vectors that can be attempted against the RAM that has the encryption keys or the running operating system that is protected by a login screen. Network attacks if network interfaces are on as well as USB or other open device ports are possible. Most of these attacks require knowledge of unpatched vulnerabilities or a high level of sophistication if all the other controls function as intended.

There is little impact on hibernating the system rather than sleeping after an appropriate time period to remediate the risk of OS level attacks. Hibernation writes the keys to disk and requires FileVault to be unlocked prior to the OS being available. In the case of unauthorized personnel with access to the computer encryption would have to be broken prior to attacking the operating system in order to recover data from the system.

<https://www.helpnetsecurity.com/2018/08/20/laptop-sleep-security/>

Mac systems should be set to hibernate after sleeping for a risk-acceptable time period. The default value for "standbydelay" is three hours (10800 seconds). This value is likely appropriate for most desktops. If Mac desktops are deployed in unmonitored, less physically secure areas with confidential data this value might be adjusted. The desktop or would have to retain power so that the running OS or physical RAM could be attacked however.

MacBooks should be set so that the standbydelay is 15 minutes (900 seconds) or less. This setting should allow laptop users in most cases to stay within physically secured areas while going to a conference room, auditorium or other internal location without having to unlock the encryption. When the user goes home at night the laptop will auto-hibernate after 15 minutes and require the FileVault password to unlock prior to logging back into system when it resumes.

MacBooks should also be set to a hibernate mode that removes power from the RAM. This will stop the possibility of cold boot attacks on the system.

**Rationale:**

To mitigate the risk of data loss the system should power down and lock the encrypted drive after a specified time. Laptops should hibernate 15 minutes or less after sleeping.

**Impact:**

The laptop will take additional time to resume normal operation then if only sleeping rather than hibernating.

## Audit:

Run the following command to verify the hibernation settings and that FileVault keys are destroyed on standby:

```
$ sudo system_profiler SPHardwareDataType | grep -e MacBook
```

If the output includes `Model Name: MacBook`, `Model Name: MacBook Air`, `Model Name: MacBook Pro` run the following:

```
$ sudo pmset -g | grep -e standby
```

The output should include a `standbydelaylow` value  $\leq 600$ , a `standbydelayhigh` value  $\leq 600$ , and a `highstandbythreshold` value  $\geq 90$ .

```
$ sudo pmset -g | grep DestroyFVKeyOnStandby
DestroyFVKeyOnStandby      1
$ sudo pmset -g | grep hibernatemode
hibernatemode              25
```

*example:*

```
$ sudo system_profiler SPHardwareDataType | grep -e MacBook
      Model Name: MacBook Pro
      Model Identifier: MacBookPro13,1
$ sudo pmset -g | grep -e standbydelay
standbydelaylow            600
standby                    1
standbydelayhigh           600
highstandbythreshold      50
$ sudo pmset -g | grep DestroyFVKeyOnStandby
DestroyFVKeyOnStandby      1
$ sudo pmset -g | grep hibernatemode
hibernatemode              25
```



## Remediation:

Run the following command to set the hibernate delays and to ensure the FileVault keys are set to be destroyed on standby:

```
$ sudo pmset -a standbydelaylow <value≤600>
$ sudo pmset -a standbydelayhigh <value≤600>
$ sudo pmset -a highstandbythreshold <value≥90>
$ sudo pmset -a destroyfvkeyonstandby 1
$ sudo pmset -a hibernatemode 25
```

*example:*

```
$ sudo pmset -a standbydelaylow 500
$ sudo pmset -a standbydelayhigh 500
$ sudo pmset -a highstandbythreshold 100
$ sudo pmset -a destroyfvkeyonstandby 1
$ sudo pmset -a hibernatemode 25
```

## Additional Information:

There are several good references to the concerns about ensuring hibernation rather than sleep is in place. A selection below:

<http://mattwashchuk.com/articles/2016/01/08/maximizing-filevault-security>







<https://www.zdziarski.com/blog/?p=6705>

<https://www.howtogeek.com/260478/how-to-choose-when-your-mac-hibernates-or-enters-standby/>

<https://www.lifewire.com/change-mac-sleep-settings-2260804>

<https://www.zdziarski.com/blog/?p=6705>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>16.11 Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## *5.10 Require an administrator password to access system-wide preferences (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

System Preferences controls system and user settings on a macOS Computer. System Preferences allows the user to tailor their experience on the computer as well as allowing the System Administrator to configure global security settings. Some of the settings should only be altered by the person responsible for the computer.

### **Rationale:**

By requiring a password to unlock system-wide System Preferences the risk is mitigated of a user changing configurations that affect the entire system and requires an admin user to re-authenticate to make changes

### **Impact:**

If Automatic login is not disabled an unauthorized user could login without supplying a user password or credential.

## Audit:

Perform the following to verify that an administrator password is required to access system-wide preferences:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select General
4. Select Advanced...
5. Verify that Require an administrator password to access system-wide preferences is set

*Terminal Method:*

Run the following command to verify that accessing system-wide preferences requires an administrator password:

```
$ sudo security authorizationdb read system.preferences 2> /dev/null | grep -
A1 shared | grep false
<false/>
```

## Remediation:

Perform the following to verify that an administrator password is required to access system-wide preferences:

*Graphical Method:*

1. Open System Preferences
2. Select Security & Privacy
3. Select General
4. Select Advanced...
5. Set Require an administrator password to access system-wide preferences







*Terminal Method:*

The authorizationdb settings cannot be written to directly, so the plist must be exported out to temporary file. Changes can be made to the temporary plist, then imported back into the authorizationdb settings.

Run the following commands to enable that an administrator password is required to access system-wide preferences:

```
$ sudo security authorizationdb read system.preferences > /tmp/system.preferences.plist  
YES (0)  
  
$ sudo defaults write /tmp/system.preferences.plist shared -bool false  
  
$ sudo security authorizationdb write system.preferences < /tmp/system.preferences.plist  
YES (0)
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 5.11 Ensure an administrator account cannot login to another user's active and locked session (Automated)

### Profile Applicability:

- Level 1

### Description:

macOS has a privilege that can be granted to any user that will allow that user to unlock active user's sessions.

### Rationale:

Disabling the admins and/or user's ability to log into another user's active and locked session prevents unauthorized persons from viewing potentially sensitive and/or personal information.

### Impact:

While Fast user switching is a workaround for some lab environments especially where there is even less of an expectation of privacy this setting change may impact some maintenance workflows.

### Audit:

Run the following command to verify that a user cannot log into another user's active and/or locked session:

```
$ sudo security authorizationdb read system.login.screensaver 2>&1 |  
/usr/bin/grep -c 'use-login-window-ui'  
  
1
```

### Remediation:







Run the following command to disable a user logging into another user's active and/or locked session:

```
$ sudo security authorizationdb write system.login.screensaver use-login-  
window-ui  
  
YES (0)
```

## References:

1. <https://derflounder.wordpress.com/2014/02/16/managing-the-authorization-database-in-os-x-mavericks/>
2. <https://www.jamf.com/jamf-nation/discussions/18195/system-login-screensaver>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.3 Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b><u>16.11 Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## *5.12 Ensure a Custom Message for the Login Screen Is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

An access warning informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored.

### **Rationale:**

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

### **Impact:**

If users are not informed of their responsibilities, unapproved activities may occur. Users that are not approved for access may take the lack of a warning banner as implied consent to access.



## Audit:

Perform the following to ensure that the a login banner is configured:

*Graphical Method:*

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Banner Text` is configured to your organization's required text

*Terminal Method:*

Run the following command to verify that a custom message on the login screen is configured:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.loginwindow.plist LoginwindowText
```

If the output is The domain/default pair of (/Library/Preferences/com.apple.loginwindow.plist, LoginwindowText) does not exist, the system is not compliant.

