Example Benchmark

Full Report - CIS Level 2

---

macOS 26 (Tahoe) • 2026-08-09

John Doe, Example Organization

Generated by M.A.C.E.

Table of Contents

Foreword

The macOS Security Compliance Project is an open source effort to provide a programmatic approach to generating security guidance. The configuration settings in this document were derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5.

This project can be used as a resource to easily create customized security baselines of technical security controls by leveraging a library of atomic actions which are mapped to the compliance requirements defined in NIST SP 800-53 (Rev. 5). It can also be used to develop customized guidance to meet the particular cybersecurity needs of any organization.

The objective of this effort was to simplify and radically accelerate the process of producing up-to-date macOS security guidance that is also accessible to any organization and tailorable to meet each organization's specific security needs.

Any and all risk based decisions to tailor the content produced by this project in order to meet the needs of a specific organization shall be approved by the responsible Information System Owner (ISO) and Authorizing Official (AO) and formally documented in their System Security Plan (SSP). While the project attempts to provide settings to meet compliance requirements, it is recommended that each rule be reviewed by your organization's Information System Security Officer (ISSO) prior to implementation.

Scope

This document provides configuration guidance for macOS based on the CIS Level 2 security baseline. The guidance applies to the operating system version specified and may need adjustment for different versions or environments.

117	116	0	6
Total Rules	Configurable	Manual Review	Sections

Authors

Name	Organization
Bob Gendler	National Institute of Standards and Technology
Dan Brodjieski	National Aeronautics and Space Administration
Allen Golbig	Jamf
Edward Byrd	Center for Internet Security
John Doe	Example Organization

Acronyms and Definitions

Acronyms and Abbreviations

Acronym	Definition
ABM	Apple Business Manager
AES	Advanced Encryption Standard
AFP	Apple Filing Protocol
ALF	Application Layer Firewall
AO	Authorizing Official
API	Application Programming Interface
ARD	Apple Remote Desktop
CA	Certificate Authority
CIS	Center for Internet Security
CMMC	Cybersecurity Maturity Model Certification
CNSSI	Committee on National Security Systems
CRL	Certificate Revocation List
DDM	Declarative Device Management
DISA	Defense Information Systems Agency
DMA	Direct Memory Access
FISMA	Federal Information Security Modernization Act
FPKI	Federal Public Key Infrastructure
ISO	Information System Owner
ISSO	Information System Security Officer
MDM	Mobile Device Management
NFS	Network File System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
ODV	Organization Defined Values
OS	Operating System
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SIP	System Integrity Protection
SMB	Server Message Block
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide
UAMDM	User Approved MDM

Definitions

Term	Definition
Baseline	A baseline is a predefined set of controls (also referred to as "a catalog" of settings) that address the protection needs of an organization's information systems. A baseline serves as a starting point for the creation of security benchmarks.
Benchmark	Benchmarks are a defined list of settings with values that an organization has defined.

Applicable Documents

Government Documents

National Institute of Standards and Technology (NIST)

Document	Title
NIST SP 800-53 Rev 5	NIST Special Publication 800-53 Rev 5.1.1
NIST SP 800-63	NIST Special Publication 800-63
NIST SP 800-171	NIST Special Publication 800-171 Rev 3
NIST SP 800-219	NIST Special Publication 800-219 Rev 1

Non-Government Documents

Apple

Document	Title
Apple Platform Security Guide	Apple Platform Security
Apple Platform Deployment	Apple Platform Deployment
Apple Platform Certifications	Apple Platform Certifications
Profile-Specific Payload Keys	Profile-Specific Payload Keys

Center for Internet Security

Document	Title
CIS Apple macOS Benchmarks	CIS Apple macOS Benchmarks

Section Summary

Section	Total	Config.	Manual	Supp.
iCloud	1	1	0	0
Operating System	42	42	0	0
Password Policy	8	8	0	0
Supplemental	1	0	0	1
Audit	21	21	0	0
System Settings	44	44	0	0
Total	**117**	**116**	**0**	**1**

7. iCloud

This section contains the configuration and enforcement of iCloud and the Apple ID service settings.

Note: The check/fix commands outlined in this section *MUST* be run by a user with with elevated privileges.

7.1 Disable iCloud Desktop and Document Folder Sync

`icloud_sync_disable`

DISCUSSION

The macOS system's ability to automatically synchronize a user's desktop and documents folder to their iCloud Drive *MUST* be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated file synchronization *MUST* be controlled by an organization approved service.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowCloudDesktopAndDocuments: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-20(1), CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-002150
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.1.1.3 (level 2)
CIS Controls v8	4.1, 4.8, 15.3
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95153-3

8. Operating System

This section contains the configuration and enforcement of operating system settings.

8.1 Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled

`os_safari_warn_fraudulent_website_enable`

DISCUSSION

Warn when visiting a fraudulent website *MUST* be enabled in Safari.

CONFIGURATION PROFILE

```
- PayloadContent:
  - WarnAboutFraudulentWebsites: true
  PayloadType: com.apple.Safari
```

REFERENCES

Framework	Values
CIS Benchmark	6.3.3 (level 1)
CIS Controls v8	9.1, 9.3
CCE	CCE-95289-5

8.2 Disable Power Nap

`os_power_nap_disable`

DISCUSSION

Power Nap *MUST* be disabled.

Note: Power Nap allows your Mac to perform actions while a Mac is asleep. This can interfere with USB power and may cause devices such as smartcards to stop functioning until a reboot and must therefore be disabled on all applicable systems.

The following Macs support Power Nap:

MacBook (Early 2015 and later) MacBook Air (Late 2010 and later) **MacBook Pro (all models with Retina display)** Mac mini (Late 2012 and later) **iMac (Late 2012 and later)** Mac Pro (Late 2013 and later)

REMEDIATION

```
/usr/bin/pmset -a powernap 0
```

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1)
800-171r3	03.04.06
CIS Benchmark	2.10.2 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	CM.L2-3.4.6, CM.L2-3.4.7

CCE	CCE-95260-6

8.3 Disable Root Login

`os_root_disable`

DISCUSSION

To assure individual accountability and prevent unauthorized access, logging in as root at the login window *MUST* be disabled.

The macOS system *MUST* require individuals to be authenticated with an individual authenticator prior to using a group authenticator, and administrator users *MUST* never log in directly as root.

REMEDIATION

```
/usr/bin/fdesetup remove –user root
/usr/bin/dscl '/Local/Default' delete '/Users/root' AuthenticationAuthority
```

REFERENCES

Framework	Values
800-53r5	IA-2, IA-2(5)
800-171r3	03.05.01
DISA STIG	APPL-26-000100
SRG	SRG-OS-000364-GPOS-00151, SRG-OS-000109-GPOS-00056, SRG-OS-000104-GPOS-00051
CIS Benchmark	5.6 (level 1)
CIS Controls v8	5.4
CMMC	IA.L1-3.5.1, IA.L1-3.5.2
CCI	CCI-000764, CCI-000770, CCI-001813, CCI-004045
CCE	CCE-95282-0

8.4 Disable Apple Intelligence Notes Transcription

`os_notes_transcription_disable`

DISCUSSION

Apple Intelligence features such as Notes Transcription that use off device AI *MUST* be disabled.

CONFIGURATION PROFILE

```
– PayloadContent:
  – allowNotesTranscription: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: Apps
ddm_value:
  Notes:
    AllowTranscription: false
declarationtype: com.apple.configuration.intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-20(1), CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.5.1.4 (level 1)
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381, CCI-001774
CCE	CCE-95238-2

8.5 Must Use an Approved Antivirus Program

`os_anti_virus_installed`

DISCUSSION

An approved antivirus product *MUST* be installed and configured to run.

Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the operating system.'

REMEDIATION

```
/bin/launchctl load -w /Library/Apple/System/Library/LaunchDaemons/com.apple.XProtect.daemon.scan.plist
/bin/launchctl load -w /Library/Apple/System/Library/LaunchDaemons/com.apple.XprotectFramework.PluginService.
plist
```

REFERENCES

Framework	Values
CIS Benchmark	5.10 (level 1)
CIS Controls v8	10.5, 10.1, 10.2
CCI	CCI-000366
CCE	CCE-95158-2

8.6 Ensure No World Writable Files Exist in the System Folder

`os_world_writable_system_folder_configure`

DISCUSSION

Folders in /System/Volumes/Data/System *MUST* not be world-writable.

REMEDIATION

```
IFS=$'\n'
for sysPermissions in $( /usr/bin/find /System/Volumes/Data/System -type d -perm -2 | /usr/bin/grep -vE "downloadDir|locks" ); do
  /bin/chmod -R o-w "$sysPermissions"
done
```

REFERENCES

Framework	Values
CIS Benchmark	5.1.6 (level 1)
CIS Controls v8	3.3
CCE	CCE-95333-1

8.7 Ensure All Internal User Storage APFS Volumes Are Encrypted

`os_internal_apfs_volumes_encrypted`

DISCUSSION

All internal user storage APFS volumes *MUST* be encrypted.

While FileVault protects the boot volume, data may be copied to other attached internal storage and reduce the protection afforded by FileVault. All internal APFS volumes that carry user data and do not have a specific role (Preboot, Recovery, VM) *MUST* be encrypted to protect user data from loss or tampering.

REFERENCES

Framework	Values
CIS Benchmark	5.3.1 (level 1)
CIS Controls v8	3.6, 3.11, 13.6, 14.8
CCE	CCE-96725-7

8.8 Disable Automatic Opening of Safe Files in Safari

`os_safari_open_safe_downloads_disable`

DISCUSSION

Open "safe" files after downloading *MUST* be disabled in Safari.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AutoOpenSafeDownloads: false
  PayloadType: com.apple.Safari
```

REFERENCES

Framework	Values
CIS Benchmark	6.3.1 (level 1)
CIS Controls v8	9.1, 9.6
CCE	CCE-95284-6

8.9 Disable Apple Intelligence Mail Summary

`os_mail_summary_disable`

DISCUSSION

Apple Intelligence features such as Apple Mail Summary that use off device AI *MUST* be disabled.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowMailSummary: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: Apps
ddm_value:
  Mail:
    AllowSummary: false
declarationtype: com.apple.configuration.intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-20(1), CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
CIS Benchmark	2.5.1.3 (level 1)
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCE	CCE-95223-4

8.10 Ensure All APFS and HFS+ External User Storage Volumes Are Encrypted

`os_external_apfs_hfs_volumes_encrypted`

DISCUSSION

All APFS and HFS+ external user storage volumes *MUST* be encrypted.

While FileVault protects the boot volume, data may be copied to attached external storage and reduce the protection afforded by FileVault. All external user data volumes (APFS or HFS+) *MUST* be encrypted to protect user data from loss or tampering. CoreStorage has been deprecated and replaced with APFS for volume encryption.

REFERENCES

Framework	Values
CIS Benchmark	5.3.2 (level 1)
CIS Controls v8	3.6, 3.11, 13.6, 14.8
CCE	CCE-96724-0

8.11 Disable Apple Intelligence Notes Transcription Summary

os_notes_transcription_summary_disable

DISCUSSION

Apple Intelligence features such as Notes Transcription Summary that use off device AI *MUST* be disabled.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowNotesTranscriptionSummary: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: Apps
ddm_value:
  Notes:
    AllowTranscriptionSummary: false
declarationtype: com.apple.configuration.intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-20(1), CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.5.1.4 (level 1)
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381, CCI-001774
CCE	CCE-95239-0

8.12 Enable Authenticated Root

`os_authenticated_root_enable`

DISCUSSION

Authenticated Root *MUST* be enabled.

When Authenticated Root is enabled the macOS is booted from a signed volume that is cryptographically protected to prevent tampering with the system volume.

Note: Authenticated Root is enabled by default on macOS systems.

WARNING: If more than one partition with macOS is detected, the csrutil command will hang awaiting input.

REMEDIATION

```
/usr/bin/csrutil authenticated-root enable
```

REFERENCES

Framework	Values
800-53r5	AC-3, CM-5, MA-4(1), SC-34, SI-7, SI-7(6)
800-171r3	03.01.02, 03.04.05
DISA STIG	APPL-26-005070
SRG	SRG-OS-000080-GPOS-00048
CIS Benchmark	5.1.4 (level 1)
CIS Controls v8	3.6, 3.11
CMMC	AC.L1-3.1.1, CM.L2-3.4.5, SC.L2-3.13.11
CCI	CCI-000213
CCE	CCE-95164-0

8.13 Ensure Advertising Privacy Protection in Safari Is Enabled

`os_safari_advertising_privacy_protection_enable`

DISCUSSION

Allow privacy-preserving measurement of ad effectiveness *MUST* be enabled in Safari.

CONFIGURATION PROFILE

```
- PayloadContent:
  - WebKitPreferences.privateClickMeasurementEnabled: true
  PayloadType: com.apple.Safari
```

REFERENCES

Framework	Values
CIS Benchmark	6.3.6 (level 1)
CIS Controls v8	9.1
CCE	CCE-95283-8

8.14 Enforce Installation of XProtect Remediator and Gatekeeper Updates Automatically

`os_config_data_install_enforce`

DISCUSSION

Software Update *MUST* be configured to update XProtect Remediator and Gatekeeper automatically.

This setting enforces definition updates for XProtect Remediator 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 the computer to be restarted.

link:https://support.apple.com/en-us/HT207005[]

Note: Software update will automatically update XProtect Remediator and Gatekeeper by default in the macOS.

