



macOS Security Compliance

macOS 12.0

Security Configuration - DISA STIG

Monterey Guidance, Revision 2 (2022-03-16)

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. Authentication	8
6.1. Enforce Multifactor Authentication for Login	8
6.2. Enforce Multifactor Authentication for the su Command	9
6.3. Enforce Multifactor Authentication for Privilege Escalation Through the sudo Command ..	11
6.4. Set Smartcard Certificate Trust to Moderate	12
6.5. Enforce Smartcard Authentication	13
7. Auditing	15
7.1. Configure Audit Log Files to Not Contain Access Control Lists	15
7.2. Configure Audit Log Folder to Not Contain Access Control Lists	16
7.3. Enable Security Auditing	16
7.4. Configure Audit Capacity Warning	17
7.5. Configure System to Shut Down Upon Audit Failure	18
7.6. Configure Audit Log Files Group to Wheel	19
7.7. Configure Audit Log Files to Mode 440 or Less Permissive	20
7.8. Configure Audit Log Files to be Owned by Root	21
7.9. Configure System to Audit All Authorization and Authentication Events	21
7.10. Configure System to Audit All Administrative Action Events	22
7.11. Configure System to Audit All Deletions of Object Attributes	23
7.12. Configure System to Audit All Changes of Object Attributes	24
7.13. Configure System to Audit All Failed Read Actions on the System	26
7.14. Configure System to Audit All Failed Write Actions on the System	27
7.15. Configure System to Audit All Log In and Log Out Events	28
7.16. Configure Audit Log Folders Group to Wheel	29
7.17. Configure Audit Log Folders to be Owned by Root	30
7.18. Configure Audit Log Folders to Mode 700 or Less Permissive	31
7.19. Configure Audit Retention to a Minimum of Seven Days	31
7.20. Configure Audit Failure Notification	32
8. macOS	34
8.1. Disable AirDrop	34
8.2. Must Use an Approved Antivirus Program	35
8.3. Disable Apple ID Setup during Setup Assistant	35

8.4. Configure Apple System Log Files Owned by Root and Group to Wheel	36
8.5. Configure Apple System Log Files To Mode 640 or Less Permissive	37
8.6. Disable Blank Blu Ray	38
8.7. Disable Blank CD	39
8.8. Disable Blank DVD	40
8.9. Enforce Blu Ray Read Only	41
8.10. Disable Bonjour Multicast	42
8.11. Disable Burn Support	43
8.12. Disable Camera	44
8.13. Enforce CD Read Only	44
8.14. Issue or Obtain Public Key Certificates from an Approved Service Provider	45
8.15. Enforce Installation of XProtect, MRT, and Gatekeeper Updates Automatically	46
8.16. Integrate System into a Directory Services Infrastructure	47
8.17. Disable Disk Images	48
8.18. Disable Blank CD	49
8.19. Disable Erase Content and Settings	50
8.20. Must Use ESS	51
8.21. FileVault Authorized Users	52
8.22. Disable FileVault Automatic Login	52
8.23. Enable Firmware Password	53
8.24. Enable Gatekeeper	54
8.25. Disable Handoff	55
8.26. Secure User's Home Folders	56
8.27. Disable the Built-in Web Server	57
8.28. Disable iCloud Storage Setup during Setup Assistant	58
8.29. Configure System Log Files Owned by Root and Group to Wheel	59
8.30. Configure System Log Files to Mode 640 or Less Permissive	60
8.31. Disable Network File System Service	60
8.32. Disable Proximity Based Password Sharing Requests	61
8.33. Display Policy Banner at Login Window	62
8.34. Display Policy Banner at Remote Login	64
8.35. Enforce SSH to Display Policy Banner	66
8.36. Disable Privacy Setup Services During Setup Assistant	67
8.37. Disable Removable Storage Devices	67
8.38. Enforce Screen Saver at Login Window	68
8.39. Ensure System Integrity Protection is Enabled	69
8.40. Disable Siri Setup during Setup Assistant	70
8.41. Disable Screen Time Prompt During Setup Assistant	71
8.42. Disable Unlock with Apple Watch During Setup Assistant	72
8.43. Set SSHD Active Client Alive Maximum to Zero	73
8.44. Configure SSHD ClientAliveInterval option set to 900 or less	74

8.45. Limit SSHD to FIPS 140 Validated Ciphers	75
8.46. Limit SSHD to FIPS 140 Validated Message Authentication Code Algorithms	76
8.47. Configure SSHD to Use Secure Key Exchange Algorithms	77
8.48. Set Login Grace Time to 30 or Less.	78
8.49. Disable Root Login for SSH.	79
8.50. Configure Sudoers to Authenticate Users on a Per -tty Basis.	80
8.51. Disable Trivial File Transfer Protocol Service.	81
8.52. Enable Time Synchronization Daemon.	82
8.53. Disable TouchID Prompt during Setup Assistant	83
8.54. Disable Unix-to-Unix Copy Protocol Service	83
9. Password Policy	85
9.1. Restrict Maximum Password Lifetime to 60 Days	85
9.2. Limit Consecutive Failed Login Attempts to Three	86
9.3. Set Account Lockout Time to 15 Minutes	87
9.4. Require Passwords Contain a Minimum of One Numeric Character.	88
9.5. Prohibit Password Reuse for a Minimum of Five Generations	89
9.6. Require a Minimum Password Length of 15 Characters.	90
9.7. Require Passwords Contain a Minimum of One Special Character	91
9.8. Automatically Remove or Disable Temporary or Emergency User Accounts within 72 Hours.	92
10. iCloud	95
10.1. Disable iCloud Address Book.	95
10.2. Disable the System Preference Pane for Apple ID	96
10.3. Disable iCloud Bookmarks	97
10.4. Disable the iCloud Calendar Services	98
10.5. Disable iCloud Document Sync	99
10.6. Disable iCloud Keychain Sync	100
10.7. Disable iCloud Mail	101
10.8. Disable iCloud Notes	102
10.9. Disable iCloud Photo Library	103
10.10. Disable iCloud Reminders	104
11. System Preferences	106
11.1. Prevent Apple Watch from Terminating a Session Lock	106
11.2. Disable Unattended or Automatic Logon to the System	107
11.3. Disable Bluetooth When no Approved Device is Connected	108
11.4. Disable the Bluetooth System Preference Pane	109
11.5. Hide the Bluetooth System Preference Pane	110
11.6. Disable Sending Diagnostic and Usage Data to Apple	111
11.7. Enforce FileVault	112
11.8. Enable macOS Application Firewall	112
11.9. Enable Firewall Stealth Mode	113

11.10. Apply Gatekeeper Settings to Block Applications from Unidentified Developers	114
11.11. Disable the Guest Account	115
11.12. Disable Hot Corners.	116
11.13. Disable the Internet Accounts System Preference Pane	117
11.14. Hide the Internet Accounts System Preference Pane	118
11.15. Disable Internet Sharing	119
11.16. Disable Location Services	120
11.17. Configure Login Window to Prompt for Username and Password	121
11.18. Disable Password Hints	122
11.19. Disable Remote Apple Events	123
11.20. Disable Screen Sharing and Apple Remote Desktop	124
11.21. Enforce Session Lock After Screen Saver is Started	125
11.22. Enforce Screen Saver Password	126
11.23. Enforce Screen Saver Timeout	127
11.24. Disable Siri.	128
11.25. Disable the System Preference Pane for Siri	129
11.26. Hide the System Preference Pane for Siri	130
11.27. Disable Server Message Block Sharing	131
11.28. Disable SSH Server for Remote Access Sessions	132
11.29. Require Administrator Password to Modify System-Wide Preferences	133
11.30. Configure macOS to Use an Authorized Time Server	133
11.31. Enable macOS Time Synchronization Daemon (timed)	134
11.32. Configure User Session Lock When a Smart Token is Removed	135
11.33. Disable the System Preference Pane for Touch ID	136
11.34. Hide the System Preference Pane for Touch ID	137
11.35. Disable the System Preference Pane for Wallet and Apple Pay	138
11.36. Hide the System Preference Pane for Wallet and Apple Pay	139
12. Supplemental	141
12.1. Out of Scope Supplemental	141
12.2. FileVault Supplemental	143
12.3. Packet Filter (pf) Supplemental	144
12.4. Password Policy Supplemental	149
12.5. Smartcard Supplemental	152

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.

2. Scope

This guide describes the actions to take when securing a macOS system against the Apple macOS 12 (Monterey) STIG - Ver 1, Rel 1.

3. Authors

Dan Brodjieski	National Aeronautics and Space Administration
Allen Golbig	Jamf
Bob Gendler	National Institute of Standards and Technology

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
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
OCSP	Online Certificate Status Protocol
OS	Operating System
PF	Packet Filter
PIV	Personal Identity Verification
PIV-M	Personal Identity Verification Mandatory
PKI	Public Key Infrastructure
SIP	System Integrity Protection
SMB	Server Message Block
SSH	Secure Shell
SSP	System Security Plan

STIG	Security Technical Implementation Guide
UAMDM	User Approved MDM
UUCP	Unix-to-Unix Copy Protocol

5. Applicable Documents

5.1. Government Documents

Table 2. 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</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 2</i>

Table 3. Defense Information Systems Agency (DISA)

Document Number or Descriptor	Document Title
STIG Ver 1, Rel 1	<i>Apple macOS 12 (Monterey) STIG</i>

Table 4. 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 5. Apple

Document Number or Descriptor	Document Title
Apple Platform Security Guide	<i>Apple Platform Security</i>
Deployment Reference for Mac	<i>Deployment Reference</i>
Mobile Device Management Settings	<i>Mobile Device Management Settings</i>
Profile-Specific Payload Keys	<i>Profile-Specific Payload Keys</i>
Security Certifications and Compliance Center	<i>Security Certifications and Compliance Center</i>

Table 6. Center for Internet Security

Document Number or Descriptor	Document Title
Apple macOS 12.0	<i>CIS Apple macOS 12.0 Benchmark version 1.0</i>

6. Authentication

This section contains the configuration of authentication settings, including the enforcement of smartcard authentication.



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

6.1. Enforce Multifactor Authentication for Login

The system *MUST* be configured to enforce multifactor authentication.

All users *MUST* go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.



Modification of Pluggable Authentication Modules (PAM) now require user authorization, or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.



/etc/pam.d/login will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -Ec  
'^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_deny.so)'  
/etc/pam.d/login
```

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

Remediation Description

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

```
/bin/cat > /etc/pam.d/login << LOGIN_END
# login: auth account password session
auth      sufficient    pam_smartcard.so
auth      optional     pam_krb5.so use_kcminit
auth      optional     pam_ntlm.so try_first_pass
auth      optional     pam_mount.so try_first_pass
auth      required     pam_opendirectory.so try_first_pass
auth      required     pam_deny.so
account   required     pam_nologin.so
account   required     pam_opendirectory.so
password  required     pam_opendirectory.so
session   required     pam_launchd.so
session   required     pam_uwtmp.so
session   optional     pam_mount.so
LOGIN_END

/bin/chmod 644 /etc/pam.d/login
/usr/sbin/chown root:wheel /etc/pam.d/login
```

ID	auth_pam_login_smartcard_enforce	
References	800-53r5	• IA-2(1), IA-2(2), IA-2(8)
	DISA STIG(s)	• APPL-12-003050
	CCE	• CCE-90877-2

6.2. Enforce Multifactor Authentication for the su Command

The system *MUST* be configured such that, when the su command is used, multifactor authentication is enforced.

All users *MUST* go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.



Modification of Pluggable Authentication Modules (PAM) now require user authorization, or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.



/etc/pam.d/su will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -Ec
'^ (auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_rootok.so)'
/etc/pam.d/su
```

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

Remediation Description

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

```
/bin/cat > /etc/pam.d/su << SU_END
# su: auth account password session
auth      sufficient    pam_smartcard.so
auth      required      pam_rootok.so
auth      required      pam_group.so no_warn group=admin,wheel ruser root_only
fail_safe
account    required      pam_permit.so
account    required      pam_opendirectory.so no_check_shell
password   required      pam_opendirectory.so
session    required      pam_launchd.so
SU_END

# Fix new file ownership and permissions
/bin/chmod 644 /etc/pam.d/su
/usr/sbin/chown root:wheel /etc/pam.d/su
```

ID	auth_pam_su_smartcard_enforce	
References	800-53r5	<ul style="list-style-type: none"> IA-2(1), IA-2(2), IA-2(8)
	DISA STIG(s)	<ul style="list-style-type: none"> APPL-12-003051
	CCE	<ul style="list-style-type: none"> CCE-90878-0

6.3. Enforce Multifactor Authentication for Privilege Escalation Through the sudo Command

The system *MUST* be configured to enforce multifactor authentication when the sudo command is used to elevate privilege.

