macOS Security Compliance
GlobalTill

iOS/iPadOS 16

Security Configuration - 800GT-53R5_MODERATE_IOS16

Tailored from 800-53R5_MODERATE

Version 16 Guidance, Revision 1.0 (2023-09-21)

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. iCloud . . . 7

6.1. Ensure iCloud Backup is set to Disabled . . . 7

6.2. Disable iCloud Keychain Sync . . . 7

6.3. Ensure Managed Apps Storing Data in iCloud is Set to Disabled . . . 8

6.4. Ensure Photo Stream is set to Disabled . . . 9

6.5. Disable iCloud Photo Library . . . 9

6.6. Ensure Shared Photo Stream is set to Disabled . . . 10

6.7. Ensure Allow iCloud Documents and Data is set to Disabled . . . 10

7. iOS . . . 12

7.1. Ensure AirDrop is set to Disabled . . . 12

7.2. Ensure Treat AirDrop as unmanaged destination is set to Enabled . . . 12

7.3. Require the User to Enter a Password when Connecting to an AirPlay-enabled device for the First Time. . . . 13

7.4. Ensure Managed Apps Cannot Read Unmanaged Contact Accounts . . . 14

7.5. Ensure Managed Apps Cannot Write to Unmanaged Contact Accounts . . . 14

7.6. Ensure Allow documents from managed sources in unmanaged destinations is set to Disabled . . . 15

7.7. Ensure Allow documents from unmanaged sources in managed destinations is set to Disabled . . . 15

7.8. Ensure Apple Watch Pairing is Disabled . . . 16

7.9. Ensure Force Apple Watch wrist detection is set to Enabled . . . 17

7.10. Define Allowed Applications . . . 17

7.11. Ensure Require Touch ID / Face ID authentication before AutoFill is set to Enabled 18

7.12. Prevent Apple Watch from Unlocking a Device . . . 19

7.13. Disable Sending Diagnostic and Usage Data to Apple . . . 19

7.14. Disallow Apps to be Installed from Unauthorized Sources . . . 20

7.15. Ensure Allow Erase All Content and Settings is set to Disabled . . . 20

7.16. Ensure Allow network drive access in Files app is set to Disabled . . . 21

7.17. Ensure Allow USB drive access in Files app is set to Disabled . . . 21

7.18. Disable Find My Friends Service . . . 22

7.19. Ensure Force automatic date and time is set to Enabled . . . 23

7.20. Ensure Force Encrypted Backups is Enabled . . . 23

7.21. Disable Handoff . . . 24

7.22. Ensure Allow adding VPN configurations is set to Disabled 24
7.23. Enable Limit Ad Tracking 25
7.24. Ensure Allow Mail Drop is set to Disabled 26
7.25. Ensure Allow user to move messages from this account is set to Disabled . . 26
7.26. Ensure Allow modifying cellular data app settings is set to Disabled 27
7.27. Ensure Allow setting up new nearby devices is set to Disabled 27
7.28. Ensure On Device Dictation is Enforced 28
7.29. Ensure On Device Translation is Enforced 28
7.30. Ensure Allow pairing with non-Configurator hosts is set to Disabled 29
7.31. Disable Password Autofill 30
7.32. Disable Proximity Based Password Sharing Requests 30
7.33. Disable Password Sharing 31
7.34. Disable Personalized Advertising 32
7.35. Disable Automatic Completion of Safari Browser Passcodes 32
7.36. Ensure Allow screenshots and screen recording is set to Disabled 33
7.37. Ensure Sharing of Location Data is Disabled 33
7.38. Ensure Calendar Notifications when the Device is Locked is set to Disabled . 34
7.39. Ensure Show Control Center in Lock screen is set to Disabled 35
7.40. Ensure Show Notification Center in Lock screen is set to Disabled 35
7.41. Ensure Allow Siri while device is locked is set to Disabled 36
7.42. Enforce Supervised Enrollment in Mobile Device Management 36
7.43. Ensure Allow USB accessories while the device is locked is set to Disabled . 37
7.44. Ensure Allow voice dialing while device is locked is set to Disabled 37
8. Password Policy 39
8.1. Limit Consecutive Failed Login Attempts to 6 39
8.2. Ensure Maximum grace period for device lock is set to 0 minutes 40
8.3. Ensure Maximum Auto-Lock is set to 2 minutes or less 40
8.4. Require a Minimum Passcode Length of 6 Characters 41
8.5. Prohibit Repeating, Ascending, and Descending Character Sequences 41
9. Supplemental 43
9.1. CIS Manual Recommendations 43
9.2. DISA STIG Supplemental 45

Chapter 1. Foreword

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

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

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

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

Chapter 2. Scope

This guide describes the actions to take when securing a iOS/iPadOS 16 system against the 800GT-53R5_MODERATE_IOS16 (based on 800-53R5_MODERATE) security baseline.