CONFIGURATION PROFILE

```
- PayloadContent:
  - ConfigDataInstall: true
  PayloadType: com.apple.SoftwareUpdate
```

REFERENCES

Framework	Values
800-53r5	SI-2(5), SI-3
800-171r3	03.14.02
DISA STIG	APPL-26-005130
SRG	SRG-OS-000480-GPOS-00227
CIS Benchmark	1.5 (level 1)
CIS Controls v8	7.3, 7.4, 7.7
CMMC	SI.L1-3.14.1, SI.L1-3.14.2, SI.L1-3.14.4
CCI	CCI-000366
CCE	CCE-95176-4

8.15 Remove Guest Folder if Present

`os_guest_folder_removed`

DISCUSSION

The guest folder *MUST* be deleted if present.

REMEDIATION

```
/bin/rm -Rf /Users/Guest
```

REFERENCES

Framework	Values
CIS Benchmark	5.9 (level 1)
CIS Controls v8	4.1
CCE	CCE-95198-8

8.16 Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices

`os_sleep_and_display_sleep_apple_silicon_enable`

DISCUSSION

Apple Silicon MacBooks should set sleep timeout to 15 minutes (900 seconds) or less and the display sleep timeout should be 10 minutes (600 seconds) or less but less than the sleep setting.

REMEDIATION

```
/usr/bin/pmset -a sleep 15
/usr/bin/pmset -a displaysleep 10
```

REFERENCES

Framework	Values
CIS Benchmark	2.10.1.2 (level 2)
CIS Controls v8	4.1
CCE	CCE-95302-6

8.17 Remove Password Hint From User Accounts

`os_password_hint_remove`

DISCUSSION

User accounts *MUST* not contain password hints.

REMEDIATION

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
  /usr/bin/dscl . -delete /Users/$u hint
done
```

REFERENCES

Framework	Values
800-53r5	IA-6
800-171r3	03.05.11
DISA STIG	APPL-26-003014
SRG	SRG-OS-000079-GPOS-00047
CIS Benchmark	2.12.1 (level 1)
CIS Controls v8	5.2
CMMC	IA.L2-3.5.11
CCI	CCI-000206
CCE	CCE-95250-7

8.18 Enforce Software Update App Update Updates Automatically

`os_software_update_app_update_enforce`

DISCUSSION

Software Update *MUST* be configured to enforce automatic updates of App Updates is enabled.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AutomaticallyInstallAppUpdates: true
  PayloadType: com.apple.SoftwareUpdate
```

REFERENCES

Framework	Values
CIS Benchmark	1.4 (level 1)
CIS Controls v8	7.3, 7.4
CCE	CCE-95402-4

8.19 Configure Sudo To Log Events

`os_sudo_log_enforce`

DISCUSSION

Sudo *MUST* be configured to log privilege escalation.

REMEDIATION

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i '' '/^Defaults[[:blank:]]*\!log_allowed/s/^/# /' '{}' \;
/bin/echo "Defaults log_allowed" >> /etc/sudoers.d/mscp
```

DECLARATIVE DEVICE MANAGEMENT

```
config_file: sudoers
configuration_key: Defaults
configuration_value: log_allowed
declarationtype: com.apple.configuration.services.configuration-files
service: com.apple.sudo
```

REFERENCES

Framework	Values
800-53r5	AC-6(9)
800-171r3	03.01.07
DISA STIG	APPL-26-000190
SRG	SRG-OS-000064-GPOS-00033
CIS Benchmark	5.11 (level 1)
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, SI.L2-3.14.3
CCI	CCI-000172
CCE	CCE-95316-6

8.20 Display Policy Banner at Login Window

`os_policy_banner_loginwindow_enforce`

DISCUSSION

Displaying a standardized and approved use notification before granting access to the operating system ensures that users are provided with privacy and security notification verbiage that is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

The policy banner will show if a "PolicyBanner.rtf" or "PolicyBanner.rtfd" exists in the "/Library/Security" folder.

The banner text of the document *MUST* read:

[source,text] ---- Center for Internet Security Test Message ----

REMEDIATION

```
bannerText="Center for Internet Security Test Message"
/bin/mkdir /Library/Security/PolicyBanner.rtfd
/usr/bin/textutil -convert rtf -output /Library/Security/PolicyBanner.rtfd/TXT.rtf -stdin <<EOF
$bannerText
EOF
```

REFERENCES

Framework	Values
800-53r5	AC-8
800-171r3	03.01.09
DISA STIG	APPL-26-000025
SRG	SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088, SRG-OS-000023-GPOS-00006
CIS Benchmark	5.8 (level 2)
CIS Controls v8	4.1
CMMC	AC.L2-3.1.9
CCI	CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388
CCE	CCE-95257-2

8.21 Disable Apple Intelligence Writing Tools

`os_writing_tools_disable`

DISCUSSION

Apple Intelligence features such as writing tools that use off device AI *MUST* be disabled.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowWritingTools: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: AllowWritingTools
ddm_value: false
declarationtype: com.apple.configuration.intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-20(1), CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-005160
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.5.1.2 (level 1)
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381, CCI-001774
CCE	CCE-95334-9

8.22 Configure Sudoers Timestamp Type

`os_sudoers_timestamp_type_configure`

DISCUSSION

The file /etc/sudoers *MUST* be configured to not include a timestamp_type of global or ppid and be configured for timestamp record types of tty.

This rule ensures that the "sudo" command will prompt for the administrator's password at least once in each newly opened terminal window. This prevents a malicious user from taking advantage of an unlocked computer or an abandoned logon session by bypassing the normal password prompt requirement.

REMEDIATION

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i '' '/timestamp_type/d; /!tty_tickets/d' '{}' \;
```

REFERENCES

Framework	Values
800-53r5	CM-5(1), IA-11
800-171r3	03.05.01
DISA STIG	APPL-26-004060
SRG	SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156
CIS Benchmark	5.5 (level 1)
CIS Controls v8	4.3
CCI	CCI-002038
CCE	CCE-95318-2

8.23 Disable Network File System Service

os_nfsd_disable

DISCUSSION

Support for Network File Systems (NFS) services is non-essential and, therefore, *MUST* be disabled.

REMEDIATION

```
/bin/launchctl disable system/com.apple.nfsd
/bin/rm -rf /etc/exports
```

REFERENCES

Framework	Values
800-53r5	AC-17, AC-3
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002003
SRG	SRG-OS-000080-GPOS-00048
CIS Benchmark	4.3 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.1
CCI	CCI-000213
CCE	CCE-95235-8

8.24 Disable the Built-in Web Server

os_httpd_disable

DISCUSSION

The built-in web server which is managed by launchd is a non-essential service built into macOS and *MUST* be disabled and not running.

Note: The built in web server service is disabled at startup by default macOS.

REMEDIATION

```
/usr/sbin/apachectl stop 2>/dev/null
/bin/launchctl disable system/org.apache.httpd
```

REFERENCES

Framework	Values
800-53r5	AC-17, AC-3
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002008
SRG	SRG-OS-000080-GPOS-00048
CIS Benchmark	4.2 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.1

CCI	CCI-000213
CCE	CCE-95204-4

8.25 Disable AirDrop

`os_airdrop_disable`

DISCUSSION

AirDrop *MUST* be disabled to prevent file transfers to or from unauthorized devices. AirDrop allows users to share and receive files from other nearby Apple devices.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowAirDrop: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-3, CM-7, CM-7(1)
800-171r3	03.01.02, 03.01.20, 03.04.06
DISA STIG	APPL-26-002009
SRG	SRG-OS-000300-GPOS-00118, SRG-OS-000080-GPOS-00048, SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.1.1 (level 1)
CIS Controls v8	4.1, 4.8, 6.7
CMMC	AC.L1-3.1.1, AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000213, CCI-000381, CCI-001443
CCE	CCE-95156-6

8.26 Ensure Show Full Website Address in Safari Is Enabled

`os_safari_show_full_website_address_enable`

DISCUSSION

Show full website address *MUST* be enabled in Safari.

CONFIGURATION PROFILE

```
- PayloadContent:
  - ShowFullURLInSmartSearchField: true
  PayloadType: com.apple.Safari
```

REFERENCES

Framework	Values
CIS Benchmark	6.3.7 (level 1)
CIS Controls v8	9.1

CCE	CCE-95287-9

8.27 Enable Apple Mobile File Integrity

`os_mobile_file_integrity_enable`

DISCUSSION

Mobile file integrity *MUST* be enabled.

REMEDIATION

```
/usr/sbin/nvram boot-args=""
```

REFERENCES

Framework	Values
CIS Benchmark	5.1.3 (level 1)
CIS Controls v8	2.3, 2.6
CCE	CCE-95231-7

8.28 Ensure System Integrity Protection is Enabled

`os_sip_enable`

DISCUSSION

System Integrity Protection (SIP) *MUST* be enabled.

SIP is vital to protecting the integrity of the system as it prevents malicious users and software from making unauthorized and/or unintended modifications to protected files and folders; ensures the presence of an audit record generation capability for defined auditable events for all operating system components; protects audit tools from unauthorized access, modification, and deletion; restricts the root user account and limits the actions that the root user can perform on protected parts of the macOS; and prevents non-privileged users from granting other users direct access to the contents of their home directories and folders.

Note: SIP is enabled by default in macOS.

REMEDIATION

```
/usr/bin/csrutil enable
```

REFERENCES

Framework	Values
800-53r5	AC-3, AU-9, AU-9(3), CM-5, CM-5(6), SC-4, SI-2, SI-7
800-171r3	03.01.02, 03.03.08, 03.04.05, 03.13.04
DISA STIG	APPL-26-005001
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000062-GPOS-00031, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000278-GPOS-00108, SRG-OS-000080-GPOS-00048, SRG-OS-000059-GPOS-00029, SRG-OS-000138-GPOS-00069, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000259-GPOS-00100, SRG-OS-000122-GPOS-00063, SRG-OS-000058-GPOS-00028
CIS Benchmark	5.1.2 (level 1)
CIS Controls v8	2.3, 2.6, 10.5

CMMC	AC.L1-3.1.1, AU.L2-3.3.8, CM.L2-3.4.5, SC.L2-3.13.4, SI.L1-3.14.1, SI.L1-3.14.4
CCI	CCI-000154, CCI-000158, CCI-000169, CCI-001493, CCI-001494, CCI-001495, CCI-001499, CCI-001875, CCI-001876, CCI-001877, CCI-001878, CCI-001879, CCI-001880, CCI-001881, CCI-001882, CCI-001090, CCI-001496
CCE	CCE-95298-6

8.29 Ensure Secure Keyboard Entry Terminal.app is Enabled

`os_terminal_secure_keyboard_enable`

DISCUSSION

Secure keyboard entry *MUST* be enabled in Terminal.app.

CONFIGURATION PROFILE

```
- PayloadContent:
  - SecureKeyboardEntry: true
  PayloadType: com.apple.Terminal
```

REFERENCES

Framework	Values
CIS Benchmark	6.4.1 (level 1)
CIS Controls v8	4.8
CCE	CCE-95321-6

8.30 Enable Gatekeeper

`os_gatekeeper_enable`

DISCUSSION

Gatekeeper *MUST* be enabled.

Gatekeeper is a security feature that ensures that applications are digitally signed by an Apple-issued certificate before they are permitted to run. Digital signatures allow the macOS host to verify that the application has not been modified by a malicious third party.

Administrator users will still have the option to override these settings on a case-by-case basis.

CONFIGURATION PROFILE

```
- PayloadContent:
  - EnableAssessment: true
  PayloadType: com.apple.systempolicy.control
```

REFERENCES

Framework	Values
800-53r5	CM-14, CM-5, SI-3, SI-7(1), SI-7(15)
800-171r3	03.14.02
DISA STIG	APPL-26-002064
SRG	SRG-OS-000366-GPOS-00153, SRG-OS-000480-GPOS-00228
CIS Benchmark	2.6.5 (level 1)
CIS Controls v8	10.1, 10.2, 10.5
CMMC	CM.L2-3.4.5, SI.L1-3.14.1, SI.L1-3.14.2, SI.L1-3.14.4
CCI	CCI-001749, CCI-003992
CCE	CCE-95195-4

8.31 Ensure No World Writable Files Exist in the Library Folder

`os_world_writable_library_folder_configure`

DISCUSSION

Folders in /System/Volumes/Data/Library *MUST* not be world-writable.

Note: Some vendors are known to create world-writable folders to the System Library folder. You may need to add more exclusions to this check and fix to match your environment.

REMEDIATION

```
IFS=$'\n'
for libPermissions in $(/usr/bin/find /Library -type d -perm -002 ! -perm -1000 ! -xattrname com.apple.rootless 2>/dev/null); do
  /bin/chmod -R o-w "$libPermissions"
done
```

REFERENCES

Framework	Values
CIS Benchmark	5.1.7 (level 2)
CIS Controls v8	3.3
CCE	CCE-95332-3

8.32 Enable Time Synchronization Daemon

`os_time_server_enabled`

DISCUSSION

The macOS time synchronization daemon (timed) *MUST* be enabled for proper time synchronization to an authorized time server.

Note: The time synchronization daemon is enabled by default on macOS.

REMEDIATION

```
/bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.timed.plist
```

REFERENCES

Framework	Values
800-53r5	AU-12(1), SC-45(1)
800-171r3	03.03.07
DISA STIG	APPL-26-000180
SRG	SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144, SRG-OS-000785-GPOS-00250
CIS Benchmark	2.3.2.2 (level 1)
CIS Controls v8	8.4
CMMC	AU.L2-3.3.7
CCI	CCI-002046, CCI-001891, CCI-004923, CCI-004926, CCI-004922
CCE	CCE-95325-7

8.33 Configure Sudo Timeout Period to 0

`os_sudo_timeout_configure`

DISCUSSION

The file /etc/sudoers *MUST* include a timestamp_timeout of 0.

