APPLE iOS/iPadOS 15 STIG CONFIGURATION TABLES

Version 1, Release 3

27 July 2022

Developed by Apple and DISA for the DoD

LIST OF TABLES

Page

Table 1: COPE Required Controls – Supervised and Non-Supervised

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
General – Security	Security	- Always - Never - With Authentication	X		Never	AIOS-15-013500	Controls when profile can be removed Configuration Profile Key: PayloadRemovalDisallowed
General – Security	Automatically Remove Profile	- Always - Never - With Authentication	X		Never	AIOS-15-013500	Settings for automatic profile removal Configuration Profile Key: PayloadRemovalDisallowed
Passcode	Allow Simple Value	Enable/Disable	X		Disable	AIOS-15-006600	Simple value passcodes include repeating, ascending, and descending character sequences. Configuration Profile Key: allowSimple
Passcode	Minimum passcode length	1–16	X		6	AIOS-15-006500	Configuration Profile Key: minLength
Passcode	Maximum auto-lock	1–15, or None	X		1–5 recommended; 15 maximum allowable	AIOS-15-006700, AIOS-15-006800	Device automatically locks when minutes elapse. If maximum auto-lock equals 15, the grace period must be set to "Immediately".

1

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
							Configuration Profile Key: maxInactivity
Passcode	Maximum grace period for device lock	- Immediately - 1 min - 5 min - 15 min - 1 hr - 4 hrs	X		15 minus value for maximum auto-lock time	AIOS-15-006700, AIOS-15-006800	Maximum amount of time device can be locked without prompting for passcode on unlock. If maximum auto-lock equals 15, the grace period must be set to "Immediately". Configuration Profile Key: maxGracePeriod
Passcode	Maximum number of failed attempts	2–10	X		10	AIOS-15-006900	Configuration Profile Key: maxFailedAttempts
Restrictions	Allow AirDrop	Enable/Disable	X	X	Enable/ Disable	AIOS-15-012500, AIOS-15-010200	Supervised only. Control must be disabled unless AO has approved AirDrop for unmanaged data. This is set in conjunction with treating AirDrop as unmanaged. Configuration Profile Key: allowAirDrop
Restrictions	Allow voice dialing while device is locked	Enable/Disable	X		Disable	AIOS-15-007300	Configuration Profile Key: allowVoiceDialing

2

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Allow Siri while device is locked	Enable/Disable	X		Disable	AIOS-15-007200	Configuration Profile Key: allowAssistantWhileLocked
Restrictions	Allow iCloud backup	Enable/Disable	X	X	Disable	AIOS-15-003000	Supervised only. This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store. Configuration Profile Key: allow CloudBackup
Restrictions	Allow iCloud Documents and Data	Enable/Disable	X	X	Disable	AIOS-15-003100	Supervised only. This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store. Configuration Profile Key: allowCloudDocumentSync
Restrictions	Allow iCloud Keychain Sync	Enable/Disable	X	X	Disable	AIOS-15-003200	Supervised only. This requirement is Not Applicable if the AO has approved unrestricted download

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
							of unmanaged apps from the Apple App Store. Configuration Profile Key: allowCloudKeychainSync
Restrictions	Allow managed apps to store data in iCloud	Enable/Disable	X		Disable	AIOS-15-003500	Configuration Profile Key: allowManagedAppsCloudSync
Restrictions	Allow backup of enterprise books	Enable/Disable	X		Disable	AIOS-15-003700	Configuration Profile Key: allowEnterpriseBookBackup
Restrictions	Allow Shared Albums	Enable/Disable	X	X	Disable	AIOS-15-011100	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store. Configuration Profile Key: allowSharedSteam
Restrictions	Allow iCloud Photos	Enable/Disable	X	X	Disable	AIOS-15-003400	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store. Configuration Profile Key: allowCloudPhotoLibrary

