



macOS Security Compliance

macOS 15.0

***Security Configuration - CIS Apple macOS 15.0 Sequoia
v1.0.0 Benchmark (Level 2)***

Sequoia Guidance, Revision 1.1 (2024-12-16)

Table of Contents

1. Foreword	1
2. Scope	2
3. Authors	3
4. Acronyms and Definitions	4
5. Applicable Documents	6
5.1. Government Documents	6
5.2. Non-Government Documents	6
6. Auditing	7
6.1. Configure Audit Log Files to Not Contain Access Control Lists	7
6.2. Configure Audit Log Folder to Not Contain Access Control Lists	8
6.3. Enable Security Auditing	8
6.4. Configure Audit_Control to Not Contain Access Control Lists	10
6.5. Configure Audit_Control Group to Wheel	10
6.6. Configure Audit_Control Owner to Mode 440 or Less Permissive	11
6.7. Configure Audit_Control Owner to Root	12
6.8. Configure Audit Log Files Group to Wheel	12
6.9. Configure Audit Log Files to Mode 440 or Less Permissive	13
6.10. Configure Audit Log Files to be Owned by Root	14
6.11. Configure System to Audit All Authorization and Authentication Events	15
6.12. Configure System to Audit All Administrative Action Events	16
6.13. Configure System to Audit All Failed Program Execution on the System	17
6.14. Configure System to Audit All Failed Change of Object Attributes	18
6.15. Configure System to Audit All Failed Read Actions on the System	19
6.16. Configure System to Audit All Failed Write Actions on the System	20
6.17. Configure System to Audit All Log In and Log Out Events	21
6.18. Configure Audit Log Folders Group to Wheel	22
6.19. Configure Audit Log Folders to be Owned by Root	23
6.20. Configure Audit Log Folders to Mode 700 or Less Permissive	24
6.21. Configure Audit Retention to 60d OR 5G	25
7. iCloud	26
7.1. Disable iCloud Desktop and Document Folder Sync	26
8. macOS	28
8.1. Disable AirDrop	28
8.2. Must Use an Approved Antivirus Program	29
8.3. Enable Authenticated Root	29
8.4. Disable Bonjour Multicast	30
8.5. Enforce Installation of XProtect Remediator and Gatekeeper Updates Automatically	31
8.6. Enable Gatekeeper	32

8.7. Remove Guest Folder if Present	33
8.8. Secure User's Home Folders	34
8.9. Disable the Built-in Web Server	35
8.10. Configure Install.log Retention to 365	35
8.11. Disable iPhone Mirroring	36
8.12. Enforce Enrollment in Mobile Device Management	37
8.13. Enable Apple Mobile File Integrity	38
8.14. Disable Network File System Service	39
8.15. Enforce On Device Dictation	40
8.16. Remove Password Hint From User Accounts	40
8.17. Display Policy Banner at Login Window	41
8.18. Disable Power Nap	42
8.19. Disable Root Login	43
8.20. Ensure Advertising Privacy Protection in Safari Is Enabled	44
8.21. Disable Automatic Opening of Safe Files in Safari	45
8.22. Ensure Prevent Cross-site Tracking in Safari Is Enabled	45
8.23. Ensure Show Full Website Address in Safari Is Enabled	46
8.24. Ensure Show Safari shows the Status Bar is Enabled	47
8.25. Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	48
8.26. Enable Show All Filename Extensions	49
8.27. Ensure System Integrity Protection is Enabled	49
8.28. Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	51
8.29. Ensure Software Update Deferment Is Less Than or Equal to 30 Days	52
8.30. Configure Sudo To Log Events	53
8.31. Configure Sudo Timeout Period to 0	53
8.32. Configure Sudoers Timestamp Type	54
8.33. Ensure Appropriate Permissions Are Enabled for System Wide Applications	55
8.34. Ensure Secure Keyboard Entry Terminal.app is Enabled	56
8.35. Enable Time Synchronization Daemon	56
8.36. Disable Login to Other User's Active and Locked Sessions	57
8.37. Ensure No World Writable Files Exist in the Library Folder	58
8.38. Ensure No World Writable Files Exist in the System Folder	59
9. Password Policy	61
9.1. Limit Consecutive Failed Login Attempts to 5	61
9.2. Set Account Lockout Time to 15 Minutes	62
9.3. Require Passwords Contain a Minimum of One Numeric Character	63
9.4. Require Passwords to Match the Defined Custom Regular Expression	64
9.5. Prohibit Password Reuse for a Minimum of 15 Generations	65
9.6. Restrict Maximum Password Lifetime to 365 Days	66
9.7. Require a Minimum Password Length of 15 Characters	67
9.8. Require Passwords Contain a Minimum of One Special Character	68

10. System Settings	70
10.1. Disable Airplay Receiver	70
10.2. Disable Unattended or Automatic Logon to the System	71
10.3. Enable Bluetooth Menu	72
10.4. Disable Bluetooth Sharing	73
10.5. Disable Content Caching Service	74
10.6. Enforce Critical Security Updates to be Installed	74
10.7. Disable Sending Diagnostic and Usage Data to Apple	75
10.8. Enforce FileVault	76
10.9. Enable macOS Application Firewall	77
10.10. Enable Firewall Stealth Mode	78
10.11. Disable Guest Access to Shared SMB Folders	79
10.12. Disable the Guest Account	80
10.13. Secure Hot Corners	81
10.14. Disable Sending Audio Recordings and Transcripts to Apple	82
10.15. Disable Improve Siri and Dictation Information to Apple	83
10.16. Enforce macOS Updates are Automatically Installed	84
10.17. Disable Internet Sharing	85
10.18. Enable Location Services	86
10.19. Ensure Location Services Is In the Menu Bar	87
10.20. Configure Login Window to Show A Custom Message	87
10.21. Configure Login Window to Prompt for Username and Password	88
10.22. Disable Media Sharing	89
10.23. Disable Password Hints	90
10.24. Disable Personalized Advertising	91
10.25. Disable Printer Sharing	92
10.26. Disable Remote Apple Events	92
10.27. Disable Remote Management	93
10.28. Disable Screen Sharing and Apple Remote Desktop	94
10.29. Enforce Session Lock After Screen Saver is Started	95
10.30. Enforce Screen Saver Timeout	96
10.31. Ensure Siri Listen For is Disabled	97
10.32. Disable Server Message Block Sharing	98
10.33. Enforce Software Update App Update Updates Automatically	98
10.34. Enforce Software Update Downloads Updates Automatically	99
10.35. Enforce Software Update Automatically	100
10.36. Ensure Software Update is Updated and Current	101
10.37. Disable SSH Server for Remote Access Sessions	102
10.38. Require Administrator Password to Modify System-Wide Preferences	103
10.39. Configure Time Machine for Automatic Backups	105
10.40. Ensure Time Machine Volumes are Encrypted	106

10.41. Configure macOS to Use an Authorized Time Server	107
10.42. Enforce macOS Time Synchronization	107
10.43. Ensure Wake for Network Access Is Disabled	108
10.44. Enable Wifi Menu	109
11. Supplemental	111
11.1. CIS Manual Recommendations	111
11.2. FileVault Supplemental	112
11.3. Password Policy Supplemental	113

Chapter 1. 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.

Chapter 2. Scope

This guide describes the actions to take when securing a macOS 15.0 system against the CIS Apple macOS 15.0 Sequoia v1.0.0 Benchmark (Level 2) security baseline.

Chapter 3. Authors

macOS Security Compliance Project

The CIS Benchmarks are referenced with the permission and support of the Center for Internet Security® (CIS®)

Edward Byrd	Center for Internet Security
Ron Colvin	Center for Internet Security
Allen Golbig	Jamf

Chapter 4. Acronyms and Definitions

Table 1. Acronyms and Abbreviations

AES	Advanced Encryption Standard
ABM	Apple Business Manager
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
DISA	Defense Information Systems Agency
DMA	Direct Memory Access
FISMA	Federal Information Security Modernization Act
FPKI	Federal Public Key Infrastructure
IR	Infrared
ISO	Information System Owner
ISSO	Information System Security Officer
MDM	Mobile Device Management
NASA	National Aeronautics and Space Administration
NFS	Network File System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSF	Online Certificate Status Protocol
ODV	Organization Defined Values
OS	Operating System
PF	Packet Filter
PIV	Personal Identity Verification
PIV-M	Personal Identity Verification Mandatory
PKI	Public Key Infrastructure
RBD	Risk Based Decision

SIP	System Integrity Protection
SMB	Server Message Block
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide
UAMDM	User Approved MDM
UUCP	Unix-to-Unix Copy Protocol

Table 2. Definitions

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.