REMEDIATION

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i '' '/timestamp_timeout/d' '{}' \;
/bin/echo "Defaults timestamp_timeout=0" >> /etc/sudoers.d/mscp
```

DECLARATIVE DEVICE MANAGEMENT

```
config_file: sudoers
configuration_key: Defaults timestamp_timeout=
configuration_value: 0
declarationtype: com.apple.configuration.services.configuration-files
service: com.apple.sudo
```

REFERENCES

Framework	Values
DISA STIG	APPL-26-004022
SRG	SRG-OS-000373-GPOS-00156
CIS Benchmark	5.4 (level 1)
CIS Controls v8	4.3
CCI	CCI-002038
CCE	CCE-95317-4

8.34 Ensure Appropriate Permissions Are Enabled for System Wide Applications

`os_system_wide_applications_configure`

DISCUSSION

Applications in the System Applications Directory (/Applications) *MUST* not be world-writable.

REMEDIATION

```
IFS=$'\n'
for apps in $( /usr/bin/find /Applications -iname "*\.app" -type d -perm -2 ); do
  /bin/chmod -R o-w "$apps"
done
```

REFERENCES

Framework	Values
CIS Benchmark	5.1.5 (level 1)
CIS Controls v8	3.3
CCE	CCE-95320-8

8.35 Ensure Software Update Deferment Is Less Than or Equal to 30 Days

`os_software_update_deferral`

DISCUSSION

Software updates *MUST* be deferred for 30 days or less.

If you need to defer software updates, create a Restrictions profile using the com.apple.applicationaccess domain and the key enforcedSoftwareUpdateDelay.

REFERENCES

Framework	Values
CIS Benchmark	1.6 (level 1)
CIS Controls v8	7.3, 7.4
CCE	CCE-95303-4

8.36 Secure User's Home Folders

`os_home_folders_secure`

DISCUSSION

The system *MUST* be configured to prevent access to other user's home folders.

The default behavior of macOS is to allow all valid users access to the top level of every other user's home folder while restricting access only to the Apple default folders within.

REMEDIATION

```
IFS=$'\n'
for userDirs in $( /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d ! \( -perm 700 -o
 -perm 711 \) | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" ); do
  /bin/chmod og-rwx "$userDirs"
done
unset IFS
```

REFERENCES

Framework	Values
800-53r5	AC-6
800-171r3	03.01.05
DISA STIG	APPL-26-002068
SRG	SRG-OS-000480-GPOS-00230, SRG-OS-000480-GPOS-00228
CIS Benchmark	5.1.1 (level 1)
CIS Controls v8	3.3
CMMC	AC.L1-3.1.1, AC.L1-3.1.2, AC.L2-3.1.5, AC.L2-3.1.6
CCI	CCI-000366
CCE	CCE-95203-6

8.37 Configure Install.log Retention to 365

`os_install_log_retention_configure`

DISCUSSION

The install.log *MUST* be configured to require records be kept for a organizational defined value before deletion, unless the system uses a central audit record storage facility.

REMEDIATION

```
/usr/bin/sed -i '' "s/\* file \/var\/log\/install.log.*/\* file \/var\/log\/install.log format='\$\(\(Time\)\
(JZ\)\) \$Host \$\(Sender\)\[\$\(PID\)\]: \$Message' rotate=utc compress file_max=50M size_only ttl=365/g" /
etc/asl/com.apple.install
```

REFERENCES

Framework	Values
800-53r5	AU-11, AU-4
800-171r3	03.03.03
DISA STIG	APPL-26-004050
SRG	SRG-OS-000341-GPOS-00132
CIS Benchmark	3.3 (level 1)
CIS Controls v8	8.1, 8.3
CMMC	AU.L2-3.3.1
CCI	CCI-001849
CCE	CCE-95211-9

8.38 Enforce On Device Dictation

`os_on_device_dictation_enforce`

DISCUSSION

The system *MUST* be configured for on device dictation.

By enforcing on device dictation this will mitigate the risk of unwanted data being sent to Apple.

CONFIGURATION PROFILE

```
- PayloadContent:
  - forceOnDeviceOnlyDictation: true
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: ForceOnDeviceOnlyTranslation
ddm_value: true
declarationtype: com.apple.configuration.intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-002220
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.18.1 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95247-3

8.39 Ensure Prevent Cross-site Tracking in Safari Is Enabled

`os_safari_prevent_cross-site_tracking_enable`

DISCUSSION

Prevent cross-site tracking *MUST* be enabled in Safari.

CONFIGURATION PROFILE

```
- PayloadContent:
  - WebKitPreferences.storageBlockingPolicy: 1
  - WebKitStorageBlockingPolicy: 1
  - BlockStoragePolicy: 2
  PayloadType: com.apple.Safari
```

REFERENCES

Framework	Values
CIS Benchmark	6.3.4 (level 1)
CIS Controls v8	9.1, 9.3
CCE	CCE-95285-3

8.40 Disable Bonjour Multicast

os_bonjour_disable

DISCUSSION

Bonjour multicast advertising *MUST* be disabled to prevent the system from broadcasting its presence and available services over network interfaces.

CONFIGURATION PROFILE

```
- PayloadContent:
  - NoMulticastAdvertisements: true
  PayloadType: com.apple.mDNSResponder
```

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1)
800-171r3	03.04.06
DISA STIG	APPL-26-002005
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	4.1 (level 2)
CIS Controls v8	4.1, 4.8
CMMC	CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95169-9

8.41 Disable Login to Other User's Active and Locked Sessions

os_unlock_active_user_session_disable

DISCUSSION

The ability to log in to another user's active or locked session *MUST* be disabled.

macOS has a privilege that can be granted to any user that will allow that user to unlock active user's sessions. 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.

Note: Configuring this setting will change the user experience and disable TouchID from unlocking the screensaver. A configuration profile will be generated to include the setting that restores the expected behavior. You can also apply the settings using `/usr/bin/sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow screenUnlockMode -int 1`.

WARNING: Do not apply this rule if your organization uses smartcards and Platform Single Sign-On (PSSO).

REMEDIATION

```
SS_RULE=$(/usr/bin/security -q authorizationdb read system.login.screensaver 2>&1 | /usr/bin/xmllint --xpath
"//dict/key[.='rule']/following-sibling::array[1]/string/text()" -)

if [[ "$SS_RULE" == *psso* ]]; then
    /usr/bin/security -q authorizationdb read psso-screensaver > "/tmp/psso-screensaver-mscp.plist"
    /usr/bin/sed -i.bak 's/<string>authenticate-session-owner-or-admin<\/string>/<string>authenticate-session
-owner<\/string>/' /tmp/psso-screensaver-mscp.plist
    /usr/bin/security -q authorizationdb write psso-screensaver-mscp < /tmp/psso-screensaver-mscp.plist
    /usr/bin/security -q authorizationdb write system.login.screensaver psso-screensaver-mscp 2>&1
else
    /usr/bin/security -q authorizationdb write system.login.screensaver "authenticate-session-owner" 2>&1
fi
```

CONFIGURATION PROFILE

```
- PayloadContent:
  - screenUnlockMode: 1
  PayloadType: com.apple.loginwindow
```

REFERENCES

Framework	Values
800-53r5	IA-2, IA-2(5)
800-171r3	03.05.01
DISA STIG	APPL-26-000090
SRG	SRG-OS-000109-GPOS-00056, SRG-OS-000104-GPOS-00051
CIS Benchmark	5.7 (level 1)
CIS Controls v8	4.3
CMMC	IA.L1-3.5.1, IA.L1-3.5.2
CCI	CCI-000764, CCI-000770, CCI-004045
CCE	CCE-95328-1

8.42 Ensure Show Safari shows the Status Bar is Enabled

`os_safari_show_status_bar_enabled`

DISCUSSION

Safari *MUST* be configured to show the status bar.

CONFIGURATION PROFILE

```
- PayloadContent:
  - ShowOverlayStatusBar: true
  PayloadType: com.apple.Safari
```

REFERENCES

Framework	Values
CIS Benchmark	6.3.10 (level 1)
CIS Controls v8	9.1

CCE	CCE-95288-7

9. Password Policy

This section contains the configuration and enforcement of settings pertaining to password policies in macOS.

Note: The check/fix commands outlined in this section *MUST* be run by a user with elevated privileges.

[IMPORTANT] ==== The password policy recommendations in the NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based off of common complexity values. But your organization may define its own password complexity rules. ====

Note: The settings outlined in this section adhere to the recommendations provided in this document for systems that utilize passwords for local accounts. If systems are integrated with a directory service, local password policies should align with domain password policies to the fullest extent feasible.

9.1 Require Passwords to Match the Defined Custom Regular Expression

`pwpolicy_custom_regex_enforce`

DISCUSSION

The macOS *MUST* be configured to meet complexity requirements defined in ^(?=.**[A-Z])(?=.**[a-z]).*$.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: To comply with Executive Order 14028, “Improving the Nation's Cybersecurity”, OMB M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, and NIST SP-800-63b, “Digital Identity Guidelines: Authentication and Lifecycle Management” federal, military, and intelligence communities must adopt the following configuration settings. Password policies must not require the use of complexity policies such as upper characters, lower characters, or special characters. Password policies must also not require the use of regular rotation. Password policies should define a minimum length. Multifactor authentication should be used where ever possible.

Note: The configuration profile generated must be installed from an MDM server.

CONFIGURATION PROFILE

```
- PayloadContent:
  - customRegex:
      passwordContentDescription:
        default: Password must match custom regex.
      passwordContentRegex: ^(?=.*[A-Z])(?=.*[a-z]).*$
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: CustomRegex
ddm_value:
  Description: Password must match custom regex.
  Regex: ^(?=.*[A-Z])(?=.*[a-z]).*$
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	IA-5(1)
800-171r3	03.05.07
DISA STIG	APPL-26-003060
SRG	SRG-OS-000070-GPOS-00038, SRG-OS-000069-GPOS-00037
CIS Benchmark	5.2.6 (level 2)
CIS Controls v8	5.2
CMMC	IA.L2-3.5.7, IA.L2-3.5.8, IA.L2-3.5.9
CCI	CCI-000192, CCI-000193, CCI-004066, CCI-004066, CCI-004064, CCI-004065
CCE	CCE-95340-6

9.2 Restrict Maximum Password Lifetime to 365 Days

`pwpolicy_max_lifetime_enforce`

DISCUSSION

The system *MUST* be configured to enforce a maximum password lifetime limit of 365 days.

This rule ensures that users are forced to change their passwords frequently enough to prevent malicious users from gaining and maintaining access to the system.

Note: To comply with Executive Order 14028, “Improving the Nation's Cybersecurity”, OMB M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, and NIST SP-800-63b, “Digital Identity Guidelines: Authentication and Lifecycle Management” federal, military, and intelligence communities must adopt the following configuration settings. Password policies must not require the use of complexity policies such as upper characters, lower characters, or special characters. Password policies must also not require the use of regular rotation. Password policies should define a minimum length. Multifactor authentication should be used where ever possible.

CONFIGURATION PROFILE

```
- PayloadContent:
  - maxPINAgeInDays: 365
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: MaximumPasscodeAgeInDays
ddm_value: 365
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	IA-5
800-171r3	03.05.12
DISA STIG	APPL-26-003008
SRG	SRG-OS-000076-GPOS-00044, SRG-OS-000775-GPOS-00230
CIS Benchmark	5.2.7 (level 1)
CIS Controls v8	5.3
CMMC	IA.L2-3.5.8, IA.L2-3.5.9
CCI	CCI-000199, CCI-004066
CCE	CCE-95345-5

9.3 Prohibit Password Reuse for a Minimum of 24 Generations

`pwpolicy_history_enforce`

DISCUSSION

The device *MUST* be configured to enforce a password history of at least 24 previous passwords when a password is created.

This rule ensures that users are not allowed to re-use a password that was used in any of the 24 previous password generations.

Limiting password reuse protects against malicious users attempting to gain access to the system via brute-force hacking methods.

CONFIGURATION PROFILE

```
- PayloadContent:
  - pinHistory: 24
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: PasscodeReuseLimit
ddm_value: 24
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	IA-5(1)
800-171r3	03.05.07
DISA STIG	APPL-15-003009
SRG	SRG-OS-000077-GPOS-00045, SRG-OS-000775-GPOS-00230
CIS Benchmark	5.2.8 (level 1)
CIS Controls v8	5.2
CMMC	IA.L2-3.5.7, IA.L2-3.5.8, IA.L2-3.5.9
CCI	CCI-000200

CCE	CCE-95343-0

9.4 Limit Consecutive Failed Login Attempts to 5

`pwpolicy_account_lockout_enforce`

DISCUSSION

The system *MUST* be configured to limit the number of failed login attempts to a maximum of 5. When the maximum number of failed attempts is reached, the system *MUST* prevent logins for a period of time after.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

CONFIGURATION PROFILE

```
- PayloadContent:
  - maxFailedAttempts: 5
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: MaximumFailedAttempts
ddm_value: 5
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	AC-7
800-171r3	03.01.08
DISA STIG	APPL-26-000022
SRG	SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005
CIS Benchmark	5.2.1 (level 1)
CIS Controls v8	6.2
CMMC	AC.L2-3.1.8
CCI	CCI-000044, CCI-002238
CCE	CCE-95337-2

9.5 Require Passwords Contain a Minimum of One Special Character

`pwpolicy_special_character_enforce`

DISCUSSION

The macOS *MUST* be configured to require at least one special character be used when a password is created.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: To comply with Executive Order 14028, "Improving the Nation's Cybersecurity", OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", and NIST SP-800-63b, "Digital Identity Guidelines: Authentication and Lifecycle Management" federal, military, and intelligence communities must adopt the following configuration settings. Password policies must not require the use of complexity policies such as upper characters, lower characters, or special characters. Password policies must also not require the use of regular rotation. Password policies should define a minimum length. Multifactor authentication should be used where ever possible.