All users *MUST* go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.



Modification of Pluggable Authentication Modules (PAM) now require user authorization, or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.



/etc/pam.d/sudo will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -Ec  
'^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_deny.so)'  
/etc/pam.d/sudo
```

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

Remediation Description

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

```
/bin/cat > /etc/pam.d/sudo << SUDO_END  
# sudo: auth account password session  
auth      sufficient    pam_smartcard.so  
auth      required      pam_opendirectory.so  
auth      required      pam_deny.so  
account    required      pam_permit.so  
password   required      pam_deny.so  
session    required      pam_permit.so  
SUDO_END  
  
/bin/chmod 444 /etc/pam.d/sudo  
/usr/sbin/chown root:wheel /etc/pam.d/sudo
```

ID	auth_pam_sudo_smartcard_enforce
----	---------------------------------

References	800-53r5	<ul style="list-style-type: none"> • IA-2(1), IA-2(2), IA-2(8)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-003052
	CCE	<ul style="list-style-type: none"> • CCE-90879-8

6.4. Set Smartcard Certificate Trust to Moderate

The macOS system *MUST* be configured to block access to users who are no longer authorized (i.e., users with revoked certificates).

To prevent the use of untrusted certificates, the certificates on a smartcard card *MUST* meet the following criteria: its issuer has a system-trusted certificate, the certificate is not expired, its "valid-after" date is in the past, and it passes Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) checking.

By setting the smartcard certificate trust level to moderate, the system will execute a soft revocation, i.e., if the OCSP/CRL server is unreachable, authentication will still succeed.



Before applying this setting, please see the smartcard supplemental guidance.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')\
.objectForKey('checkCertificateTrust').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.security.smartcard) payload type:

```
<key>checkCertificateTrust</key>
<integer>2</integer>
```

ID	auth_smartcard_certificate_trust_enforce_moderate
-----------	---

References	800-53r5	<ul style="list-style-type: none"> • IA-5(2) • SC-17
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-001060
	CCE	<ul style="list-style-type: none"> • CCE-90882-2

6.5. Enforce Smartcard Authentication

Smartcard authentication *MUST* be enforced.

The use of smartcard credentials facilitates standardization and reduces the risk of unauthorized access.

When enforceSmartCard is set to "true", the smartcard must be used for login, authorization, and unlocking the screensaver.



enforceSmartCard will apply to the whole system. No users will be able to login with their password unless the profile is removed or a user is exempt from smartcard enforcement.



enforceSmartcard requires allowSmartcard to be set to true in order to work.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')\
.objectForKey('enforceSmartCard').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.smartcard) payload type:

```
<key>enforceSmartCard</key>
<true/>
```

ID	auth_smartcard_enforce	
References	800-53r5 <ul style="list-style-type: none"> • IA-2, IA-2(1), IA-2(12), IA-2(2), IA-2(6), IA-2(8) • IA-5(2) DISA STIG(s) <ul style="list-style-type: none"> • APPL-12-003020 CCE <ul style="list-style-type: none"> • CCE-90883-0 	

7. 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.

7.1. 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 $(/usr/bin/awk -F: '/^dir/{print $2}' /etc/security/audit_control)
```

ID	audit_acls_files_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-9
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-000030
	CCE	<ul style="list-style-type: none">• CCE-90851-7

7.2. 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 $(/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 -N $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

ID	audit_acls_folders_configure	
References	800-53r5	• AU-9
	DISA STIG(s)	• APPL-12-000031
	CCE	• CCE-90852-5

7.3. 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 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.auditd
```

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.auditd.plist
```

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)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-001003
	CCE	<ul style="list-style-type: none">• CCE-90854-1

7.4. Configure Audit Capacity Warning

The audit service *MUST* be configured to notify the system administrator when the amount of free disk space remaining reaches an organization defined value.

This rule ensures that the system administrator is notified in advance that action is required to free up more disk space for audit logs.

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

```
/usr/bin/grep -c "^minfree:25" /etc/security/audit_control
```

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/sed -i.bak 's/.*minfree.*/minfree:25/' /etc/security/audit_control;  
/usr/sbin/audit -s
```

ID	audit_configure_capacity_notify	
References	800-53r5	• AU-5(1)
	DISA STIG(s)	• APPL-12-001030
	CCE	• CCE-90855-8

7.5. Configure System to Shut Down Upon Audit Failure

The audit service *MUST* be configured to shut down the computer if it is unable to audit system events.

Once audit failure occurs, user and system activity are no longer recorded, and malicious activity could go undetected. Audit processing failures can occur due to software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

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

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

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/sed -i.bak 's/^policy.*/policy: ahlt,argv/' /etc/security/audit_control;  
/usr/sbin/audit -s
```

ID	audit_failure_halt	
References	800-53r5	• AU-5
	DISA STIG(s)	• APPL-12-001010
	CCE	• CCE-90857-4

7.6. 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 $(/usr/bin/grep '^dir' /etc/security/audit_control |  
/usr/bin/awk -F: '{print $2}')/*
```


ID	audit_files_group_configure	
References	800-53r5 <ul style="list-style-type: none"> • AU-9 	
	DISA STIG(s) <ul style="list-style-type: none"> • APPL-12-001014 	
	CCE <ul style="list-style-type: none"> • CCE-90858-2 	

7.7. 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 $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')/*
```

ID	audit_files_mode_configure	
References	800-53r5 <ul style="list-style-type: none"> • AU-9 	
	DISA STIG(s) <ul style="list-style-type: none"> • APPL-12-001016 	
	CCE <ul style="list-style-type: none"> • CCE-90859-0 	

7.8. 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 $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')/*
```

ID	audit_files_owner_configure	
References	800-53r5	• AU-9
	DISA STIG(s)	• APPL-12-001012
	CCE	• CCE-90860-8

7.9. 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-12• AU-2• CM-5(1)• MA-4(1)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-001044
	CCE	<ul style="list-style-type: none">• CCE-90861-6

7.10. 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)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-001001
	CCE	<ul style="list-style-type: none">• CCE-90862-4

7.11. Configure System to Audit All Deletions of Object Attributes

The audit system *MUST* be configured to record enforcement actions of attempts to delete file attributes (fd).

***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 delete 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 '\-fd'
```

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

ID	audit_flags_fd_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)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-001020
	CCE	<ul style="list-style-type: none">• CCE-90864-0

7.12. Configure System to Audit All Changes of Object Attributes

The audit system *MUST* be configured to record enforcement actions of 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., modifications to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions 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_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)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-001020
	CCE	<ul style="list-style-type: none">• CCE-91086-9

7.13. 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)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-001020
	CCE	<ul style="list-style-type: none"> • CCE-90866-5

7.14. 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	800-53r5 <ul style="list-style-type: none"> • AC-2(12) • AU-12 • AU-2 • AU-9 • CM-5(1) • MA-4(1) 	
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-001020
	CCE	<ul style="list-style-type: none"> • CCE-90867-3

7.15. 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.*[^\n]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) 	
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-001002
	CCE	<ul style="list-style-type: none"> • CCE-90868-1

7.16. 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 $(/usr/bin/awk -F : '/^dir/{print $2}' /etc/security/audit_control)
```

ID	audit_folder_group_configure
-----------	------------------------------

References	800-53r5	<ul style="list-style-type: none"> • AU-9
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-001015
	CCE	<ul style="list-style-type: none"> • CCE-90869-9

7.17. Configure Audit Log Folders 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 -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 $(/usr/bin/awk -F : '/^dir/{print $2}' /etc/security/audit_control)
```

ID	audit_folder_owner_configure	
References	800-53r5	<ul style="list-style-type: none"> • AU-9
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-001013
	CCE	<ul style="list-style-type: none"> • CCE-90870-7

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

ID	audit_folders_mode_configure	
References	800-53r5	• AU-9
	DISA STIG(s)	• APPL-12-001017
	CCE	• CCE-90871-5

7.19. Configure Audit Retention to a Minimum of Seven Days

The audit service *MUST* be configured to require records be kept for seven days or longer before deletion, unless the system uses a central audit record storage facility.

When "expire-after" is set to "7d", the audit service will not delete audit logs until the log data is at least seven days old.

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 **7d**, 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:7d/'  
/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
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-001029
	CCE	<ul style="list-style-type: none">• CCE-90875-6

7.20. Configure Audit Failure Notification

The audit service *MUST* be configured to immediately print messages to the console or email administrator users when an auditing failure occurs.

It is critical for the appropriate personnel to be made aware immediately if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of a potentially harmful failure in the auditing system's capability, and system operation may be adversely affected.

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

```
/usr/bin/grep -c "logger -s -p" /etc/security/audit_warn
```

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/sed -i.bak 's/logger -p/logger -s -p/' /etc/security/audit_warn;  
/usr/sbin/audit -s
```

ID	audit_settings_failure_notify	
References	800-53r5	• AU-5, AU-5(2)
	DISA STIG(s)	• APPL-12-001031
	CCE	• CCE-90876-4

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)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002009
	CCE	<ul style="list-style-type: none">• CCE-90898-8

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):

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

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 enable system/com.apple.mrt
```

ID	os_anti_virus_installed	
References	800-53r5	• N/A
	DISA STIG(s)	• APPL-12-002070
	CCE	• CCE-90900-2

8.3. Disable Apple ID Setup during Setup Assistant

The prompt for Apple ID setup during Setup Assistant *MUST* be disabled.

macOS will automatically prompt new users to set up an Apple ID while they are going through Setup Assistant if this is not disabled, misleading new users to think they need to create Apple ID accounts upon their first login.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipCloudSetup').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.SetupAssistant.managed) payload type:

```
<key>SkipCloudSetup</key>
<true/>
```

ID	os_appleid_prompt_disable	
References	800-53r5	• AC-20
	DISA STIG(s)	• APPL-12-002035
	CCE	• CCE-90902-8

8.4. Configure Apple System Log Files Owned by Root and Group to Wheel

The Apple System Logs (ASL) *MUST* be owned by root.

ASL logs contain sensitive data about the system and users. If ASL 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):

```
/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* |
/usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{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:

```
/usr/sbin/chown root:wheel $(/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/awk -F":" '!/^root:wheel:/{print $3}')
```

ID	os_asl_log_files_owner_group_configure	
References	800-53r5	<ul style="list-style-type: none">• SI-11
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-004001
	CCE	<ul style="list-style-type: none">• CCE-90904-4

8.5. Configure Apple System Log Files To Mode 640 or Less Permissive

The Apple System Logs (ASL) *MUST* be configured to be writable by root and readable only by the root user and group wheel. To achieve this, ASL log files *MUST* be configured to mode 640 permissive or less; thereby preventing normal users from reading, modifying or deleting audit logs. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

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

```
/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/640/{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 640 $(/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf  
/etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk -F":"  
'!/640/{print $2}')
```

ID	os_asl_log_files_permissions_configure	
References	800-53r5	• SI-11
	DISA STIG(s)	• APPL-12-004002
	CCE	• CCE-90905-1

8.6. Disable Blank Blu Ray

Blank Blu Ray media *MUST* be disabled.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS  
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\  
.objectForKey('mount-controls'))["blankbd"]  
EOS
```

If the result is not **deny,eject**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_blank_bluray_disable	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91094-3

8.7. Disable Blank CD

Blank CD media *MUST* be disabled.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["blankcd"]
EOS
```

If the result is not **deny,eject**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_blank_cd_disable	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91095-0

8.8. Disable Blank DVD

Blank DVD media *MUST* be disabled.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["blankdvd"]
EOS
```

If the result is not **deny,eject**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_blank_dvd_disable	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91096-8

8.9. Enforce Blu Ray Read Only

Blu Ray media *MUST* be set to read only.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["bd"]
EOS
```

If the result is not **read-only**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_bluray_read_only_enforce	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91097-6

8.10. 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	<ul style="list-style-type: none"> • CM-7, CM-7(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002005
	CCE	<ul style="list-style-type: none"> • CCE-90908-5

8.11. Disable Burn Support

Burn support *MUST* be disabled. [IMPORTANT] ==== Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization. ====

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -Ec '(ProhibitBurn = 0|BurnSupport = "off")'
```

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.finder) payload type:

```
<key>ProhibitBurn</key>
<true/>
```

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

```
<key>BurnSupport</key>
<string>off</string>
```

ID	os_burn_support_disable
-----------	-------------------------

References	800-53r5	<ul style="list-style-type: none"> • MP-7
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-005053
	CCE	<ul style="list-style-type: none"> • CCE-91098-4

8.12. Disable Camera

macOS *MUST* be configured to disable the camera.