*example:*

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.loginwindow.plist LoginwindowText  
  
Center for Internet Security Test Message
```

**or**

Run the following command to verify that a profile is installed that configures a login banner:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "LoginwindowText"
```

The output should include `LoginwindowText` set to your organization's required text.

*example:*

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "LoginwindowText"  
  
LoginwindowText = "This computer is configured to the  
CIS Benchmarks.";
```

## Remediation:

Perform the following to enable a login banner set to your organization's required text:

### *Terminal Method:*

Run the following command to enable a custom login screen message:

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow  
LoginwindowText "<custom.message>"
```







### *example:*

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow  
LoginwindowText "Center for Internet Security Test Message"
```

### *Profile Method:*

1. Create or edit a configuration profile with the PayloadType of `com.apple.loginwindow`
2. Add the key `LoginwindowText`
3. Set the key to `<Your organization's required text>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### *5.13 Create a Login window banner (Automated)*

**Profile Applicability:**

- Level 2

**Description:**

A Login window banner warning informs the user that the system is reserved for authorized use only. It enforces an acknowledgment by the user that they have been informed of the use policy in the banner if required. The system recognizes either the `.txt` and the `.rtf` formats.

**Rationale:**

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

**Impact:**

Users will have to click on the window with the Login text before logging into the computer.

## Audit:

Run the following command to verify the login window text:

```
$ sudo cat /Library/Security/PolicyBanner.*
```

If the output includes `no matches found: /Library/Security/PolicyBanner.*` the system is not compliant.

*example:*

```
$ sudo cat /Library/Security/PolicyBanner.txt
Center for Internet Security Test Message

$ sudo cat /Library/Security/PolicyBanner.rtf
{\rtf1\ansi\ansicpg1252\cocoartf1561\cocoasubrtf610
{\fonttbl\f0\fswiss\fcharset0 Helvetica;}
{\colortbl;\red255\green255\blue255;}
{\*\expandedcolortbl;;}
\margl1440\margr1440\vieww10800\viewh8400\viewkind0
\pard\tx566\tx1133\tx1700\tx2267\tx2834\tx3401\tx3968\tx4535\tx5102\tx5669\tx
6236\tx6803\pardirnatural\partightenfactor0

\f0\fs24 \cf0 Center for Internet Security Test Message}







$ sudo cat /Library/Security/PolicyBanner.*
{\rtf1\ansi\ansicpg1252\cocoartf1561\cocoasubrtf610
{\fonttbl\f0\fswiss\fcharset0 Helvetica;}
{\colortbl;\red255\green255\blue255;}
{\*\expandedcolortbl;;}
\margl1440\margr1440\vieww10800\viewh8400\viewkind0
\pard\tx566\tx1133\tx1700\tx2267\tx2834\tx3401\tx3968\tx4535\tx5102\tx5669\tx
6236\tx6803\pardirnatural\partightenfactor0

\f0\fs24 \cf0 Center for Internet Security Test Message}Center for Internet
Security Test Message
```

## Remediation:

Edit (or create) a `PolicyBanner.txt` or `PolicyBanner.rtf` file, in the `/Library/Security/` folder, to include the required login window banner text.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 5.14 Do not enter a password-related hint (Automated)

### Profile Applicability:

- Level 1

### Description:

Password hints help the user recall their passwords for various systems and/or accounts. In most cases, password hints are simple and closely related to the user's password.

### Rationale:

Password hints that are closely related to the user's password are a security vulnerability, especially in the social media age. Unauthorized users are more likely to guess a user's password if there is a password hint. The password hint is very susceptible to social engineering attacks and information exposure on social media networks.

### Audit:

Run the following command to verify that no users have a password hint:

```
$ sudo dscl . -list /Users hint
```

The output will list all users. If there are any text listed with the user, then the machine is not compliant.

*example:*

```
$ sudo dscl . -list /Users hint  
  
firstuser      passwordhint  
seconduser     passwordhint2  
thirduser  
fourthuser  
Guest
```

## Remediation:

Perform the following to remove a user's password hint:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select the Current User
4. Select Change Password
5. Change the password and ensure that no text is entered in the Password hint box

*Terminal Method:*

Run the following command to remove a user's password hint:

```
$ sudo dscl . -delete /Users/<username> hint
```

*example:*






```
$ sudo dscl . -delete /Users/firstuser hint
```

```
$ sudo dscl . -delete /Users/seconduser hint
```

## Additional Information:

Organizations might consider entering an organizational help desk phone number or other text (such as a warning to the user). A help desk number is only appropriate for organizations with trained help desk personnel that are validating user identities for password resets.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

## *5.15 Ensure Fast User Switching Is Disabled (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Fast user switching allows a person to quickly log in to the computer with a different account. While only a minimal security risk, when a second user is logged in, that user might be able to see what processes the first user is using, or possibly gain other information about the first user. In a large directory environment where it is difficult to limit log in access many valid users can login to other user's assigned computers.

### **Rationale:**

Fast user switching allows multiple users to run applications simultaneously at console. There can be information disclosed about processes running under a different user. Without a specific configuration to save data and log out users can have unsaved data running in a background session that is not obvious.

### **Impact:**

When support staff visits a user's computer console, they will not be able to log in to their own session if there is an active and locked session.



## Audit:

Perform the following to ensure that fast user switching is not enabled:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Login Options
4. Verify make sure the "Show fast user switching menu as..." is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Multiple Session Enabled` set to `False`

*Terminal Method:*

Run the following command to verify that fast user switching is disabled:

```
$ sudo /usr/bin/defaults read /Library/Preferences/.GlobalPreferences.plist
MultipleSessionEnabled
```

If the output is neither `0` or The domain/default pair of (/Library/Preferences/.GlobalPreferences.plist, MultipleSessionEnabled) does not exist, the computer is not compliant.

**or**

Run the following command to verify that a profile is installed that disables Fast User Switching:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep MultipleSessionEnabled

MultipleSessionEnabled = 0;
```

## Remediation:

Perform the following to disable fast user switching:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Login Options
4. Uncheck "Show fast user switching menu as..."