Chapter 5. Applicable Documents

5.1. Government Documents

Table 3. National Institute of Standards and Technology (NIST)

Document Number or Descriptor	Document Title
NIST Special Publication 800-53 Rev 5	<i>NIST Special Publication 800-53 Rev 5.1.1</i>
NIST Special Publication 800-63	<i>NIST Special Publication 800-63</i>
NIST Special Publication 800-171	<i>NIST Special Publication 800-171 Rev 3</i>
NIST Special Publication 800-219	<i>NIST Special Publication 800-219 Rev 1</i>

Table 4. Defense Information Systems Agency (DISA)

Document Number or Descriptor	Document Title
STIG Ver 1, Rel 1	<i>Apple macOS 15 (Sequoia) STIG</i>

Table 5. Cybersecurity Maturity Model Certification (CMMC)

Document Number or Descriptor	Document Title
CMMC Model Overview v2.0	<i>Cybersecurity Maturity Model Certification (CMMC) Model Overview v2.0</i>

Table 6. Committee on National Security Systems (CNSS)

Document Number or Descriptor	Document Title
CNSSI No. 1253	<i>Security Categorization and Control Selection for National Security Systems</i>

5.2. Non-Government Documents

Table 7. Apple

Document Number or Descriptor	Document Title
Apple Platform Security Guide	<i>Apple Platform Security</i>
Apple Platform Deployment	<i>Apple Platform Deployment</i>
Apple Platform Certifications	<i>Apple Platform Certifications</i>
Profile-Specific Payload Keys	<i>Profile-Specific Payload Keys</i>

Table 8. Center for Internet Security

Document Number or Descriptor	Document Title
Apple macOS 14.0	<i>CIS Apple macOS 14.0 Benchmark version 1.1.0</i>

Chapter 6. Auditing

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



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



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

6.1. Configure Audit Log Files to Not Contain Access Control Lists

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.

To check the state of the system, run the following command(s):

```
/bin/ls -le $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":"
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_acls_files_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94101-3

6.2. Configure Audit Log Folder to Not Contain Access Control Lists

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.

To check the state of the system, run the following command(s):

```
/bin/ls -lde /var/audit | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":"
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/bin/chmod -N /var/audit
```

ID	audit_acls_folders_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94102-1

6.3. Enable Security Auditing

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.



Security auditing is NOT enabled by default on macOS Sequoia.

To check the state of the system, run the following command(s):

```
LAUNCHD_RUNNING=$(/bin/launchctl list | /usr/bin/grep -c com.apple.auditd)
AUDITD_RUNNING=$(/usr/sbin/audit -c | /usr/bin/grep -c "AUC_AUDITING")
if [[ $LAUNCHD_RUNNING == 1 ]] && [[ -e /etc/security/audit_control ]] && [[
$AUDITD_RUNNING == 1 ]]; then
    echo "pass"
else
    echo "fail"
fi
```

If the result is not **pass**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
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
```

ID	audit_auditd_enabled	
References	800-53r5	<ul style="list-style-type: none">• AU-12, AU-12(1), AU-12(3)• AU-14(1)• AU-3, AU-3(1)• AU-8• CM-5(1)• MA-4(1)
	CIS Benchmark	<ul style="list-style-type: none">• 3.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.2• 8.5
	CCE	<ul style="list-style-type: none">• CCE-94104-7

6.4. Configure Audit_Control to Not Contain Access Control Lists

/etc/security/audit_control *MUST* not contain Access Control Lists (ACLs).

To check the state of the system, run the following command(s):

```
/bin/ls -le /etc/security/audit_control | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":",
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_control_acls_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94106-2

6.5. Configure Audit_Control Group to Wheel

/etc/security/audit_control *MUST* have the group set to wheel.

To check the state of the system, run the following command(s):

```
/bin/ls -dn /etc/security/audit_control | /usr/bin/awk '{print $4}'
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_control_group_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94107-0

6.6. Configure Audit_Control Owner to Mode 440 or Less Permissive

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

To check the state of the system, run the following command(s):

```
/bin/ls -l /etc/security/audit_control | /usr/bin/awk '!/-r--[r-]-----  
|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_control_mode_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94108-8

6.7. Configure Audit_Control Owner to Root

/etc/security/audit_control *MUST* have the owner set to root.

To check the state of the system, run the following command(s):

```
/bin/ls -dn /etc/security/audit_control | /usr/bin/awk '{print $3}'
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_control_owner_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94109-6

6.8. Configure Audit Log Files Group to Wheel

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.

To check the state of the system, run the following command(s):

```
/bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$4} END {print s}'
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_files_group_configure	
References	800-53r5	• AU-9
	CIS Benchmark	• 3.5 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94112-0

6.9. Configure Audit Log Files to Mode 440 or Less Permissive

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.

To check the state of the system, run the following command(s):

```
/bin/ls -l $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '!/--r-----|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_files_mode_configure
----	----------------------------

References	800-53r5	<ul style="list-style-type: none">• AU-9
	CIS Benchmark	<ul style="list-style-type: none">• 3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94113-8

6.10. Configure Audit Log Files to be Owned by Root

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.

To check the state of the system, run the following command(s):

```
/bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$3} END {print s}'
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_files_owner_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-9
	CIS Benchmark	<ul style="list-style-type: none">• 3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94114-6

6.11. Configure System to Audit All Authorization and Authentication Events

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).

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr
',' '\n' | /usr/bin/grep -Ec 'aa'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	audit_flags_aa_configure	
References	800-53r5	<ul style="list-style-type: none">AC-2(12)AU-12AU-2CM-5(1)MA-4(1)
	CIS Benchmark	<ul style="list-style-type: none">3.2 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">3.148.28.5
	CCE	<ul style="list-style-type: none">CCE-94115-3

6.12. Configure System to Audit All Administrative Action Events

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.



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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr
',' '\n' | /usr/bin/grep -Ec 'ad'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	audit_flags_ad_configure
----	--------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-2(12), AC-2(4) • AC-6(9) • AU-12 • AU-2 • CM-5(1) • MA-4(1)
	CIS Benchmark	<ul style="list-style-type: none"> • 3.2 (level 2)
	CIS Controls V8	<ul style="list-style-type: none"> • 3.14 • 8.2 • 8.5
	CCE	<ul style="list-style-type: none"> • CCE-94116-1

6.13. Configure System to Audit All Failed Program Execution on the System

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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr
',' '\n' | /usr/bin/grep -Ec '\-ex'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	audit_flags_ex_configure	
References	800-53r5 <ul style="list-style-type: none"> • AC-2(12) • AU-12 • AU-2 • CM-5(1) • 3.2 (level 2) 	
	CIS Benchmark	
	CIS Controls V8	<ul style="list-style-type: none"> • 3.14 • 8.2 • 8.5
	CCE	<ul style="list-style-type: none"> • CCE-94117-9

6.14. Configure System to Audit All Failed Change of Object Attributes

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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr
',' '\n' | /usr/bin/grep -Ec '\-fm'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	audit_flags_fm_failed_configure	
References	800-53r5	<ul style="list-style-type: none">• AC-2(12)• AU-12• AU-2• AU-9• CM-5(1)• MA-4(1)
	CIS Benchmark	<ul style="list-style-type: none">• 3.2 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 3.14• 8.2• 8.5
	CCE	<ul style="list-style-type: none">• CCE-94120-3

6.15. Configure System to Audit All Failed Read Actions on the System

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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' ' /^flags/ { print $NF } ' /etc/security/audit_control | /usr/bin/tr ', ' '\n' | /usr/bin/grep -Ec '\-fr'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:


```
/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
```

ID	audit_flags_fr_configure	
References	800-53r5	<ul style="list-style-type: none"> • AC-2(12) • AU-12 • AU-2 • AU-9 • CM-5(1) • MA-4(1)
	CIS Benchmark	<ul style="list-style-type: none"> • 3.2 (level 2)
	CIS Controls V8	<ul style="list-style-type: none"> • 3.14 • 8.2 • 8.5
	CCE	<ul style="list-style-type: none"> • CCE-94121-1

6.16. Configure System to Audit All Failed Write Actions on the System

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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr
',' '\n' | /usr/bin/grep -Ec '\-fw'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	audit_flags_fw_configure	
References	<div><div>800-53r5</div><div>CIS Benchmark</div><div>CIS Controls V8</div><div>CCE</div></div>	<div><ul style="list-style-type: none">• AC-2(12)• AU-12• AU-2• AU-9• CM-5(1)• MA-4(1)• 3.2 (level 2)</div> <div><ul style="list-style-type: none">• 3.14• 8.2• 8.5</div> <div><ul style="list-style-type: none">• CCE-94122-9</div>

6.17. Configure System to Audit All Log In and Log Out Events

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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr  
' ,' '\n' | /usr/bin/grep -Ec '^lo'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	audit_flags_lo_configure	
References	800-53r5	<ul style="list-style-type: none">• AC-17(1)• AC-2(12)• AU-12• AU-2• MA-4(1)
	CIS Benchmark	<ul style="list-style-type: none">• 3.2 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 3.14• 8.2• 8.5
	CCE	<ul style="list-style-type: none">• CCE-94123-7

6.18. Configure Audit Log Folders Group to Wheel

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.

To check the state of the system, run the following command(s):

```
/bin/ls -dn $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $4}'
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_folder_group_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-9
	CIS Benchmark	<ul style="list-style-type: none">• 3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94124-5

6.19. Configure Audit Log Folders to be Owned by Root

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.

To check the state of the system, run the following command(s):

```
/bin/ls -dn $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $3}'
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_folder_owner_configure
-----------	------------------------------

References	800-53r5	<ul style="list-style-type: none">• AU-9
	CIS Benchmark	<ul style="list-style-type: none">• 3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94125-2

6.20. Configure Audit Log Folders to Mode 700 or Less Permissive

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.

To check the state of the system, run the following command(s):

```
/usr/bin/stat -f %A $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

If the result is not 700, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_folders_mode_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-9
	CIS Benchmark	<ul style="list-style-type: none">• 3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94126-0

6.21. Configure Audit Retention to 60d OR 5G

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.