Information System Security Officers and benchmark creators can use this catalog of settings in order to assist them in security benchmark creation. This list is a catalog, not a checklist or benchmark, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios.

Chapter 3. Authors

Security configuration adapted by:

Michael MacKinnon	GlobalTill

Security configuration reviewed and approved by:

Douglas Wilson	GlobalTill

macOS Security Compliance Project

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

Chapter 4. Acronyms and Definitions

Table 1. Acronyms and Abbreviations

AES	Advanced Encryption Standard
ABM	Apple Business Manager
AFP	Apple Filing Protocol
ALF	Application Layer Firewall
AO	Authorizing Official
API	Application Programming Interface
ARD	Apple Remote Desktop
CA	Certificate Authority
CIS	Center for Internet Security
CMMC	Cybersecurity Maturity Model Certification
CNSSI	Committee on National Security Systems
CRL	Certificate Revocation List
DISA	Defense Information Systems Agency
DMA	Direct Memory Access
FISMA	Federal Information Security Modernization Act
FPKI	Federal Public Key Infrastructure
IR	Infrared
ISO	Information System Owner
ISSO	Information System Security Officer
MDM	Mobile Device Management
NASA	National Aeronautics and Space Administration
NFS	Network File System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
ODV	Organization Defined Values
OS	Operating System
PF	Packet Filter
PIV	Personal Identity Verification

PIV-M	Personal Identity Verification Mandatory
PKI	Public Key Infrastructure
RBD	Risk Based Decision
SIP	System Integrity Protection
SMB	Server Message Block
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide
UAMDM	User Approved MDM
UUCP	Unix-to-Unix Copy Protocol

Table 2. Definitions

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

Chapter 5. Applicable Documents

5.1. Government Documents

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

Document Number or Descriptor	Document Title
NIST Special Publication 800-53 Rev 5	*NIST Special Publication 800-53 Rev 5*
NIST Special Publication 800-63	*NIST Special Publication 800-63*
NIST Special Publication 800-171	*NIST Special Publication 800-171 Rev 2*
NIST Special Publication 800-219	*NIST Special Publication 800-219 Rev 1*

Table 4. Defense Information Systems Agency (DISA)

Document Number or Descriptor	Document Title
STIG Ver 1, Rel 2	*Apple iOS/iPadOS 16 STIG - Ver 1, Rel 2*
STIG Ver 1, Rel 1	*Apple iOS/iPadOS 16 BYOAD STIG - Ver 1, Rel 1*

Table 5. Cybersecurity Maturity Model Certification (CMMC)

Document Number or Descriptor	Document Title
CMMC Model Overview v2.0	*Cybersecurity Maturity Model Certification (CMMC) Model Overview v2.0*

Table 6. Committee on National Security Systems (CNSS)

Document Number or Descriptor	Document Title
CNSSI No. 1253	*Security Categorization and Control Selection for National Security Systems*

5.2. Non-Government Documents

Table 7. Apple

Document Number or Descriptor	Document Title
Apple Platform Security Guide	*Apple Platform Security*
Apple Platform Deployment	*Apple Platform Deployment*
Apple Platform Certifications	*Apple Platform Certifications*
Profile-Specific Payload Keys	*Profile-Specific Payload Keys*

Table 8. Center for Internet Security

Document Number or Descriptor	Document Title
Apple iOS/iPadOS	*CIS Apple iOS 16 and iPadOS 16 Version 1.1.0*

Chapter 6. iCloud

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

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

6.1. Ensure iCloud Backup is set to Disabled

iCloud backup *MUST* be disabled.

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>allowCloudBackup</key>
<false/>
```

ID	icloud_backup_disabled	
References	**800-53r5**	AC-20, AC-20(1) CM-7, CM-7(1) SC-4 SC-7(10)
	800-171r2	N/A
	CCE	CCE-93201-2

6.2. Disable iCloud Keychain Sync

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

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	• AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93202-0

6.3. Ensure Managed Apps Storing Data in iCloud is Set to Disabled

Managed Apps *MUST* not store data in iCloud.

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>allowManagedAppsCloudSync</key>
<false/>
```

ID	icloud_managed_apps_store_data_disabled	
References	800-53r5	• AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93203-8

6.4. Ensure Photo Stream is set to Disabled

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DoD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DoD sensitive information.