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('allowCamera').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>allowCamera</key>
<false/>
```

ID	os_camera_disable	
References	800-53r5	<ul style="list-style-type: none"> • N/A
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002017
	CCE	<ul style="list-style-type: none"> • CCE-90910-1

8.13. Enforce CD Read Only

CD media *MUST* be set to read only.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["cd"]
EOS
```

If the result is not **read-only**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_cd_read_only_enforce	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91099-2

8.14. Issue or Obtain Public Key Certificates from an Approved Service Provider

The organization *MUST* issue or obtain public key certificates from an organization-approved service provider and ensure only approved trust anchors are in the System Keychain.

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

```
/usr/bin/security dump-keychain /Library/Keychains/System.keychain | /usr/bin/awk -F'"' '/labl/ {print $4}'
```

If the result is not a **list containing approved root certificates**, this is a finding.

Remediation Description

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

Obtain the approved certificates from the appropriate authority and install them to the System Keychain.

ID	os_certificate_authority_trust	
References	800-53r5	• SC-17
	DISA STIG(s)	• APPL-12-003001
	CCE	• CCE-90911-9

8.15. Enforce Installation of XProtect, MRT, and Gatekeeper Updates Automatically

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

This setting enforces definition updates for XProtect, MRT, 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, MRT, 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
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002070
	CCE	<ul style="list-style-type: none">• CCE-90913-5

8.16. Integrate System into a Directory Services Infrastructure

The macOS system *MUST* be integrated into a directory services infrastructure.

A directory service infrastructure enables centralized user and rights management, as well as centralized control over computer and user configurations. Integrating the macOS systems used throughout an organization into a directory services infrastructure ensures more administrator oversight and security than allowing distinct user account databases to exist on each separate system.

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

```
/usr/bin/dscl localhost -list . | /usr/bin/grep -qvE '(Contact|Search|Local|^$)';
/bin/echo $?
```

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

Remediation Description

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

Integrate the system into an existing directory services infrastructure.

ID	os_directory_services_configured	
References	800-53r5	• N/A
	DISA STIG(s)	• APPL-12-000016
	CCE	• CCE-91087-7

8.17. Disable Disk Images

Disk images *MUST* be disabled.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["disk-image"]
EOS
```

If the result is not **deny**,**eject**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_disk_image_disable	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91100-8

8.18. Disable Blank CD

Blank CD media *MUST* be disabled.



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["dvdram"]
EOS
```

If the result is not **deny,eject**, 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.systemuiserver) payload type:

```
<key>mount-controls</key>
```

ID	os_dvdram_disable	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-91101-6

8.19. Disable Erase Content and Settings

Erase Content and Settings *MUST* be disabled.

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('allowEraseContentAndSettings').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>allowEraseContentAndSettings</key>
<false/>
```

ID	os_erase_content_and_settings_disable	
References	800-53r5	<ul style="list-style-type: none"> • CM-7, CM-7(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-005061
	CCE	<ul style="list-style-type: none"> • CCE-91103-2

8.20. Must Use ESS

The approved ESS solution *MUST* be installed and configured to run.

The macOS system must employ automated mechanisms to determine the state of system components. The DoD requires the installation and use of an approved ESS solution to be implemented on the operating system. For additional information, reference all applicable ESS OPODs and FRAGOs on SIPRNET.

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

Ask the System Administrator (SA) or Information System Security Officer (ISSO) **if** the approved ESS solution is loaded on the system.
 If the installed components of the ESS solution are not at the DoD approved minimal versions, this is a finding.

If the result is not N/A, this is a finding.

Remediation Description

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

Install the approved ESS solution onto the system.

ID	os_ess_installed	
References	800-53r5	<ul style="list-style-type: none"> • N/A
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000015
	CCE	<ul style="list-style-type: none"> • CCE-90930-9

8.21. FileVault Authorized Users

macOS *MUST* be configured to only allow authorized users to unlock FileVault upon startup.

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

```
/usr/bin/fdesetup list | /usr/bin/awk -F',' '{print $1}'
```

If the result is not **a list containing authorized users that can unlock FileVault**, this is a finding.

Remediation Description

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

Remove the user that is not authorized to unlock FileVault using the fdesetup command.

```
/usr/bin/fdesetup remove -user NOT_AUTHORIZED_USERNAME
```

ID	os_filevault_authorized_users	
References	800-53r5	• AC-2(11)
	DISA STIG(s)	• APPL-12-000032
	CCE	• CCE-90921-8

8.22. Disable FileVault Automatic Login

If FileVault is enabled, automatic login *MUST* be disabled, so that both FileVault and login window authentication are required.

The default behavior of macOS when FileVault is enabled is to automatically log in to the computer once successfully passing your FileVault credentials.



DisableFDEAutoLogin does not have to be set on Apple Silicon based macOS systems that are smartcard enforced as smartcards are available at pre-boot.

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('DisableFDEAutoLogin').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>DisableFDEAutoLogin</key>
<true/>
```

ID	os_filevault_autologin_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-2(11)• AC-3• IA-5(13)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-000033
	CCE	<ul style="list-style-type: none">• CCE-90922-6

8.23. Enable Firmware Password

A firmware password *MUST* be enabled and set.

Single user mode, recovery mode, the Startup Manager, and several other tools are available on macOS by holding the "Option" key down during startup. Setting a firmware password restricts access to these tools.

To set a firmware passcode use the following command:

```
/usr/sbin/firmwarepasswd -setpasswd
```



If firmware password or passcode is forgotten, the only way to reset the forgotten password is through the use of a machine specific binary generated and provided by Apple. Schedule a support call, and provide proof of purchase before the firmware binary will be generated.



Firmware passwords are not supported on Apple Silicon devices. This rule is only applicable to Intel devices.

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

```
/usr/sbin/firmwarepasswd -check | /usr/bin/grep -c "Password Enabled: Yes"
```

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

Remediation Description

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



See discussion on remediation and how to enable firmware password.

ID	os_firmware_password_require	
References	800-53r5	• AC-6
	DISA STIG(s)	• APPL-12-003013
	CCE	• CCE-90925-9

8.24. 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/sbin/spctl --status | /usr/bin/grep -c "assessments enabled"
```

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.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)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002064
	CCE	<ul style="list-style-type: none">• CCE-90926-7

8.25. Disable Handoff

Handoff *MUST* be disabled.

Handoff allows you to continue working on a document or project when the user switches from one Apple device to another. Disabling Handoff prevents data transfers to unauthorized 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('allowActivityContinuation').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>allowActivityContinuation</key>
<false/>
```

ID	os_handoff_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• AC-3• CM-7, CM-7(1)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-005058
	CCE	<ul style="list-style-type: none">• CCE-90929-1

8.26. 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 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 -1 |
/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 $( /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth
1 -type d -perm -1 | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" ); do
  /bin/chmod og-rwx "$userDirs"
done
unset IFS
```

ID	os_home_folders_secure	
References	800-53r5	• AC-6
	DISA STIG(s)	• APPL-12-002068
	CCE	• CCE-90931-7

8.27. 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" => true'
```

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
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002008
	CCE	<ul style="list-style-type: none"> • CCE-90932-5

8.28. Disable iCloud Storage Setup during Setup Assistant

The prompt to set up iCloud storage services during Setup Assistant *MUST* be disabled.

The default behavior of macOS is to prompt new users to set up storage in iCloud. Disabling the iCloud storage setup prompt provides organizations more control over the storage of their data.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipiCloudStorageSetup').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.SetupAssistant.managed) payload type:

```
<key>SkipiCloudStorageSetup</key>
<true/>
```

ID	os_icloud_storage_prompt_disable
----	----------------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002037
	CCE	<ul style="list-style-type: none"> • CCE-90933-3

8.29. Configure System Log Files Owned by Root and Group to Wheel

The system log files *MUST* be owned by root.

System 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):

```
/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf |
/usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{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:

```
/usr/sbin/chown root:wheel $(/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#'
/etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk -
F":" '!/^root:wheel:/{print $3}')
```

ID	os_newsyslog_files_owner_group_configure	
References	800-53r5	<ul style="list-style-type: none"> • SI-11
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-004001
	CCE	<ul style="list-style-type: none"> • CCE-90954-9

8.30. Configure System Log Files to Mode 640 or Less Permissive

The system logs *MUST* be configured to be writable by root and readable only by the root user and group wheel. To achieve this, system log files *MUST* be configured to mode 640 permissive or less; thereby preventing normal users from reading, modifying or deleting audit logs. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

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

```
/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{
print $1 }') 2> /dev/null | /usr/bin/awk '!/640/{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 640 $(/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#'
/etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk
'!/640/{print $1}' | awk -F":" '!/640/{print $2}')
```

ID	os_newsyslog_files_permissions_configure	
References	800-53r5	• SI-11
	DISA STIG(s)	• APPL-12-004002
	CCE	• CCE-90955-6

8.31. 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" => true'
```

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-17• AC-3
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002003
	CCE	<ul style="list-style-type: none">• CCE-90956-4

8.32. Disable Proximity Based Password Sharing Requests

Proximity based password sharing requests *MUST* be disabled.

The default behavior of macOS is to allow users to request passwords from other known devices (macOS and iOS). This feature *MUST* be disabled to prevent passwords from being shared.

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('allowPasswordProximityRequests').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>allowPasswordProximityRequests</key>
<false/>
```

ID	os_password_proximity_disable	
References	800-53r5	• IA-5
	DISA STIG(s)	• APPL-12-005060
	CCE	• CCE-90968-9

8.33. 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. NOTE: The banner text of the document *MUST* read:

"You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and for any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning."

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="You are accessing a U.S. Government information system, which
includes: 1) this computer, 2) this computer network, 3) all Government-furnished
computers connected to this network, and 4) all Government-furnished devices and
storage media attached to this network or to a computer on this network. You
understand and consent to the following: you may access this information system
for authorized use only; unauthorized use of the system is prohibited and subject
to criminal and civil penalties; you have no reasonable expectation of privacy
regarding any communication or data transiting or stored on this information
system at any time and for any lawful Government purpose, the Government may
monitor, intercept, audit, and search and seize any communication or data
transiting or stored on this information system; and any communications or data
transiting or stored on this information system may be disclosed or used for any
lawful Government purpose. This information system may contain Controlled
Unclassified Information (CUI) that is subject to safeguarding or dissemination
controls in accordance with law, regulation, or Government-wide policy. Accessing
and using this system indicates your understanding of this warning."
/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	<ul style="list-style-type: none">• AC-8
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-000025
	CCE	<ul style="list-style-type: none">• CCE-90973-9

8.34. Display Policy Banner at Remote Login

Remote login service *MUST* be configured to display a policy banner at login.

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.

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

```
bannerText="You are accessing a U.S. Government information system, which includes: 1)
this computer, 2) this computer network, 3) all Government-furnished computers
connected to this network, and 4) all Government-furnished devices and storage media
attached to this network or to a computer on this network. You understand and consent
to the following: you may access this information system for authorized use only;
unauthorized use of the system is prohibited and subject to criminal and civil
penalties; you have no reasonable expectation of privacy regarding any communication
or data transiting or stored on this information system at any time and for any lawful
Government purpose, the Government may monitor, intercept, audit, and search and seize
any communication or data transiting or stored on this information system; and any
communications or data transiting or stored on this information system may be
disclosed or used for any lawful Government purpose. This information system may
contain Controlled Unclassified Information (CUI) that is subject to safeguarding or
dissemination controls in accordance with law, regulation, or Government-wide policy.
Accessing and using this system indicates your understanding of this warning."
/usr/bin/grep -c "$bannerText" /etc/banner
```

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

Remediation Description

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