CONFIGURATION PROFILE

```
- PayloadContent:
  - minComplexChars: 1
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: MinimumComplexCharacters
ddm_value: 1
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	IA-5(1)
800-171r3	03.05.07
DISA STIG	APPL-26-003011
SRG	SRG-OS-000266-GPOS-00101
CIS Benchmark	5.2.5 (level 2)
CIS Controls v8	5.2
CMMC	IA.L2-3.5.7, IA.L2-3.5.8, IA.L2-3.5.9
CCI	CCI-001619, CCI-004066
CCE	CCE-95350-5

9.6 Set Account Lockout Time to 15 Minutes

`pwpolicy_account_lockout_timeout_enforce`

DISCUSSION

The macOS *MUST* be configured to enforce a lockout time period of at least 15 minutes when the maximum number of failed logon attempts is reached.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

CONFIGURATION PROFILE

```
- PayloadContent:
  - minutesUntilFailedLoginReset: 15
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: MaximumGracePeriodInMinutes
ddm_value: 15
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	AC-7
800-171r3	03.01.08
DISA STIG	APPL-26-000060
SRG	SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005
CIS Benchmark	5.2.1 (level 1)
CIS Controls v8	6.2
CMMC	AC.L2-3.1.8
CCI	CCI-002238, CCI-000044
CCE	CCE-95338-0

9.7 Require Passwords Contain a Minimum of One Numeric Character

`pwpolicy_alpha_numeric_enforce`

DISCUSSION

The macOS *MUST* be configured to require at least one numeric character be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: To comply with Executive Order 14028, "Improving the Nation's Cybersecurity", OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", and NIST SP-800-63b, "Digital Identity Guidelines: Authentication and Lifecycle Management" federal, military, and intelligence communities must adopt the following configuration settings. Password policies must not require the use of complexity policies such as upper characters, lower characters, or special characters. Password policies must also not require the use of regular rotation. Password policies should define a minimum length. Multifactor authentication should be used where ever possible.

CONFIGURATION PROFILE

```
- PayloadContent:
  - requireAlphanumeric: true
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: RequireAlphanumericPasscode
ddm_value: true
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	IA-5(1)
800-171r3	03.05.07
DISA STIG	APPL-26-003007
SRG	SRG-OS-000071-GPOS-00039, SRG-OS-000775-GPOS-00230
CIS Benchmark	5.2.3 (level 2), 5.2.4 (level 2)
CIS Controls v8	5.2
CMMC	IA.L2-3.5.7, IA.L2-3.5.8, IA.L2-3.5.9
CCI	CCI-000194, CCI-004066
CCE	CCE-95339-8

9.8 Require a Minimum Password Length of 15 Characters

`pwpolicy_minimum_length_enforce`

DISCUSSION

The macOS *MUST* be configured to require a minimum of 15 characters be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: To comply with Executive Order 14028, "Improving the Nation's Cybersecurity", OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", and NIST SP-800-63b, "Digital Identity Guidelines: Authentication and Lifecycle Management" federal, military, and intelligence communities must adopt the following configuration settings. Password policies must not require the use of complexity policies such as upper characters, lower characters, or special characters. Password policies must also not require the use of regular rotation. Password policies should define a minimum length. Multifactor authentication should be used where ever possible.

CONFIGURATION PROFILE

```
- PayloadContent:
  - minLength: 15
  PayloadType: com.apple.mobiledevice.passwordpolicy
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: MinimumLength
ddm_value: 15
declarationtype: com.apple.configuration.passcode.settings
```

REFERENCES

Framework	Values
800-53r5	IA-5(1)
800-171r3	03.05.07
DISA STIG	APPL-26-003010
SRG	SRG-OS-000078-GPOS-00046
CIS Benchmark	5.2.2 (level 1)
CIS Controls v8	5.2
CMMC	IA.L2-3.5.7, IA.L2-3.5.8, IA.L2-3.5.9
CCI	CCI-000205, CCI-004066
CCE	CCE-95346-3

10. Supplemental

This section provides additional information to support the guidance provided by the baselines.

10.1 CIS Manual Recommendations

supplemental_cis_manual

SUPPLEMENTAL

DISCUSSION

List of CIS recommendations that are manual check in the CIS macOS Benchmark.

[cols="15%h, 85%a"] |=== |Section |System Settings

|Recommendations | 1.7 Ensure the System is Managed by a Mobile Device Management (MDM) Software |===

[cols="15%h, 85%a"] |=== |Section |System Settings

|Recommendations |2.1.1.1 Audit iCloud Keychain + 2.1.1.2 Audit iCloud Drive + 2.1.1.4 Audit Security Keys Used With Apple Accounts + 2.1.1.5 Audit Freeform Sync to iCloud + 2.1.1.6 Audit Find My Mac + 2.1.2 Audit App Store Password Settings + 2.3.3.11 Ensure Computer Name Does Not Contain PII or Protected Organizational Information + 2.4.1 Audit Menu Bar and Control Center Icons + 2.5.2.2 Ensure Listen for Siri is Disabled + 2.6.1.3 Audit Location Services Access + 2.6.2.1 Audit Full Disk Access for Applications + 2.6.3.5 Ensure Share iCloud Analytics Is Disabled + 2.6.7 Audit Lockdown Mode + 2.7.2 Audit iPhone Mirroring + 2.8.1 Audit Universal Control Settings + 2.10.1.1 Ensure the OS Is Not Active When Resuming from Standby (Intel) + 2.12.2 Audit Touch ID + 2.14.1 Audit Game Center Settings + 2.15.1 Audit Notification & Focus Settings + 2.16.1 Audit Wallet & Apple Pay Settings + 2.17.1 Audit Internet Accounts for Authorized Use + |===

[cols="15%h, 85%a"] |=== |Section |Logging and Auditing

|Recommendations |3.6 Audit Software Inventory |===

[cols="15%h, 85%a"] |=== |Section |System Access, Authentication and Authorization

|Recommendations |5.2.3 Ensure Complex Password Must Contain Alphabetic Characters Is Configured + 5.2.4 Ensure Complex Password Must Contain Numeric Character Is Configured + 5.2.5 Ensure Complex Password Must Contain Special Character Is Configured + 5.2.6 Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured + 5.3.1 Ensure All User Storage APFS Volumes are Encrypted + 5.3.2 Ensure All User Storage CoreStorage Volumes are Encrypted + |===

[cols="15%h, 85%a"] |=== |Section |Applications

|Recommendations |6.1.1 Ensure Show All

11. Audit

This section contains the configuration and enforcement of the OpenBSM settings.

Note: The BSM Audit subsystem has been marked as deprecated by Apple.

Note: The check/fix commands outlined in this section *MUST* be run with elevated privileges.

11.1 Configure System to Audit All Failed Change of Object Attributes

`audit_flags_fm_failed_configure`

DISCUSSION

The audit system *MUST* be configured to record enforcement actions of failed attempts to modify file attributes (-fm).

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. One common and effective enforcement action method is using access restrictions (i.e., denying modifications to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to modify a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

REMEDIATION

```
/usr/bin/grep -qE "^flags.*-fm" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-fm/' /etc/security/audit_control;/usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-2(12), AU-12, AU-2, AU-9, CM-5(1), MA-4(1)
800-171r3	03.03.01, 03.03.03, 03.03.08
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, AU.L2-3.3.8, SI.L2-3.14.3
CCE	CCE-95120-2

11.2 Configure Audit Log Folders Group to Wheel

`audit_folder_group_configure`

DISCUSSION

Audit log files *MUST* have the group set to wheel.

The audit service *MUST* be configured to create log files with the correct group ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

REMEDIATION

```
/usr/bin/chgrp wheel /var/audit
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001015
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95124-4

11.3 Configure Audit_Control Owner to Mode 440 or Less Permissive

audit_control_mode_configure

DISCUSSION

/etc/security/audit*control* MUST_ be configured so that it is readable only by the root user and group wheel.

REMEDIATION

```
/bin/chmod 440 /etc/security/audit_control
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001130
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000063-GPOS-00032, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-000171, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95108-7

11.4 Configure System to Audit All Authorization and Authentication Events

audit_flags_aa_configure

DISCUSSION

The auditing system *MUST* be configured to flag authorization and authentication (aa) events.

Authentication events contain information about the identity of a user, server, or client. Authorization events contain information about permissions, rights, and rules. If audit records do not include aa events, it is difficult to identify incidents and to correlate incidents to subsequent events.

Audit records can be generated from various components within the information system (e.g., via a module or policy filter).

REMEDIATION

```
/usr/bin/grep -qE "^flags.*[^-]aa" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,aa/' /etc/security/audit_control; /usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-2(12), AU-12, AU-2, CM-5(1), MA-4(1)
800-171r3	03.03.01, 03.03.03
DISA STIG	APPL-26-001044
SRG	SRG-OS-000392-GPOS-00172, SRG-OS-000365-GPOS-00152, SRG-OS-000475-GPOS-00220, SRG-OS-000463-GPOS-00207, SRG-OS-000467-GPOS-00211, SRG-OS-000465-GPOS-00209, SRG-OS-000477-GPOS-00222, SRG-OS-000471-GPOS-00216, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215, SRG-OS-000458-GPOS-00203, SRG-OS-000468-GPOS-00212
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, SI.L2-3.14.3
CCI	CCI-000172, CCI-001814, CCI-002884, CCI-003938
CCE	CCE-95115-2

11.5 Configure System to Audit All Administrative Action Events

audit_flags_ad_configure

DISCUSSION

The auditing system *MUST* be configured to flag administrative action (ad) events.

Administrative action events include changes made to the system (e.g. modifying authentication policies). If audit records do not include ad events, it is difficult to identify incidents and to correlate incidents to subsequent events.

Audit records can be generated from various components within the information system (e.g., via a module or policy filter).

The information system audits the execution of privileged functions.

Note: We recommend changing the line "43127:AUE*MAC*SYSCALL:mac*syscall(2):ad" to "43127:AUE*MAC*SYSCALL:mac*syscall(2):zz" in the file /etc/security/audit_event. This will prevent sandbox violations from being audited by the ad flag.

REMEDIATION

```
/usr/bin/grep -qE "^flags.*[^-]ad" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,ad/' /etc/security/audit_control; /usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-2(12), AC-2(4), AC-6(9), AU-12, AU-2, CM-5(1), MA-4(1)
800-171r3	03.01.07, 03.03.01, 03.03.03
DISA STIG	APPL-26-001001
SRG	SRG-OS-000304-GPOS-00121, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000004-GPOS-00004, SRG-OS-000241-GPOS-00091, SRG-OS-000274-GPOS-00104, SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00216, SRG-OS-000476-GPOS-00221, SRG-OS-000471-GPOS-00215, SRG-OS-000458-GPOS-00203, SRG-OS-000303-GPOS-00120, SRG-OS-000755-GPOS-00220
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, SI.L2-3.14.3
CCI	CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-001814, CCI-002234, CCI-002884, CCI-000015, CCI-000015, CCI-003938, CCI-004083
CCE	CCE-95116-0

11.6 Configure System to Audit All Failed Program Execution on the System

`audit_flags_ex_configure`

DISCUSSION

The audit system *MUST* be configured to record enforcement actions of access restrictions, including failed program execute (-ex) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using program execution restrictions (e.g., denying users access to execute certain processes).

This configuration ensures that audit lists include events in which program execution has failed. Without auditing the enforcement of program execution, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

REMEDIATION

```
/usr/bin/grep -qE "^flags.*-ex" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-ex/' /etc/security/audit_control; /usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-2(12), AU-12, AU-2, CM-5(1)
800-171r3	03.03.01, 03.03.03
DISA STIG	APPL-26-001024
SRG	SRG-OS-000365-GPOS-00152, SRG-OS-000465-GPOS-00209, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, SI.L2-3.14.3
CCI	CCI-000172, CCI-001814, CCI-003938
CCE	CCE-95117-8

11.7 Enable Security Auditing

audit_auditd_enabled

DISCUSSION

The information system *MUST* be configured to generate audit records.

Audit records establish what types of events have occurred, when they occurred, and which users were involved. These records aid an organization in their efforts to establish, correlate, and investigate the events leading up to an outage or attack.

The content required to be captured in an audit record varies based on the impact level of an organization's system. Content that may be necessary to satisfy this requirement includes, for example, time stamps, source addresses, destination addresses, user identifiers, event descriptions, success/fail indications, filenames involved, and access or flow control rules invoked.

The information system initiates session audits at system start-up.

Note: Security auditing is NOT enabled by default on macOS 14 and later.

REMEDIATION

```
if [[ ! -e /etc/security/audit_control ]] && [[ -e /etc/security/audit_control.example ]];then
  /bin/cp /etc/security/audit_control.example /etc/security/audit_control
fi