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>allowPhotoStream</key>
<false/>
```

ID	icloud_photo_stream_disable	
References	**800-53r5**	• AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93204-6

6.5. Disable iCloud Photo Library

The iOS 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.

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	AC-20, AC-20(1) CM-7, CM-7(1) SC-7(10)
	800-171r2	N/A
	CCE	CCE-93205-3

6.6. Ensure Shared Photo Stream is set to Disabled

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DoD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DoD sensitive information.

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>allowSharedStream</key>
<false/>
```

ID	icloud_shared_photo_stream_disable	
References	800-53r5	AC-20, AC-20(1) CM-7, CM-7(1) SC-7(10)
	800-171r2	N/A
	CCE	CCE-93206-1

6.7. Ensure Allow iCloud Documents and Data is set to Disabled

Institutionally owned devices *MUST* not sync data through iCloud.

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_sync_disable	
References	**800-53r5**	• AC-20, AC-20(1) • CM-7, CM-7(1) • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93207-9

Chapter 7. iOS

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

7.1. Ensure AirDrop is set to Disabled

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.

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**	AC-20 AC-3 CM-7, CM-7(1)
	800-171r2	N/A
	CCE	CCE-93208-7

7.2. Ensure Treat AirDrop as unmanaged destination is set to Enabled

AirDrop *MUST* be treated as an unmanaged destination.

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>forceAirDropUnmanaged</key>
```

```
<true/>
```

ID	os_airdrop_unmanaged_destination_enable	
References	800-53r5	- AC-20 - AC-3 - CM-7, CM-7(1) - MP-2 - SC-7(10)
	800-171r2	- N/A
	CCE	- CCE-93209-5

7.3. Require the User to Enter a Password when Connecting to an AirPlay-enabled device for the First Time.

When a user is allowed to use AirPlay without a password, it may mistakenly associate the iPhone and iPad with an AirPlay-enabled device other than the one intended (i.e., by choosing the wrong one from the AirPlay list displayed). This creates the potential for someone in control of a mistakenly associated device to obtain DoD sensitive information without authorization. Requiring a password before such an association mitigates this risk. Passwords do not require any administration and are not required to comply with any complexity requirements.

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>forceAirPlayOutgoingRequestsPairingPassword</key>
<true/>
```

ID	os_airplay_password_require	
References	800-53r5	- IA-3
	800-171r2	- N/A
	CCE	- CCE-93210-3

7.4. Ensure Managed Apps Cannot Read Unmanaged Contact Accounts

Managed Apps *MUST* not be allowed to read contacts from unamanged contact destinations.

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>allowUnmanagedToReadManagedContacts</key>
<false/>
```

ID	os_allow_contacts_read_managed_sources_unmanaged_destinations_disable	
References	**800-53r5**	AC-3 MP-2 SC-39 SC-7(10)
	800-171r2	N/A
	CCE	CCE-93211-1

7.5. Ensure Managed Apps Cannot Write to Unmanaged Contact Accounts

Managed Apps *MUST* not be allowed to write contacts to unamanged contact destinations.

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>allowManagedToWriteUnmanagedContacts</key>
<false/>
```

ID	os_allow_contacts_write_managed_sources_unmanaged_destinations_disable	
References	800-53r5	• AC-3 • MP-2 • SC-39 • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93212-9

7.6. Ensure Allow documents from managed sources in unmanaged destinations is set to Disabled

Documents from managed sources *MUST* not be allowed in unmanaged destinations.

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>allowOpenFromManagedToUnmanaged</key>
<false/>
```

ID	os_allow_documents_managed_sources_unmanaged_destinations_disable	
References	800-53r5	• AC-3 • MP-2 • SC-39 • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93213-7

7.7. Ensure Allow documents from unmanaged sources in managed destinations is set to Disabled

Documents from unmanaged sources *MUST* not be allowed in managed destinations.

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>allowOpenFromUnmanagedToManaged</key>
<false/>
```

ID	os_allow_documents_unmanaged_sources_managed_destinations_disable	
References	**800-53r5**	- AC-3 - MP-2 - SC-39 - SC-7(10)
	800-171r2	- N/A
	CCE	- CCE-93214-5

7.8. Ensure Apple Watch Pairing is Disabled

Pairing an Apple Watch *MUST* be disabled.