```
bannerText="You are accessing a U.S. Government information system, which
includes: 1) this computer, 2) this computer network, 3) all Government-furnished
computers connected to this network, and 4) all Government-furnished devices and
storage media attached to this network or to a computer on this network. You
understand and consent to the following: you may access this information system
for authorized use only; unauthorized use of the system is prohibited and subject
to criminal and civil penalties; you have no reasonable expectation of privacy
regarding any communication or data transiting or stored on this information
system at any time and for any lawful Government purpose, the Government may
monitor, intercept, audit, and search and seize any communication or data
transiting or stored on this information system; and any communications or data
transiting or stored on this information system may be disclosed or used for any
lawful Government purpose. This information system may contain Controlled
Unclassified Information (CUI) that is subject to safeguarding or dissemination
controls in accordance with law, regulation, or Government-wide policy. Accessing
and using this system indicates your understanding of this warning."
/bin/echo "${bannerText}" > /etc/banner
```

ID

os_policy_banner_ssh_configure

References	800-53r5	<ul style="list-style-type: none"> • AC-8
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000023
	CCE	<ul style="list-style-type: none"> • CCE-90974-7

8.35. Enforce SSH to Display Policy Banner

SSH *MUST* be configured to display a policy banner.

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



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^Banner /etc/banner" /etc/ssh/sshd_config
```

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/sed -i.bak 's/^[^#]*Banner.*/Banner \etc\banner/' /etc/ssh/sshd_config
```

ID	os_policy_banner_ssh_enforce	
References	800-53r5	<ul style="list-style-type: none"> • AC-8
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000024
	CCE	<ul style="list-style-type: none"> • CCE-90975-4

8.36. Disable Privacy Setup Services During Setup Assistant

The prompt for Privacy Setup services during Setup Assistant *MUST* be disabled.

Organizations *MUST* apply organization-wide configuration settings. The macOS Privacy Setup services prompt guides new users through enabling their own specific privacy settings; this is not essential and, therefore, *MUST* be disabled to prevent against the risk of individuals electing privacy settings with the potential to override organization-wide settings.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipPrivacySetup').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.SetupAssistant.managed) payload type:

```
<key>SkipPrivacySetup</key>
<true/>
```

ID	os_privacy_setup_prompt_disable	
References	800-53r5	• CM-7, CM-7(1)
	DISA STIG(s)	• APPL-12-002036
	CCE	• CCE-90981-2

8.37. Disable Removable Storage Devices

Removable media, such as USB connected external hard drives, thumb drives, and optical media, *MUST* be disabled for users.

Disabling removable storage devices reduces the risks and known vulnerabilities of such devices (e.g., malicious code insertion)



Some organizations rely on the use of removable media for storing and sharing data. Information System Security Officers (ISSOs) may make the risk-based decision not to disable external hard drives to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.



Apple has deprecated the use of media mount controls, using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

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

```
/usr/bin/osascript -l JavaScript << EOS
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systemuiserver')\
.objectForKey('mount-controls'))["hddisk-external"]
EOS
```

If the result is not **deny,eject**, 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.systemuiserver) payload type:

<key>mount-controls</key>

ID	os_removable_media_disable	
References	800-53r5	• MP-7
	DISA STIG(s)	• APPL-12-005051
	CCE	• CCE-90991-1

8.38. Enforce Screen Saver at Login Window

A default screen saver *MUST* be configured to display at the login window and *MUST* not display any sensitive information.

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

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

If the result is not `/System/Library/Screen Savers/Flurry.saver`, 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>loginWindowModulePath</key>
<string>/System/Library/Screen Savers/Flurry.saver</string>
```

ID	os_screensaver_loginwindow_enforce	
References	800-53r5	• AC-11(1)
	DISA STIG(s)	• APPL-12-000006
	CCE	• CCE-90995-2

8.39. 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 reenable "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
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-005001
	CCE	<ul style="list-style-type: none">• CCE-91000-0

8.40. Disable Siri Setup during Setup Assistant

The prompt for Siri during Setup Assistant *MUST* be disabled.

Organizations *MUST* apply organization-wide configuration settings. The macOS Siri Assistant Setup prompt guides new users through enabling their own specific Siri settings; this is not essential and, therefore, *MUST* be disabled to prevent against the risk of individuals electing Siri settings with the potential to override organization-wide settings.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipSiriSetup').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.SetupAssistant.managed) payload type:

```
<key>SkipSiriSetup</key>
<true/>
```

ID	os_siri_prompt_disable	
References	800-53r5	<ul style="list-style-type: none"> • AC-20 • CM-7, CM-7(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002039
	CCE	<ul style="list-style-type: none"> • CCE-91001-8

8.41. Disable Screen Time Prompt During Setup Assistant

The prompt for Screen Time setup during Setup Assistant *MUST* be disabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipScreenTime').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.SetupAssistant.managed) payload type:

```
<key>SkipScreenTime</key>
<true/>
```

ID	os_skip_screen_time_prompt_enable	
References	800-53r5	• CM-7, CM-7(1)
	DISA STIG(s)	• APPL-12-005055
	CCE	• CCE-91113-1

8.42. Disable Unlock with Apple Watch During Setup Assistant

The prompt for Apple Watch unlock setup during Setup Assistant *MUST* be disabled.

Disabling Apple watches is a necessary step to ensuring that the information system retains a session lock until the user reestablishes access using an authorized identification and authentication procedures.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipUnlockWithWatch').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.SetupAssistant.managed) payload type:

```
<key>SkipUnlockWithWatch</key>
<true/>
```

ID	os_skip_unlock_with_watch_enable	
References	800-53r5	• AC-20
	DISA STIG(s)	• APPL-12-005056
	CCE	• CCE-91002-6

8.43. Set SSHD Active Client Alive Maximum to Zero

If SSHD is enabled it *MUST* be configured with an Active Client Alive Maximum Count set to zero. Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session or an incomplete login attempt will also free up resources committed by the managed network element.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^ClientAliveCountMax 0" /etc/ssh/sshd_config
```

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/sed -i.bak 's/.*ClientAliveCountMax.*/ClientAliveCountMax 0/'  
/etc/ssh/sshd_config; /bin/launchctl kickstart -k system/com.openssh.sshd
```

ID	os_sshd_client_alive_count_max_configure	
References	800-53r5	• SC-10
	DISA STIG(s)	• APPL-12-000052
	CCE	• CCE-91007-5

8.44. Configure SSHD ClientAliveInterval option set to 900 or less

If SSHD is enabled then it *MUST* be configured with an Active Client Alive Maximum Count set to 900 or less.

Setting the Active Client Alive Maximum Count to 900 (second) will log users out after a 15-minute interval of inactivity.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^ClientAliveInterval 900" /etc/ssh/sshd_config
```

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/sed -i.bak 's/.*ClientAliveInterval.*/ClientAliveInterval 900/'  
/etc/ssh/sshd_config; /bin/launchctl kickstart -k system/com.openssh.sshd
```

ID	os_sshd_client_alive_interval_configure	
References	800-53r5	<ul style="list-style-type: none"> • AC-12 • SC-10
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000051
	CCE	<ul style="list-style-type: none"> • CCE-91008-3

8.45. Limit SSHD to FIPS 140 Validated Ciphers

If SSHD is enabled then it *MUST* be configured to limit the ciphers to algorithms that are FIPS 140 validated.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meet federal requirements.

Operating systems utilizing encryption *MUST* use FIPS validated mechanisms for authenticating to cryptographic modules.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^Ciphers aes256-ctr,aes192-ctr,aes128-ctr" /etc/ssh/sshd_config
```

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 -q '^Ciphers' /etc/ssh/sshd_config && /usr/bin/sed -i.bak
's/^Ciphers.*/Ciphers aes256-ctr,aes192-ctr,aes128-ctr/' /etc/ssh/sshd_config ||
/bin/echo 'Ciphers aes256-ctr,aes192-ctr,aes128-ctr' >> /etc/ssh/sshd_config;
/bin/launchctl kickstart -k system/com.openssh.sshd
```

ID	os_sshd_fips_140_ciphers
-----------	--------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-17(2) • IA-7 • SC-13 • SC-8(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000054
	CCE	<ul style="list-style-type: none"> • CCE-91114-9

8.46. Limit SSHD to FIPS 140 Validated Message Authentication Code Algorithms

If SSHD is enabled then it *MUST* be configured to limit the Message Authentication Codes (MACs) to algorithms that are FIPS 140 validated.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets federal requirements.

Operating systems utilizing encryption *MUST* use FIPS validated mechanisms for authenticating to cryptographic modules.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^MACs hmac-sha2-256,hmac-sha2-512" /etc/ssh/sshd_config
```

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 -q '^MACs' /etc/ssh/sshd_config && /usr/bin/sed -i.bak
's/. *MACs.* /MACs hmac-sha2-256,hmac-sha2-512/' /etc/ssh/sshd_config || /bin/echo
'MACs hmac-sha2-256,hmac-sha2-512' >> /etc/ssh/sshd_config; /bin/launchctl
kickstart -k system/com.openssh.sshd
```

ID	os_sshd_fips_140_macs
-----------	-----------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-17(2) • IA-7 • SC-13 • SC-8(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000055
	CCE	<ul style="list-style-type: none"> • CCE-91115-6

8.47. Configure SSHD to Use Secure Key Exchange Algorithms

Unapproved mechanisms for authentication to the cryptographic module are not verified, and therefore cannot be relied upon to provide confidentiality or integrity, resulting in the compromise of DoD data.

Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

The implementation of OpenSSH that is included with macOS does not utilize a FIPS 140-2 validated cryptographic module. While the listed Key Exchange Algorithms are FIPS 140-2 approved, the module implementing them has not been validated.

By specifying a Key Exchange Algorithm list with the order of hashes being in a "strongest to weakest" orientation, the system will automatically attempt to use the strongest Key Exchange Algorithm for securing SSH connections.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^KexAlgorithms diffie-hellman-group-exchange-sha256"
/etc/ssh/sshd_config
```

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 -q '^KexAlgorithms' /etc/ssh/sshd_config && /usr/bin/sed -i.bak  
's/. *KexAlgorithms.*/KexAlgorithms diffie-hellman-group-exchange-sha256/'  
/etc/ssh/sshd_config || /bin/echo 'KexAlgorithms diffie-hellman-group-exchange-  
sha256' >> /etc/ssh/sshd_config; /bin/launchctl kickstart -k  
system/com.openssh.sshd
```

ID	os_sshd_key_exchange_algorithm_configure	
References	800-53r5	<ul style="list-style-type: none">• AC-17(2)• IA-7• MA-4(6)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-000056
	CCE	<ul style="list-style-type: none">• CCE-91011-7

8.48. Set Login Grace Time to 30 or Less

If SSHD is enabled then it *MUST* be configured to wait only 30 seconds before timing out logon attempts.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^LoginGraceTime 30" /etc/ssh/sshd_config
```

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/sed -i.bak 's/.*LoginGraceTime.*/LoginGraceTime 30/'  
/etc/ssh/sshd_config; /bin/launchctl kickstart -k system/com.openssh.sshd
```

ID	os_sshd_login_grace_time_configure	
References	800-53r5	• SC-10
	DISA STIG(s)	• APPL-12-000053
	CCE	• CCE-91012-5

8.49. Disable Root Login for SSH

If SSH is enabled to assure individual accountability and prevent unauthorized access, logging in as root via SSH *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.



/etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

```
/usr/bin/grep -c "^PermitRootLogin no" /etc/ssh/sshd_config
```

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/sed -i.bak 's/^[^#]*PermitRootLogin.*/PermitRootLogin no/'  
/etc/ssh/sshd_config; /bin/launchctl kickstart -k system/com.openssh.sshd
```

ID	os_sshd_permit_root_login_configure	
References	800-53r5 <ul style="list-style-type: none"> • IA-2(5) 	
	DISA STIG(s) <ul style="list-style-type: none"> • APPL-12-001100 	
	CCE <ul style="list-style-type: none"> • CCE-91013-3 	

8.50. Configure Sudoers to Authenticate Users on a Per-tty Basis

The file `/etc/sudoers` *MUST* be configured to include `tty_tickets`.

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. Without the "tty_tickets" option, all open local and remote logon sessions would be authenticated to use sudo without a password for the duration of the configured password timeout window.

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

```
/usr/bin/find /etc/sudoers* -type f -exec /usr/bin/grep -E "^Defaults\s+\\!tty_tickets"
'{}' \; | /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:

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

ID	os_sudoers_tty_configure
-----------	--------------------------

References	800-53r5	<ul style="list-style-type: none"> • CM-5(1) • IA-11
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-004021
	CCE	<ul style="list-style-type: none"> • CCE-91015-8

8.51. Disable Trivial File Transfer Protocol Service

If the system does not require Trivial File Transfer Protocol (TFTP), support it is non-essential and *MUST* be disabled.