*Terminal Method:*

Run the following command to turn fast user switching off:

```
$ sudo /usr/bin/defaults write /Library/Preferences/.GlobalPreferences  
MultipleSessionEnabled -bool false
```







*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of .GlobalPreferences
2. Add the key MultipleSessionEnabled
3. Set the key to </false>

## Additional Information:

macOS is a multi-user operating system, and there are other similar methods that might provide the same kind of risk. The Remote Login service that can be turned on in the Sharing System Preferences pane is another.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## ***6 User Accounts and Environment***

Account management is a central part of security for any computer system including macOS. General practices should be followed to ensure that all accounts on a system are still needed and that default accounts have been removed. Users with admin roles should have distinct accounts for admin functions as well as day to day work where the passwords are different and known only by the user assigned to the account. Accounts with elevated privileges should not be easily discerned from the account name from standard accounts.

When any computer system is added to a directory system there are additional controls available including user account management that are not available in a standalone computer. One of the drawbacks is the local computer is no longer in control of the accounts that can access or manage it if given permission. For macOS, if the computer is connected to a directory, any standard user can now login to the computer at console which by default may be desirable or not depending on the use case. If an admin group is allowed to administer the local computer the membership of that group is controlled completely in the directory.

macOS computers connected to a directory should be configured so that the risk is appropriate for the mission use of the computer. Only those accounts that require local authentication should be allowed, and only required administrator accounts should be in the local administrator group. Authenticated users for console access and domain admins for administration may be too broad or too limited.

## ***6.1 Accounts Preferences Action Items***

Proper account management is critical to computer security. Many options and settings in the Account System Preference Pane can be used to increase the security of the Mac.

### ***6.1.1 Ensure Login Window Displays as Name and Password Is Enabled (Automated)***

#### **Profile Applicability:**

- Level 1

#### **Description:**

The login window prompts a user for his/her credentials, verifies their authorization level and then allows or denies the user access to the system.

#### **Rationale:**

Prompting the user to enter both their username and password makes it twice as hard for unauthorized users to gain access to the system since they must discover two attributes.

## Audit:

Perform the following to verify that the login window displays name and password:

*Graphical Method:*

1. Open System Preferences
2. Select Users and Groups
3. Select Login Options
4. Verify that Name and Password is set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Show Full Name` set to `True`

*Terminal Method:*

Run the following command to verify the login window displays name and password:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.loginwindow  
SHOWFULLNAME
```

```
1
```

**Note:** If the system returns `The domain/default pair of (/Library/Preferences/com.apple.loginwindow, SHOWFULLNAME) does not exist` then this setting was not initially set and may not have left an auditable artifact.

**or**

Run the following command to verify that a profile is installed that configures the login window to display as name and password:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep 'SHOWFULLNAME'  
  
SHOWFULLNAME = 1;
```

## Remediation:

Perform the following to ensure the login window display name and password:

*Graphical Method:*

1. Open System Preferences
2. Select Users and Groups
3. Select Login Options
4. Set Name and Password

*Terminal Method:*

Run the following command to enable the login window to display name and password:







```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow  
SHOWFULLNAME -bool true
```

**Note:** The GUI will not display the updated setting until the current user(s) logs out.

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.loginwindow
2. Add the key SHOWFULLNAME
3. Set the key to </true>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### *6.1.2 Ensure Show Password Hints Is Disabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Password hints are user-created text displayed when an incorrect password is used for an account.

**Rationale:**

Password hints make it easier for unauthorized persons to gain access to systems by providing information to anyone that the user provided to assist in remembering the password. This info could include the password itself or other information that might be readily discerned with basic knowledge of the end user.

**Impact:**

The user can set the hint to any value including the password itself or clues that allow trivial social engineering attacks.

## Audit:

Perform the following to verify if password hints are shown:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Login Options
4. Verify that Show password hints is not shown

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `Retires Before Hint Shown` is set to 0

*Terminal Method:*

Run the following command to verify that password hints are not displayed:

```
$ sudo /usr/bin/defaults read /Library/Preferences/com.apple.loginwindow  
RetriesUntilHint
```

If the output is either by 0 or The domain/default pair of (/Library/Preferences/com.apple.loginwindow, RetriesUntilHint) does not exist, then the system is compliant.

**or**

Run the following command to verify that a profile is installed that disables password hints shown on retries:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep 'RetriesUntilHint'  
  
RetriesUntilHint = 0;
```



## Remediation:

Perform the to disable password hints from being shown:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Login Options
4. Uncheck Show password hints

*Terminal Method:*







Run the following command to disable password hints:

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow  
RetriesUntilHint -int 0
```

*Profile Method:*

1. Create or edit a configuration profile with the PayLoadType of `com.apple.mobiledevice.passwordpolicy`
2. Add the key `RetriesUntilHint`
3. Set the key to `<integer>0</integer>`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### *6.1.3 Ensure Guest Account Is Disabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

The guest account allows users access to the system without having to create an account or password. Guest users are unable to make setting changes cannot remotely login to the system. All files, caches, and passwords created by the guest user are deleted upon logging out.

**Rationale:**

Disabling the guest account mitigates the risk of an untrusted user doing basic reconnaissance and possibly using privilege escalation attacks to take control of the system.

**Impact:**

A guest user can use that access to find out additional information about the system and might be able to use privilege escalation vulnerabilities to establish greater access.

## Audit:

Perform the following to ensure that the guest account is not available:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Guest User
4. Verify that Allow guests to log in to this computer is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `DisableGuestAccount` set to 1
4. Verify that the same installed profile has `EnableGuestAccount` set to 0

*Terminal Method:*

Run the following command to verify if the guest account is enabled:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/com.apple.loginwindow.plist GuestEnabled  
  
0
```

**or**

Run the following command to verify that the Guest account is disabled:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep 'DisableGuestAccount'  
  
        DisableGuestAccount = 1;  
  
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep 'DisableGuestAccount'  
  
        EnableGuestAccount = 0;
```

## Remediation:

Perform the following to disable guest account availability:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Guest User
4. Uncheck Allow guests to log in to this computer

*Terminal Method:*

Run the following command to disable the guest account:

```
$ sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow  
GuestEnabled -bool false
```

*Profile Method:*










1. Create or edit a configuration profile with the PayloadType of `com.apple.loginwindow`
2. Add the key `DisableGuestAccount`
3. Set the key to `</true>`
4. Add the key `EnableGuestAccount`
5. Set the key to `</false>`

## Additional Information:

By default, the guest account is enabled for access to sharing services but is not allowed to log in to the computer.

The guest account does not need a password when it is enabled to log in to the computer.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>5.2 Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v8	<b><u>6.2 Establish an Access Revoking Process</u></b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v8	<b><u>6.8 Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			
v7	<b><u>4.4 Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

#### *6.1.4 Ensure Guest Access to Shared Folders Is Disabled (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Allowing guests to connect to shared folders enables users to access selected shared folders and their contents from different computers on a network.