/bin/launchctl enable system/com.apple.auditd
/bin/launchctl bootstrap system /System/Library/LaunchDaemons/com.apple.auditd.plist
/usr/sbin/audit -i
```

REFERENCES

Framework	Values
800-53r5	AU-12, AU-12(1), AU-12(3), AU-14(1), AU-3, AU-3(1), AU-8, CM-5(1), MA-4(1)
800-171r3	03.03.02, 03.03.03, 03.03.07
DISA STIG	APPL-26-001003
SRG	SRG-OS-000255-GPOS-00096, SRG-OS-000474-GPOS-00219, SRG-OS-000465-GPOS-00209, SRG-OS-000473-GPOS-00218, SRG-OS-000337-GPOS-00129, SRG-OS-000359-GPOS-00146, SRG-OS-000472-GPOS-00217, SRG-OS-000257-GPOS-00098, SRG-OS-000466-GPOS-00210, SRG-OS-000042-GPOS-00020, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000039-GPOS-00017, SRG-OS-000467-GPOS-00211, SRG-OS-000470-GPOS-00214, SRG-OS-000461-GPOS-00205, SRG-OS-000258-GPOS-00099, SRG-OS-000471-GPOS-00215, SRG-OS-000458-GPOS-00203, SRG-OS-000037-GPOS-00015, SRG-OS-000040-GPOS-00018, SRG-OS-000471-GPOS-00216, SRG-OS-000476-GPOS-00221, SRG-OS-000254-GPOS-00095, SRG-OS-000042-GPOS-00021, SRG-OS-000358-GPOS-00145, SRG-OS-000477-GPOS-00222, SRG-OS-000365-GPOS-00152, SRG-OS-000475-GPOS-00220, SRG-OS-000041-GPOS-00019, SRG-OS-000038-GPOS-00016, SRG-OS-000462-GPOS-00206, SRG-OS-000055-GPOS-00026, SRG-OS-000755-GPOS-00220
CIS Benchmark	3.1 (level 1)
CIS Controls v8	8.2, 8.5
CMMC	AU.L2-3.3.2, AU.L2-3.3.6
CCI	CCI-000130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-000135, CCI-000159, CCI-001464, CCI-001487, CCI-001889, CCI-001890, CCI-001914, CCI-002130, CCI-003938, CCI-004188
CCE	CCE-95104-6

11.8 Configure Audit Log Files to be Owned by Root

`audit_files_owner_configure`

DISCUSSION

Audit log files *MUST* be owned by root.

The audit service *MUST* be configured to create log files with the correct ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log files are set to only be readable and writable by system administrators, the risk is mitigated.

REMEDIATION

```
/usr/sbin/chown -R root /var/audit/*
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001012
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8

CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95114-5

11.9 Configure Audit Log Files to Mode 440 or Less Permissive

audit_files_mode_configure

DISCUSSION

The audit service *MUST* be configured to create log files that are readable only by the root user and group wheel. To achieve this, audit log files *MUST* be configured to mode 440 or less permissive; thereby preventing normal users from reading, modifying or deleting audit logs.

REMEDIATION

```
/bin/chmod 440 /var/audit/*
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001016
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95113-7

11.10 Configure Audit_Control Owner to Root

audit_control_owner_configure

DISCUSSION

/etc/security/audit*control* MUST_ have the owner set to root.

REMEDIATION

```
/usr/sbin/chown root /etc/security/audit_control
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001120
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000063-GPOS-00032, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-000171, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95109-5

11.11 Configure Audit Log Folders to be Owned by Root

`audit_folder_owner_configure`

DISCUSSION

Audit log folders *MUST* be owned by root.

The audit service *MUST* be configured to create log folders with the correct ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log folders are set to only be readable and writable by system administrators, the risk is mitigated.

REMEDIATION

```
/usr/sbin/chown root /var/audit
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001013
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95125-1

11.12 Configure System to Audit All Failed Read Actions on the System

audit_flags_fr_configure

DISCUSSION

The audit system *MUST* be configured to record enforcement actions of access restrictions, including failed file read (-fr) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using access restrictions (e.g., denying access to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to read a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

REMEDIATION

```
/usr/bin/grep -qE "^flags.*-fr" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-fr/' /etc/security/audit_control;/usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-2(12), AU-12, AU-2, AU-9, CM-5(1), MA-4(1)
800-171r3	03.03.01, 03.03.03, 03.03.08
DISA STIG	APPL-26-001022
SRG	SRG-OS-000392-GPOS-00172, SRG-OS-000256-GPOS-00097, SRG-OS-000365-GPOS-00152, SRG-OS-000474-GPOS-00219, SRG-OS-000057-GPOS-00027, SRG-OS-000064-GPOS-00033, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209, SRG-OS-000461-GPOS-00205, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000458-GPOS-00203, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, AU.L2-3.3.8, SI.L2-3.14.3
CCI	CCI-000172, CCI-001814, CCI-003938
CCE	CCE-95121-0

11.13 Configure System to Audit All Failed Write Actions on the System

audit_flags_fw_configure

DISCUSSION

The audit system *MUST* be configured to record enforcement actions of access restrictions, including failed file write (-fw) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using access restrictions (e.g., denying users access to edit a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to change a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

REMEDIATION

```
/usr/bin/grep -qE "^flags.*-fw" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-fw/' /etc/security/audit_control;/usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-2(12), AU-12, AU-2, AU-9, CM-5(1), MA-4(1)
800-171r3	03.03.01, 03.03.03, 03.03.08
DISA STIG	APPL-26-001023
SRG	SRG-OS-000392-GPOS-00172, SRG-OS-000256-GPOS-00097, SRG-OS-000365-GPOS-00152, SRG-OS-000057-GPOS-00027, SRG-OS-000064-GPOS-00033, SRG-OS-000463-GPOS-00207, SRG-OS-000467-GPOS-00211, SRG-OS-000465-GPOS-00209, SRG-OS-000468-GPOS-00212, SRG-OS-000466-GPOS-00210, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000458-GPOS-00203, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AU.L2-3.3.3, AU.L2-3.3.6, AU.L2-3.3.8, SI.L2-3.14.3
CCI	CCI-000172, CCI-001814, CCI-003938
CCE	CCE-95122-8

11.14 Configure Audit Retention to 60d OR 5G

`audit_retention_configure`

DISCUSSION

The audit service *MUST* be configured to require records be kept for a organizational defined value before deletion, unless the system uses a central audit record storage facility.

When "expire-after" is set to "60d OR 5G", the audit service will not delete audit logs until the log data criteria is met.

REMEDIATION

```
/usr/bin/sed -i.bak 's/^expire-after.*/expire-after:60d OR 5G/' /etc/security/audit_control; /usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AU-11, AU-4
800-171r3	03.03.03
DISA STIG	APPL-26-001029
SRG	SRG-OS-000341-GPOS-00132
CIS Benchmark	3.4 (level 1)
CIS Controls v8	8.1, 8.3
CMMC	AU.L2-3.3.1
CCI	CCI-001849

CCE	CCE-95130-1

11.15 Configure Audit_Control to Not Contain Access Control Lists

audit_control_acls_configure

DISCUSSION

/etc/security/audit*control* MUST_ not contain Access Control Lists (ACLs).

REMEDIATION

```
/bin/chmod –N /etc/security/audit_control
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001140
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000063-GPOS-00032, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-000171, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95106-1

11.16 Configure Audit Log Folders to Mode 700 or Less Permissive

audit_folders_mode_configure

DISCUSSION

The audit log folder *MUST* be configured to mode 700 or less permissive so that only the root user is able to read, write, and execute changes to folders.

Because audit logs contain sensitive data about the system and users, the audit service *MUST* be configured to mode 700 or less permissive; thereby preventing normal users from reading, modifying or deleting audit logs.

REMEDIATION

```
/bin/chmod 700 /var/audit
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001017
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95126-9

11.17 Configure System to Audit All Log In and Log Out Events

audit_flags_lo_configure

DISCUSSION

The audit system *MUST* be configured to record all attempts to log in and out of the system (lo).

Frequently, an attacker that successfully gains access to a system has only gained access to an account with limited privileges, such as a guest account or a service account. The attacker must attempt to change to another user account with normal or elevated privileges in order to proceed. Auditing both successful and unsuccessful attempts to switch to another user account (by way of monitoring login and logout events) mitigates this risk.

The information system monitors login and logout events.

REMEDIATION

```
/usr/bin/grep -qE "^flags.*[^-]lo" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,lo/' /etc/security/audit_control; /usr/sbin/audit -s
```

REFERENCES

Framework	Values
800-53r5	AC-17(1), AC-2(12), AU-12, AU-2, MA-4(1)
800-171r3	03.03.01, 03.03.03
DISA STIG	APPL-26-001002
SRG	SRG-OS-000032-GPOS-00013, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033, SRG-OS-000473-GPOS-00218, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00216, SRG-OS-000472-GPOS-00217, SRG-OS-000471-GPOS-00215, SRG-OS-000458-GPOS-00203, SRG-OS-000755-GPOS-00220
CIS Benchmark	3.2 (level 2)
CIS Controls v8	3.14, 8.2, 8.5
CMMC	AC.L2-3.1.12, AU.L2-3.3.3, AU.L2-3.3.6, SI.L2-3.14.3
CCI	CCI-000067, CCI-000172, CCI-002884
CCE	CCE-95123-6

11.18 Configure Audit_Control Group to Wheel

audit_control_group_configure

DISCUSSION

/etc/security/audit*control* MUST_ have the group set to wheel.

REMEDIATION

```
/usr/bin/chgrp wheel /etc/security/audit_control
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001110
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000063-GPOS-00032, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-000171, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95107-9

11.19 Configure Audit Log Files Group to Wheel

audit_files_group_configure

DISCUSSION

Audit log files *MUST* have the group set to wheel.

The audit service *MUST* be configured to create log files with the correct group ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

REMEDIATION

```
/usr/bin/chgrp -R wheel /var/audit/*
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-001014
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95112-9

11.20 Configure Audit Log Files to Not Contain Access Control Lists `audit_acls_files_configure`

DISCUSSION

The audit log files *MUST* not contain access control lists (ACLs).

This rule ensures that audit information and audit files are configured to be readable and writable only by system administrators, thereby preventing unauthorized access, modification, and deletion of files.

REMEDIATION

```
/bin/chmod -RN /var/audit
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-000030
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000163, CCI-000164, CCI-001314, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95101-2

11.21 Configure Audit Log Folder to Not Contain Access Control Lists

audit_acls_folders_configure

DISCUSSION

The audit log folder *MUST* not contain access control lists (ACLs).

Audit logs contain sensitive data about the system and users. This rule ensures that the audit service is configured to create log folders that are readable and writable only by system administrators in order to prevent normal users from reading audit logs.

REMEDIATION

```
/bin/chmod –N /var/audit
```

REFERENCES

Framework	Values
800-53r5	AU-9
800-171r3	03.03.08
DISA STIG	APPL-26-000031
SRG	SRG-OS-000256-GPOS-00097, SRG-OS-000057-GPOS-00027, SRG-OS-000059-GPOS-00029, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000058-GPOS-00028
CIS Benchmark	3.5 (level 1)
CIS Controls v8	3.3
CMMC	AU.L2-3.3.8
CCI	CCI-000162, CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495
CCE	CCE-95102-0

12. System Settings

This section contains the configuration and enforcement of the settings within the macOS System Settings application.

Note: The check/fix commands outlined in this section *MUST* be run by a user with elevated privileges.

12.1 Ensure Location Services Is In the Menu Bar

`system_settings_location_services_menu_enforce`

DISCUSSION

Location Services menu item *MUST* be enabled.

REMEDIATION

```
/usr/bin/defaults write /Library/Preferences/com.apple.locationmenu.plist ShowSystemServices -bool true
```

REFERENCES

Framework	Values
CIS Benchmark	2.6.1.2 (level 2)
CIS Controls v8	4.1, 4.8
CCE	CCE-95385-1

12.2 Enforce macOS Updates are Automatically Installed

`system_settings_install_macos_updates_enforce`

DISCUSSION

Software Update *MUST* be configured to enforce automatic installation of macOS updates is enabled.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AutomaticallyInstallMacOSUpdates: true
  PayloadType: com.apple.SoftwareUpdate
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: AutomaticActions
ddm_value:
  InstallOSUpdates: AlwaysOn
declarationtype: com.apple.configuration.softwareupdate.settings
```

REFERENCES

Framework	Values
CIS Benchmark	1.3 (level 1)
CIS Controls v8	7.3, 7.4
CCE	CCE-95380-2

12.3 Enforce Session Lock After Screen Saver is Started

`system_settings_screensaver_ask_for_password_delay_enforce`

DISCUSSION

A screen saver *MUST* be enabled and the system *MUST* be configured to require a password to unlock once the screensaver has been on for a maximum of 5 seconds.

An unattended system with an excessive grace period is vulnerable to a malicious user.

CONFIGURATION PROFILE

```
- PayloadContent:
  - askForPasswordDelay: 5
  PayloadType: com.apple.screensaver
```

REFERENCES

Framework	Values
800-53r5	AC-11
800-171r3	03.01.10
DISA STIG	APPL-26-000003
SRG	SRG-OS-000028-GPOS-00009
CIS Benchmark	2.11.2 (level 1)
CIS Controls v8	4.7
CMMC	AC.L2-3.1.10
CCI	CCI-000056
CCE	CCE-95395-0

12.4 Ensure Time Machine Volumes are Encrypted

`system_settings_time_machine_encrypted_configure`

DISCUSSION

Time Machine volumes *MUST* be encrypted.

REFERENCES

Framework	Values
CIS Benchmark	2.3.4.2 (level 1)
CIS Controls v8	3.6, 3.11, 11.3
CCE	CCE-95410-7

12.5 Disable Guest Access to Shared SMB Folders

system_settings_guest_access_smb_disable

DISCUSSION

Guest access to shared Server Message Block (SMB) folders *MUST* be disabled.

Turning off guest access prevents anonymous users from accessing files shared via SMB.

REMEDIATION

```
/usr/sbin/sysadminctl -smbGuestAccess off
```

REFERENCES

Framework	Values
800-53r5	AC-2, AC-2(9)
800-171r3	03.01.01
CIS Benchmark	2.13.2 (level 1)
CIS Controls v8	3.3
CMMC	AC.L1-3.1.2
CCE	CCE-95373-7

12.6 Disable Printer Sharing

system_settings_printer_sharing_disable

DISCUSSION

Printer Sharing *MUST* be disabled.