To check the state of the system, run the following command(s):

```
/usr/bin/awk -F: '/expire-after/{print $2}' /etc/security/audit_control
```

If the result is not **60d OR 5G**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	audit_retention_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-11• AU-4
	CIS Benchmark	<ul style="list-style-type: none">• 3.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.1• 8.3
	CCE	<ul style="list-style-type: none">• CCE-94130-2

Chapter 7. iCloud

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



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

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudDesktopAndDocuments').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowCloudDesktopAndDocuments</key>
<false/>
```

ID	icloud_sync_disable
----	---------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	CIS Benchmark	<ul style="list-style-type: none"> • 2.1.1.3 (level 2)
	CIS Controls V8	<ul style="list-style-type: none"> • 4.1 • 4.8 • 15.3
	CCE	<ul style="list-style-type: none"> • CCE-94153-4

Chapter 8. macOS

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



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

8.1. Disable AirDrop

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirDrop').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowAirDrop</key>
<false/>
```

ID	os_airdrop_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• AC-3• CM-7, CM-7(1)• 2.3.1.1 (level 1)
	CIS Benchmark	
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8• 6.7
	CCE	<ul style="list-style-type: none">• CCE-94156-7

8.2. Must Use an Approved Antivirus Program

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.'

To check the state of the system, run the following command(s):


```
/usr/bin/xprotect status | /usr/bin/grep -cE "(launch scans: enabled|background scans: enabled)"
```

If the result is not 2, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```



These services cannot be unloaded or loaded while System Integrity Protection (SIP) is enabled.

ID	os_anti_virus_installed	
References	800-53r5	<ul style="list-style-type: none">N/A
	CIS Benchmark	<ul style="list-style-type: none">5.10 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">10.510.110.2
	CCE	<ul style="list-style-type: none">CCE-94158-3

8.3. Enable Authenticated Root

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.



Authenticated Root is enabled by default on macOS systems.



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

To check the state of the system, run the following command(s):

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c
"AuthenticatedRootVolumeEnabled = 1;"
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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



To re-enable "Authenticated Root", boot the affected system into "Recovery" mode, launch "Terminal" from the "Utilities" menu, and run the command.

ID	os_authenticated_root_enable	
References	800-53r5	<ul style="list-style-type: none">• AC-3• CM-5• MA-4(1)• SC-34• SI-7, SI-7(6)
	CIS Benchmark	<ul style="list-style-type: none">• 5.1.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.6• 3.11
	CCE	<ul style="list-style-type: none">• CCE-94164-1

8.4. Disable Bonjour Multicast

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mDNSResponder')\
.objectForKey('NoMulticastAdvertisements').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mDNSResponder) payload type:

```
<key>NoMulticastAdvertisements</key>
<true/>
```

ID	os_bonjour_disable	
References	800-53r5	• CM-7, CM-7(1)
	CIS Benchmark	• 4.1 (level 2)
	CIS Controls V8	• 4.1
	CCE	• 4.8
		• CCE-94169-0

8.5. Enforce Installation of XProtect Remediator and Gatekeeper Updates Automatically

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.

<https://support.apple.com/en-us/HT207005>



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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('ConfigDataInstall').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>ConfigDataInstall</key>
<true/>
```

ID	os_config_data_install_enforce	
References	800-53r5	<ul style="list-style-type: none">• SI-2(5)• SI-3
	CIS Benchmark	<ul style="list-style-type: none">• 1.6 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4• 7.7
	CCE	<ul style="list-style-type: none">• CCE-94176-5

8.6. Enable Gatekeeper

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.systempolicy.control')\
.objectForKey('EnableAssessment').js
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.systempolicy.control) payload type:

```
<key>EnableAssessment</key>
<true/>
```

ID	os_gatekeeper_enable	
References	800-53r5	<ul style="list-style-type: none">• CM-14• CM-5• SI-3• SI-7(1), SI-7(15)
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 10.1• 10.2• 10.5
	CCE	<ul style="list-style-type: none">• CCE-94195-5

8.7. Remove Guest Folder if Present

The guest folder *MUST* be deleted if present.

To check the state of the system, run the following command(s):

```
/bin/ls /Users/ | /usr/bin/grep -c "Guest"
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_guest_folder_removed	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 5.9 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1
	CCE	<ul style="list-style-type: none">• CCE-94198-9

8.8. Secure User's Home Folders

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.

To check the state of the system, run the following command(s):

```
/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" | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
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
```

ID	os_home_folders_secure
----	------------------------

References	800-53r5	<ul style="list-style-type: none">• AC-6
	CIS Benchmark	<ul style="list-style-type: none">• 5.1.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94204-5

8.9. Disable the Built-in Web Server

The built-in web server is a non-essential service built into macOS and *MUST* be disabled.



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

To check the state of the system, run the following command(s):

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"org.apache.httpd" => disabled'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/bin/launchctl disable system/org.apache.httpd
```

ID	os_httpd_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 4.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94205-2

8.10. Configure Install.log Retention to 365

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.

To check the state of the system, run the following command(s):


```
/usr/sbin/aslmanager -dd 2>&1 | /usr/bin/awk '/\/var\/log\/install.log$/ {count++}
/Processing module com.apple.install/,/Finished/ { for (i=1;i<=NR;i++) { if ($i ==
"TTL" && $(i+2) >= 365) { ttl="True" }; if ($i == "MAX") {max="True"}}} END{if (count
> 1) { print "Multiple config files for /var/log/install, manually remove the extra
files"} else if (max == "True") { print "all_max setting is configured, must be
removed" } if (ttl != "True") { print "TTL not configured" } else { print "Yes" }}}
```

If the result is not **Yes**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```



If there are multiple configuration files in /etc/asl that are set to process the file /var/log/install.log, these files will have to be manually removed.

ID	os_install_log_retention_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-11• AU-4
	CIS Benchmark	<ul style="list-style-type: none">• 3.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.1• 8.3
	CCE	<ul style="list-style-type: none">• CCE-94212-8

8.11. Disable iPhone Mirroring

iPhone Mirroring *MUST* be disabled to prevent file transfers to or from unauthorized devices. Disabling iPhone Mirroring also prevents potentially unauthorized applications from appearing as if they are installed on the Mac.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\n
```

```
.objectForKey('allowiPhoneMirroring').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowiPhoneMirroring</key>
<false/>
```

ID	os_iphone_mirroring_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• AC-3• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.1.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8• 6.7
	CCE	<ul style="list-style-type: none">• CCE-94213-6

8.12. Enforce Enrollment in Mobile Device Management

You *MUST* enroll your Mac in a Mobile Device Management (MDM) software.

User Approved MDM (UAMDM) enrollment or enrollment via Apple Business Manager (ABM)/Apple School Manager (ASM) is required to manage certain security settings. Currently these include:

- Allowed Kernel Extensions
- Allowed Approved System Extensions
- Privacy Preferences Policy Control Payload
- ExtensibleSingleSignOn
- FDEFileVault

In macOS 11, UAMDM grants Supervised status on a Mac, unlocking the following MDM features, which were previously locked behind ABM:

- Activation Lock Bypass
- Access to Bootstrap Tokens
- Scheduling Software Updates
- Query list and delete local users

To check the state of the system, run the following command(s):

```
/usr/bin/profiles status -type enrollment | /usr/bin/awk -F: '/MDM enrollment/ {print $2}' | /usr/bin/grep -c "Yes (User Approved)"
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Ensure that system is enrolled via UAMDM.

ID	os_mdm_require	
References	800-53r5	<ul style="list-style-type: none">• CM-2• CM-6
	CIS Benchmark	<ul style="list-style-type: none">• 1.8 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 5.1
	CCE	<ul style="list-style-type: none">• CCE-94227-6

8.13. Enable Apple Mobile File Integrity

Mobile file integrity *MUST* be enabled.

To check the state of the system, run the following command(s):

```
/usr/sbin/nvram -p | /usr/bin/grep -c "amfi_get_out_of_my_way=1"
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_mobile_file_integrity_enable	
References	800-53r5	<ul style="list-style-type: none">N/A
	CIS Benchmark	<ul style="list-style-type: none">5.1.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">2.32.6
	CCE	<ul style="list-style-type: none">CCE-94231-8

8.14. Disable Network File System Service

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

To check the state of the system, run the following command(s):

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.nfsd" => disabled'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

The system may need to be restarted for the update to take effect.

ID	os_nfsd_disable	
References	800-53r5	<ul style="list-style-type: none">AC-17AC-3
	CIS Benchmark	<ul style="list-style-type: none">4.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">4.14.8
	CCE	<ul style="list-style-type: none">CCE-94235-9

8.15. Enforce On Device Dictation

Dictation *MUST* be restricted to on device only to prevent potential data exfiltration.

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('forceOnDeviceOnlyDictation').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>forceOnDeviceOnlyDictation</key>
<true/>
```

ID	os_on_device_dictation_enforce	
References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7, CM-7(1)• SC-7(10)
	CIS Benchmark	<ul style="list-style-type: none">• 2.18.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94245-8

8.16. Remove Password Hint From User Accounts

User accounts *MUST* not contain password hints.

To check the state of the system, run the following command(s):

```
HINT=$( /usr/bin/dscl . -list /Users hint | /usr/bin/awk '{ print $2 }' )
```

```
if [ -z "$HINT" ]; then
  echo "PASS"
else
  echo "FAIL"
fi
```

If the result is not **PASS**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
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
```

ID	os_password_hint_remove	
References	800-53r5	• IA-6
	CIS Benchmark	• 2.11.1 (level 1)
	CIS Controls V8	• 5.2
	CCE	• CCE-94248-2

8.17. Display Policy Banner at Login Window

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.rtf.d" exists in the "/Library/Security" folder.