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



TFTP 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 '"com.apple.tftpd" => true'
```

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.tftpd
```

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

ID	os_tftpd_disable
-----------	------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-17 • AC-3 • IA-5(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002038
	CCE	<ul style="list-style-type: none"> • CCE-91018-2

8.52. 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
```

ID	os_time_server_enabled	
References	800-53r5	<ul style="list-style-type: none"> • AU-12(1) • SC-45(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000014
	CCE	<ul style="list-style-type: none"> • CCE-91019-0

8.53. Disable TouchID Prompt during Setup Assistant

The prompt for TouchID during Setup Assistant *MUST* be disabled.

macOS prompts new users through enabling TouchID during Setup Assistant; this is not essential and, therefore, *MUST* be disabled to prevent against the risk of individuals electing to enable TouchID to override organization-wide settings.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipTouchIDSetup').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.SetupAssistant.managed) payload type:

```
<key>SkipTouchIDSetup</key>
<true/>
```

ID	os_touchid_prompt_disable	
References	800-53r5	• CM-6
	DISA STIG(s)	• APPL-12-005054
	CCE	• CCE-91020-8

8.54. Disable Unix-to-Unix Copy Protocol Service

The system *MUST* not have the Unix-to-Unix Copy Protocol (UUCP) service active.

UUCP, a set of programs that enable the sending of files between different UNIX systems as well as sending commands to be executed on another system, is not essential and *MUST* be disabled in order to prevent the unauthorized connection of devices, transfer of information, and tunneling.



UUCP 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 '"com.apple.uucp" => true'
```

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.uucp
```

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

ID	os_uucp_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002006
	CCE	<ul style="list-style-type: none">• CCE-91024-0

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. Restrict Maximum Password Lifetime to 60 Days

The macOS *MUST* be configured to enforce a maximum password lifetime limit of at least 60 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.



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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('maxPINAgeInDays').js
EOS
```

If the result is not **60**, 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>60</integer>
```

ID	pwpolicy_60_day_enforce	
References	800-53r5	• IA-5
	DISA STIG(s)	• APPL-12-003008
	CCE	• CCE-91027-3

9.2. Limit Consecutive Failed Login Attempts to Three

The macOS *MUST* be configured to limit the number of failed login attempts to a maximum of three. 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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('maxFailedAttempts').js
EOS
```

If the result is not 3, 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>3</integer>
```

ID	pwpolicy_account_lockout_enforce	
References	800-53r5	• AC-7
	DISA STIG(s)	• APPL-12-000022
	CCE	• CCE-91029-9

9.3. 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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('minutesUntilFailedLoginReset').js
EOS
```

If the result is not 15, 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	• AC-7
	DISA STIG(s)	• APPL-12-000022
	CCE	• CCE-91030-7

9.4. 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.



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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('requireAlphanumeric').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.mobiledevice.passwordpolicy) payload type:

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

ID	pwpolicy_alpha_numeric_enforce	
References	800-53r5	• IA-5(1)
	DISA STIG(s)	• APPL-12-003007
	CCE	• CCE-91031-5

9.5. Prohibit Password Reuse for a Minimum of Five Generations

The macOS *MUST* be configured to enforce a password history of at least five 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 five 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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('pinHistory').js
EOS
```

If the result is not 5, 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>5</integer>
```

ID	pwpolicy_history_enforce	
References	800-53r5	• IA-5(1)
	DISA STIG(s)	• APPL-12-003009
	CCE	• CCE-91034-9

9.6. 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.



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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('minLength').js
EOS
```

If the result is not 15, 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)
	DISA STIG(s)	• APPL-12-003010
	CCE	• CCE-91036-4

9.7. 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.



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/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mobiledevice.passwordpolicy')\
.objectForKey('minComplexChars').js
EOS
```


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

ID	pwpolicy_special_character_enforce	
References	800-53r5	• IA-5(1)
	DISA STIG(s)	• APPL-12-003011
	CCE	• CCE-91040-6

9.8. Automatically Remove or Disable Temporary or Emergency User Accounts within 72 Hours

The macOS is able to be configured to set an automated termination for 72 hours or less for all temporary or emergency accounts upon account creation.

Emergency administrator accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Although the ability to create and use emergency administrator accounts is necessary for performing system maintenance during emergencies, these accounts present vulnerabilities to the system if they are not disabled and removed when they are no longer needed. Configuring the macOS to automatically remove or disable emergency accounts within 72 hours of creation mitigates the risks posed if one were to be created and accidentally left active once the crisis is resolved.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon is not available). Infrequently used accounts also remain available and are not subject to automatic termination dates. However, an emergency administrator account is normally a different account created for

use by vendors or system maintainers.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

If temporary or emergency user accounts remain active when no longer needed or for an excessive period, these accounts may be targeted by attackers to gain unauthorized access. To mitigate this risk, automated termination of all temporary or emergency accounts *MUST* be set to 72 hours (or less) when the temporary or emergency account is created.

If no policy is enforced by a directory service, a password policy can be set with the "pwpolicy" utility. The variable names may vary depending on how the policy was set.

If there are no temporary or emergency accounts defined on the system, this is Not Applicable.

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

Verify **if** a password policy is enforced by a directory service by asking the System Administrator (SA) or Information System Security Officer (ISSO).

If no policy is enforced by a directory service, a password policy can be **set** with the "pwpolicy" utility. The variable names may vary depending on how the policy was set.

If there are no temporary or emergency accounts defined on the system, this is Not Applicable.

To check **if** the password policy is configured to disable a temporary or emergency account after 72 hours, run the following **command** to output the password policy to the screen, substituting the correct user name **in** place of username:

```
/usr/bin/pwpolicy -u username getaccountpolicies | tail -n +2
```

If there is no output, and password policy is not controlled by a directory service, this is a finding.

Otherwise, look **for** the line "<key>policyCategoryAuthentication</key>".

In the array that follows, there should be a <dict> section that contains a check <string> that allows **users** to log **in** **if** "policyAttributeCurrentTime" is less than the result of adding "policyAttributeCreationTime" to 72 hours (259200 seconds). The check might use a variable defined **in** its "policyParameters" section.

If the check does not exist or **if** the check adds too great an amount of **time** to "policyAttributeCreationTime", this is a finding.

If the result is not N/A, this is a finding.

Remediation Description

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

This setting may be enforced using local policy or by a directory service.

To set local policy to disable a temporary or emergency user, create a plain text file containing the following:

```
<dict> <key>policyCategoryAuthentication</key> <array> <dict> <key>policyContent</key>
<string>policyAttributeCurrentTime < policyAttributeCreationTime+259299</string>
<key>policyIdentifier</key> <string>Disable Tmp Accounts </string> </dict> </array> </dict>
```

After saving the file and exiting to the command prompt, run the following command to load the new policy file, substituting the correct user name in place of "username" and the path to the file in place of "/path/to/file".

```
/usr/bin/pwppolicy -u username setaccountpolicies /path/to/file
```

ID	pwppolicy_temporary_or_emergency_accounts_disable	
References	800-53r5	• AC-2(2)
	DISA STIG(s)	• APPL-12-000012
	CCE	• CCE-91042-2

10. 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.

10.1. Disable iCloud Address Book

The macOS built-in Contacts.app connection to Apple's iCloud service *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 contact 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('allowCloudAddressBook').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>allowCloudAddressBook</key>
<false/>
```

ID	icloud_addressbook_disable
----	----------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002014
	CCE	<ul style="list-style-type: none"> • CCE-90885-5

10.2. Disable the System Preference Pane for Apple ID

The system preference pane for Apple ID *MUST* be disabled.

Disabling the system preference pane prevents login to Apple ID and iCloud.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.AppleID' |
/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.systempreferences) payload type:

```
<key>DisabledPreferencePanes</key>
<array>
  <string>com.apple.preferences.AppleIDPrefPane</string>
</array>
```

ID	icloud_appleid_prefpane_disable
-----------	---------------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002031
	CCE	<ul style="list-style-type: none"> • CCE-90886-3

10.3. Disable iCloud Bookmarks

The macOS built-in Safari.app bookmark synchronization via the iCloud service *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 bookmark 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('allowCloudBookmarks').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>allowCloudBookmarks</key>
<false/>
```

ID	icloud_bookmarks_disable
-----------	--------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002042
	CCE	<ul style="list-style-type: none"> • CCE-90887-1

10.4. Disable the iCloud Calendar Services

The macOS built-in Calendar.app connection to Apple's iCloud service *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 calendar 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('allowCloudCalendar').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>allowCloudCalendar</key>
<false/>
```

ID	icloud_calendar_disable
-----------	-------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002012
	CCE	<ul style="list-style-type: none"> • CCE-90888-9

10.5. Disable iCloud Document Sync

The macOS built-in iCloud document synchronization service *MUST* be disabled to prevent organizational data from being synchronized to personal or non-approved storage.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated document 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('allowCloudDocumentSync').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>allowCloudDocumentSync</key>
<false/>
```

ID	icloud_drive_disable
----	----------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002041
	CCE	<ul style="list-style-type: none"> • CCE-90889-7

10.6. Disable iCloud Keychain Sync

The macOS system's ability to automatically synchronize a user's passwords to their iCloud account *MUST* be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, password management and 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('allowCloudKeychainSync').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>allowCloudKeychainSync</key>
<false/>
```

ID	icloud_keychain_disable
-----------	-------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002040
	CCE	<ul style="list-style-type: none"> • CCE-90890-5

10.7. Disable iCloud Mail

The macOS built-in Mail.app connection to Apple's iCloud service *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 mail 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('allowCloudMail').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>allowCloudMail</key>
<false/>
```

ID	icloud_mail_disable
-----------	---------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002015
	CCE	<ul style="list-style-type: none"> • CCE-90891-3

10.8. Disable iCloud Notes

The macOS built-in Notes.app connection to Apple's iCloud service *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 Notes 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('allowCloudNotes').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>allowCloudNotes</key>
<false/>
```

ID	icloud_notes_disable
-----------	----------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002016
	CCE	<ul style="list-style-type: none"> • CCE-90892-1

10.9. Disable iCloud Photo Library

The macOS built-in Photos.app connection to Apple's iCloud service *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 photo 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('allowCloudPhotoLibrary').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>allowCloudPhotoLibrary</key>
<false/>
```

ID	icloud_photos_disable
-----------	-----------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002043
	CCE	<ul style="list-style-type: none"> • CCE-90893-9

10.10. Disable iCloud Reminders

The macOS built-in Reminders.app connection to Apple's iCloud service *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 reminders 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('allowCloudReminders').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>allowCloudReminders</key>
<false/>
```

ID	icloud_reminders_disable
-----------	--------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002013
	CCE	<ul style="list-style-type: none"> • CCE-90895-4

11. System Preferences

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



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

11.1. Prevent Apple Watch from Terminating a Session Lock

Apple Watches are not an approved authenticator and their use *MUST* be disabled.

Disabling Apple watches is a necessary step to ensuring that the information system retains a session lock until the user reestablishes access using an authorized identification and authentication procedures.

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('allowAutoUnlock').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>allowAutoUnlock</key>
<false/>
```

ID	sysprefs_apple_watch_unlock_disable
----	-------------------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-11
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000001
	CCE	<ul style="list-style-type: none"> • CCE-91045-5

11.2. 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	sysprefs_automatic_login_disable
----	----------------------------------

References	800-53r5	<ul style="list-style-type: none"> • IA-2 • IA-5(13)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002066
	CCE	<ul style="list-style-type: none"> • CCE-91046-3

11.3. Disable Bluetooth When no Approved Device is Connected

The macOS system *MUST* be configured to disable Bluetooth unless there is an approved device connected.



Information System Security Officers (ISSOs) may make the risk-based decision not to disable Bluetooth, so as to maintain necessary functionality, but they are advised to first fully weigh the potential risks posed to their organization.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCXBluetooth')\
.objectForKey('DisableBluetooth').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 their defined payload types.