REMEDIATION

```
/usr/sbin/cupsctl --no-share-printers
/usr/bin/lpstat -p | awk '{print $2}'| /usr/bin/xargs -I{} lpadmin -p {} -o printer-is-shared=false
```

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1)
800-171r3	03.04.06
DISA STIG	APPL-26-002240
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.3.3 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95391-9

12.7 Disable the Guest Account

`system_settings_guest_account_disable`

DISCUSSION

Guest access *MUST* be disabled.

Turning off guest access prevents anonymous users from accessing files.

CONFIGURATION PROFILE

```
- PayloadContent:
  - DisableGuestAccount: true
  - EnableGuestAccount: false
  PayloadType: com.apple.MCX
```

REFERENCES

Framework	Values
800-53r5	AC-2, AC-2(9)
800-171r3	03.01.01
DISA STIG	APPL-26-002063
SRG	SRG-OS-000364-GPOS-00151, SRG-OS-000480-GPOS-00228
CIS Benchmark	2.13.1 (level 1)
CIS Controls v8	5.2, 6.2, 6.8
CMMC	AC.L1-3.1.2
CCI	CCI-001813
CCE	CCE-95374-5

12.8 Enable Location Services

`system_settings_location_services_enable`

DISCUSSION

Location Services *MUST* be enabled.

REMEDIATION

```
/usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd LocationServicesEnabled -bool true;
pid=$(/bin/launchctl list | /usr/bin/awk '/com.apple.locationd/ { print $1 }')
kill -9 $pid
```

REFERENCES

Framework	Values
CIS Benchmark	2.6.1.1 (level 2)
CIS Controls v8	4.1, 4.8
CCE	CCE-95384-4

12.9 Require Administrator Password to Modify System-Wide Preferences

`system_settings_system_wide_preferences_configure`

DISCUSSION

The system *MUST* be configured to require an administrator password in order to modify the system-wide preferences in System Settings.

Some Preference Panes in System Settings contain settings that affect the entire system. Requiring a password to unlock these system-wide settings reduces the risk of a non-authorized user modifying system configurations.

REMEDIATION

```
authDBs=("system.preferences" "system.preferences.energysaver" "system.preferences.network" "system.preferenc
es.printing" "system.preferences.sharing" "system.preferences.softwareupdate" "system.preferences.startupdisk
" "system.preferences.timemachine")

for section in ${authDBs[@]}; do
  /usr/bin/security -q authorizationdb read "$section" > "/tmp/$section.plist"

  class_key_value=$(/usr/libexec/PlistBuddy -c "Print :class" "/tmp/$section.plist" 2>&1)
  if [[ "$class_key_value" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :class string user" "/tmp/$section.plist"
  else
    /usr/libexec/PlistBuddy -c "Set :class user" "/tmp/$section.plist"
  fi

  key_value=$(/usr/libexec/PlistBuddy -c "Print :shared" "/tmp/$section.plist" 2>&1)
  if [[ "$key_value" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :shared bool false" "/tmp/$section.plist"
  else
    /usr/libexec/PlistBuddy -c "Set :shared false" "/tmp/$section.plist"
  fi

  auth_user_key=$(/usr/libexec/PlistBuddy -c "Print :authenticate-user" "/tmp/$section.plist" 2>&1)
  if [[ "$auth_user_key" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :authenticate-user bool true" "/tmp/$section.plist"
  else
    /usr/libexec/PlistBuddy -c "Set :authenticate-user true" "/tmp/$section.plist"
  fi

  session_owner_key=$(/usr/libexec/PlistBuddy -c "Print :session-owner" "/tmp/$section.plist" 2>&1)
  if [[ "$session_owner_key" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :session-owner bool false" "/tmp/$section.plist"
  else
    /usr/libexec/PlistBuddy -c "Set :session-owner false" "/tmp/$section.plist"
  fi

  group_key=$(/usr/libexec/PlistBuddy -c "Print :group" "/tmp/$section.plist" 2>&1)
  if [[ "$group_key" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :group string admin" "/tmp/$section.plist"
  else
    /usr/libexec/PlistBuddy -c "Set :group admin" "/tmp/$section.plist"
  fi

  /usr/bin/security -q authorizationdb write "$section" < "/tmp/$section.plist"
done
```

REFERENCES

Framework	Values
800-53r5	AC-6, AC-6(1), AC-6(2)
800-171r3	03.01.07
DISA STIG	APPL-26-002069
SRG	SRG-OS-000324-GPOS-00125, SRG-OS-000480-GPOS-00228
CIS Benchmark	2.6.8 (level 1)
CIS Controls v8	4.1
CMMC	AC.L1-3.1.1, AC.L2-3.1.5, AC.L2-3.1.6
CCI	CCI-002235
CCE	CCE-95408-1

12.10 Disable Improve Search Information to Apple

`system_settings_improve_search_disable`

DISCUSSION

Sending data to Apple to help improve search *MUST* be disabled. This will disable "Improve Search" within Spotlight in System Settings.

The information system *MUST* be configured to provide only essential capabilities. Disabling the submission of search data will mitigate the risk of unwanted data being sent to Apple.

CONFIGURATION PROFILE

```
- PayloadContent:
  - Search Queries Data Sharing Status: 2
  PayloadType: com.apple.assistant.support
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-002024
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.9.1
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95378-6

12.11 Disable Server Message Block Sharing

`system_settings_smbd_disable`

DISCUSSION

Support for Server Message Block (SMB) file sharing is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities.

REMEDIATION

```
/bin/launchctl disable system/com.apple.smbd
```

REFERENCES

Framework	Values
800-53r5	AC-17, AC-3
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002001
SRG	SRG-OS-000080-GPOS-00048
CIS Benchmark	2.3.3.2 (level 1)
CIS Controls v8	4.1, 4.8, 5.4
CMMC	AC.L1-3.1.1
CCI	CCI-000213
CCE	CCE-95401-6

12.12 Secure Hot Corners

`system_settings_hot_corners_secure`

DISCUSSION

Hot corners *MUST* be secured.

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Although hot comers can be used to initiate a session lock or to launch useful applications, they can also be configured to disable an automatic session lock from initiating. Such a configuration introduces the risk that a user might forget to manually lock the screen before stepping away from the computer.

[NOTE] ==== The check and fix are for the last logged in user. To get the last logged in user, run the following. [source,bash] ---- CURRENT_USER=$(/usr/bin/defaults read /Library/Preferences/com.apple.loginwindow lastUserName) ---- ====

REMEDIATION

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults delete /Users/"$CURRENT_USER"/Library/Preferences/com.appl
e.dock wvous-bl-corner 2>/dev/null
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults delete /Users/"$CURRENT_USER"/Library/Preferences/com.appl
e.dock wvous-tl-corner 2>/dev/null
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults delete /Users/"$CURRENT_USER"/Library/Preferences/com.appl
e.dock wvous-tr-corner 2>/dev/null
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults delete /Users/"$CURRENT_USER"/Library/Preferences/com.appl
e.dock wvous-br-corner 2>/dev/null
```

REFERENCES

Framework	Values
800-53r5	AC-11(1)
800-171r3	03.01.10
CIS Benchmark	2.7.1 (level 1)
CIS Controls v8	4.3
CMMC	AC.L2-3.1.10
CCE	CCE-95376-0

12.13 Disable Remote Management

`system_settings_remote_management_disable`

DISCUSSION

Remote Management *MUST* be disabled.

REMEDIATION

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

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1)
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002250
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.3.5 (level 1)
CIS Controls v8	4.1, 4.8, 5.4
CMMC	CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95393-5

12.14 Configure Login Window to Prompt for Username and Password

`system_settings_loginwindow_prompt_username_password_enforce`

DISCUSSION

The login window *MUST* be configured to prompt all users for both a username and a password.

By default, the system displays a list of known users on the login window, which can make it easier for a malicious user to gain access to someone else's account. Requiring users to type in both their username and password mitigates the risk of unauthorized users gaining access to the information system.

CONFIGURATION PROFILE

```
- PayloadContent:
  - SHOWFULLNAME: true
  PayloadType: com.apple.loginwindow
```

REFERENCES

Framework	Values
800-53r5	IA-2
800-171r3	03.05.01
DISA STIG	APPL-26-005052
SRG	SRG-OS-000104-GPOS-00051
CIS Benchmark	2.11.4 (level 1)
CIS Controls v8	4.1
CMMC	IA.L1-3.5.1, IA.L1-3.5.2
CCI	CCI-000764
CCE	CCE-95387-7

12.15 Disable Personalized Advertising

`system_settings_personalized_advertising_disable`

DISCUSSION

Ad tracking and targeted ads *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling ad tracking ensures that applications and advertisers are unable to track users' interests and deliver targeted advertisements.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowApplePersonalizedAdvertising: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-002200
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.6.4 (level 1)
CIS Controls v8	4.8
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95390-1

12.16 Configure Time Machine for Automatic Backups

`system_settings_time_machine_auto_backup_enable`

DISCUSSION

Automatic backups *MUST* be enabled when using Time Machine.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AutoBackup: true
  PayloadType: com.apple.TimeMachine
```

REFERENCES

Framework	Values
CIS Benchmark	2.3.4.1 (level 2)
CIS Controls v8	11.2
CCE	CCE-95409-9

12.17 Disable Password Hints

`system_settings_password_hints_disable`

DISCUSSION

Password hints *MUST* be disabled.

Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

CONFIGURATION PROFILE

```
- PayloadContent:
  - RetriesUntilHint: 0
  PayloadType: com.apple.loginwindow
```

REFERENCES

Framework	Values
800-53r5	IA-6
800-171r3	03.05.11
DISA STIG	APPL-26-003012
SRG	SRG-OS-000079-GPOS-00047
CIS Benchmark	2.11.5 (level 1)
CIS Controls v8	4.1
CMMC	IA.L2-3.5.11
CCI	CCI-000206
CCE	CCE-95389-3

12.18 Disable Screen Sharing and Apple Remote Desktop

`system_settings_screen_sharing_disable`

DISCUSSION

Support for both Screen Sharing and Apple Remote Desktop (ARD) is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling screen sharing and ARD helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

REMEDIATION

```
/bin/launchctl disable system/com.apple.screensharing
```

REFERENCES

Framework	Values
800-53r5	AC-17, AC-3
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002050
SRG	SRG-OS-000080-GPOS-00048
CIS Benchmark	2.3.3.1 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.1
CCI	CCI-000213
CCE	CCE-95394-3

12.19 Disable External Intelligence Integrations

`system_settings_external_intelligence_disable`

DISCUSSION

Integration with external intelligence systems *MUST* be disabled unless approved by the organization. Disabling external intelligence integration will mitigate the risk of data being sent to unapproved third party.

The information system *MUST* be configured to provide only essential capabilities.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowExternalIntelligenceIntegrations: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: Enabled
ddm_value: false
declarationtype: com.apple.configuration.external-intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1)
800-171r3	03.01.20, 03.04.06
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.5.1.1 (level 1)
CIS Controls v8	4.1, 4.8, 15.3
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95365-3

12.20 Enforce Screen Saver Timeout

`system_settings_screensaver_timeout_enforce`

DISCUSSION

The screen saver timeout *MUST* be set to 900 seconds or a shorter length of time.

This rule ensures that a full session lock is triggered within no more than 900 seconds of inactivity.

CONFIGURATION PROFILE

```
- PayloadContent:
  - idleTime: 900
  PayloadType: com.apple.screensaver
```

REFERENCES

Framework	Values
800-53r5	AC-11, IA-11
800-171r3	03.01.10, 03.05.01
DISA STIG	APPL-26-000070
SRG	SRG-OS-000029-GPOS-00010
CIS Benchmark	2.11.1 (level 1)
CIS Controls v8	4.3
CMMC	AC.L2-3.1.10
CCI	CCI-000057
CCE	CCE-95397-6

12.21 Ensure Software Update is Updated and Current

`system_settings_softwareupdate_current`

DISCUSSION

Make sure Software Update is updated and current.

link:https://support.apple.com/en-us/108382[Update macOS on Mac] or if enrolled in an MDM consult your MDM's documentation for automated methods.

REMEDIATION

```
/usr/sbin/softwareupdate -i -a
```

REFERENCES

Framework	Values
800-53r5	SI-2
800-171r3	03.14.01, 03.14.02
DISA STIG	APPL-26-999999
SRG	SRG-OS-000439-GPOS-00195
CIS Benchmark	1.1 (level 1)
CIS Controls v8	7.3, 7.4
CMMC	SI.L1-3.14.1, SI.L1-3.14.2, SI.L1-3.14.4
CCI	CCI-002605
CCE	CCE-95405-7

12.22 Disable SSH Server for Remote Access Sessions

`system_settings_ssh_disable`

DISCUSSION

SSH service *MUST* be disabled for remote access.

REMEDIATION

```
/usr/sbin/systemsetup -f -setremotelogin off >/dev/null
/bin/launchctl disable system/com.openssh.sshd
```

REFERENCES

Framework	Values
800-53r5	AC-17, CM-7, CM-7(1)
800-171r3	03.01.02, 03.04.06
CIS Benchmark	2.3.3.4 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.1, CM.L2-3.4.6, CM.L2-3.4.7
CCE	CCE-95406-5

12.23 Enforce FileVault

`system_settings_filevault_enforce`

DISCUSSION

FileVault *MUST* be enforced.

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Note: See the FileVault supplemental to implement this rule.

CONFIGURATION PROFILE