The banner text of the document *MUST* read:

```
Center for Internet Security Test Message
```

To check the state of the system, run the following command(s):

```
/bin/ls -ld /Library/Security/PolicyBanner.rtf* | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_policy_banner_loginwindow_enforce	
References	800-53r5	• AC-8
	CIS Benchmark	• 5.8 (level 2)
	CIS Controls V8	• 4.1
	CCE	• CCE-94254-0

8.18. Disable Power Nap

Power Nap *MUST* be disabled.



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)

To check the state of the system, run the following command(s):

```
/usr/bin/pmset -g custom | /usr/bin/awk '/powernap/ { sum+=$2 } END {print sum}'
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_power_nap_disable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.9.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94257-3

8.19. Disable Root Login

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.

To check the state of the system, run the following command(s):

```
/usr/bin/dscl . -read /Users/root UserShell 2>&1 | /usr/bin/grep -c "/usr/bin/false"
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:


```
/usr/bin/dscl . -create /Users/root UserShell /usr/bin/false
```

ID	os_root_disable	
References	800-53r5	• IA-2, IA-2(5)
	CIS Benchmark	• 5.6 (level 1)
	CIS Controls V8	• 5.4
	CCE	• CCE-94279-7

8.20. Ensure Advertising Privacy Protection in Safari Is Enabled

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

To check the state of the system, run the following command(s):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c  
'"WebKitPreferences.privateClickMeasurementEnabled" = 1' | /usr/bin/awk '{ if ($1 >=  
1) {print "1"} else {print "0"}}'
```

If the result is not **1**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Safari) payload type:

```
<key>WebKitPreferences.privateClickMeasurementEnabled</key>  
<true/>
```

ID	os_safari_advertising_privacy_protection_enable
----	---

References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 6.3.6 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 9.1
	CCE	<ul style="list-style-type: none">• CCE-94280-5

8.21. Disable Automatic Opening of Safe Files in Safari

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

To check the state of the system, run the following command(s):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'AutoOpenSafeDownloads = 0' |  
/usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print "0"}}'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Safari) payload type:

```
<key>AutoOpenSafeDownloads</key>  
<false/>
```

ID	os_safari_open_safe_downloads_disable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 6.3.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 9.1• 9.6
	CCE	<ul style="list-style-type: none">• CCE-94281-3

8.22. Ensure Prevent Cross-site Tracking in Safari Is Enabled

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

To check the state of the system, run the following command(s):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -cE
'"WebKitPreferences.storageBlockingPolicy" = 1|"WebKitStorageBlockingPolicy" =
1|"BlockStoragePolicy" =2' | /usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print
"0"}}'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Safari) payload type:

```
<key>WebKitPreferences.storageBlockingPolicy</key>
<integer>1</integer>
<key>WebKitStorageBlockingPolicy</key>
<integer>1</integer>
<key>BlockStoragePolicy</key>
<integer>2</integer>
```

ID	os_safari_prevent_cross-site_tracking_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 6.3.4 (level 1)
	CIS Controls V8	• 9.1
		• 9.3
	CCE	• CCE-94282-1

8.23. Ensure Show Full Website Address in Safari Is Enabled

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

To check the state of the system, run the following command(s):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'ShowFullURLInSmartSearchField = 1'
| /usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print "0"}}'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Safari) payload type:

```
<key>ShowFullURLInSmartSearchField</key>
<true/>
```

ID	os_safari_show_full_website_address_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 6.3.7 (level 1)
	CIS Controls V8	• 9.1
	CCE	• CCE-94283-9

8.24. Ensure Show Safari shows the Status Bar is Enabled

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

To check the state of the system, run the following command(s):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'ShowOverlayStatusBar = 1' |
/usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print "0"}}'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Safari) payload type:

```
<key>ShowOverlayStatusBar</key>
<true/>
```

ID	os_safari_show_status_bar_enabled	
References	800-53r5	<ul style="list-style-type: none"> • N/A
	CIS Benchmark	<ul style="list-style-type: none"> • 6.3.10 (level 1)
	CIS Controls V8	<ul style="list-style-type: none"> • 9.1
	CCE	<ul style="list-style-type: none"> • CCE-94284-7

8.25. Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled

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

To check the state of the system, run the following command(s):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'WarnAboutFraudulentWebsites = 1' |
/usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print "0"}}'
```

If the result is not **1**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Safari) payload type:

```
<key>WarnAboutFraudulentWebsites</key>
<true/>
```

ID	os_safari_warn_fraudulent_website_enable	
References	800-53r5	<ul style="list-style-type: none"> • N/A
	CIS Benchmark	<ul style="list-style-type: none"> • 6.3.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none"> • 9.1 • 9.3
	CCE	<ul style="list-style-type: none"> • CCE-94285-4

8.26. Enable Show All Filename Extensions

Show all filename extensions *MUST* be enabled in the Finder.



The check and fix are for the currently logged in user. To get the currently logged in user, run the following.

```
CURRENT_USER=$( /usr/sbin/scutil <<< "show State:/Users/ConsoleUser" |
/usr/bin/awk '/Name :/ && ! /loginwindow/ { print $3 }' )
```

To check the state of the system, run the following command(s):

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults read .GlobalPreferences
AppleShowAllExtensions 2>/dev/null
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults write /Users/"$CURRENT_USER"
"/Library/Preferences/.GlobalPreferences AppleShowAllExtensions -bool true
```

ID	os_show_filename_extensions_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 6.1.1 (level 1)
	CIS Controls V8	• 2.3
	CCE	• CCE-94293-8

8.27. Ensure System Integrity Protection is Enabled

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.



SIP is enabled by default in macOS.

To check the state of the system, run the following command(s):

```
/usr/bin/csrutil status | /usr/bin/grep -c 'System Integrity Protection status: enabled.'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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



To reenale "System Integrity Protection", boot the affected system into "Recovery" mode, launch "Terminal" from the "Utilities" menu, and run the command.

ID	os_sip_enable	
References	800-53r5	<ul style="list-style-type: none">• AC-3• AU-9, AU-9(3)• CM-5, CM-5(6)• SC-4• SI-2• SI-7
	CIS Benchmark	<ul style="list-style-type: none">• 5.1.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 2.3• 2.6• 10.5
	CCE	<ul style="list-style-type: none">• CCE-94294-6

8.28. Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices

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.

To check the state of the system, run the following command(s):

```
error_count=0
if /usr/sbin/ioreg -rd1 -c IOPlatformExpertDevice 2>&1 | /usr/bin/grep -q "MacBook";
then
    sleepMode=$(/usr/bin/pmset -b -g | /usr/bin/grep '^s*sleep' 2>&1 | /usr/bin/awk
'{print $2}')
    displaysleepMode=$(/usr/bin/pmset -b -g | /usr/bin/grep displaysleep 2>&1 |
/usr/bin/awk '{print $2}')

    if [[ "$sleepMode" == "" ]] || [[ "$sleepMode" -gt 15 ]]; then
        ((error_count++))
    fi
    if [[ "$displaysleepMode" == "" ]] || [[ "$displaysleepMode" -gt 10 ]] || [[
"$displaysleepMode" -gt "$sleepMode" ]]; then
        ((error_count++))
    fi
fi
echo "$error_count"
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_sleep_and_display_sleep_apple_silicon_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 2.9.1.2 (level 2)
	CIS Controls V8	• 4.1
	CCE	• CCE-94200-3

8.29. Ensure Software Update Deferral Is Less Than or Equal to 30 Days

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let timeout = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('enforcedSoftwareUpdateDelay')) || 0
  if ( timeout <= 30 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>enforcedSoftwareUpdateDelay</key>
<integer>30</integer>
```

ID	os_software_update_deferral	
References	800-53r5	• N/A
	CIS Benchmark	• 1.7 (level 1)
	CIS Controls V8	• 7.3 • 7.4
	CCE	• CCE-94298-7

8.30. Configure Sudo To Log Events

Sudo *MUST* be configured to log privilege escalation.

To check the state of the system, run the following command(s):

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Log when a command is allowed by sudoers"
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_sudo_log_enforce	
References	800-53r5	<ul style="list-style-type: none">AC-6(9)
	CIS Benchmark	<ul style="list-style-type: none">5.11 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">N/A
	CCE	<ul style="list-style-type: none">CCE-94310-0

8.31. Configure Sudo Timeout Period to 0

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

To check the state of the system, run the following command(s):

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Authentication timestamp timeout: 0.0 minutes"
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_sudo_timeout_configure	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 5.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.3
	CCE	<ul style="list-style-type: none">• CCE-94311-8

8.32. Configure Sudoers Timestamp Type

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.

To check the state of the system, run the following command(s):

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/awk -F": " '/Type of authentication  
timestamp record/{print $2}'
```

If the result is not `tty`, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_sudoers_timestamp_type_configure
----	-------------------------------------

References	800-53r5	<ul style="list-style-type: none">• CM-5(1)• IA-11
	CIS Benchmark	<ul style="list-style-type: none">• 5.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.3
	CCE	<ul style="list-style-type: none">• CCE-94312-6

8.33. Ensure Appropriate Permissions Are Enabled for System Wide Applications

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

To check the state of the system, run the following command(s):

```
/usr/bin/find /Applications -iname "*\.app" -type d -perm -2 -ls | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	os_system_wide_applications_configure	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 5.1.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.3
	CCE	<ul style="list-style-type: none">• CCE-94314-2

8.34. Ensure Secure Keyboard Entry Terminal.app is Enabled

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Terminal')\
.objectForKey('SecureKeyboardEntry').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Terminal) payload type:

```
<key>SecureKeyboardEntry</key>
<true/>
```

ID	os_terminal_secure_keyboard_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 6.4.1 (level 1)
	CIS Controls V8	• 4.8
	CCE	• CCE-94315-9

8.35. Enable Time Synchronization Daemon

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



The time synchronization daemon is enabled by default on macOS.

To check the state of the system, run the following command(s):


```
/bin/launchctl list | /usr/bin/grep -c com.apple.timed
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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




The service `timed` cannot be unloaded or loaded while System Integrity Protection (SIP) is enabled.