**Rationale:**

Not allowing guests to connect to shared folders mitigates the risk of an untrusted user doing basic reconnaissance and possibly use privilege escalation attacks to take control of the system.

**Impact:**

Unauthorized users could access shared files on the system.

## Audit:

Perform the following to ensure that guests cannot connect to shared folders:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Guest User
4. Verify that Allow guests to connect to shared folders is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `AllowGuestAccess = 0` is set

*Terminal Method:*

Run the following commands to verify that shared folders are not accessible to guest users:

```
$ sudo /usr/bin/defaults read  
/Library/Preferences/SystemConfiguration/com.apple.smb.server  
AllowGuestAccess  
  
0
```

The computer is also compliant if the command outputs The domain/default pair of (/Library/Preferences/SystemConfiguration/com.apple.smb.server, AllowGuestAccess) does not exist

**or**

Run the following command to verify that a profile is installed that disables the Guest account to connect to shared folders:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep AllowGuestAccess  
  
AllowGuestAccess = 0;
```

## Remediation:

Perform the following to no longer allow guest user access to shared folders:

*Graphical Method:*

1. Open System Preferences
2. Select Users & Groups
3. Select Guest User
4. Uncheck Allow guests to connect to shared folders

*Terminal Method:*

Run the following commands to verify that shared folders are not accessible to guest users:

```
$ sudo /usr/bin/defaults write  
/Library/Preferences/SystemConfiguration/com.apple.smb.server  
AllowGuestAccess -bool false
```







*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.smb.server
2. Add the key Forced
3. Set the key to the following:

```
<array>  
  <dict>  
    <key>mcx_preference_settings</key>  
    <dict>  
      <key>AllowGuestAccess</key>  
      <false/>  
    </dict>  
  </dict>  
</array>
```



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>3.3 Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b><u>14.6 Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 6.1.5 Remove Guest home folder (Automated)

#### Profile Applicability:

- Level 1

#### Description:

In the previous two controls the guest account login has been disabled and sharing to guests has been disabled as well. There is no need for the legacy Guest home folder to remain in the file system. When normal user accounts are removed you have the option to archive it, leave it in place or delete. In the case of the guest folder the folder remains in place without a GUI option to remove it. If at some point in the future a Guest account is needed it will be re-created. The presence of the Guest home folder can cause automated audits to fail when looking for compliant settings within all User folders as well. Rather than ignoring the folder's continued existence, it is best removed.

#### Rationale:

The Guest home folders are unneeded after the Guest account is disabled and could be used inappropriately.

#### Impact:

The Guest account should not be necessary after it is disabled, and it will be automatically re-created if the Guest account is re-enabled

#### Audit:

Run the following command to verify if the Guest user home folder exists:

```
$ sudo ls /Users/ | grep Guest
```







#### Remediation:

Run the following command to remove the Guest user home folder:

1. Run the following command in Terminal:

```
$ sudo rm -R /Users/Guest
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## *6.2 Ensure Show All Filename Extensions Setting is Enabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

A filename extension is a suffix added to a base filename that indicates the base filename's file format.

### **Rationale:**

Visible filename extensions allow the user to identify the file type and the application it is associated with which leads to quick identification of misrepresented malicious files.

### **Impact:**

The user of the system can open files of unknown or unexpected filetypes if the extension is not visible.

## Audit:

Perform the following to ensure that file extensions are shown:

*Graphical Method:*

1. Open Finder
2. Select Finder in the Menu Bar
3. Select Preferences
4. Select Advanced
5. Verify that Show all filename extensions is set

*Terminal Method:*

Run the following command to verify that displaying of file extensions is enabled:

```
$ sudo -u <username> /usr/bin/defaults read  
/Users/<username>/Library/Preferences/.GlobalPreferences.plist  
AppleShowAllExtensions  
1
```

*example:*

```
$ sudo -u firstuser /usr/bin/defaults read  
/Users/firstuser/Library/Preferences/.GlobalPreferences.plist  
AppleShowAllExtensions  
1  
  
$ sudo -u seconduser /usr/bin/defaults read  
/Users/secondname/Library/Preferences/.GlobalPreferences.plist  
AppleShowAllExtensions  
  
The domain/default pair of  
(/Users/secondname/Library/Preferences/.GlobalPreferences.plist,  
AppleShowAllExtensions) does not exist
```

## Remediation:

Perform the following to ensure file extensions are shown:

*Graphical Method:*

1. Open Finder
2. Select Finder in the Menu Bar
3. Select Preferences
4. Select Advanced
5. Set Show all filename extensions

*Terminal Method:*







Run the following command to enable displaying of file extensions:

```
$ sudo -u <username> /usr/bin/defaults write  
/Users/<username>/Library/Preferences/.GlobalPreferences.plist  
AppleShowAllExtensions -bool true
```

*example:*

```
$ sudo -u seconduser /usr/bin/defaults write  
/Users/secondname/Library/Preferences/.GlobalPreferences.plist  
AppleShowAllExtensions -bool true
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.3 <u>Address Unauthorized Software</u></b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

## *6.3 Ensure Automatic Opening of Safe Files in Safari Is Disabled (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Safari will automatically run or execute what it considers safe files. This can include installers and other files that execute on the operating system. Safari evaluates file safety by using a list of filetypes maintained by Apple. The list of files include text, image, video and archive formats that would be run in the context of the OS rather than the browser.

### **Rationale:**

Hackers have taken advantage of this setting via drive-by attacks. These attacks occur when a user visits a legitimate website that has been corrupted. The user unknowingly downloads a malicious file either by closing an infected pop-up or hovering over a malicious banner. An attacker can create a malicious file that will fall within Safari's safe file list that will download and execute without user input.

### **Impact:**

Apple considers many files that the operating system itself auto-executes as "safe files." Many of these files could be malicious and could execute locally without the user even knowing that a file of a specific type had been downloaded.

## Audit:

Perform the following to verify that safe files are not opened on download in Safari:

*Graphical Method:*

1. Open Safari
2. Select Safari from the menu bar
3. Select Preferences
4. Select General
5. Verify that Open "safe" files after downloading is not set

**or**

1. Open System Preferences
2. Select Profiles
3. Verify that an installed profile has `AutoOpenSafeDownloads = 0` is set

*Terminal Method:*

Run the following command to verify that opening safe files in Safari is disabled:

```
$ sudo -u <username> /usr/bin/defaults read  
/Users/<username>/Library/Containers/com.apple.Safari/Data/Library/Preference  
s/com.apple.Safari AutoOpenSafeDownloads  
  
0
```

*example:*

```
$ sudo -u firstuser /usr/bin/defaults read  
/Users/firstuser/Library/Containers/com.apple.Safari/Data/Library/Preferences  
/com.apple.Safari AutoOpenSafeDownloads  
  