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

```
<key>DisableBluetooth</key>
<true/>
```

ID	sysprefs_bluetooth_disable	
References	800-53r5	<ul style="list-style-type: none"> • AC-18, AC-18(3) • SC-8
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002062
	CCE	<ul style="list-style-type: none"> • CCE-91048-9

11.4. Disable the Bluetooth System Preference Pane

The Bluetooth System Preference pane *MUST* be disabled to prevent access to the bluetooth configuration.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.Bluetooth' |
/usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>DisabledPreferencePanes</key>
<array>
  <string>com.apple.preferences.Bluetooth</string>
</array>
```

ID	sysprefs_bluetooth_prefpane_disable
-----------	-------------------------------------

References	800-53r5	<ul style="list-style-type: none"> • N/A
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002062
	CCE	<ul style="list-style-type: none"> • CCE-91150-3

11.5. Hide the Bluetooth System Preference Pane

The Bluetooth System Preference pane *MUST* be hidden to prevent access to the bluetooth configuration.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.Bluetooth' |
/usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>HiddenPreferencePanes</key>
<array>
  <string>com.apple.preferences.Bluetooth</string>
</array>
```

ID	sysprefs_bluetooth_prefpane_hide	
References	800-53r5	<ul style="list-style-type: none"> • N/A
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002062
	CCE	<ul style="list-style-type: none"> • CCE-91125-5

11.6. 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	sysprefs_diagnostics_reports_disable
----	--------------------------------------

References	800-53r5	<ul style="list-style-type: none"> • AC-20 • SC-7(10) • SI-11
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002021
	CCE	<ul style="list-style-type: none"> • CCE-91052-1

11.7. 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):

```
/usr/bin/fdesetup status | /usr/bin/grep -c "FileVault is On."
```

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

Remediation Description

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



See the FileVault supplemental to implement this rule.

ID	sysprefs_filevault_enforce	
References	800-53r5	<ul style="list-style-type: none"> • SC-28, SC-28(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-005020
	CCE	<ul style="list-style-type: none"> • CCE-91053-9

11.8. 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	sysprefs_firewall_enable	
References	800-53r5	<ul style="list-style-type: none">• AC-4• CM-7, CM-7(1)• SC-7, SC-7(12)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-005050
	CCE	<ul style="list-style-type: none">• CCE-91055-4

11.9. 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/>
```

ID	sysprefs_firewall_stealth_mode_enable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)• SC-7, SC-7(16)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-005050
	CCE	<ul style="list-style-type: none">• CCE-91056-2

11.10. Apply Gatekeeper Settings to Block Applications from Unidentified Developers

The information system implements cryptographic mechanisms to authenticate software prior to installation.

Gatekeeper settings must be configured correctly to only allow the system to run applications downloaded from the Mac App Store or applications signed with a valid Apple Developer ID code.

Administrator users will still have the option to override these settings on a per-app basis. Gatekeeper is a security feature that ensures that applications must be digitally signed by an Apple-issued certificate in order to run. Digital signatures allow the macOS to verify that the application has not been modified by a malicious third party.

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

```
/usr/sbin/spctl --status --verbose | /usr/bin/grep -c "developer id enabled"
```

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.systempolicy.control) payload type:

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

ID	sysprefs_gatekeeper_identified_developers_allowed	
References	800-53r5	<ul style="list-style-type: none">• CM-14• CM-5• SI-7(1), SI-7(15)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002060
	CCE	<ul style="list-style-type: none">• CCE-91057-0

11.11. 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
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('DisableGuestAccount').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>DisableGuestAccount</key>
<true/>
```

ID	sysprefs_guest_account_disable	
References	800-53r5	<ul style="list-style-type: none"> • AC-2, AC-2(9)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002063
	CCE	<ul style="list-style-type: none"> • CCE-91060-4

11.12. Disable Hot Corners

Hot corners *MUST* be disabled.

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):

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -Ec '"wvous-bl-corner" = 0|"wvous-br-corner" = 0|"wvous-tl-corner" = 0|"wvous-tr-corner" = 0'
```

If the result is not 4, 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.dock) payload type:

```
<key>wvous-bl-corner</key>
<integer>0</integer>
<key>wvous-br-corner</key>
<integer>0</integer>
<key>wvous-tr-corner</key>
<integer>0</integer>
<key>wvous-tl-corner</key>
<integer>0</integer>
```

ID	sysprefs_hot_corners_disable	
References	800-53r5	• AC-11(1)
	DISA STIG(s)	• APPL-12-000007
	CCE	• CCE-91061-2

11.13. Disable the Internet Accounts System Preference Pane

The Internet Accounts System Preference pane *MUST* be disabled to prevent the addition of unauthorized internet accounts.



Some organizations may allow the use and configuration of the built-in Mail.app, Calendar.app, and Contacts.app for organizational communication. Information System Security Officers (ISSOs) may make the risk-based decision not to disable the Internet Accounts System Preference pane to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c
'com.apple.preferences.internetaccounts' | /usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>DisabledPreferencePanes</key>
<array>
  <string>com.apple.preferences.internetaccounts</string>
</array>
```

ID	sysprefs_internet_accounts_prefpane_disable	
References	800-53r5	<ul style="list-style-type: none"> • AC-20 • CM-7(5)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002032
	CCE	<ul style="list-style-type: none"> • CCE-90938-2

11.14. Hide the Internet Accounts System Preference Pane

The Internet Accounts System Preference pane *MUST* be hidden to prevent the addition of unauthorized internet accounts.



Some organizations may allow the use and configuration of the built-in Mail.app, Calendar.app, and Contacts.app for organizational communication. Information System Security Officers (ISSOs) may make the risk-based decision not to disable the Internet Accounts System Preference pane to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c  
'com.apple.preferences.internetaccounts' | /usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>HiddenPreferencePanes</key>  
<array>  
  <string>com.apple.preferences.internetaccounts</string>  
</array>
```

ID	sysprefs_internet_accounts_prefpane_hide	
References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7(5)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002032
	CCE	<ul style="list-style-type: none">• CCE-91130-5

11.15. 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	sysprefs_internet_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• AC-4
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002007
	CCE	<ul style="list-style-type: none">• CCE-91063-8

11.16. Disable Location Services

Location Services *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling Location Services 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/defaults read
/var/db/locationd/Library/Preferences/ByHost/com.apple.locationd.plist
LocationServicesEnabled
```

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/defaults write
/var/db/locationd/Library/Preferences/ByHost/com.apple.locationd
LocationServicesEnabled -bool false; /bin/launchctl kickstart -k
system/com.apple.locationd
```

ID	sysprefs_location_services_disable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)• SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002004
	CCE	<ul style="list-style-type: none">• CCE-91064-6

11.17. 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	sysprefs_loginwindow_prompt_username_password_enforce	
References	800-53r5	• IA-2
	DISA STIG(s)	• APPL-12-005052
	CCE	• CCE-91065-3

11.18. 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	sysprefs_password_hints_disable	
References	800-53r5	• IA-6
	DISA STIG(s)	• APPL-12-003012
	CCE	• CCE-91067-9

11.19. 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" => true'
```

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 it's parent process. Requires UAMDM.

ID	sysprefs_rae_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002022
	CCE	<ul style="list-style-type: none">• CCE-91070-3

11.20. 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" =>  
true'
```

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	sysprefs_screen_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002050
	CCE	<ul style="list-style-type: none">• CCE-91071-1

11.21. 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 five 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
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('askForPasswordDelay').js
EOS
```

If the result is not 5, 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	sysprefs_screensaver_ask_for_password_delay_enforce	
References	800-53r5	• AC-11
	DISA STIG(s)	• APPL-12-000003
	CCE	• CCE-91072-9

11.22. Enforce Screen Saver Password

Users *MUST* authenticate when unlocking the screen saver.

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

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('askForPassword').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.screensaver) payload type:

```
<key>askForPassword</key>
<true/>
```

ID	sysprefs_screensaver_password_enforce	
References	800-53r5	• AC-11
	DISA STIG(s)	• APPL-12-000002
	CCE	• CCE-91073-7

11.23. Enforce Screen Saver Timeout

The screen saver timeout *MUST* be set to 20 minutes or a shorter length of time.

This rule ensures that a full session lock is triggered within no more than 20 minutes of inactivity.

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

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

If the result is not **1200**, 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	sysprefs_screensaver_timeout_enforce	
References	800-53r5	<ul style="list-style-type: none">• AC-11• IA-11
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-000004
	CCE	<ul style="list-style-type: none">• CCE-91074-5

11.24. Disable Siri

Support for Siri 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.ironwood.support')\
.objectForKey('Ironwood Allowed').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.ironwood.support) payload type:

```
<key>Ironwood Allowed</key>
<false/>
```

ID	sysprefs_siri_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7, CM-7(1)• SC-7(10)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-002020
	CCE	<ul style="list-style-type: none">• CCE-91075-2

11.25. Disable the System Preference Pane for Siri

The system preference pane for Siri *MUST* be disabled.

Disabling the system preference pane prevents the users from configuring Siri.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.speech' |
/usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>DisabledPreferencePanes</key>
<array>
  <string>com.apple.preferences.speech</string>
</array>
```

ID	sysprefs_siri_prefpane_disable	
References	800-53r5	• CM-7, CM-7(5)
	DISA STIG(s)	• APPL-12-002053
	CCE	• CCE-91136-2

11.26. Hide the System Preference Pane for Siri

The system preference pane for Siri *MUST* be hidden.

Hiding the system preference pane prevents the users from configuring Siri.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.speech' |
/usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>HiddenPreferencePanes</key>
<array>
  <string>com.apple.preferences.speech</string>
</array>
```

ID	sysprefs_siri_prefpane_hide	
References	800-53r5	• CM-7, CM-7(5)
	DISA STIG(s)	• APPL-12-002053
	CCE	• CCE-91137-0

11.27. 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" => true'
```

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	sysprefs_smbd_disable	
References	800-53r5	<ul style="list-style-type: none"> • AC-17 • AC-3
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-002001
	CCE	<ul style="list-style-type: none"> • CCE-91076-0

11.28. Disable SSH Server for Remote Access Sessions

SSH service *MUST* be disabled for remote access.

Remote access sessions *MUST* use FIPS validated encrypted methods to protect unauthorized individuals from gaining 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" => true'
```

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.openssh.sshd
```

ID	sysprefs_ssh_disable	
References	800-53r5	<ul style="list-style-type: none"> • AC-17 • CM-7, CM-7(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000011
	CCE	<ul style="list-style-type: none"> • CCE-91077-8

11.29. 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 Preferences.

Some Preference Panes in System Preferences 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):

```
/usr/bin/security authorizationdb read system.preferences 2> /dev/null |  
/usr/bin/grep -A 1 "<key>shared</key>" | /usr/bin/grep -c "<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/security authorizationdb read system.preferences >  
/tmp/system.preferences.plist  
/usr/libexec/PlistBuddy -c "Set :shared false" /tmp/system.preferences.plist  
/usr/bin/security authorizationdb write system.preferences <  
/tmp/system.preferences.plist
```

ID	sysprefs_system_wide_preferences_configure	
References	800-53r5	• AC-6, AC-6(1), AC-6(2)
	DISA STIG(s)	• APPL-12-002069
	CCE	• CCE-91079-4

11.30. Configure macOS to Use an Authorized Time Server

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

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-a.nist.gov,time-b.nist.gov**, 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-a.nist.gov,time-b.nist.gov</string>
```

ID	sysprefs_time_server_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-12(1)• SC-45(1)
	DISA STIG(s)	<ul style="list-style-type: none">• APPL-12-000014
	CCE	<ul style="list-style-type: none">• CCE-91080-2

11.31. Enable macOS Time Synchronization Daemon (timed)

The timed service *MUST* be enabled on all networked systems and configured to set time automatically from the approved time server.

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 their defined payload types.

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

```

<key>TMAutomaticTimeOnlyEnabled</key>
<true/>

```

ID	sysprefs_time_server_enforce	
References	800-53r5	<ul style="list-style-type: none"> • AU-12(1) • SC-45(1)
	DISA STIG(s)	<ul style="list-style-type: none"> • APPL-12-000014
	CCE	<ul style="list-style-type: none"> • CCE-91081-0

11.32. Configure User Session Lock When a Smart Token is Removed

The screen lock *MUST* be configured to initiate automatically when the smart token is removed from the system.

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the information system but do not want to log out because of the temporary nature of their absences. While a session lock is not an acceptable substitute for logging out of an information system for longer periods of time, they prevent a malicious user from accessing the information system when a user has removed their smart token.



Information System Security Officers (ISSOs) may make the risk-based decision not to enforce a session lock when a smart token is removed, so as to maintain necessary workflow capabilities, but they are advised to first fully weigh the potential risks posed to their organization.

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

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

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.security.smartcard) payload type:

```
<key>tokenRemovalAction</key>
<integer>1</integer>
```

ID	sysprefs_token_removal_enforce	
References	800-53r5	• AC-11
	DISA STIG(s)	• APPL-12-000005
	CCE	• CCE-91082-8

11.33. Disable the System Preference Pane for Touch ID

The system preference pane for Touch ID *MUST* be disabled.