ID	os_time_server_enabled	
References	800-53r5	<ul style="list-style-type: none">• AU-12(1)• SC-45(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.2.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.4
	CCE	<ul style="list-style-type: none">• CCE-94319-1

8.36. Disable Login to Other User’s Active and Locked Sessions

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.



Configuring this setting will change the user experience and disable TouchID from unlocking the screensaver. To restore the user experience and allow TouchID to unlock the screensaver, you can run `/usr/bin/sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow screenUnlockMode -int 1`. This setting can also be deployed with a configuration profile.

To check the state of the system, run the following command(s):

```
/usr/bin/security authorizationdb read system.login.screensaver 2>&1 | /usr/bin/grep
```

```
-c '<string>authenticate-session-owner</string>'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/usr/bin/security authorizationdb write system.login.screensaver "authenticate-session-owner"
```

ID	os_unlock_active_user_session_disable	
References	800-53r5	• IA-2, IA-2(5)
	CIS Benchmark	• 5.7 (level 1)
	CIS Controls V8	• 4.3
	CCE	• CCE-94322-5

8.37. Ensure No World Writable Files Exist in the Library Folder

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



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.

To check the state of the system, run the following command(s):

```
/usr/bin/find /System/Volumes/Data/Library -type d -perm -2 -ls 2>&1 | /usr/bin/grep -v Caches | /usr/bin/grep -v /Preferences/Audio/Data | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
IFS=$'\n'
for libPermissions in $( /usr/bin/find /System/Volumes/Data/Library -type d -perm
```

```
-2 2>&1 | /usr/bin/grep -v Caches | /usr/bin/grep -v /Preferences/Audio/Data ); do  
/bin/chmod -R o-w "$libPermissions"  
done
```

ID	os_world_writable_library_folder_configure	
References	800-53r5	• N/A
	CIS Benchmark	• 5.1.7 (level 2)
	CIS Controls V8	• 3.3
	CCE	• CCE-94326-6

8.38. Ensure No World Writable Files Exist in the System Folder

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

To check the state of the system, run the following command(s):

```
/usr/bin/find /System/Volumes/Data/System -type d -perm -2 -ls | /usr/bin/grep -vE  
"downloadDir|locks" | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
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
```

ID	os_world_writable_system_folder_configure
----	---

References	800-53r5	<ul style="list-style-type: none"> • N/A
	CIS Benchmark	<ul style="list-style-type: none"> • 5.1.6 (level 1)
	CIS Controls V8	<ul style="list-style-type: none"> • 3.3
	CCE	<ul style="list-style-type: none"> • CCE-94327-4

Chapter 9. Password Policy

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



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



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.



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. Limit Consecutive Failed Login Attempts to 5

The macOS *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 account *MUST* be locked for a period of time after.

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

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |  
/usr/bin/xmllint --xpath  
'//dict/key[text()="policyAttributeMaximumFailedAuthentications"]/following-  
sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1 <= 5) {print "yes"} else {print  
"no"}}' | /usr/bin/uniq
```

If the result is not **yes**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>maxFailedAttempts</key>
```

```
<integer>5</integer>
```

ID	pwpolicy_account_lockout_enforce	
References	800-53r5	• AC-7
	CIS Benchmark	• 5.2.1 (level 1)
	CIS Controls V8	• 6.2
	CCE	• CCE-94331-6

9.2. Set Account Lockout Time to 15 Minutes

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.

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |  
/usr/bin/xmllint --xpath '//dict/key[text()="autoEnableInSeconds"]/following-  
sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1/60 >= 15 ) {print "yes"} else  
{print "no"}}' | /usr/bin/uniq
```

If the result is not **yes**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>minutesUntilFailedLoginReset</key>  
<integer>15</integer>
```

ID	pwpolicy_account_lockout_timeout_enforce
----	--

References	800-53r5	<ul style="list-style-type: none">• AC-7
	CIS Benchmark	<ul style="list-style-type: none">• 5.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 6.2
	CCE	<ul style="list-style-type: none">• CCE-94332-4

9.3. Require Passwords Contain a Minimum of One Numeric Character

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.



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.

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |  
/usr/bin/xmllint --xpath '//dict/key[text()="policyIdentifier"]/following-  
sibling::*[1]/text()' - | /usr/bin/grep "requireAlphanumeric" -c
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>requireAlphanumeric</key>  
<true/>
```

ID	pwpolicy_alpha_numeric_enforce	
References	800-53r5 <ul style="list-style-type: none"> • IA-5(1) 	
	CIS Benchmark <ul style="list-style-type: none"> • 5.2.3 (level 2) • 5.2.4 (level 2) 	
	CIS Controls V8 <ul style="list-style-type: none"> • 5.2 	
	CCE <ul style="list-style-type: none"> • CCE-94333-2 	

9.4. Require Passwords to Match the Defined Custom Regular Expression

The macOS *MUST* be configured to meet complexity requirements defined in `^(?=.*[A-Z])(?=.*[a-z])(?=.*[0-9]).$`.

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



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.



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

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |
/usr/bin/xmllint --xpath 'boolean(//*[contains(text(),"policyAttributePassword matches
'\'^(?=.*[A-Z])(?=.*[a-z])(?=.*[0-9]).*$\'\'"])]' -
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```

<key>customRegex</key>
<dict>
  <key>passwordContentRegex</key>
  <string>^(?=.*[A-Z])(?=.*[a-z])(?=.*[0-9]).*$</string>
  <key>passwordContentDescription</key>
  <dict>
    <key>default</key>
    <string>Password must match custom regex.</string>
  </dict>
</dict>

```

ID	pwpolicy_custom_regex_enforce	
References	800-53r5	<ul style="list-style-type: none"> • IA-5(1)
	CIS Benchmark	<ul style="list-style-type: none"> • 5.2.6 (level 2)
	CIS Controls V8	<ul style="list-style-type: none"> • 5.2
	CCE	<ul style="list-style-type: none"> • CCE-94334-0

9.5. Prohibit Password Reuse for a Minimum of 15 Generations

The macOS *MUST* be configured to enforce a password history of at least 15 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 15 previous password generations.

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



The guidance for password based authentication in 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.

To check the state of the system, run the following command(s):

```

/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |
/usr/bin/xmllint --xpath
'//dict/key[text()="policyAttributePasswordHistoryDepth"]/following-
sibling::*[1]/text()' - | /usr/bin/awk '{ if ($1 >= 15 ) {print "yes"} else {print
"no"}}' | /usr/bin/uniq

```

If the result is not **yes**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>pinHistory</key>
<integer>15</integer>
```

ID	pwpolicy_history_enforce	
References	800-53r5	• IA-5(1)
	CIS Benchmark	• 5.2.8 (level 1)
	CIS Controls V8	• 5.2
	CCE	• CCE-94337-3

9.6. Restrict Maximum Password Lifetime to 365 Days

The macOS *MUST* be configured to enforce a maximum password lifetime limit of at least 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.



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.

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |
/usr/bin/xmllint --xpath
'//dict/key[text()="policyAttributeExpiresEveryNDays"]/following-sibling:.*[1]/text()'
-
```

If the result is not 365, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>maxPINAgeInDays</key>
<integer>365</integer>
```

ID	pwpolicy_max_lifetime_enforce	
References	800-53r5	• IA-5
	CIS Benchmark	• 5.2.7 (level 1)
	CIS Controls V8	• 5.3
	CCE	• CCE-94339-9

9.7. Require a Minimum Password Length of 15 Characters

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.



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.

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |
/usr/bin/xmllint --xpath 'boolean(//*[contains(text(),"policyAttributePassword matches
```



```
'\'.{15,}'\'''))]' -
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>minLength</key>
<integer>15</integer>
```

ID	pwpolicy_minimum_length_enforce	
References	800-53r5	• IA-5(1)
	CIS Benchmark	• 5.2.2 (level 1)
	CIS Controls V8	• 5.2
	CCE	• CCE-94340-7

9.8. Require Passwords Contain a Minimum of One Special Character

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.



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.