0
```

**Note:** To run the Terminal commands, Terminal must be granted Full Disk Access in the Security & Privacy pane in System Preferences.

**or**

Run the following command to verify that a profile is installed that disables safe files from opening in Safari:

```
$ sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep AutoOpenSafeDownloads  
  
AutoOpenSafeDownloads = 0;
```



## Remediation:

Perform the following to set safe files to not open after downloading in Safari:

*Graphical Method:*

1. Open Safari
2. Select Safari from the menu bar
3. Select Preferences
4. Select General
5. Uncheck Open "safe" files after downloading

*Terminal Method:*

Run the following command to disable safe files from not opening in Safari:

```
$ sudo -u <username> /usr/bin/defaults write  
/Users/<username>/Library/Containers/com.apple.Safari/Data/Library/Preference  
s/com.apple.Safari AutoOpenSafeDownloads -bool false
```

*example:*

```
$ sudo -u firstuser /usr/bin/defaults write  
/Users/firstuser/Library/Containers/com.apple.Safari/Data/Library/Preferences  
/com.apple.Safari AutoOpenSafeDownloads -bool false
```




**Note:** To run the Terminal commands, Terminal must be granted Full Disk Access in the Security & Privacy pane in System Preferences.

*Profile Method:*

1. Create or edit a configuration profile with the PayloadType of com.apple.Safari
2. Add the key Forced
3. Set the key to the following:

```
<array>  
  <dict>  
    <key>mcx_preference_settings</key>  
    <dict>  
      <key>AutoOpenSafeDownloads</key>  
      <false/>  
    </dict>  
  </dict>  
</array>
```

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>9 Email and Web Browser Protections</u></b> Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.			
v7	<b><u>8.5 Configure Devices Not To Auto-run Content</u></b> Configure devices to not auto-run content from removable media.			

## ***7 Appendix: Additional Considerations***

This section is for guidance on topics for which the Benchmark does not include a prescribed state, and for security controls that were previously represented in macOS security guides.

## 7.1 Extensible Firmware Interface (EFI) password (Manual)

### Profile Applicability:

- Level 2

### Description:

EFI is the software link between the motherboard hardware and the software operating system. EFI determines which partition or disk to load macOS from, and it also determines whether the user can enter single user mode. The main reasons to set a firmware password have been protections against an alternative boot disk, protection against a passwordless root shell through single user mode and protection against firewire DMA attacks. While it was easier in the past to reset the firmware password by removing RAM, it did make tampering slightly harder because having to remove RAM remediated memory scraping attacks through DMA. It has always been difficult to manage the firmware password on macOS computers, though some tools did make it much easier.

Apple patched OS X in 10.7 to mitigate the DMA attacks, and the use of FileVault 2 Full-Disk Encryption mitigates the risk of damage to the boot volume if an unauthorized user uses a different boot volume or uses single user mode. Apple's reliance on the recovery partition and the additional features it provides make controls that do not allow the user to boot into the recovery partition less attractive.

Starting in late 2010 with the MacBook Air Apple has slowly updated the requirements to recover from a lost firmware password. Apple only supports taking the computer to an Apple authorized service provider. This change makes managing the firmware password effectively more critical if it is used.

Setting the firmware password may be a good practice in some environments. We cannot recommend it as a standard security practice at this time.

<http://support.apple.com/kb/ts3554>

<https://jamfnation.jamfsoftware.com/article.html?id=58>

<http://derflounder.wordpress.com/2012/02/05/protecting-yourself-against-firewire-dma-attacks-on-10-7-x/>

<http://derflounder.wordpress.com/2013/04/26/booting-into-single-user-mode-on-a-filevault-2-encrypted-mac/>

**Impact:**

In environments where strict processes are mandated for change control, allowing the user to boot to recovery and possibly change configurations on the boot volume will be unacceptable. The risk analysis for this control is that the user of the computer already has login rights, decryption rights, and access to user data. In most known use cases device management controls will be sufficient to mitigate and discover insider threat control circumvention. Some organizations will not accept the risk of even temporary control changes on devices and may need set an EFI password to block unauthorized changes even from trusted insiders.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2 <u>Inventory and Control of Software Assets</u></b> Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.			
v7	<b>2 <u>Inventory and Control of Software Assets</u></b> Inventory and Control of Software Assets			

## 7.2 FileVault and Local Account Password Reset using AppleID (Manual)

### Profile Applicability:

- Level 2

### Description:

Apple has provided services for several years that allowed a user to reset a local account password on a computer using their Apple ID and a service to store the FileVault Master Password with Apple that would be controlled by access to an Apple ID. These distinct services have been more cleanly integrated starting in 10.12.

This integrated service for password and decryption is a concern in enterprise environments. Normal enterprise management controls mitigate the risk of external control of organizational systems. The user of the system already has the ability to unlock the disk in order to log in and use it and some form of password recovery function is likely already in place for any approved accounts. In addition:

- You cannot reset anything but a local account
- You need physical access to the computer on a network that can phone home to Apple
- Enterprise FileVault management precludes the use of Apple's personal encryption recovery tied to a User's Apple ID
- The current login keychain will have to be discarded unless the user remembers the old password

This service allows for organizational computer users to utilize AppleIDs for encryption key escrow and user account management. The use of Apple's services rather than enterprise services may be considered inappropriate.

<https://support.apple.com/en-us/HT204837>

### References:

1. <https://support.apple.com/en-us/HT211672>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>16 <u>Account Monitoring and Control</u></b> Account Monitoring and Control			

# Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
<b>1</b>	<b>Install Updates, Patches and Additional Security Software</b>		
1.1	Verify all Apple-provided software is current (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure Auto Update Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure Download New Updates When Available is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Installation of App Update Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure System Data Files and Security Updates Are Downloaded Automatically Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure Install of macOS Updates Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Audit Computer Name (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>System Preferences</b>		
<b>2.1</b>	<b>Bluetooth</b>		
2.1.1	Turn off Bluetooth, if no paired devices exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure Show Bluetooth Status in Menu Bar Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.2</b>	<b>Date &amp; Time</b>		
2.2.1	Ensure "Set time and date automatically" Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure time set is within appropriate limits (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.3</b>	<b>Desktop &amp; Screen Saver</b>		
2.3.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure Screen Saver Corners Are Secure (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Audit Lock Screen and Start Screen Saver Tools (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.4</b>	<b>Sharing</b>		
2.4.1	Ensure Remote Apple Events Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure Internet Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure Screen Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Ensure Printer Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure Remote Login Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Ensure DVD or CD Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Ensure Bluetooth Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Ensure File Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Ensure Remote Management Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure Content Caching Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>



2.4.11	Ensure AirDrop Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure Media Sharing Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.5</b>	<b>Security &amp; Privacy</b>		
<b>2.5.1</b>	<b>Encryption</b>		
2.5.1.1	Ensure FileVault Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1.2	Ensure all user storage APFS volumes are encrypted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1.3	Ensure all user storage CoreStorage volumes are encrypted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.5.2</b>	<b>Firewall</b>		
2.5.2.1	Ensure Gatekeeper is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2.2	Ensure Firewall Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2.3	Ensure Firewall Stealth Mode Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure Location Services Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.4	Audit Location Services Access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.5	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.6	Ensure Limit Ad Tracking Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.7	Audit Camera Privacy and Confidentiality (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.6</b>	<b>Apple ID</b>		
<b>2.6.1</b>	<b>iCloud</b>		
2.6.1.1	Audit iCloud Configuration (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1.2	Audit iCloud Keychain (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1.3	Audit iCloud Drive (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1.4	Ensure iCloud Drive Document and Desktop Sync is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Audit App Store Password Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.7</b>	<b>Time Machine</b>		
2.7.1	Ensure Backup Up Automatically is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure Time Machine Volumes Are Encrypted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure Wake for Network Access Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure Power Nap Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure Secure Keyboard Entry terminal.app is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.11	Ensure EFI Version Is Valid and Checked Regularly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Audit Automatic Actions for Optical Media (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Audit Siri Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Audit Sidecar Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Audit Touch ID and Wallet & Apple Pay Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Audit Notification System Preference Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Logging and Auditing</b>		