> Any currently paired Apple Watch is unpaired and the watch’s content is erased.

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>allowPairedWatch</key>
<false/>
```

ID	os_apple_watch_pairing_disable

References	**800-53r5**	- CM-7, CM-7(1)
	800-171r2	- N/A
	CCE	- CCE-93215-2

7.9. Ensure Force Apple Watch wrist detection is set to Enabled

Wrist detection *MUST* be enabled for paired Apple Watches.

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>forceWatchWristDetection</key>
<true/>
```

ID	os_apple_watch_wrist_detection_enable	
References	**800-53r5**	- AC-3 - CM-7, CM-7(1)
	800-171r2	- N/A
	CCE	- CCE-93216-0

7.10. Define Allowed Applications

Requiring all authorized applications to be in an application allow list prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allow list. Failure to configure an application allow list properly could allow unauthorized and malicious applications to be downloaded, installed, and executed on the mobile device, causing a compromise of DoD data accessible by these applications. Applications with the listed characteristics have features that can cause the compromise of sensitive DoD data or have features with no known application in the DoD environment.

Application note: The application allow list, in addition to controlling the installation of applications on the MD, must control user access/execution of all core and preinstalled applications, or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

Core application: Any application integrated into the OS by the OS or MD vendors.

Preinstalled application: Additional noncore applications included in the OS build by the OS vendor, MD vendor, or wireless carrier.

See rule YAML file for implementation comments.

Remediation Description

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

This is implemented by a Configuration Profile

ID	os_application_allow_list	
References	**800-53r5**	CM-7(5)
	800-171r2	N/A
	CCE	CCE-93217-8

7.11. Ensure Require Touch ID / Face ID authentication before AutoFill is set to Enabled

Re-authentication *MUST* be enabled at each Autofill operation.

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>forceAuthenticationBeforeAutoFill</key>
<true/>
```

ID	os_authentication_password_autofill_enable	
References	**800-53r5**	AC-3 IA-11
	800-171r2	N/A
	CCE	CCE-93218-6

7.12. Prevent Apple Watch from Unlocking a Device

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.

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	os_auto_unlock_disable	
References	**800-53r5**	AC-11
	800-171r2	N/A
	CCE	CCE-93219-4

7.13. 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.

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

ID	os_diagnostics_reports_disable	
References	**800-53r5**	• AC-20 • SC-7(10) • SI-11
	800-171r2	• N/A
	CCE	• CCE-93220-2

7.14. Disallow Apps to be Installed from Unauthorized Sources

Apps *MUST* be installed from authorized application repositories. Disallowing enterprise app trust prevents apps from being provisioned by universal provisioning profiles.

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:

```xml
<key>allowEnterpriseAppTrust</key>
<false/>
```

ID	os_disallow_enterprise_app_trust	
References	**800-53r5**	• CM-11
	800-171r2	• N/A
	CCE	• CCE-93262-4

7.15. Ensure Allow Erase All Content and Settings is set to Disabled

Erase all contents and settings *MUST* be disabled on institutionally owned iOS devices.

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_contents_and_settings_disable	
References	**800-53r5**	• CM-6 • CM-7, CM-7(1)
	800-171r2	• N/A
	CCE	• CCE-93222-8

7.16. Ensure Allow network drive access in Files app is set to Disabled

Network drive acces in Files app *MUST* be disabled.

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>allowFilesNetworkDriveAccess</key>
<false/>
```

ID	os_files_network_drive_access_disable	
References	**800-53r5**	• AC-20(2)
	800-171r2	• N/A
	CCE	• CCE-93223-6

7.17. Ensure Allow USB drive access in Files app is set to Disabled

USB drive acces in Files app *MUST* be disabled.

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>allowFilesUSBDriveAccess</key>
<false/>
```

ID	os_files_usb_drive_access_disable	
References	**800-53r5**	• AC-20(2)
	800-171r2	• N/A
	CCE	• CCE-93224-4

7.18. Disable Find My Friends Service

The Find My Friends service *MUST* be disabled.

Sharing the location of a device may be an violation to an organization and potentially put users at risk.

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>allowFindMyFriends</key>
<false/>
```

ID	os_find_my_friends_disable	
References	**800-53r5**	• AC-20 • CM-7, CM-7(1)
	800-171r2	• N/A
	CCE	• CCE-93225-1

7.19. Ensure Force automatic date and time is set to Enabled

Automatic date and time *MUST* be enabled.