```
- PayloadContent:
  - dontAllowFDEDisable: true
  PayloadType: com.apple.MCX
```

REFERENCES

Framework	Values
800-53r5	SC-28, SC-28(1)
800-171r3	03.13.08
DISA STIG	APPL-26-005020
SRG	SRG-OS-000185-GPOS-00079, SRG-OS-000405-GPOS-00184, SRG-OS-000404-GPOS-00183
CIS Benchmark	2.6.6 (level 1)
CIS Controls v8	3.6, 3.11
CMMC	SC.L2-3.13.16
CCI	CCI-001199, CCI-002475, CCI-002476
CCE	CCE-95367-9

12.24 Disable Content Caching Service

`system_settings_content_caching_disable`

DISCUSSION

Content caching *MUST* be disabled.

Content caching is a macOS service that helps reduce Internet data usage and speed up software installation on Mac computers. It is not recommended for devices furnished to employees to act as a caching server.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowContentCaching: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1)
800-171r3	03.04.06
DISA STIG	APPL-26-002140
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.3.8 (level 2)
CIS Controls v8	4.8
CMMC	CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95362-0

12.25 Disable Internet Sharing

`system_settings_internet_sharing_disable`

DISCUSSION

If the system does not require Internet sharing, support for it is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling Internet sharing helps prevent the unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

CONFIGURATION PROFILE

```
- PayloadContent:
  - forceInternetSharingOff: true
  PayloadType: com.apple.MCX
```

REFERENCES

Framework	Values
800-53r5	AC-20, AC-4
800-171r3	03.01.03, 03.01.20
DISA STIG	APPL-26-002007
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.3.7 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.20, AC.L2-3.1.3
CCI	CCI-000381
CCE	CCE-95382-8

12.26 Enable macOS Application Firewall

`system_settings_firewall_enable`

DISCUSSION

The macOS Application Firewall is the built-in firewall that comes with macOS, and it *MUST* be enabled.

When the macOS Application Firewall is enabled, the flow of information within the information system and between interconnected systems will be controlled by approved authorizations.

REMEDIATION

```
/usr/bin/defaults write /Library/Preferences/com.apple.alf globalstate -int 1
```

CONFIGURATION PROFILE

```
- PayloadContent:
  - EnableFirewall: true
  PayloadType: com.apple.security.firewall
```

REFERENCES

Framework	Values
800-53r5	AC-4, CM-7, CM-7(1), SC-7, SC-7(12)
800-171r3	03.01.03, 03.04.06, 03.13.01
DISA STIG	APPL-26-005050
SRG	SRG-OS-000480-GPOS-00232
CIS Benchmark	2.2.1 (level 1)
CIS Controls v8	4.1, 4.5, 13.1
CMMC	AC.L2-3.1.3, CM.L2-3.4.6, CM.L2-3.4.7, SC.L1-3.13.1
CCI	CCI-000366
CCE	CCE-95369-5

12.27 Enforce Software Update Downloads Updates Automatically

`system_settings_software_update_download_enforce`

DISCUSSION

Software Update *MUST* be configured to enforce automatic downloads of updates is enabled.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AutomaticDownload: true
  PayloadType: com.apple.SoftwareUpdate
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: AutomaticActions
ddm_value:
  Download: AlwaysOn
declarationtype: com.apple.configuration.softwareupdate.settings
```

REFERENCES

Framework	Values
CIS Benchmark	1.2 (level 1)
CIS Controls v8	7.3, 7.4
CCE	CCE-95403-2

12.28 Enforce Critical Security Updates to be Installed

`system_settings_critical_update_install_enforce`

DISCUSSION

Ensure that security updates are installed as soon as they are available from Apple.

CONFIGURATION PROFILE

```
- PayloadContent:
  - CriticalUpdateInstall: true
  PayloadType: com.apple.SoftwareUpdate
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: AutomaticActions
ddm_value:
  InstallSecurityUpdates: AlwaysOn
declarationtype: com.apple.configuration.softwareupdate.settings
```

REFERENCES

Framework	Values
800-53r5	SI-2
800-171r3	03.14.01
CIS Benchmark	1.5 (level 1)
CIS Controls v8	7.3, 7.4, 7.7
CMMC	SI.L1-3.14.1, SI.L1-3.14.4
CCE	CCE-95363-8

12.29 Disable Siri

system_settings_siri_disable

DISCUSSION

Support for Siri is non-essential and *MUST* be disabled to prevent organizational data from being synchronized to Apple servers.

Apple's Siri service does not provide an organization with enough control over the storage and access of data, and, therefore, automated synchronization *MUST* be controlled by an organization approved service.

The information system *MUST* be configured to provide only essential capabilities.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowAssistant: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: Enabled
ddm_value: false
declarationtype: com.apple.configuration.siri.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06, 03.04.08
DISA STIG	APPL-26-002020
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.5.2.1 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-B.1.III, AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381, CCI-001774
CCE	CCE-95398-4

12.30 Disable Bluetooth Sharing

system_settings_bluetooth_sharing_disable

DISCUSSION

Bluetooth Sharing *MUST* be disabled.

Bluetooth Sharing allows users to wirelessly transmit files between the macOS and Bluetooth-enabled devices, including personally owned cellphones and tablets. A malicious user might introduce viruses or malware onto the system or extract sensitive files via Bluetooth Sharing. When Bluetooth Sharing is disabled, this risk is mitigated.

[NOTE] ==== The check and fix are for the last logged in user. To get the last logged in user, run the following. [source,bash] ---- CURRENT_USER=$(/usr/bin/defaults read /Library/Preferences/com.apple.loginwindow lastUserName) ---- ====

REMEDIATION

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost write com.apple.Bluetooth PrefKeyServicesEnabled -bool false
```

REFERENCES

Framework	Values
800-53r5	AC-18(4), AC-3, CM-7, CM-7(1)
800-171r3	03.04.06
DISA STIG	APPL-26-002110
SRG	SRG-OS-000080-GPOS-00048, SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.3.10 (level 1)
CIS Controls v8	3.3, 4.1
CMMC	AC.L1-3.1.1, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000213, CCI-000381
CCE	CCE-95361-2

12.31 Ensure Wake for Network Access Is Disabled

`system_settings_wake_network_access_disable`

DISCUSSION

Wake for network access *MUST* be disabled.

REMEDIATION

```
/usr/bin/pmset -a womp 0
```

REFERENCES

Framework	Values
CIS Benchmark	2.10.3 (level 1)
CIS Controls v8	4.8
CCE	CCE-95417-2

12.32 Disable Sending Diagnostic and Usage Data to Apple

`system_settings_diagnostics_reports_disable`

DISCUSSION

The ability to submit diagnostic data to Apple *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling the submission of diagnostic and usage information will mitigate the risk of unwanted data being sent to Apple.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AutoSubmit: false
  PayloadType: com.apple.SubmitDiagInfo
- PayloadContent:
  - allowDiagnosticSubmission: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	AC-20, SC-7(10), SI-11
800-171r3	03.01.20
DISA STIG	APPL-26-002021
SRG	SRG-OS-000206-GPOS-00084, SRG-OS-000205-GPOS-00083
CIS Benchmark	2.6.3.1 (level 1), 2.6.3.4 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.20
CCI	CCI-001312, CCI-001314
CCE	CCE-95364-6

12.33 Disable Improve Siri and Dictation Information to Apple

`system_settings_improve_siri_dictation_disable`

DISCUSSION

The ability for Apple to store and review audio of your Siri and Dictation interactions *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling the submission of Siri and Dictation information will mitigate the risk of unwanted data being sent to Apple.

CONFIGURATION PROFILE

```
- PayloadContent:
  - Siri Data Sharing Opt-In Status: 2
  PayloadType: com.apple.assistant.support
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-002210
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.6.3.2 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381

CCE	CCE-95379-4

12.34 Configure Login Window to Show A Custom Message

`system_settings_loginwindow_loginwindowtext_enable`

DISCUSSION

The login window *MUST* be configured to show a custom access warning message.

CONFIGURATION PROFILE

```
- PayloadContent:
  - LoginwindowText: Center for Internet Security Test Message
  PayloadType: com.apple.loginwindow
```

REFERENCES

Framework	Values
CIS Benchmark	2.11.3 (level 1)
CIS Controls v8	4.1
CCE	CCE-95386-9

12.35 Disable Unattended or Automatic Logon to the System

`system_settings_automatic_login_disable`

DISCUSSION

Automatic logon *MUST* be disabled.

When automatic logons are enabled, the default user account is automatically logged on at boot time without prompting the user for a password. Even if the screen is later locked, a malicious user would be able to reboot the computer and find it already logged in. Disabling automatic logons mitigates this risk.

CONFIGURATION PROFILE

```
- PayloadContent:
  - com.apple.login.mcx.DisableAutoLoginClient: true
  PayloadType: com.apple.loginwindow
```

REFERENCES

Framework	Values
800-53r5	IA-2, IA-5(13)
800-171r3	03.05.01
DISA STIG	APPL-26-002066
SRG	SRG-OS-000480-GPOS-00229, SRG-OS-000104-GPOS-00051, SRG-OS-000480-GPOS-00228
CIS Benchmark	2.13.3 (level 1)
CIS Controls v8	4.7
CMMC	IA.L1-3.5.1, IA.L1-3.5.2

CCI	CCI-000366
CCE	CCE-95356-2

12.36 Disable External Intelligence Integration Sign In

`system_settings_external_intelligence_sign_in_disable`

DISCUSSION

The ability to sign into an external intelligence systems *MUST* be disabled unless approved by the organization. Disabling external intelligence integration will mitigate the risk of data being sent to unapproved third party.

The information system *MUST* be configured to provide only essential capabilities.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowExternalIntelligenceIntegrationsSignIn: false
  PayloadType: com.apple.applicationaccess
```

DECLARATIVE DEVICE MANAGEMENT

```
ddm_key: AllowSignIn
ddm_value: false
declarationtype: com.apple.configuration.external-intelligence.settings
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1)
800-171r3	03.01.20, 03.04.06
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.5.1.1 (level 1)
CIS Controls v8	4.1, 4.8, 15.3
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95366-1

12.37 Disable Sending Audio Recordings and Transcripts to Apple

`system_settings_improve_assistive_voice_disable`

DISCUSSION

The ability for Apple to store and review audio of your audio recordings and transcripts of your vocal shortcuts and voice control interactions *MUST* be disabled. This will disable "Improve Assistive Voice Features" in Privacy & Security within System Settings.

The information system *MUST* be configured to provide only essential capabilities. Disabling the submission of this information will mitigate the risk of unwanted data being sent to Apple.

CONFIGURATION PROFILE

```
- PayloadContent:
  - AXSAudioDonationSiriImprovementEnabled: false
  PayloadType: com.apple.Accessibility
```

REFERENCES

Framework	Values
800-53r5	AC-20, CM-7, CM-7(1), SC-7(10)
800-171r3	03.01.20, 03.04.06
DISA STIG	APPL-26-002023
SRG	SRG-OS-000095-GPOS-00049
CIS Benchmark	2.6.3.3 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.20, CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381
CCE	CCE-95377-8

12.38 Enforce macOS Time Synchronization

`system_settings_time_server_enforce`

DISCUSSION

Time synchronization *MUST* be enforced on all networked systems.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

CONFIGURATION PROFILE

```
- PayloadContent:
  - com.apple.timed:
      TMAutomaticTimeOnlyEnabled: true
  PayloadType: com.apple.ManagedClient.preferences
```

REFERENCES

Framework	Values
800-53r5	AU-12(1), SC-45(1)
800-171r3	03.03.07
DISA STIG	APPL-26-000014
SRG	SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144
CIS Benchmark	2.3.2.1 (level 1)
CIS Controls v8	8.4
CMMC	AU.L2-3.3.7
CCI	CCI-001891, CCI-002046, CCI-004923, CCI-004926, CCI-004922
CCE	CCE-95412-3

12.39 Enforce Screen Saver Password

`system_settings_screensaver_password_enforce`

DISCUSSION

Users *MUST* authenticate when unlocking the screen saver.

The screen saver acts as a session lock and prevents unauthorized users from accessing the current user's account.

CONFIGURATION PROFILE

```
- PayloadContent:
  - askForPassword: true
  PayloadType: com.apple.screensaver
```

REFERENCES

Framework	Values
800-53r5	AC-11
800-171r3	03.01.10, 03.05.01
DISA STIG	APPL-26-000002
SRG	SRG-OS-000028-GPOS-00009
CIS Benchmark	2.11.2 (level 1)
CIS Controls v8	4.7
CMMC	AC.L2-3.1.10
CCI	CCI-000056
CCE	CCE-95396-8

12.40 Configure macOS to Use an Authorized Time Server

`system_settings_time_server_configure`

DISCUSSION

Approved time server *MUST* be the only server configured for use.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Note: As of macOS 10.13 only one time server is supported.

CONFIGURATION PROFILE

```
- PayloadContent:
  - timeServer: time.apple.com
  PayloadType: com.apple.MCX
```

REFERENCES

Framework	Values
800-53r5	AU-12(1), SC-45(1)
800-171r3	03.03.07
DISA STIG	APPL-26-000170
SRG	SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144
CIS Benchmark	2.3.2.1 (level 1)
CIS Controls v8	8.4
CMMC	AU.L2-3.3.7
CCI	CCI-001891, CCI-002046, CCI-004923, CCI-004923, CCI-004926, CCI-004926
CCE	CCE-95411-5

12.41 Disable Media Sharing

`system_settings_media_sharing_disabled`

DISCUSSION

Media sharing *MUST* be disabled.

When Media Sharing is enabled, the computer starts a network listening service that shares the contents of the user's music collection with other users in the same subnet.

The information system *MUST* be configured to provide only essential capabilities. Disabling Media Sharing helps prevent the unauthorized connection of devices and the unauthorized transfer of information. Disabling Media Sharing mitigates this risk.