3.1	Ensure Security Auditing Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.2	Ensure Security Auditing Flags Are Configured Per Local Organizational Requirements (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure Security Auditing Retention Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure Access to Audit Records Is Controlled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure Firewall Logging Is Enabled and Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Audit Software Inventory (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Network Configurations</b>		
4.1	Ensure Bonjour Advertising Services Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure Show Wi-Fi status in Menu Bar Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Audit Network Specific Locations (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure HTTP Server Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure NFS Server Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Audit Wi-Fi Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5</b>	<b>System Access, Authentication and Authorization</b>		
<b>5.1</b>	<b>File System Permissions and Access Controls</b>		
5.1.1	Ensure Home Folders Are Secure (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure System Integrity Protection Status (SIPS) Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure Apple Mobile File Integrity Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure Library Validation Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure Sealed System Volume (SSV) Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure No World Writable Files Exist in the System Folder (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure No World Writable Files Exist in the Library Folder (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.2</b>	<b>Password Management</b>		
5.2.1	Ensure Password Account Lockout Threshold Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure Password Minimum Length Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

5.2.5	Ensure Complex Password Must Contain Special Character Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure Password Age Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure Password History Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	Ensure the Sudo Timeout Period Is Set to Zero (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	Ensure login keychain is locked when the computer sleeps (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure the "root" Account Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure Automatic Login Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure a Password is Required to Wake the Computer From Sleep or Screen Saver Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure system is set to hibernate (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.10	Require an administrator password to access system-wide preferences (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure an administrator account cannot login to another user's active and locked session (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure a Custom Message for the Login Screen Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Create a Login window banner (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.14	Do not enter a password-related hint (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.15	Ensure Fast User Switching Is Disabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6</b>	<b>User Accounts and Environment</b>		
<b>6.1</b>	<b>Accounts Preferences Action Items</b>		
6.1.1	Ensure Login Window Displays as Name and Password Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure Show Password Hints Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure Guest Account Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure Guest Access to Shared Folders Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Remove Guest home folder (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure Show All Filename Extensions Setting is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure Automatic Opening of Safe Files in Safari Is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>7</b>	<b>Appendix: Additional Considerations</b>		
7.1	Extensible Firmware Interface (EFI) password (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	FileVault and Local Account Password Reset using AppleID (Manual)	<input type="checkbox"/>	<input type="checkbox"/>



# Appendix: Change History

Date	Version	Changes for this version
Apr 6, 2020	1.0.0	Initial Release
Oct 14, 2020	1.1.0	1.1 - Updated Description, Audit, and Remediation
Oct 14, 2020	1.1.0	1.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	1.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	1.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	1.5 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.1.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.1.2 – Removed Previous Recommendation; Formerly 2.1.3; Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.1.3 – Moved to 2.1.2
Oct 14, 2020	1.1.0	2.2.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.2.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.3.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.3.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.3.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.1 - Updated Audit and Remediation

Oct 14, 2020	1.1.0	2.4.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.5 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.6 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.7 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.8 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.9 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.4.10 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.1.1 - Updated Description, Audit, and Remediation
Oct 14, 2020	1.1.0	2.5.1.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.1.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.3 - Updated Audit and Remediation

Oct 14, 2020	1.1.0	2.5.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.5 - Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	2.5.6 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.7 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.8 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.5.9 – Added Recommendation
Oct 14, 2020	1.1.0	2.6.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.6.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.6.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.6.4 - Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	2.7.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.7.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	2.8 - Updated Title, Description, Audit, and Remediation; Formerly 2.12
Oct 14, 2020	1.1.0	2.9 – Added Recommendation
Oct 14, 2020	1.1.0	2.10 - Updated Audit and Remediation; Formerly 2.9

Oct 14, 2020	1.1.0	2.11 - Updated Audit and Remediation; Formerly 2.10
Oct 14, 2020	1.1.0	2.12 - Formerly 2.11
Oct 14, 2020	1.1.0	3.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	3.2 - Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	3.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	3.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	3.5 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	3.6 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	4.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	4.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	4.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	4.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	4.5 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.1.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.1.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.1.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.1.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.2 - Updated Audit and Remediation



Oct 14, 2020	1.1.0	5.2.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.5 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.6 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.7 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.2.8 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.3 - Updated Audit, Remediation, and Additional Information
Oct 14, 2020	1.1.0	5.4 – Formerly 5.5; Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	5.5 - Formerly 5.4; Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.6 - Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	5.7 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.8 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.9 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.10 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.11 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.12 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.13 - Updated Audit and Remediation

Oct 14, 2020	1.1.0	5.14 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.15 - Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	5.16 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.17 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.18 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	5.19 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.1.1 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.1.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.1.3 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.1.4 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.1.5 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.2 - Updated Audit and Remediation
Oct 14, 2020	1.1.0	6.3 - Updated Audit and Remediation; Switched to Manual
Oct 14, 2020	1.1.0	6.4 – Removed Previous Recommendation