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>forceAutomaticDateAndTime</key>
<true/>
```

ID	os_force_date_and_time_enable	
References	**800-53r5**	• AU-12(1) • SC-45(1)
	800-171r2	• N/A
	CCE	• CCE-93226-9

7.20. Ensure Force Encrypted Backups is Enabled

iOS and iPadOS backups *MUST* be encrypted.

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>forceEncryptedBackup</key>
<true/>
```

ID	os_force_encrypted_backups_enable

References	**800-53r5**	- CM-7, CM-7(1) - CP-09(8) - SC-28
	800-171r2	- N/A
	CCE	- CCE-93227-7

7.21. 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.

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**	- AC-20 - AC-3 - CM-7, CM-7(1)
	800-171r2	- N/A
	CCE	- CCE-93228-5

7.22. Ensure Allow adding VPN configurations is set to Disabled

VPN configurations *MUST* be installed via an organization’s MDM.

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>allowVPNCreation</key>
<false/>
```

ID	os_install_vpn_configuration_disable	
References	**800-53r5**	• AC-17, AC-17(1), AC-17(3)
	800-171r2	• N/A
	CCE	• CCE-93462-0

7.23. Enable Limit Ad Tracking

Ad tracking and targeted ads *MUST* be disabled.

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

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>forceLimitAdTracking</key>
<true/>
```

ID	os_limit_ad_tracking_enable	
References	**800-53r5**	• AC-20 • CM-7, CM-7(1) • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93231-9

7.24. Ensure Allow Mail Drop is set to Disabled

Mail Drop *MUST* be disabled.

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.mail.managed) payload type:

```
<key>allowMailDrop</key>
<false/>
```

ID	os_mail_maildrop_disable	
References	**800-53r5**	AC-20 AC-3 CM-7, CM-7(1) SC-07(10)
	800-171r2	N/A
	CCE	CCE-93232-7

7.25. Ensure Allow user to move messages from this account is set to Disabled

Mail from institutionally configured mail accounts *MUST* not be allowed to move to personaly mail accounts.

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.mail.managed) payload type:

```
<key>PreventMove</key>
<false/>
```

ID	os_mail_move_messages_disable	
References	800-53r5	AC-21 CM-7, CM-7(1) SC-07(10) SC-4
	800-171r2	N/A
	CCE	CCE-93233-5

7.26. Ensure Allow modifying cellular data app settings is set to Disabled

The ability to modify cellular data app settings *MUST* be disabled.

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>allowAppCellularDataModification</key>
<false/>
```

ID	os_modify_cellular_data_app_settings_disable	
References	800-53r5	CM-7, CM-7(1)
	800-171r2	N/A
	CCE	CCE-93234-3

7.27. Ensure Allow setting up new nearby devices is set to Disabled

The setting up of new nearby devices *MUST* be disabled.

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>allowProximitySetupToNewDevice</key>
<false/>
```

ID	os_new_device_proximity_disable	
References	**800-53r5**	- CM-6 - CM-7, CM-7(1)
	800-171r2	- N/A
	CCE	- CCE-93235-0

7.28. Ensure On Device Dictation is Enforced

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

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

Remediation Description

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

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

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

ID	os_on_device_dictation_enforce	
References	**800-53r5**	- AC-20 - SC-7(10) - SI-11
	800-171r2	- N/A
	CCE	- CCE-93236-8

7.29. Ensure On Device Translation is Enforced

The device *MUST* be configured for on device translation.

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

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>forceOnDeviceOnlyTranslation</key>
<true/>
```

ID	os_on_device_translation_enforce	
References	**800-53r5**	• AC-20 • SC-7(10) • SI-11
	800-171r2	• N/A
	CCE	• CCE-93237-6

7.30. Ensure Allow pairing with non-Configurator hosts is set to Disabled

Host pairing with a non-Configurator host *MUST* be disabled.

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>allowHostPairing</key>
<false/>
```

ID	os_pairing_non_configurator_hosts_disable

References	**800-53r5**	- CM-6 - CM-7, CM-7(1)
	800-171r2	- N/A
	CCE	- CCE-93238-4

7.31. Disable Password Autofill

Password Autofill *MUST* be disabled.

iOS allows users to save passwords and use the Password Autofill feature in Safari and compatible apps. To protect against malicious users gaining access to the device, this feature *MUST* be disabled to prevent users from being prompted to save passwords in applications.