To check the state of the system, run the following command(s):

```
/usr/bin/pwpolicy -getaccountpolicies 2>/dev/null | /usr/bin/tail -n +2 |
/usr/bin/xmllint --xpath "//string[contains(text(), \"policyAttributePassword matches
'(.^[a-zA-Z0-9].*){\\\"}]\" - 2>/dev/null | /usr/bin/awk -F\"{|}\" '{if ($2 >= 1) {print
\"true\"} else {print \"false\"}}'
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.mobiledevice.passwordpolicy) payload type:

```
<key>minComplexChars</key>
<integer>1</integer>
```

ID	pwpolicy_special_character_enforce	
References	800-53r5	• IA-5(1)
	CIS Benchmark	• 5.2.5 (level 2)
	CIS Controls V8	• 5.2
	CCE	• CCE-94344-9

Chapter 10. System Settings

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



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

10.1. Disable Airplay Receiver

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirPlayIncomingRequests').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowAirPlayIncomingRequests</key>
<false/>
```

ID	system_settings_airplay_receiver_disable
----	--

References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.1.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94348-0

10.2. Disable Unattended or Automatic Logon to the System

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('com.apple.login.mcx.DisableAutoLoginClient').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>com.apple.login.mcx.DisableAutoLoginClient</key>
<true/>
```

ID	system_settings_automatic_login_disable
----	---

References	800-53r5	<ul style="list-style-type: none">• IA-2• IA-5(13)
	CIS Benchmark	<ul style="list-style-type: none">• 2.12.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.7
	CCE	<ul style="list-style-type: none">• CCE-94350-6

10.3. Enable Bluetooth Menu

The bluetooth menu *MUST* be enabled.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.controlcenter')\
.objectForKey('Bluetooth').js
EOS
```

If the result is not **18**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.controlcenter) payload type:

```
<key>Bluetooth</key>
<integer>18</integer>
```

ID	system_settings_bluetooth_menu_enable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.4.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.8• 13.9
	CCE	<ul style="list-style-type: none">• CCE-94353-0

10.4. Disable Bluetooth Sharing

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.



The check and fix are for the currently logged in user. To get the currently logged in user, run the following.

```
CURRENT_USER=$( /usr/sbin/scutil <<< "show State:/Users/ConsoleUser" |  
/usr/bin/awk '/Name :/ && ! /loginwindow/ { print $3 }' )
```

To check the state of the system, run the following command(s):

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

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_bluetooth_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">AC-18(4)AC-3CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">2.3.3.11 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">3.34.1
	CCE	<ul style="list-style-type: none">CCE-94355-5

10.5. Disable Content Caching Service

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowContentCaching').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowContentCaching</key>
<false/>
```

ID	system_settings_content_caching_disable	
References	800-53r5	• CM-7, CM-7(1)
	CIS Benchmark	• 2.3.3.9 (level 2)
	CIS Controls V8	• 4.8
	CCE	• CCE-94357-1

10.6. Enforce Critical Security Updates to be Installed

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
```

```
.objectForKey('CriticalUpdateInstall').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>CriticalUpdateInstall</key>
<true/>
```

ID	system_settings_critical_update_install_enforce	
References	800-53r5	<ul style="list-style-type: none">• SI-2
	CIS Benchmark	<ul style="list-style-type: none">• 1.6 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4• 7.7
	CCE	<ul style="list-style-type: none">• CCE-94358-9

10.7. Disable Sending Diagnostic and Usage Data to Apple

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.SubmitDiagInfo')\
.objectForKey('AutoSubmit').js
let pref2 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowDiagnosticSubmission').js
if ( pref1 == false && pref2 == false ){
```



```
        return("true")
    } else {
        return("false")
    }
}
}
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SubmitDiagInfo) payload type:

```
<key>AutoSubmit</key>
<false/>
```

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowDiagnosticSubmission</key>
<false/>
```

ID	system_settings_diagnostics_reports_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• SC-7(10)• SI-11
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.3.1 (level 1)• 2.6.3.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94359-7

10.8. Enforce FileVault

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.

To check the state of the system, run the following command(s):

```
dontAllowDisable=$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('dontAllowFDEDisable').js
EOS
)
fileVault=$(/usr/bin/fdesetup status | /usr/bin/grep -c "FileVault is On.")
if [[ "$dontAllowDisable" == "true" ]] && [[ "$fileVault" == 1 ]]; then
    echo "1"
else
    echo "0"
fi
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.MCX) payload type:

```
<key>dontAllowFDEDisable</key>
<true/>
```

ID	system_settings_filevault_enforce	
References	800-53r5	• SC-28, SC-28(1)
	CIS Benchmark	• 2.6.6 (level 1)
	CIS Controls V8	• 3.6
		• 3.11
	CCE	• CCE-94360-5

10.9. Enable macOS Application Firewall

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableFirewall').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.security.firewall) payload type:

```
<key>EnableFirewall</key>
<true/>
```

ID	system_settings_firewall_enable	
References	800-53r5	<ul style="list-style-type: none">• AC-4• CM-7, CM-7(1)• SC-7, SC-7(12)
	CIS Benchmark	<ul style="list-style-type: none">• 2.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.5• 13.1
	CCE	<ul style="list-style-type: none">• CCE-94362-1

10.10. Enable Firewall Stealth Mode

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.



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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableStealthMode').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.security.firewall) payload type:

```
<key>EnableStealthMode</key>
<true/>
<key>EnableFirewall</key>
<true/>
```

ID	system_settings_firewall_stealth_mode_enable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)• SC-7, SC-7(16)
	CIS Benchmark	<ul style="list-style-type: none">• 2.2.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.5• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94363-9

10.11. Disable Guest Access to Shared SMB Folders

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.

To check the state of the system, run the following command(s):

```
/usr/bin/defaults read /Library/Preferences/SystemConfiguration/com.apple.smb.server
AllowGuestAccess
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_guest_access_smb_disable	
References	800-53r5	• N/A
	CIS Benchmark	• 2.12.2 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-94366-2

10.12. Disable the Guest Account

Guest access *MUST* be disabled.

Turning off guest access prevents anonymous users from accessing files.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('DisableGuestAccount'))
  let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('EnableGuestAccount'))
  if ( pref1 == true && pref2 == false ) {
    return("true")
  } else {
    return("false")
  }
}
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.MCX) payload

type:

```
<key>DisableGuestAccount</key>
<true/>
<key>EnableGuestAccount</key>
<false/>
```

ID	system_settings_guest_account_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-2, AC-2(9)
	CIS Benchmark	<ul style="list-style-type: none">• 2.12.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 5.2• 6.2• 6.8
	CCE	<ul style="list-style-type: none">• CCE-94367-0

10.13. Secure Hot Corners

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 corners 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.

To check the state of the system, run the following command(s):

```
bl_corner="$(/usr/bin/defaults read /Users/"$CURRENT_USER
/Library/Preferences/com.apple.dock wvous-bl-corner 2>/dev/null)"
tl_corner="$(/usr/bin/defaults read /Users/"$CURRENT_USER
/Library/Preferences/com.apple.dock wvous-tl-corner 2>/dev/null)"
tr_corner="$(/usr/bin/defaults read /Users/"$CURRENT_USER
/Library/Preferences/com.apple.dock wvous-tr-corner 2>/dev/null)"
br_corner="$(/usr/bin/defaults read /Users/"$CURRENT_USER
/Library/Preferences/com.apple.dock wvous-br-corner 2>/dev/null)"

if [[ "$bl_corner" != "6" ]] && [[ "$tl_corner" != "6" ]] && [[ "$tr_corner" != "6" ]]
&& [[ "$br_corner" != "6" ]]; then
    echo "0"
fi
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_hot_corners_secure	
References	800-53r5	<ul style="list-style-type: none">• AC-11(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.7.1 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 4.3
	CCE	<ul style="list-style-type: none">• CCE-94369-6

10.14. Disable Sending Audio Recordings and Transcripts to Apple

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.

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Accessibility')\
.objectForKey('AXSAudioDonationSiriImprovementEnabled').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Accessibility) payload type:

```
<key>AXSAudioDonationSiriImprovementEnabled</key>
<false/>
```

ID	system_settings_improve_assistive_voice_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7, CM-7(1)• SC-7(10)
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.3.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94370-4

10.15. Disable Improve Siri and Dictation Information to Apple

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.assistant.support')\
.objectForKey('Siri Data Sharing Opt-In Status').js
EOS
```

If the result is not 2, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.assistant.support) payload type:

<key>Siri Data Sharing Opt-In Status</key>
<integer>2</integer>

ID	system_settings_improve_siri_dictation_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7, CM-7(1)• SC-7(10)
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.3.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94372-0

10.16. Enforce macOS Updates are Automatically Installed

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticallyInstallMacOSUpdates').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

<key>AutomaticallyInstallMacOSUpdates</key>
<true/>

ID	system_settings_install_macos_updates_enforce
----	---

References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 1.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-94373-8

10.17. Disable Internet Sharing

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('forceInternetSharingOff').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.MCX) payload type:

```
<key>forceInternetSharingOff</key>
<true/>
```

ID	system_settings_internet_sharing_disable
----	--

References	800-53r5	<ul style="list-style-type: none">• AC-20• AC-4
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.8 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94375-3

10.18. Enable Location Services

Location Services *MUST* be enabled.

To check the state of the system, run the following command(s):

```
/usr/bin/sudo -u _locationd /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.locationd')\
.objectForKey('LocationServicesEnabled').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/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
```

ID	system_settings_location_services_enable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.1.1 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94377-9

10.19. Ensure Location Services Is In the Menu Bar

Location Services menu item *MUST* be enabled.

To check the state of the system, run the following command(s):

```
/usr/bin/defaults read /Library/Preferences/com.apple.locationmenu.plist
ShowSystemServices
```

If the result is not **1**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_location_services_menu_enforce	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.1.2 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94378-7

10.20. Configure Login Window to Show A Custom Message

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS | /usr/bin/base64
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('LoginwindowText').js
EOS
```

If the result is not **Center for Internet Security Test Message**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>LoginwindowText</key>
<string>Center for Internet Security Test Message</string>
```

ID	system_settings_loginwindow_loginwindowtext_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 2.10.3 (level 1)
	CIS Controls V8	• 4.1
	CCE	• CCE-94379-5

10.21. Configure Login Window to Prompt for Username and Password

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('SHOWFULLNAME').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>SHOWFULLNAME</key>
```