Oct 14, 2020	1.1.0	7.4 – Updated Description
Oct 14, 2020	1.1.0	7.6 – Added Audit and Remediation
Oct 14, 2020	1.1.0	7.12 - Added Audit and Remediation
Oct 14, 2020	1.1.0	7.16 - Added Rationale, Audit, and Remediation

Nov 11, 2020	1.1.0	First Revision Released
Mar 1, 2021	1.2.0	1.1 – Description Updated
Mar 1, 2021	1.2.0	1.2 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	1.3 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	1.4 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	1.5 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	1.6 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	1.7 – Moved from 7.3, Updated Rationale, Description, Audit, and Remediation
Mar 1, 2021	1.2.0	2.3.3 – Updated Rationale
Mar 1, 2021	1.2.0	2.4.3 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	2.4.4 – Updated Audit
Mar 1, 2021	1.2.0	2.4.6 – Updated Impact Statement, Description, Audit, and Remediation
Mar 1, 2021	1.2.0	2.4.7 – Updated Audit
Mar 1, 2021	1.2.0	2.4.8 – Updated Audit
Mar 1, 2021	1.2.0	2.4.10 – Updated Description
Mar 1, 2021	1.2.0	2.5.2 – Subsection Created
Mar 1, 2021	1.2.0	2.5.2.1 – Moved from 2.5.2, Updated Audit and Remediation
Mar 1, 2021	1.2.0	2.5.2.2 – Moved from 2.5.3, Updated Notes, References
Mar 1, 2021	1.2.0	2.5.2.3 – Moved from 2.5.4

Mar 1, 2021	1.2.0	2.5.3 – Moved from 2.5.6, Updated Description, Audit, and Remediation
Mar 1, 2021	1.2.0	2.5.3 – Moved from 2.5.6
Mar 1, 2021	1.2.0	2.5.4 – Moved from 2.5.7, Updated Description
Mar 1, 2021	1.2.0	2.5.5 – Moved from 2.5.8
Mar 1, 2021	1.2.0	2.5.6 – Moved from 2.5.9, Updated Title, Impact Statement, Description, Audit, and Remediation
Mar 1, 2021	1.2.0	2.5.7 – Moved from 7.2, Updated Title, Description, Rationale, Audit, and Remediation
Mar 1, 2021	1.2.0	2.6 – Updated Overview
Mar 1, 2021	1.2.0	2.6.1 – Updated Impact Statement and Description
Mar 1, 2021	1.2.0	2.6.4 – Updated Title, Audit, and Remediation
Mar 1, 2021	1.2.0	2.7.2 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	2.8 – Updated Description
Mar 1, 2021	1.2.0	2.9 - Updated, Description, Rationale, Audit, and Remediation
Mar 1, 2021	1.2.0	2.11 – Removed Previous Recommendation, Moved from 2.12, Updated Description
Mar 1, 2021	1.2.0	2.12 – Moved from 7.6, Updated Title
Mar 1, 2021	1.2.0	2.13 – Moved from 7.12, Updated Title, Audit, and Remediation

Mar 1, 2021	1.2.0	3.2 – Updated Rationale, Audit, Remediation, and Notes
Mar 1, 2021	1.2.0	3.5 – Updated Rationale, Audit, and Remediation
Mar 1, 2021	1.2.0	3.6 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	3.7 – Moved from 7.3, Updated Description, Audit, Remediation, and Notes
Mar 1, 2021	1.2.0	4.1 – Updated Audit
Mar 1, 2021	1.2.0	4.3 – Updated Description and Impact Statement
Mar 1, 2021	1.2.0	4.4 – Updated Audit and Remediation
Mar 1, 2021	1.2.0	4.5 – Updated Description, Audit, and Remediation
Mar 1, 2021	1.2.0	4.6 – Moved from 7.1, Updated Description, Rationale, Audit, and Remediation
Mar 1, 2021	1.2.0	5.1.2 - Updated Impact Statement and Description
Mar 1, 2021	1.2.0	5.2.1 - Updated Impact Statement, Remediation, and References
Mar 1, 2021	1.2.0	5.2.2 – Updated Remediation
Mar 1, 2021	1.2.0	5.2.3 – Updated Remediation
Mar 1, 2021	1.2.0	5.2.4 – Updated Remediation
Mar 1, 2021	1.2.0	5.2.5 – Updated Remediation
Mar 1, 2021	1.2.0	5.2.6 – Updated Remediation
Mar 1, 2021	1.2.0	5.2.7 – Updated Remediation

Mar 1, 2021	1.2.0	5.2.8 – Updated Remediation
Mar 1, 2021	1.2.0	5.3 - Updated Impact Statement and Description
Mar 1, 2021	1.2.0	5.5 – Updated Rationale Statement
Mar 1, 2021	1.2.0	5.6 – Updated Description
Mar 1, 2021	1.2.0	5.7 – Updated Description, Audit, and Remediation
Mar 1, 2021	1.2.0	5.8 – Updated Impact Statement, Audit, and Remediation
Mar 1, 2021	1.2.0	5.9 – Updated Description
Mar 1, 2021	1.2.0	5.10 - Updated Description, Audit, Remediation, and Notes
Mar 1, 2021	1.2.0	5.12 - Updated Tile, Audit, Remediation, and References
Mar 1, 2021	1.2.0	5.13 – Updated Impact Statement
Mar 1, 2021	1.2.0	5.14 – Updated Audit
Mar 1, 2021	1.2.0	5.16 – Updated Impact Statement
Mar 1, 2021	1.2.0	5.17 –Description
Mar 1, 2021	1.2.0	5.18 – Removed Previous Recommendation, Moved from 5.19, Updated Description
Mar 1, 2021	1.2.0	5.19 – Added Recommendation
Mar 1, 2021	1.2.0	6.1.2 – Updated Rationale Statement
Mar 1, 2021	1.2.0	6.2 – Updated Rationale Statement
Mar 1, 2021	1.2.0	7.1 – Moved from 7.8
Mar 1, 2021	1.2.0	7.2 – Moved from 7.9

Mar 1, 2021	1.2.0	7.3 – Moved from 7.10
Mar 1, 2021	1.2.0	7.4 – Moved from 7.11
Mar 1, 2021	1.2.0	7.5 – Removed Previous Recommendation, Moved from 7.13
Mar 1, 2021	1.2.0	7.6 – Moved from 7.14
Mar 1, 2021	1.2.0	7.7 – Moved from 7.15
Mar 1, 2021	1.2.0	7.8 – Moved from 7.16
Mar 1, 2021	1.2.0	7.9 – Moved from 7.17
Mar 1, 2021	1.2.0	7.10 – Moved from 7.18
Mar 1, 2021	1.2.0	7.11 – Moved from 7.19
Mar 1, 2021	1.2.0	Second Iteration Released
Mar 11, 2021	1.3.0	2.4.7 – Moved to Manual from Automated
Mar 12, 2021	1.3.0	Third Iteration Released
May 30, 2021	1.4.0	1.1 – Grammatical Updates
May 30, 2021	1.4.0	1.3 – Grammatical Updates
May 30, 2021	1.4.0	1.4 – Grammatical Updates
May 30, 2021	1.4.0	1.5 – Grammatical Updates
May 30, 2021	1.4.0	1.6 – Grammatical Updates
May 30, 2021	1.4.0	1.7 – Grammatical Updates
May 30, 2021	1.4.0	2.1.1 – Grammatical Updates
May 30, 2021	1.4.0	2.1.2 – Grammatical Updates
May 30, 2021	1.4.0	2.2.2 – Grammatical Updates
May 30, 2021	1.4.0	2.3.1 – Grammatical Updates

May 30, 2021	1.4.0	2.3.2 – Grammatical Updates
May 30, 2021	1.4.0	2.4.2 – Grammatical Updates, Updated Audit
May 30, 2021	1.4.0	2.4.3 – Grammatical Updates, Updated Audit
May 30, 2021	1.4.0	2.4.4 – Grammatical Updates
May 30, 2021	1.4.0	2.4.5 – Grammatical Updates
May 30, 2021	1.4.0	2.4.7 – Grammatical Updates, Updated Audit, Remediation, and Switched from Manual to Automatic
May 30, 2021	1.4.0	2.4.8 – Grammatical Updates
May 30, 2021	1.4.0	2.4.9 – Grammatical Updates
May 30, 2021	1.4.0	2.4.10 – Grammatical Updates
May 30, 2021	1.4.0	2.4.11 – Grammatical Updates
May 30, 2021	1.4.0	2.4.12 – Moved from 7.8
May 30, 2021	1.4.0	2.5.1 – Grammatical Updates
May 30, 2021	1.4.0	2.5.1.1 – Grammatical Updates
May 30, 2021	1.4.0	2.5.1.2 – Grammatical Updates
May 30, 2021	1.4.0	2.5.2 – Grammatical Updates
May 30, 2021	1.4.0	2.5.2.1 – Grammatical Updates
May 30, 2021	1.4.0	2.5.2.2 – Grammatical Updates
May 30, 2021	1.4.0	2.5.3 – Grammatical Updates
May 30, 2021	1.4.0	2.5.4 – Grammatical Updates
May 30, 2021	1.4.0	2.5.5 – Grammatical Updates
May 30, 2021	1.4.0	2.5.6 – Grammatical Updates



May 30, 2021	1.4.0	2.5.7 – Grammatical Updates
May 30, 2021	1.4.0	2.6.1 – Grammatical Updates
May 30, 2021	1.4.0	2.6.2 – Grammatical Updates
May 30, 2021	1.4.0	2.6.4 – Grammatical Updates
May 30, 2021	1.4.0	2.7 – Grammatical Updates
May 30, 2021	1.4.0	2.7.1 – Grammatical Updates
May 30, 2021	1.4.0	2.7.2 – Grammatical Updates
May 30, 2021	1.4.0	2.8 – Grammatical Updates
May 30, 2021	1.4.0	2.9 – Grammatical Updates
May 30, 2021	1.4.0	2.10 – Grammatical Updates
May 30, 2021	1.4.0	2.11 – Grammatical Updates
May 30, 2021	1.4.0	2.12 – Grammatical Updates
May 30, 2021	1.4.0	2.13 – Grammatical Updates
May 30, 2021	1.4.0	2.14 – Grammatical Updates, Moved from 7.10
May 30, 2021	1.4.0	3 – Grammatical Updates, Updated Overview
May 30, 2021	1.4.0	3.2 – Grammatical Updates
May 30, 2021	1.4.0	3.3 – Grammatical Updates
May 30, 2021	1.4.0	3.4 – Grammatical Updates
May 30, 2021	1.4.0	3.5 – Grammatical Updates
May 30, 2021	1.4.0	3.6 – Grammatical Updates
May 30, 2021	1.4.0	3.7 – Grammatical Updates
May 30, 2021	1.4.0	4.1 – Grammatical Updates

May 30, 2021	1.4.0	4.2 – Grammatical Updates
May 30, 2021	1.4.0	4.3 – Grammatical Updates
May 30, 2021	1.4.0	4.4 – Grammatical Updates
May 30, 2021	1.4.0	4.5 – Grammatical Updates
May 30, 2021	1.4.0	4.6 – Grammatical Updates
May 30, 2021	1.4.0	5.1.1 – Grammatical Updates
May 30, 2021	1.4.0	5.1.2 – Grammatical Updates
May 30, 2021	1.4.0	5.1.3 – Grammatical Updates
May 30, 2021	1.4.0	5.1.4 – Grammatical Updates
May 30, 2021	1.4.0	5.2.1 – Grammatical Updates
May 30, 2021	1.4.0	5.2.2 – Grammatical Updates
May 30, 2021	1.4.0	5.2.5 – Grammatical Updates
May 30, 2021	1.4.0	5.2.6 – Grammatical Updates
May 30, 2021	1.4.0	5.2.7 – Grammatical Updates
May 30, 2021	1.4.0	5.2.8 – Grammatical Updates
May 30, 2021	1.4.0	5.3 – Grammatical Updates
May 30, 2021	1.4.0	5.4 – Grammatical Updates
May 30, 2021	1.4.0	5.5 – Grammatical Updates
May 30, 2021	1.4.0	5.6 – Grammatical Updates
May 30, 2021	1.4.0	5.7 – Grammatical Updates
May 30, 2021	1.4.0	5.8 – Grammatical Updates
May 30, 2021	1.4.0	5.9 – Grammatical Updates
May 30, 2021	1.4.0	5.10 – Grammatical Updates

May 30, 2021	1.4.0	5.11 – Grammatical Updates
May 30, 2021	1.4.0	5.12 – Grammatical Updates
May 30, 2021	1.4.0	5.13 – Grammatical Updates
May 30, 2021	1.4.0	5.14 – Grammatical Updates
May 30, 2021	1.4.0	5.15 – Grammatical Updates
May 30, 2021	1.4.0	5.16 – Grammatical Updates
May 30, 2021	1.4.0	5.17 – Grammatical Updates
May 30, 2021	1.4.0	5.18 – Grammatical Updates
May 30, 2021	1.4.0	5.19 – Grammatical Updates
May 30, 2021	1.4.0	5.20 – Grammatical Updates, Updated Audit and Remediation
May 30, 2021	1.4.0	6.1.1 – Grammatical Updates
May 30, 2021	1.4.0	6.1.2 – Grammatical Updates
May 30, 2021	1.4.0	6.1.3 – Grammatical Updates
May 30, 2021	1.4.0	6.1.5 – Grammatical Updates
May 30, 2021	1.4.0	6.3 - Grammatical Updates, Updated Audit, Remediation, and Switched from Manual to Automatic
May 30, 2021	1.4.0	7.3 – Previous Recommendation Removed, Moved from 7.4
May 30, 2021	1.4.0	7.4 – Moved from 7.5
May 30, 2021	1.4.0	7.5 – Moved from 7.6
May 30, 2021	1.4.0	7.6 – Previous Recommendation Removed, Moved from 7.9

May 30, 2021	1.4.0	7.7 – Previous Recommendation Removed, Added to Section 3 Overview
May 30, 2021	1.4.0	7.8 –Moved to 2.4.12
May 30, 2021	1.4.0	7.9 –Moved to 7.6
May 30, 2021	1.4.0	7.10 –Moved to 2.14
May 30, 2021	1.4.0	7.11 – Previous Recommendation Removed
	2.0.0	Initial Draft Release
Oct 28, 2021	2.0.0	6.2 – Updated Title
Nov 1, 2021	2.0.0	Initial Release