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>allowPasswordAutoFill</key>
<false/>
```

ID	os_password_autofill_disable	
References	**800-53r5**	- CM-7, CM-7(1) - IA-11 - IA-5, IA-5(13)
	800-171r2	- N/A
	CCE	- CCE-93239-2

7.32. Disable Proximity Based Password Sharing Requests

Proximity based password sharing requests *MUST* be disabled.

The default behavior of iOS 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.

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
	800-171r2	• N/A
	CCE	• CCE-93240-0

7.33. Disable Password Sharing

Password Sharing *MUST* be disabled.

The default behavior of iOS/iPadOS is to allow users to share a password over Airdrop between other macOS and iOS devices. This feature *MUST* be disabled to prevent passwords from being shared.

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>allowPasswordSharing</key>
<false/>
```

ID	os_password_sharing_disable	
References	**800-53r5**	• IA-5
	800-171r2	• N/A
	CCE	• CCE-93241-8

7.34. Disable Personalized Advertising

Ad tracking and targeted ads *MUST* be disabled.

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

Remediation Description

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

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

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

ID	os_personalized_advertising_disable	
References	**800-53r5**	- AC-20 - CM-7, CM-7(1)
	800-171r2	- N/A
	CCE	- CCE-93242-6

7.35. Disable Automatic Completion of Safari Browser Passcodes

The AutoFill functionality in the Safari web browser allows the user to complete a form that contains sensitive information, such as PII, without previous knowledge of the information. By allowing the use of the AutoFill functionality, an adversary who learns a user’s iPhone or iPad passcode, or who otherwise is able to unlock the device, may be able to further breach other systems by relying on the AutoFill feature to provide information unknown to the adversary. By disabling the AutoFill functionality, the risk of an adversary gaining additional information about the device’s user or compromising other systems is significantly mitigated.

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>safariAllowAutoFill</key>
<false/>
```

ID	os_safari_password_autofill_disable	
References	**800-53r5**	CM-7, CM-7(1) IA-11 IA-5, IA-5(13)
	800-171r2	N/A
	CCE	CCE-93245-9

7.36. Ensure Allow screenshots and screen recording is set to Disabled

Screenshots and screen recordings on iOS *MUST* be disabled.

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>allowScreenShot</key>
<false/>
```

ID	os_screenshots_disable	
References	**800-53r5**	CM-7, CM-7(1) SC-07(10)
	800-171r2	N/A
	CCE	CCE-93246-7

7.37. Ensure Sharing of Location Data is Disabled

Sharing of location data is an operational security (OPSEC) risk because it potentially allows an adversary to determine a DoD user's location, movements, and patterns in those movements over time. An adversary could use this information to target the user or gather intelligence on the user's likely activities. Using commercial cloud services to store and handle location data could leave the data vulnerable to breach, particularly by sophisticated adversaries. Disabling the use of such services mitigates this risk.

Remediation Description

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

This is implemented by a Configuration Profile

ID	os_share_location_data_disable	
References	**800-53r5**	AC-20
	800-171r2	N/A
	CCE	CCE-93247-5

7.38. Ensure Calendar Notifications when the Device is Locked is set to Disabled

Many mobile devices display notifications on the lock screen so users can obtain relevant information in a timely manner without having to frequently unlock the phone to determine if there are new notifications. However, in many cases, these notifications can contain sensitive information. When they are available on the lock screen, an adversary can see them merely by being in close physical proximity to the device. Configuring the MOS to not send notifications to the lock screen mitigates this risk.

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>allowLockScreenTodayView</key>
<false/>
```

ID	os_show_calendar_lock_screen_disable	
References	**800-53r5**	AC-11(1)
	800-171r2	N/A
	CCE	CCE-93248-3

7.39. Ensure Show Control Center in Lock screen is set to Disabled

Control Center *MUST* be disabled in the lock screen.

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:

```xml
<key>allowLockScreenControlCenter</key>
<false/>
```

ID	os_show_control_center_lock_screen_disable	
References	**800-53r5**	AC-11(1)
	800-171r2	N/A
	CCE	CCE-93249-1

7.40. Ensure Show Notification Center in Lock screen is set to Disabled

Notification Center *MUST* be disabled in the lock screen.

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:

```xml
<key>allowLockScreenNotificationsView</key>
<false/>
```

ID	os_show_notification_center_lock_screen_disable

References	**800-53r5**	• AC-11(1)
	800-171r2	• N/A
	CCE	• CCE-93250-9

7.41. Ensure Allow Siri while device is locked is set to Disabled

Accessing Siri while the device is locked *MUST* be disabled.

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>allowAssistantWhileLocked</key>
<false/>
```

ID	os_siri_when_locked_disabled	
References	**800-53r5**	• AC-20 • CM-7, CM-7(1) • SC-7(10)
	800-171r2	• N/A
	CCE	• CCE-93251-7

7.42. Enforce Supervised Enrollment in Mobile Device Management

iOS/iPadOS *MUST* be supervised by a Mobile Device Management (MDM) software.

Remediation Description

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

Enroll the iOS/iPadOS device in a supervised MDM.

ID	os_supervised_mdm_require	
References	800-53r5	- CM-2 - CM-6
	800-171r2	- N/A
	CCE	- CCE-93253-3

7.43. Ensure Allow USB accessories while the device is locked is set to Disabled

USB devices *MUST* not be allowed to connect while the device is locked.

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>allowUSBRestrictedMode</key>
<false/>
```

ID	os_usb_accessories_when_locked_disable	
References	800-53r5	- CM-8(3) - MP-7 - SC-41 - SC-7(10)
	800-171r2	- N/A
	CCE	- CCE-93254-1

7.44. Ensure Allow voice dialing while device is locked is set to Disabled

Voice dialing while the device is locked *MUST* be disabled.

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>allowVoiceDialing</key>
<false/>
```

ID	os_voice_dialing_when_locked_disabled
References	**800-53r5**: CM-7, CM-7(1) **800-171r2**: N/A **CCE**: CCE-93255-8

Chapter 8. Password Policy

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

> ℹ 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.

> ℹ 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.

8.1. Limit Consecutive Failed Login Attempts to 6

The iOS *MUST* be configured to limit the number of failed login attempts to a maximum of 6.

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

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>6</integer>
```

ID	pwpolicy_account_lockout_enforce	
References	**800-53r5**	AC-7
	800-171r2	N/A
	CCE	CCE-93256-6

8.2. Ensure Maximum grace period for device lock is set to 0 minutes

The iOS grace period for device lock *MUST* be configured to 0 minutes.

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>maxGracePeriod</key>
<integer>0</integer>
```

ID	pwpolicy_max_grace_period_enforce	
References	**800-53r5**	AC-11 IA-11
	800-171r2	N/A
	CCE	CCE-93258-2

8.3. Ensure Maximum Auto-Lock is set to 2 minutes or less

The iOS *MUST* be configured to auto-lock after 2 minutes.

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>maxInactivity</key>
<integer>2</integer>
```

ID	pwpolicy_max_inactivity_enforce

References	**800-53r5**	• AC-11 • IA-11
	800-171r2	• N/A
	CCE	• CCE-93259-0

8.4. Require a Minimum Passcode Length of 6 Characters

The iOS *MUST* be configured to require a minimum of 6 characters be used when a passcode is created.

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

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>6</integer>
```

ID	pwpolicy_minimum_length_enforce	
References	**800-53r5**	• IA-5(1)
	800-171r2	• N/A
	CCE	• CCE-93260-8

8.5. Prohibit Repeating, Ascending, and Descending Character Sequences

The iOS device *MUST* be configured to prohibit the use of repeating, ascending, and descending character sequences when a passcode is created.