Note: On macOS versions prior to 15, the Media Sharing settings panel may still allow you to check "Home Sharing" and "Share media with guests," but the service itself will not be activated.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowMediaSharing: false
  - allowMediaSharingModification: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	AC-17, AC-3
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002100
SRG	SRG-OS-000080-GPOS-00048
CIS Benchmark	2.3.3.9 (level 2)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.1
CCI	CCI-000213
CCE	CCE-95388-5

12.42 Disable Airplay Receiver

`system_settings_airplay_receiver_disable`

DISCUSSION

Airplay Receiver allows you to send content from another Apple device to be displayed on the screen as it's being played from your other device.

Support for Airplay Receiver is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities.

CONFIGURATION PROFILE

```
- PayloadContent:
  - allowAirPlayIncomingRequests: false
  PayloadType: com.apple.applicationaccess
```

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1)
800-171r3	03.04.06
DISA STIG	APPL-26-002080
SRG	SRG-OS-000300-GPOS-00118, SRG-OS-000095-GPOS-00049
CIS Benchmark	2.3.1.2 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	CM.L2-3.4.6, CM.L2-3.4.7
CCI	CCI-000381, CCI-001443
CCE	CCE-95354-7

12.43 Disable Remote Apple Events

`system_settings_rae_disable`

DISCUSSION

If the system does not require Remote Apple Events, support for Apple Remote Events is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling Remote Apple Events helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

REMEDIATION

```
/usr/sbin/systemsetup -setremoteappleevents off
/bin/launchctl disable system/com.apple.AEServer
```

REFERENCES

Framework	Values
800-53r5	AC-17, AC-3
800-171r3	03.01.02, 03.04.06
DISA STIG	APPL-26-002022
SRG	SRG-OS-000080-GPOS-00048, SRG-OS-000096-GPOS-00050
CIS Benchmark	2.3.3.6 (level 1)
CIS Controls v8	4.1, 4.8
CMMC	AC.L1-3.1.1
CCI	CCI-000213, CCI-000382
CCE	CCE-95392-7

12.44 Enable Firewall Stealth Mode

`system_settings_firewall_stealth_mode_enable`

DISCUSSION

Firewall Stealth Mode *MUST* be enabled.

When stealth mode is enabled, the Mac will not respond to any probing requests, and only requests from authorized applications will still be authorized.

[IMPORTANT] ==== Enabling firewall stealth mode may prevent certain remote mechanisms used for maintenance and compliance scanning from properly functioning. Information System Security Officers (ISSOs) are advised to first fully weigh the potential risks posed to their organization before opting not to enable stealth mode. ====

REMEDIATION

```
/usr/bin/defaults write /Library/Preferences/com.apple.alf stealthenabled -int 1
```

CONFIGURATION PROFILE

```
- PayloadContent:
  - EnableStealthMode: true
  - EnableFirewall: true
  PayloadType: com.apple.security.firewall
```

REFERENCES

Framework	Values
800-53r5	CM-7, CM-7(1), SC-7, SC-7(16)
800-171r3	03.04.06, 03.13.01
CIS Benchmark	2.2.2 (level 1)
CIS Controls v8	4.1, 4.5, 4.8
CMMC	CM.L2-3.4.6, CM.L2-3.4.7, SC.L1-3.13.1
CCE	CCE-95370-3

Quick Reference

Complete listing of all rules in this baseline for quick lookup. Click any rule ID to jump to its details.

Rule ID	Title	Section
icloud_sync_disable	Disable iCloud Desktop and Document Folder Sync	iCloud
os_safari_warn_fraudulent_website_enable	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	Operating System
os_power_nap_disable	Disable Power Nap	Operating System
os_root_disable	Disable Root Login	Operating System
os_notes_transcription_disable	Disable Apple Intelligence Notes Transcription	Operating System
os_anti_virus_installed	Must Use an Approved Antivirus Program	Operating System
os_world_writable_system_folder_configure	Ensure No World Writable Files Exist in the System Folder	Operating System
os_internal_apfs_volumes_encrypted	Ensure All Internal User Storage APFS Volumes Are Encrypted	Operating System
os_safari_open_safe_downloads_disable	Disable Automatic Opening of Safe Files in Safari	Operating System
os_mail_summary_disable	Disable Apple Intelligence Mail Summary	Operating System
os_external_apfs_hfs_volumes_encrypted	Ensure All APFS and HFS+ External User Storage Volumes Are Encrypted	Operating System
os_notes_transcription_summary_disable	Disable Apple Intelligence Notes Transcription Summary	Operating System
os_authenticated_root_enable	Enable Authenticated Root	Operating System
os_safari_advertising_privacy_protection_enable	Ensure Advertising Privacy Protection in Safari Is Enabled	Operating System
os_config_data_install_enforce	Enforce Installation of XProtect Remediator and Gatekeeper Updates Automatically	Operating System
os_guest_folder_removed	Remove Guest Folder if Present	Operating System
os_sleep_and_display_sleep_apple_silicon_enable	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	Operating System
os_password_hint_remove	Remove Password Hint From User Accounts	Operating System
os_software_update_app_update_enforce	Enforce Software Update App Update Updates Automatically	Operating System
os_sudo_log_enforce	Configure Sudo To Log Events	Operating System
os_policy_banner_loginwindow_enforce	Display Policy Banner at Login Window	Operating System
os_writing_tools_disable	Disable Apple Intelligence Writing Tools	Operating System
os_sudoers_timestamp_type_configure	Configure Sudoers Timestamp Type	Operating System
os_nfsd_disable	Disable Network File System Service	Operating System
os_httpd_disable	Disable the Built-in Web Server	Operating System
os_airdrop_disable	Disable AirDrop	Operating System
os_safari_show_full_website_address_enable	Ensure Show Full Website Address in Safari Is Enabled	Operating System
os_mobile_file_integrity_enable	Enable Apple Mobile File Integrity	Operating System
os_sip_enable	Ensure System Integrity Protection is Enabled	Operating System
os_terminal_secure_keyboard_enable	Ensure Secure Keyboard Entry Terminal.app is Enabled	Operating System
os_gatekeeper_enable	Enable Gatekeeper	Operating System

os_world_writable_library_folder_configure	Ensure No World Writable Files Exist in the Library Folder	Operating System
os_time_server_enabled	Enable Time Synchronization Daemon	Operating System
os_sudo_timeout_configure	Configure Sudo Timeout Period to 0	Operating System
os_system_wide_applications_configure	Ensure Appropriate Permissions Are Enabled for System Wide Applications	Operating System
os_software_update_deferral	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	Operating System
os_home_folders_secure	Secure User's Home Folders	Operating System
os_install_log_retention_configure	Configure Install.log Retention to 365	Operating System
os_on_device_dictation_enforce	Enforce On Device Dictation	Operating System
os_safari_prevent_cross-site_tracking_enable	Ensure Prevent Cross-site Tracking in Safari Is Enabled	Operating System
os_bonjour_disable	Disable Bonjour Multicast	Operating System
os_unlock_active_user_session_disable	Disable Login to Other User's Active and Locked Sessions	Operating System
os_safari_show_status_bar_enabled	Ensure Show Safari shows the Status Bar is Enabled	Operating System
pwpolicy_custom_regex_enforce	Require Passwords to Match the Defined Custom Regular Expression	Password Policy
pwpolicy_max_lifetime_enforce	Restrict Maximum Password Lifetime to 365 Days	Password Policy
pwpolicy_history_enforce	Prohibit Password Reuse for a Minimum of 24 Generations	Password Policy
pwpolicy_account_lockout_enforce	Limit Consecutive Failed Login Attempts to 5	Password Policy
pwpolicy_special_character_enforce	Require Passwords Contain a Minimum of One Special Character	Password Policy
pwpolicy_account_lockout_timeout_enforce	Set Account Lockout Time to 15 Minutes	Password Policy
pwpolicy_alpha_numeric_enforce	Require Passwords Contain a Minimum of One Numeric Character	Password Policy
pwpolicy_minimum_length_enforce	Require a Minimum Password Length of 15 Characters	Password Policy
supplemental_cis_manual	CIS Manual Recommendations	Supplemental
audit_flags_fm_failed_configure	Configure System to Audit All Failed Change of Object Attributes	Audit
audit_folder_group_configure	Configure Audit Log Folders Group to Wheel	Audit
audit_control_mode_configure	Configure Audit_Control Owner to Mode 440 or Less Permissive	Audit
audit_flags_aa_configure	Configure System to Audit All Authorization and Authentication Events	Audit
audit_flags_ad_configure	Configure System to Audit All Administrative Action Events	Audit
audit_flags_ex_configure	Configure System to Audit All Failed Program Execution on the System	Audit
audit_auditd_enabled	Enable Security Auditing	Audit
audit_files_owner_configure	Configure Audit Log Files to be Owned by Root	Audit
audit_files_mode_configure	Configure Audit Log Files to Mode 440 or Less Permissive	Audit
audit_control_owner_configure	Configure Audit_Control Owner to Root	Audit
audit_folder_owner_configure	Configure Audit Log Folders to be Owned by Root	Audit
audit_flags_fr_configure	Configure System to Audit All Failed Read Actions on the System	Audit
audit_flags_fw_configure	Configure System to Audit All Failed Write Actions on the System	Audit
audit_retention_configure	Configure Audit Retention to 60d OR 5G	Audit
audit_control_acls_configure	Configure Audit_Control to Not Contain Access Control Lists	Audit
audit_folders_mode_configure	Configure Audit Log Folders to Mode 700 or Less Permissive	Audit
audit_flags_lo_configure	Configure System to Audit All Log In and Log Out Events	Audit

audit_control_group_configure	Configure Audit_Control Group to Wheel	Audit
audit_files_group_configure	Configure Audit Log Files Group to Wheel	Audit
audit_acls_files_configure	Configure Audit Log Files to Not Contain Access Control Lists	Audit
audit_acls_folders_configure	Configure Audit Log Folder to Not Contain Access Control Lists	Audit
system_settings_location_services_menu_enforce	Ensure Location Services Is In the Menu Bar	System Settings
system_settings_install_macos_updates_enforce	Enforce macOS Updates are Automatically Installed	System Settings
system_settings_screensaver_ask_for_password_delay_enforce	Enforce Session Lock After Screen Saver is Started	System Settings
system_settings_time_machine_encrypted_configure	Ensure Time Machine Volumes are Encrypted	System Settings
system_settings_guest_access_smb_disable	Disable Guest Access to Shared SMB Folders	System Settings
system_settings_printer_sharing_disable	Disable Printer Sharing	System Settings
system_settings_guest_account_disable	Disable the Guest Account	System Settings
system_settings_location_services_enable	Enable Location Services	System Settings
system_settings_system_wide_preferences_configure	Require Administrator Password to Modify System-Wide Preferences	System Settings
system_settings_improve_search_disable	Disable Improve Search Information to Apple	System Settings
system_settings_smbd_disable	Disable Server Message Block Sharing	System Settings
system_settings_hot_corners_secure	Secure Hot Corners	System Settings
system_settings_remote_management_disable	Disable Remote Management	System Settings
system_settings_loginwindow_prompt_username_password_enforce	Configure Login Window to Prompt for Username and Password	System Settings
system_settings_personalized_advertising_disable	Disable Personalized Advertising	System Settings
system_settings_time_machine_auto_backup_enable	Configure Time Machine for Automatic Backups	System Settings
system_settings_password_hints_disable	Disable Password Hints	System Settings
system_settings_screen_sharing_disable	Disable Screen Sharing and Apple Remote Desktop	System Settings
system_settings_external_intelligence_disable	Disable External Intelligence Integrations	System Settings
system_settings_screensaver_timeout_enforce	Enforce Screen Saver Timeout	System Settings
system_settings_softwareupdate_current	Ensure Software Update is Updated and Current	System Settings
system_settings_ssh_disable	Disable SSH Server for Remote Access Sessions	System Settings
system_settings_filevault_enforce	Enforce FileVault	System Settings
system_settings_content_caching_disable	Disable Content Caching Service	System Settings
system_settings_internet_sharing_disable	Disable Internet Sharing	System Settings
system_settings_firewall_enable	Enable macOS Application Firewall	System Settings
system_settings_software_update_download_enforce	Enforce Software Update Downloads Updates Automatically	System Settings
system_settings_critical_update_install_enforce	Enforce Critical Security Updates to be Installed	System Settings
system_settings_siri_disable	Disable Siri	System Settings

system_settings_bluetooth_sharing_disable	Disable Bluetooth Sharing	System Settings
system_settings_wake_network_access_disable	Ensure Wake for Network Access Is Disabled	System Settings
system_settings_diagnostics_reports_disable	Disable Sending Diagnostic and Usage Data to Apple	System Settings
system_settings_improve_siri_dictation_disable	Disable Improve Siri and Dictation Information to Apple	System Settings
system_settings_loginwindow_loginwindowtext_enable	Configure Login Window to Show A Custom Message	System Settings
system_settings_automatic_login_disable	Disable Unattended or Automatic Logon to the System	System Settings
system_settings_external_intelligence_sign_in_disable	Disable External Intelligence Integration Sign In	System Settings
system_settings_improve_assistive_voice_disable	Disable Sending Audio Recordings and Transcripts to Apple	System Settings
system_settings_time_server_enforce	Enforce macOS Time Synchronization	System Settings
system_settings_screensaver_password_enforce	Enforce Screen Saver Password	System Settings
system_settings_time_server_configure	Configure macOS to Use an Authorized Time Server	System Settings
system_settings_media_sharing_disabled	Disable Media Sharing	System Settings
system_settings_airplay_receiver_disable	Disable Airplay Receiver	System Settings
system_settings_rae_disable	Disable Remote Apple Events	System Settings
system_settings_firewall_stealth_mode_enable	Enable Firewall Stealth Mode	System Settings

John Doe, Example Organization

Generated by M.A.C.E.

(macOS Advanced Compliance Editor)

Document generated on August 9, 2026