Disabling the system preference pane prevents the users from configuring Touch ID.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.password' |  
/usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>DisabledPreferencePanes</key>  
<array>  
  <string>com.apple.preferences.password</string>  
</array>
```

ID	sysprefs_touchid_prefpane_disable	
References	800-53r5	• CM-7, CM-7(5)
	DISA STIG(s)	• APPL-12-002051
	CCE	• CCE-91144-6

11.34. Hide the System Preference Pane for Touch ID

The system preference pane for Touch ID *MUST* be hidden.

Hiding the system preference pane prevents the users from configuring Touch ID.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.password' |  
/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.systempreferences) payload type:

```
<key>HiddenPreferencePanes</key>
<array>
  <string>com.apple.preferences.password</string>
</array>
```

ID	sysprefs_touchid_prefpane_hide	
References	800-53r5	• CM-7, CM-7(5)
	DISA STIG(s)	• APPL-12-002051
	CCE	• CCE-91145-3

11.35. Disable the System Preference Pane for Wallet and Apple Pay

The system preference pane for Wallet and Apple Pay *MUST* be disabled.

Disabling the system preference pane prevents the users from configuring Wallet and Apple Pay.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.wallet' |
/usr/bin/awk '{ if ($1 >= 2) {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.systempreferences) payload type:

```
<key>DisabledPreferencePanes</key>
<array>
  <string>com.apple.preferences.wallet</string>
</array>
```

ID	sysprefs_wallet_applepay_prefpane_disable	
References	800-53r5	• CM-7, CM-7(5)
	DISA STIG(s)	• APPL-12-002052
	CCE	• CCE-91147-9

11.36. Hide the System Preference Pane for Wallet and Apple Pay

The system preference pane for Wallet and Apple Pay *MUST* be hidden.

Hiding the system preference pane prevents the users from configuring Wallet and Apple Pay.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'com.apple.preferences.wallet' |
/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.systempreferences) payload type:

```
<key>HiddenPreferencePanes</key>
<array>
  <string>com.apple.preferences.wallet</string>
</array>
```

ID	sysprefs_wallet_applepay_prefpane_hide	
References	800-53r5	• CM-7, CM-7(5)
	DISA STIG(s)	• APPL-12-002052
	CCE	• CCE-91148-7

12. Supplemental

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

12.1. Out of Scope Supplemental

There are several requirements defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5 that can be met by making configuration changes to the operating system. However, NIST SP 800-53 (Rev. 5) contains a broad set of guidelines that attempt to address all aspects of an information system or systems within an organization. Because the macOS Security Compliance Project is tailored specifically to macOS, some requirements defined in NIST SP 800-53 (Rev. 5) are not applicable.

This supplemental contains those controls that are assigned to a baseline in NIST SP 800-53 (Rev. 5) which cannot be addressed with a technical configuration for macOS. These controls can be accomplished through administrative or procedural processes within an organization or via integration of the macOS system into enterprise information systems which are configured to protect the systems within.

Family	Access Control (AC)
Controls	AC-1 , AC-2 , AC-3(14) , AC-14 , AC-17(4) , AC-22

Family	Awareness and Training (AT)
Controls	AT-1 , AT-2 , AT-3 , AT-4

Family	Audit and Accountability (AU)
Controls	AU-1 , AU-6 , AU-9(2)

Family	Security Assessment and Authorization (CA)
Controls	CA-1 , CA-2 , CA-3 , CA-3(6) , CA-5 , CA-6 , CA-7 , CA-7(4) , CA-9

Family	Configuration Management (CM)
Controls	CM-1 , CM-4 , CM-8 , CM-10 , CM-11

Family	Contingency Planning (CP)
---------------	---------------------------

Controls	CP-1, CP-2, CP-3, CP-4, CP-9, CP-10
-----------------	-------------------------------------

Family	Identification and Authentication (IA)
Controls	IA-1, IA-8(1), IA-8(2), IA-8(3), IA-8(4)

Family	Incident Response (IR)
Controls	IR-1, IR-2, IR-4, IR-5, IR-6, IR-7, IR-8

Family	Maintenance (MA)
Controls	MA-1, MA-2, MA-5

Family	Media Protection (MP)
Controls	MP-1, MP-2, MP-6, MP-7

Family	Physical and Environmental Protection (PE)
Controls	PE-1, PE-2, PE-3, PE-6, PE-8, PE-12, PE-13, PE-14, PE-15, PE-16

Family	Planning (PL)
Controls	PL-1, PL-2, PL-4

Family	Personnel Security (PS)
Controls	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8

Family	Risk Assessment (RA)
Controls	RA-1, RA-2, RA-3, RA-5

Family	System and Services Acquisition (SA)
Controls	SA-1, SA-2, SA-3, SA-4, SA-4(10), SA-5, SA-9

Family	System and Communications Protection (SC)
Controls	SC-1 , SC-7(3) , SC-7(7) , SC-7(8) , SC-7(18) , SC-7(21) , SC-12 , SC-12(1) , SC-20 , SC-22 , SC-23

Family	System and Information Integrity (SI)
Controls	SI-1 , SI-4 , SI-4(2) , SI-4(4) , SI-4(5) , SI-4(12) , SI-4(14) , SI-4(20) , SI-4(22) , SI-5 , SI-7(2) , SI-8(2) , SI-12

12.2. FileVault Supplemental

The supplemental guidance found in this section is applicable for the following rules: *
sysprefs_filevault_enforce

In macOS 11 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.



FileVault currently only uses password-based authentication and cannot be done using a smartcard or any other type of multi-factor authentication.

12.3. Packet Filter (pf) Supplemental

The supplemental guidance found in this section is applicable for the following rules:

- `os_firewall_default_deny_require`

macOS contains an application layer firewall (ALF) and a packet filter (PF) firewall.

- The ALF can block incoming traffic on a per-application basis and prevent applications from gaining control of network ports, but it cannot be configured to block outgoing traffic.

- More information on the ALF can be found here: <https://support.apple.com/en-ca/HT201642>
- The PF firewall can manipulate virtually any packet data and is highly configurable.
 - More information on the BF firewall can be found here: <https://www.openbsd.org/faq/pf/index.html>

Below is a script that configures ALF and the PF firewall to meet the requirements defined in NIST SP 800-53 (Rev. 5). The script will make sure the application layer firewall is enabled, set logging to "detailed", set built-in signed applications to automatically receive incoming connections, and set downloaded signed applications to automatically receive incoming connections. It will then create a custom rule set and copy `com.apple.pfctl.plist` from `/System/Library/LaunchDaemons/` into the `/Library/LaunchDaemons` folder and name it `800-53.pfctl.plist`. This is done to not conflict with the system's pf ruleset.

The custom pf rules are created at `/etc/pf.anchors/800_53_pf_anchors`.

The ruleset will block connections on the following ports:

Port	Service
548	Apple File Protocol (AFP)
1900	Bonjour
79	Finger
20, 21	File Transfer Protocol (FTP)
80	HTTP
icmp	ping
143	Internet Message Access Protocol (IMAP)
993	Internet Message Access Protocol over SSL (IMAPS)
3689	Music Sharing
5353	mDNSResponder
2049	Network File System (NFS)
49152	Optical Media Sharing
110	Post Office Protocol (POP3)
995	Post Office Protocol Secure (POP3S)
631	Printer Sharing
3031	Remote Apple Events
5900	Screen Sharing
137, 138, 139, 445	Samba (SMB)
25	Simple Mail Transfer Protocol (SMTP)
22	Secure Shell (SSH)
23	Telnet

Port	Service
69	Trivial File Transfer Protocol (TFTP)
540	Unix-to-Unix Copy (UUCP)

For more on configuring the PF firewall check out the man pages on [pf.conf](#) and [pfctl](#).

```
#!/bin/bash

#enabling macos application firewall
enable_macos_application_firewall () {

    /usr/libexec/ApplicationFirewall/socketfilterfw --setglobalstate on
    /usr/libexec/ApplicationFirewall/socketfilterfw --setloggingopt detail
    /usr/libexec/ApplicationFirewall/socketfilterfw --setallowsigned on
    /usr/libexec/ApplicationFirewall/socketfilterfw --setallowsignedapp on

}

#enabling pf firewall with macsec rules
enable_pf_firewall_with_macsec_rules () {
    macsec_pfctl_plist="/Library/LaunchDaemons/macsec.pfctl.plist"

    if [[ -e "$macsec_pfctl_plist" ]]; then
        echo "LaunchDaemon already exists, flushing and reloading rules..."
        pfctl -e 2> /dev/null
        pfctl -f /etc/pf.conf 2> /dev/null
        return 0
    fi

    # copy system provided launchd for custom ruleset
    cp "/System/Library/LaunchDaemons/com.apple.pfctl.plist" "$macsec_pfctl_plist"
    #allow pf to be enabled when the job is loaded
    /usr/libexec/PlistBuddy -c "Add :ProgramArguments:1 string -e" $macsec_pfctl_plist
    #use new label to not conflict with System's pfctl
    /usr/libexec/PlistBuddy -c "Set :Label macsec.pfctl" $macsec_pfctl_plist

    # enable the firewall
    pfctl -e 2> /dev/null

    #make pf run at system startup
    launchctl enable system/macsec.pfctl
    launchctl bootstrap system $macsec_pfctl_plist

    pfctl -f /etc/pf.conf 2> /dev/null #flush the pf ruleset (reload the rules)

}

# append the macsec anchors to pf.conf
configure_pf_config_add_macsec_anchors () {
```

```

# check to see if macsec anchors exists
anchors_exist=$(grep -c '^anchor "macsec_pf_anchors"' /etc/pf.conf)

if [[ $anchors_exist == "0" ]];then
    echo 'anchor "macsec_pf_anchors"' >> /etc/pf.conf
    echo 'load anchor "macsec_pf_anchors" from
/etc/pf.anchors/macsec_pf_anchors"' >> /etc/pf.conf
else
    echo "macsec anchors exist, continuing..."
fi
}

# Create /etc/pf.anchors/macsec_pf_anchors
create_macsec_pf_anchors () {
if [[ -e /etc/pf.anchors/macsec_pf_anchors ]]; then
    echo "macsec Anchor file exists, deleting and recreating..."
    rm -f /etc/pf.anchors/macsec_pf_anchors
fi

cat > /etc/pf.anchors/macsec_pf_anchors <<'ENDCONFIG'

anchor macsec_pf_anchors

#default deny all in, allow all out and keep state
block in all
pass out all keep state

## Allow DHCP
pass in inet proto udp from port 67 to port 68
pass in inet6 proto udp from port 547 to port 546

## Allow incoming SSH
pass in proto tcp to any port 22

#apple file service --port 548-- pf firewall rule
block in log proto tcp to any port { 548 }

#bonjour component SSDP --port 1900-- pf firewall rule
block log proto udp to any port 1900

#finger --port 79-- pf firewall rule
block log proto tcp to any port 79

#ftp --ports 20 21-- pf firewall rule
block in log proto { tcp udp } to any port { 20 21 }

#http --port 80-- pf firewall rule

```



```
block in log proto { tcp udp } to any port 80

#icmp pf firewall rule
block in log proto icmp

#imap --port 143-- pf firewall rule
block in log proto tcp to any port 143

#imaps --port 993-- pf firewall rule
block in log proto tcp to any port 993

#iTunes sharing --port 3689-- pf firewall rule
block log proto tcp to any port 3689

#mDNSResponder --port 5353-- pf firewall rule
block log proto udp to any port 5353

#nfs --port 2049-- pf firewall rule
block log proto tcp to any port 2049

#optical drive sharing --port 49152-- pf firewall rule
block log proto tcp to any port 49152

#pop3 --port 110-- pf firewall rule
block in log proto tcp to any port 110

#pop3s --port 995-- pf firewall rule
block in log proto tcp to any port 995

#remote apple events --port 3031-- pf firewall rule
block in log proto tcp to any port 3031

#screen_sharing --port 5900-- pf firewall rule
block in log proto tcp to any port 5900
#allow screen sharing from localhost while tunneled via SSH
pass in quick on lo0 proto tcp from any to any port 5900

#smb --ports 139 445 137 138-- pf firewall rule
block in log proto tcp to any port { 139 445 }
block in log proto udp to any port { 137 138 }

#smtp --port 25-- pf firewall rule
block in log proto tcp to any port 25

#telnet --port 23-- pf firewall rule
block in log proto { tcp udp } to any port 23