<true/>

ID	system_settings_loginwindow_prompt_username_password_enforce	
References	800-53r5	• IA-2
	CIS Benchmark	• 2.10.4 (level 1)
	CIS Controls V8	• 4.1
	CCE	• CCE-94380-3

10.22. Disable Media Sharing

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowMediaSharing'))
  let pref2 = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowMediaSharingModification'))
  if ( pref1 == false && pref2 == false ) {
    return("true")
  } else {
    return("false")
  }
}
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowMediaSharing</key>
<false/>
<key>allowMediaSharingModification</key>
<false/>
```

ID	system_settings_media_sharing_disabled	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.10 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94381-1

10.23. Disable Password Hints

Password hints *MUST* be disabled.

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('RetriesUntilHint').js
EOS
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>RetriesUntilHint</key>
<integer>0</integer>
```

ID	system_settings_password_hints_disable	
References	800-53r5	• IA-6
	CIS Benchmark	• 2.10.5 (level 1)
	CIS Controls V8	• 4.1
	CCE	• CCE-94382-9

10.24. Disable Personalized Advertising

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowApplePersonalizedAdvertising').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowApplePersonalizedAdvertising</key>
<false/>
```

ID	system_settings_personalized_advertising_disable
----	--

References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7, CM-7(1)• SC-7(10)
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94383-7

10.25. Disable Printer Sharing

Printer Sharing *MUST* be disabled.

To check the state of the system, run the following command(s):

```
/usr/sbin/cupsctl | /usr/bin/grep -c "_share_printers=0"
```

If the result is not **1**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_printer_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94384-5

10.26. Disable Remote Apple Events

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.

To check the state of the system, run the following command(s):


```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.AEServer" => disabled'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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



Systemsetup with -setremoteappleevents flag will fail unless you grant Full Disk Access to systemsetup or its parent process. Requires supervision.

ID	system_settings_rae_disable	
References	800-53r5	<ul style="list-style-type: none">AC-17AC-3
	CIS Benchmark	<ul style="list-style-type: none">2.3.3.7 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">4.14.8
	CCE	<ul style="list-style-type: none">CCE-94385-2

10.27. Disable Remote Management

Remote Management *MUST* be disabled.

To check the state of the system, run the following command(s):

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "RemoteDesktopEnabled = 0"
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_remote_management_disable	
References	800-53r5	• CM-7, CM-7(1)
	CIS Benchmark	• 2.3.3.6 (level 1)
	CIS Controls V8	• 4.1
		• 4.8
		• 5.4
	CCE	• CCE-94386-0

10.28. Disable Screen Sharing and Apple Remote Desktop

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.

To check the state of the system, run the following command(s):

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.screensharing" =>  
disabled'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

NOTE - This will apply to the whole system

ID	system_settings_screen_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94387-8

10.29. Enforce Session Lock After Screen Saver is Started

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.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
    let delay = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('askForPasswordDelay'))
    if ( delay <= 5 ) {
        return("true")
    } else {
        return("false")
    }
}
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.screensaver) payload type:

<key>askForPasswordDelay</key>
<integer>5</integer>

ID	system_settings_screensaver_ask_for_password_delay_enforce	
References	800-53r5	• AC-11
	CIS Benchmark	• 2.10.2 (level 1)
	CIS Controls V8	• 4.7
	CCE	• CCE-94388-6

10.30. Enforce Screen Saver Timeout

The screen saver timeout *MUST* be set to 1200 seconds or a shorter length of time.

This rule ensures that a full session lock is triggered within no more than 1200 seconds of inactivity.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let timeout = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('idleTime'))
  if ( timeout <= 1200 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.screensaver) payload type:

<key>idleTime</key>
<integer>1200</integer>

ID	system_settings_screensaver_timeout_enforce	
References	800-53r5 <ul style="list-style-type: none"> • AC-11 • IA-11 	
	CIS Benchmark	• 2.10.1 (level 1)
	CIS Controls V8	• 4.3
	CCE	• CCE-94390-2

10.31. Ensure Siri Listen For is Disabled

Siri has the ability to listen for "Hey Siri" or "Siri". Listen for *MUST* be disabled.

To check the state of the system, run the following command(s):

```
/usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Siri')\
.objectForKey('VoiceTriggerUserEnabled').js
EOS
```

If the result is not **false**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.Siri) payload type:

```
<key>VoiceTriggerUserEnabled</key>
<false/>
```

ID	system_settings_siri_listen_disable	
References	800-53r5 <ul style="list-style-type: none"> • N/A 	
	CIS Benchmark	• 2.5.2 (level 1)
	CIS Controls V8	• 4.1
		• 4.8
	CCE	• CCE-94392-8

10.32. Disable Server Message Block Sharing

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.

To check the state of the system, run the following command(s):

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.smbd" => disabled'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

The system may need to be restarted for the update to take effect.

ID	system_settings_smbd_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8• 5.4
	CCE	<ul style="list-style-type: none">• CCE-94394-4

10.33. Enforce Software Update App Update Updates Automatically

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticallyInstallAppUpdates').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>AutomaticallyInstallAppUpdates</key>
<true/>
```

ID	system_settings_software_update_app_update_enforce	
References	800-53r5	• N/A
	CIS Benchmark	• 1.5 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
	CCE	• CCE-94395-1

10.34. Enforce Software Update Downloads Updates Automatically

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticDownload').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:


```
<key>AutomaticDownload</key>
<true/>
```

ID	system_settings_software_update_download_enforce	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 1.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-94396-9

10.35. Enforce Software Update Automatically

Software Update *MUST* be configured to enforce automatic update is enabled.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticCheckEnabled').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>AutomaticCheckEnabled</key>
<true/>
```

ID	system_settings_software_update_enforce
----	---

References	800-53r5	<ul style="list-style-type: none">• SI-2(5)
	CIS Benchmark	<ul style="list-style-type: none">• 1.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-94397-7

10.36. Ensure Software Update is Updated and Current

Make sure Software Update is updated and current.



Automatic fix can cause unplanned restarts and may lose work.

To check the state of the system, run the following command(s):

```
softwareupdate_date_epoch=$(/bin/date -j -f "%Y-%m-%d" "$( /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate.plist LastFullSuccessfulDate | /usr/bin/awk '{print $1}' )" "+%s")
thirty_days_epoch=$(/bin/date -v -30d "+%s")
if [[ $softwareupdate_date_epoch -lt $thirty_days_epoch ]]; then
  /bin/echo "0"
else
  /bin/echo "1"
fi
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

NOTE - This will apply to the whole system

ID	system_settings_softwareupdate_current
-----------	--

References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 1.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-94398-5

10.37. Disable SSH Server for Remote Access Sessions

SSH service *MUST* be disabled for remote access.

To check the state of the system, run the following command(s):


```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.openssh.sshd" => disabled'
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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



Systemsetup with -setremotelogin flag will fail unless you grant Full Disk Access to systemsetup or its parent process. Requires supervision.

ID	system_settings_ssh_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-94399-3

10.38. Require Administrator Password to Modify System-Wide Preferences

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.

To check the state of the system, run the following command(s):

```
authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")
result="1"
for section in ${authDBs[@]}; do
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
-xpath 'name(//*[contains(text(), "shared")]/following-sibling::*[1])' -) != "false"
]]; then
        result="0"
    fi
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
-xpath '//*[contains(text(), "group")]/following-sibling::*[1]/text()' -) != "admin"
]]; then
        result="0"
    fi
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
-xpath 'name(//*[contains(text(), "authenticate-user")]/following-sibling::*[1])' -)
!= "true" ]]; then
        result="0"
    fi
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
-xpath 'name(//*[contains(text(), "session-owner")]/following-sibling::*[1])' -) !=
"false" ]]; then
        result="0"
    fi
done
echo $result
```

If the result is not 1, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
authDBs=("system.preferences" "system.preferences.energysaver"
```

```

"system.preferences.network" "system.preferences.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"

```

ID	system_settings_system_wide_preferences_configure	
References	800-53r5	<ul style="list-style-type: none">• AC-6, AC-6(1), AC-6(2)
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.8 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1
	CCE	<ul style="list-style-type: none">• CCE-94401-7

10.39. Configure Time Machine for Automatic Backups

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.TimeMachine')\
.objectForKey('AutoBackup').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.TimeMachine) payload type:

```
<key>AutoBackup</key>
<true/>
```

ID	system_settings_time_machine_auto_backup_enable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.4.1 (level 2)
	CIS Controls V8	<ul style="list-style-type: none">• 11.2
	CCE	<ul style="list-style-type: none">• CCE-94402-5

10.40. Ensure Time Machine Volumes are Encrypted

Time Machine volumes *MUST* be encrypted.

To check the state of the system, run the following command(s):

```
error_count=0
for tm in $(/usr/bin/tmutil destinationinfo 2>/dev/null | /usr/bin/awk -F': '
'/Name/{print $2}'); do
    tmMounted=$(/usr/sbin/diskutil info "${tm}" 2>/dev/null | /usr/bin/awk
'/Mounted/{print $2}')
    tmEncrypted=$(/usr/sbin/diskutil info "${tm}" 2>/dev/null | /usr/bin/awk
'/FileVault/{print $2}')
    if [[ "$tmMounted" = "Yes" && "$tmEncrypted" = "No" ]]; then
        ((error_count++))
    fi
done
echo "$error_count"
```

If the result is not 0, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

1. Go to System Settings → Time Machine
2. Click **Select Disk**
3. Select existing Backup Disk under **Available Disks**
4. Click **Encrypt Backups**
5. Click **Use Disk**

ID	system_settings_time_machine_encrypted_configure	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.4.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.6• 3.11• 11.3
	CCE	<ul style="list-style-type: none">• CCE-94403-3

10.41. Configure macOS to Use an Authorized Time Server

Approved time server *MUST* be the only server configured for use. As of macOS 10.13 only one time server is supported.

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

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('timeServer').js
EOS
```

If the result is not **time.apple.com**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.MCX) payload type:

```
<key>timeServer</key>
<string>time.apple.com</string>
```

ID	system_settings_time_server_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-12(1)• SC-45(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.4
	CCE	<ul style="list-style-type: none">• CCE-94404-1

10.42. Enforce macOS Time Synchronization

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.