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

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>allowSimple</key>
<false/>
```

ID	pwpolicy_simple_sequence_disable	
References	**800-53r5**	• IA-5(1)
	800-171r2	• N/A
	CCE	• CCE-93261-6

Chapter 9. Supplemental

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

9.1. CIS Manual Recommendations

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

Section	General
Recommendations	2.1.1 Ensure a Consent Message has been Configured 2.1.2 Ensure Controls when the profile can be removed is set to Always 3.1.1 Ensure Controls when the profile can be removed is set to Never

Section	Restrictions
Recommendations	2.2.1.5 Ensure Allow personalized ads delivered by Apple is set to Disabled 2.2.1.7 Ensure Force automatic date and time is set to Enabled 2.2.1.12 Ensure Allow sending diagnostic and usage data to Apple is set to Disabled

Section	Domains
Recommendations	2.3.1 Ensure Managed Safari Web Domains is Configured

Section	Passcode
Recommendations	2.4.2 Ensure Require alphanumeric value is set to Enabled

Section	Wi-Fi
Recommendations	2.5.1 Ensure Disable Association MAC Randomization is Configured

Section	VPN
Recommendations	2.6.1 Ensure VPN is Configured

Section	Notifications
Recommendations	2.8.1 Ensure Notification Settings are configured for all Managed Apps

Section	Functionality

Recommendations	3.2.1.14 Ensure "Allow trusting new enterprise app authors" is set to "Disabled" 3.2.1.17 Ensure "Force automatic date and time" is set to "Enabled" 3.2.1.25 Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled" 3.2.1.30 Ensure "Allow password sharing (supervised only)" is set to "Disabled"

Section	Domains
Recommendations	3.3.1 Ensure "Managed Safari Web Domains" is "Configured"

Section	Passcode
Recommendations	3.4.2 Ensure Require alphanumeric value is set to Enabled

Section	Wi-Fi
Recommendations	3.5.1 Ensure Disable Association MAC Randomization is Configured

Section	VPN
Recommendations	3.6.1 Ensure VPN is Configured

Section	Notifications
Recommendations	2.8.1 Ensure Notification Settings are configured for all Managed Apps

Section	Lock Screen Message
Recommendations	3.9.1. Ensure "If Lost, Return to..." Message is "Configured"

Section	Additional Reccomendations

Recommendations	4.1.1 Review Manage Sharing & Access 4.1.2 Review Emergency Reset 4.1.3 Review Lockdown Mode 4.1.4 Ensure "App Privacy Report" is enabled 4.2 Ensure device is not obviously jailbroken or compromised 4.3 Ensure Install iOS Updates of Automatic Updates is set to Enabled 4.4 Ensure Software Update returns Your software is up to date 4.5 Review iCloud Private Relay settings 4.6 Review Mail Privacy Protection settings 4.7 Ensure Automatic Downloads of App Updates is set to Enabled 4.8 Ensure Find My iPhone/iPad is set to Enabled on end user-owned devices 4.9 Ensure the latest iOS device architecture is used by high-value targets

9.2. DISA STIG Supplemental

These controls are controls that require additional considerations for your environment.

Please refer to your vendor’s MDM documentation for instructions on how to implement these controls.

STIG ID	Rule Title
AIOS-16-004900	Apple iOS/iPadOS 16 must [selection: wipe protected data, wipe sensitive data] upon unenrollment from MDM.
AIOS-16-005000	Apple iOS/iPadOS 16 must [selection: remove Enterprise application, remove all noncore applications (any nonfactory-installed application)] upon unenrollment from MDM.
AIOS-16-007400 **AIOS-16-707400**	Apple iOS/iPadOS 16 allowlist must be configured to not include applications with the following characteristics: - Backs up MD data to non-DoD cloud servers (including user and application access to cloud backup services); - Transmits MD diagnostic data to non-DoD servers; - Allows synchronization of data or applications between devices associated with user; and - Allows unencrypted (or encrypted but not FIPS 140-2/FIPS 140-3 validated) data sharing with other MDs or printers.
AIOS-16-008400 **AIOS-16-708400**	Apple iOS/iPadOS 16 must be configured to display the DoD advisory warning message at startup or each time the user unlocks the device.
AIOS-16-009200 **AIOS-16-709200**	Apple iOS/iPadOS 16 must be configured to not allow backup of [all applications, configuration data] to locally connected systems.
AIOS-16-009800	Apple iOS/iPadOS 16 must be configured to disable multiuser modes.
AIOS-16-009900 **AIOS-16-709900**	Apple iOS/iPadOS 16 must be configured to [selection: wipe protected data, wipe sensitive data] upon unenrollment from MDM.
AIOS-16-010000	Apple iOS/iPadOS 16 must be configured to [selection: remove Enterprise applications, remove all noncore applications (any nonfactory installed application)] upon unenrollment from MDM.

AIOS-16-011200 **AIOS-16-711200**	iPhone and iPad must have the latest available iOS/iPadOS operating system installed.
AIOS-16-011600	Apple iOS/iPadOS 16 must implement the management setting: Not have any Family Members in Family Sharing.
AIOS-16-011900 **AIOS-16-711900**	Apple iOS/iPadOS 16 users must complete required training.
AIOS-16-012000 **AIOS-16-712000**	A managed photo app must be used to take and store work-related photos.
AIOS-16-013500	Apple iOS must implement the management setting: Not allow a user to remove Apple iOS configuration profiles that enforce DoD security requirements.