#tftp --port 69-- pf firewall rule
block log proto { tcp udp } to any port 69

#uucp --port 540-- pf firewall rule
```

```
block log proto tcp to any port 540
```

```
ENDCONFIG
```

```
}
```

```
####
```

```
enable_macos_application_firewall  
create_macsec_pf_anchors  
configure_pf_config_add_macsec_anchors  
enable_pf_firewall_with_macsec_rules
```

12.4. Password Policy Supplemental

The supplemental guidance found in this section is applicable for the following 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>(policyAttributeFailedAuthentications &lt;  
policyAttributeMaximumFailedAuthentications) OR (policyAttributeCurrentTime &gt;  
(policyAttributeLastFailedAuthenticationTime + autoEnableInSeconds))</string>  
        <key>policyIdentifier</key>  
        <string>Authentication Lockout</string>  
        <key>policyParameters</key>
```

```

    <dict>
      <key>autoEnableInSeconds</key>
      <integer>300</integer>
      <key>policyAttributeMaximumFailedAuthentications</key>
      <integer>3</integer>
    </dict>
  </dict>
  <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>policyCategoryPasswordChange</key>
<array>
  <dict>
    <key>policyContent</key>
    <string>policyAttributeCurrentTime &gt; policyAttributeLastPasswordChangeTime
+ (policyAttributeExpiresEveryNDays * 24 * 60 * 60)</string>
    <key>policyIdentifier</key>
    <string>Password Expires after 60 days</string>
    <key>policyParameters</key>
    <dict>
      <key>policyAttributeExpiresEveryNDays</key>
      <integer>60</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>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>
<dict>
  <key>policyContent</key>
  <string>policyAttributePassword matches '.{15,}+'</string>
  <key>policyIdentifier</key>
  <string>Must be at least 15 characters</string>
  <key>policyParameters</key>
  <dict>
    <key>minimumLength</key>
    <integer>15</integer>
  </dict>
</dict>
<dict>
  <key>policyContent</key>
  <string>policyAttributePassword matches '(. *[0-9]. *){1,}+'</string>
  <key>policyIdentifier</key>
  <string>Must have at least 1 numeric value</string>
  <key>policyParameters</key>
  <dict>
    <key>minimumNumericCharacters</key>
    <integer>2</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>policyAttributePassword matches '(. *[A-Za-z]. *){1,}+'</string>
  <key>policyIdentifier</key>
  <string>Must have at least 1 Letter</string>
  <key>policyParameters</key>
  <dict>
    <key>minimumAlphaCharacters</key>
    <integer>1</integer>

```

```

    </dict>
  </dict>
  <dict>
    <key>policyContent</key>
    <string>policyAttributePassword matches '(.^[a-zA-Z0-9].*){1,}+'</string>
    <key>policyIdentifier</key>
    <string>Must have at least 1 special characters</string>
    <key>policyParameters</key>
    <dict>
      <key>minimumSymbols</key>
      <integer>1</integer>
    </dict>
  </dict>
  <dict>
    <key>policyContent</key>
    <string>none policyAttributePasswordHashes in
policyAttributePasswordHistory</string>
    <key>policyIdentifier</key>
    <string>Cannot match the last 5 passwords</string>
    <key>policyParameters</key>
    <dict>
      <key>policyAttributePasswordHistoryDepth</key>
      <integer>5</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.

12.5. Smartcard Supplemental

The supplemental guidance found in this section is applicable for the following rules:

- auth_ssh_password_authentication_disable
- auth_smartcard_enforce
- auth_smartcard_certificate_trust_enforce_moderate
- auth_smartcard_certificate_trust_enforce_high
- auth_smartcard_allow

- `auth_pam_sudo_smartcard_enforce`
- `auth_pam_su_smartcard_enforce`
- `auth_pam_login_smartcard_enforce`

macOS supports smartcards, such as U.S. Personal Identity Verification (PIV) cards and U.S. Department of Defense Common Access Cards (CAC). Smartcards can be used on a macOS for the following:

- Authentication (Loginwindow, Screensaver, SSH, PKINIT, Safari, Finder, and PAM Authorization (`sudo`, `login`, and `su`))
- Digital Encryption
- Digital Signing
- Remote Access (VPN:L2TP)
- Port-based Network Access Control (802.1X)
- Keychain Unlock

macOS has built-in support for USB CCID class-compliant smartcard readers.

Smartcard Pairing

The default method for using smartcards in macOS is a method called "local account pairing". Local account pairing is automatically initiated when a user inserts a smartcard into the Mac. The user is prompted to pair their smartcard with their account. If a user receives a new smartcard, the previous card must be unpaired, and the new card paired to the account. Local account pairing employs fixed key mapping with the hash of a public key on the user's smartcard with a local account.

Smartcard Attribute Mapping

Smartcards can be used to authenticate against a directory via attribute mapping configured in `/private/etc/SmartcardLogin.plist`. This file takes precedence over local account pairing. Attribute mapping matches the configured certificate field values from the smart card to the value in a directory. This may be used with network accounts, mobile accounts, or local accounts.

Smartcard Management in macOS

The following settings are available to manage smartcards (`com.apple.security.smartcard`):

Key	Type	Value
<code>userPairing</code>	bool	If false, users will not get the pairing dialog, although existing pairings will still work.
<code>allowSmartCard</code>	bool	If false, the SmartCard is disabled for logins, authorizations, and screensaver unlocking. It is still allowed for other functions, such as signing emails and web access. A restart is required for a change of setting to take effect.

Key	Type	Value
checkCertificateTrust	int	Valid values are 0-3: <ul style="list-style-type: none"> • 0: certificate trust check is turned off • 1: certificate trust check is turned on. Standard validity check is being performed but this does not include additional revocation checks. • 2: certificate trust check is turned on, and a soft revocation check is performed. Until the certificate is explicitly rejected by CRL/OCSP, it is considered valid. This implies that unavailable/unreachable CRL/OCSP allows this check to succeed. • 3: certificate trust check is turned on, plus a hard revocation check is performed. Unless CRL/OCSP explicitly states that "this certificate is OK", the certificate is considered invalid. This is the most secure value for this setting.
oneCardPerUser	bool	If true, a user can pair with only one smartcard, although existing pairings will be allowed if already set up.
enforceSmartCard	bool	If true, a user can only login or authenticate with a smartcard.
tokenRemovalAction	int	If 1, the screen saver will automatically when the smartcard is removed.
allowUnmappedUsers	int	If 1, allows users who are in a directory group to be exempt from smartcard-only enforcement. The group allowed for exemption is defined in /private/etc/SmartcardLogin.plist

A custom configuration profile (`com.apple.loginwindow`) should be created to disable automatic login when FileVault is enabled. This ensures that authorized users boot their Macs, enter a password at the pre-boot screen (which decrypts the boot volume), and are then presented with a login window where they can authenticate with a smartcard.

Key	Type	Value
DisableFDEAutoLogin	bool	If true, both Extensible Firmware Interface (EFI) login password and loginwindow PIN are required.



DisableFDEAutoLogin does not have to be set on Apple Silicon based macOS systems that are smartcard enforced as smartcards are available at pre-boot.

Trusted Authorities

The macOS allows users to specify which certificate authorities (CA) can be used for trust evaluation during smartcard authentication. Only CAs listed in the TrustedAuthorities section of the SmartcardLogin.plist will be evaluated as trusted. This setting only works if `checkCertificateTrust` is set to either 1, 2, or 3 in `com.apple.security.smartcard`.

To get the SHA-256 hash in the correct format, run the following command within terminal:

```
/usr/bin/openssl x509 -noout -fingerprint -sha256 -inform pem -in <issuer cert> |  
/usr/bin/awk -F '=' '{print $2}' | /usr/bin/sed 's://g'
```

To configure Trusted Authorities, the `SmartcardLogin.plist` should be minimally configured as below:

```
<?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>AttributeMapping</key>  
    <dict>  
      <key>fields</key>  
      <array>  
        <string>NT Principal Name</string>  
      </array>  
      <key>formatString</key>  
      <string>Kerberos:$1</string>  
      <key>dsAttributeString</key>  
      <string>dsAttrTypeStandard:AltSecurityIdentities</string>  
    </dict>  
    <key>TrustedAuthorities</key>  
    <array>  
      <string>SHA256_HASH_OF_CERTDOMAIN_1,SHA256_HASH_OF_CERTDOMAIN_2</string>  
    </array>  
  </dict>  
</plist>
```

Smartcard Enforcement Exemption

Group Exemption

Starting in macOS 10.15, enforcement on a system can be granularly configured by adding a field to `/private/etc/SmartcardLogin.plist`. The `NotEnforcedGroup` can be added to the file to list a Directory group that will not be included in smartcard enforcement. In order to activate this feature, `enforceSmartCard` and `allowUnmappedUsers` must be applied via a configuration profile (`com.apple.security.smartcard`).

To configure the `NotEnforcedGroup`, the `SmartcardLogin.plist` should be minimally configured as follows:


```
<?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>AttributeMapping</key>
  <dict>
    <key>fields</key>
    <array>
      <string>NT Principal Name</string>
    </array>
    <key>formatString</key>
    <string>Kerberos:$1</string>
    <key>dsAttributeString</key>
    <string>dsAttrTypeStandard:AltSecurityIdentities</string>
  </dict>
  <key>TrustedAuthorities</key>
  <array>
    <string>SHA256_HASH_OF_CERTDOMAIN_1,SHA256_HASH_OF_CERTDOMAIN_2</string>
  </array>
  <key>NotEnforcedGroup</key>
  <string>EXEMPTGROUP</key>
</dict>
</plist>
```

Once a system is configured for the `NotEnforcedGroup` a user can be added to the assigned group by running the following:

```
/usr/sbin/dseditgroup -o edit -a <exempt_user> -t user <notenforcegroup>
```

User Exemption

Alternatively, if a single user needs to be exempt for a period of time, `kDSNativeAttrTypePrefix:SmartCardEnforcement` can be set in the user's Open Directory record. The following values can be set:

- 0 - The system default is respected.
- 1 - Smartcard enforcement is enabled.
- 2 - Smartcard enforcement is disabled.



In Active Directory environments, the value of the `userAccountControl` attribute is respected.

Run the following command to set the exemption when booted from macOS:

```
/usr/bin/dscl . -append /Users/<username> SmartCardEnforcement 2
```

Run the following command to set the exemption when booted from Recovery:

```
/usr/bin/defaults write /Volumes/Macintosh\
HD/var/db/dslocal/nodes/Default/users/<username> SmartCardEnforcement -array-add 2
```



When booted to recovery on an Apple Silicon Mac, run the following after setting the exemption. `/usr/sbin/diskutil apfs updatePreboot /Volumes/Macintosh\ HD`

Temporary Exemption

On an Apple Silicon Mac, if a temporary exemption is needed, `security filevault skip-sc-enforcement` will disable smartcard enforcement on next boot only.

Run the following command to set the temporary exemption when booted from Recovery:

```
/usr/bin/security filevault skip-sc-enforcement <data volume UUID> set
```

To obtain the `data volume UUID` run the following:

```
/usr/sbin/diskutil apfs listGroups | /usr/bin/awk -F: '/ Data/ { getline; gsub(/
/, ""); print $2}'
```

Pluggable Authentication Module (PAM)

Terminal sessions in macOS can be configured for smartcard enforcement by modifying the PAM modules for `sudo`, `su`, and `login`.

```
/etc/pam.d/sudo
# sudo: auth account password session
auth      sufficient      pam_smartcard.so
auth      required        pam_opendirectory.so
auth      required        pam_deny.so
account   required        pam_permit.so
password  required        pam_deny.so
session   required        pam_permit.so
```

```
/etc/pam.d/su
```

```
# su: auth account password session
```

```
auth      sufficient    pam_smartcard.so
```

```
auth      required      pam_rootok.so
```

```
auth      required      pam_group.so no_warn group=admin,wheel ruser root_only
```

```
fail_safe
```

```
account    required      pam_permit.so
```

```
account    required      pam_opendirectory.so no_check_shell
```

```
password   required      pam_opendirectory.so
```

```
session    required      pam_launchd.so
```

```
/etc/pam.d/login
```

```
# login: auth account password session
```

```
auth      sufficient    pam_smartcard.so
```

```
auth      optional      pam_krb5.so use_kcminit
```

```
auth      optional      pam_ntlm.so try_first_pass
```

```
auth      optional      pam_mount.so try_first_pass
```

```
auth      required      pam_opendirectory.so try_first_pass
```

```
auth      required      pam_deny.so
```

```
account    required      pam_nologin.so
```

```
account    required      pam_opendirectory.so
```

```
password   required      pam_opendirectory.so
```

```
session    required      pam_launchd.so
```

```
session    required      pam_uwtmp.so
```

```
session    optional      pam_mount.so
```