To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.timed')\
.objectForKey('TMAutomaticTimeOnlyEnabled').js
EOS
```

If the result is not **true**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:



The following settings are in the (com.apple.ManagedClient.preferences) payload. This payload requires the additional settings to be sub-payloads within, containing their defined payload types.

Create a configuration profile containing the following keys in the (com.apple.timed) payload type:

```
<key>TMAutomaticTimeOnlyEnabled</key>
<true/>
```

ID	system_settings_time_server_enforce	
References	800-53r5	<ul style="list-style-type: none">• AU-12(1)• SC-45(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.4
	CCE	<ul style="list-style-type: none">• CCE-94405-8

10.43. Ensure Wake for Network Access Is Disabled

Wake for network access *MUST* be disabled.

To check the state of the system, run the following command(s):

```
/usr/bin/pmset -g custom | /usr/bin/awk '/womp/ { sum+=$2 } END {print sum}'
```

If the result is not **0**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

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

ID	system_settings_wake_network_access_disable	
References	800-53r5	<ul style="list-style-type: none">N/A
	CIS Benchmark	<ul style="list-style-type: none">2.9.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">4.8
	CCE	<ul style="list-style-type: none">CCE-94410-8

10.44. Enable Wifi Menu

The WiFi menu *MUST* be enabled.

To check the state of the system, run the following command(s):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.controlcenter')\
.objectForKey('WiFi').js
EOS
```

If the result is not **18**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

Create a configuration profile containing the following keys in the (com.apple.controlcenter) payload type:

```
<key>WiFi</key>
<integer>18</integer>
```

ID	system_settings_wifi_menu_enable
----	----------------------------------

References	800-53r5	<ul style="list-style-type: none"> • N/A
	CIS Benchmark	<ul style="list-style-type: none"> • 2.4.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none"> • 4.8 • 12.6
	CCE	<ul style="list-style-type: none"> • CCE-94414-0

Chapter 11. Supplemental

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

11.1. CIS Manual Recommendations

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

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 AppleIDs 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 2.3.3.12 Ensure Computer Name Does Not Contain PII or Protected Organizational Information 2.5.1 Audit Siri Settings 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 2.9.1.1 Ensure the OS Is Not Active When Resuming from Standby (Intel) 2.11.2 Audit Touch ID 2.13.1 Audit Passwords System Preference Setting 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

Section	Logging and Auditing
Recommendations	3.6 Audit Software Inventory

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

Section	Applications
Recommendations	6.2.1 Ensure Protect Mail Activity in Mail Is Enabled 6.3.2 Audit History and Remove History Items 6.3.5 Audit Hide IP Address in Safari Setting 6.3.8 Audit Autofill 6.3.9 Audit Pop-up Windows

11.2. FileVault Supplemental

The supplemental guidance found in this section is applicable for the following rules: *
system_settings_filevault_enforce

In macOS the internal Apple File System (APFS) data volume can be protected by FileVault. The system volume is always cryptographically protected (T2 and Apple Silicon) and is a read-only volume.



FileVault uses an AES-XTS data encryption algorithm to protect full volumes of internal and external storage. Macs with a secure enclave (T2 and Apple Silicon) utilize the hardware security features of the architecture.

FileVault is described in detail here: <https://support.apple.com/guide/security/volume-encryption-with-filevault-sec4c6dc1b6e/web>.

FileVault can be enabled in two ways within the macOS. It can be managed using the `fdsetup` command or by a Configuration Profile. When enabling FileVault via either of the aforementioned methods, you will be required to enter a username and password, which must be a local Open Directory account with a valid SecureToken password.

Using the `fdsetup` Command

When enabling FileVault via the command line in the Terminal application, you can run the following command.

```
/usr/bin/fdsetup enable
```

Running this command will prompt you for a username and password and then enable FileVault and return the personal recovery key. There are a number of management features available when managing FileVault via the command line that are not available when using a configuration profile. More information on these management features is available in the man page for `fdsetup`.



Apple has deprecated `fdsetup` command line tool from recognizing user name and password for security reasons and may remove the ability in future versions of macOS.

Using a Configuration Profile

When managing FileVault with a configuration profile, you must deploy a profile with the payload type `com.apple.MCX.FileVault2`. When using the Enable key to enable FileVault with a configuration profile, you must include 1 of the following:

```
<key>Enable</key>
<string>On</string>
<key>Defer</key>
<true/>
```

```
<key>Enable</key>
<string>On</string>
<key>UserEntersMissingInfo</key>
<true/>
```

If using the Defer key it will prompt for the user name and password at logout.

The `UserEntersMissingInfo` key will only work if installed through manual installation, and it will prompt for the username and password immediately.

When using a configuration profile, you can escrow the Recovery key to a Mobile Device Management (MDM) server. Documentation for that can be found on Apple's Developer site: <https://developer.apple.com/documentation/devicemanagement/fderecoverykeyescrow>.

It's recommended that you use a Personal Recovery key instead of an Institutional key as it will generate a specific key for each device. You can find more guidance on choosing a recover key here: https://docs.jamf.com/technical-papers/jamf-pro/administering-filevault-macos/10.7.1/Choosing_a_Recovery_Key.html.



On Intel Macs, FileVault only supports password-based unlock and cannot be done using a smartcard. Smartcard unlock for FileVault is supported on Apple Silicon Macs.

11.3. Password Policy Supplemental

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.

In accordance with these requirements, the following rules, while they remain on specific

benchmarks, have been removed from any of the NIST 800-53r5 baselines as recommendations.

- pwpolicy_alpha_numeric_enforce
- pwpolicy_custom_regex_enforce
- pwpolicy_lower_case_character_enforce.yaml
- pwpolicy_max_lifetime_enforce
- pwpolicy_minimum_lifetime_enforce
- pwpolicy_prevent_dictionary_words
- pwpolicy_simple_sequence_disable
- pwpolicy_special_character_enforce
- pwpolicy_upper_case_character_enforce.yaml

If an organization has requirements to implement additional password policies, the remainder of this supplemental discusses the following password policy rules:

- pwpolicy_lower_case_character_enforce
- pwpolicy_upper_case_character_enforce
- pwpolicy_account_inactivity_enforce
- pwpolicy_minimum_lifetime_enforce

Password policies should be enforced as much as possible via Configuration Profiles. However, the following policies are currently not enforceable via Configuration Profiles, and must therefore be enabled using the `pwpolicy` command:

- Enforcing at least 1 lowercase character
- Enforcing at least 1 uppercase character
- Disabling an account after 35 days of inactivity
- Password minimum lifetime

To set the local policy to meet these requirements, save the following XML password policy to a file.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>policyCategoryAuthentication</key>
  <array>
    <dict>
      <key>policyContent</key>
      <string>policyAttributeLastAuthenticationTime &gt; policyAttributeCurrentTime
- (policyAttributeInactiveDays * 24 * 60 * 60)</string>
      <key>policyIdentifier</key>
      <string>Inactive Account</string>
```

```

    <key>policyParameters</key>
    <dict>
      <key>policyAttributeInactiveDays</key>
      <integer>35</integer>
    </dict>
  </dict>
</array>
<key>policyCategoryPasswordContent</key>
<array>
  <dict>
    <key>policyContent</key>
    <string>policyAttributePassword matches '(*[A-Z].*){1,+}'</string>
    <key>policyIdentifier</key>
    <string>Must have at least 1 uppercase letter</string>
    <key>policyParameters</key>
    <dict>
      <key>minimumAlphaCharactersUpperCase</key>
      <integer>1</integer>
    </dict>
  </dict>
  <dict>
    <key>policyContent</key>
    <string>policyAttributePassword matches '(*[a-z].*){1,+}'</string>
    <key>policyIdentifier</key>
    <string>Must have at least 1 lowercase letter</string>
    <key>policyParameters</key>
    <dict>
      <key>minimumAlphaCharactersLowerCase</key>
      <integer>1</integer>
    </dict>
  </dict>
  <dict>
    <key>policyContent</key>
    <string>policyAttributeLastPasswordChangeTime &lt; policyAttributeCurrentTime
- (policyAttributeMinimumLifetimeHours * 60 * 60)</string>
    <key>policyIdentifier</key>
    <string>Minimum Password Lifetime</string>
    <key>policyParameters</key>
    <dict>
      <key>policyAttributeMinimumLifetimeHours</key>
      <integer>24</integer>
    </dict>
  </dict>
</array>
</dict>
</plist>

```

Run the following command to load the new policy file, substituting the path to the file in place of "\$pwpolicy_file".


```
/usr/bin/pwpolicy setaccountpolicies $pwpolicy_file
```



If directory services is being utilized, password policies should come from the domain.