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Allow My Photo Stream	Enable/Disable	X	X	Disable	AIOS-15-003300	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store. Configuration Profile Key: allowPhotoStream
Restrictions	Allow USB drive access in Files app	Enable/Disable	X	X	Disable	AIOS-15-013300	Supervised only. Must be disabled unless AO approved (DoD-approved flash drive must be used). Configuration Profile Key: allowFilesUSBDriveAccess
Restrictions	Allow network drive access in Files access	Enable/Disable	X	X	Disable	AIOS-15-014300	Supervised only. Configuration Profile Key: allowFilesNetworkDriveAccess
Restrictions	Force encrypted backups	Enable/Disable	X		Enable	AIOS-15-010700	Configuration Profile Key: forceEncryptedBackup
Restrictions	Force limited ad tracking	Enable/Disable	X		Enable	AIOS-15-010500	Configuration Profile Key: forceLimitAdTracking

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Allow Trusting New Enterprise App Authors	Enable/Disable	X		Disable	AIOS-15-007000	Configuration Profile Key: allowEnterpriseAppTrust
Restrictions	Allow Find My Friends	Enable/Disable	X		Disable	AIOS-15-013100	Supervised only. Configuration Profile Key: allowFindMyFriends
Restrictions	Allow modifying Find My Friends settings	Enable/Disable	X		Disable	AIOS-15-013100	Supervised only. Configuration Profile Key: allowFindMyFriends Modification
Restrictions	Allow USB Restricted Mode	Enable/Disable	X		Enable	AIOS-15-012200	Supervised only. Enable prevents the device from connecting to a USB accessory while locked. Configuration Profile Key: allowUSBRestrictedMode **Note:** This control is called "Allow USB accessories while device is locked" in Apple Configurator and the control logic is opposite to what is listed here. Ensure the MDM

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
							policy rule is set correctly (to disable USB accessory connections when the device is locked).
Restrictions	Allow documents from managed sources in unmanaged destinations	Enable/Disable	X		Disable	AIOS-15-009700	Configuration Profile Key: allowOpenFromManagedTo Unmanaged
Restrictions	Treat AirDrop as unmanaged destination	Enable/Disable	X		Enable	AIOS-15-011500	Configuration Profile Key: forceAirDropUnmanaged
Restrictions	Allow Handoff	Enable/Disable	X		Disable	AIOS-15-010800	Configuration Profile Key: allowActivityContinuation
Restrictions	Allow sending diagnostic and usage data to Apple	Enable/Disable	X		Disable	AIOS-15-013400	Configuration Profile Key: allowDiagnosticSubmission
Restrictions	Allow password Autofill	Enable/Disable	X		Disable	AIOS-15-012700	Supervised only. Disable password autofill in browsers and applications. Configuration Profile Key: allowPasswordAutoFill
Restrictions	Force Apple Watch wrist detection	Enable/Disable	X		Enable	AIOS-15-011800	Configuration Profile Key: forceWatchWristDetection

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Allow pairing with Apple Watch	Enable/Disable	X	X	Enable/ Disable	AIOS-15-012600	Supervised only. Control must be disabled unless AO has approved Apple Watch. Configuration Profile Key: allowPairedWatch
Restrictions	Require passcode on first AirPlay pairing	Enable/Disable	X		Enable	AIOS-15-010900	Configuration Profile Key: forceAirPlayOutgoingRequests PairingPassword
Restrictions	Allow setting up new nearby devices	Enable/Disable	X		Disable	AIOS-15-012800	Supervised only. Allows the prompt to set up new devices that are nearby. Configuration Profile Key: allowProximitySetupToNew Device
Restrictions	Allow proximity-based password sharing requests	Enable/Disable	X		Disable	AIOS-15-012900	Supervised only. Allows an Apple device to request a password of a nearby device. Configuration Profile Key: allowPasswordProximity Requests

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Allow password sharing	Enable/Disable	X		Disable	AIOS-15-013000	Supervised only. Disables sharing passwords with the AirDrop passwords feature. Configuration Profile Key: allowPasswordSharing
Restrictions	Show Notification Center in Lock screen	Enable/Disable	X		Disable	AIOS-15-007500	Configuration Profile Key: ShowInLockScreen
Restrictions	Show Today view in Lock screen	Enable/Disable	X		Disable	AIOS-15-007600	Configuration Profile Key: allowLockScreenTodayView
Restrictions	Allow managed apps to write contacts to unmanaged contacts accounts	Enable/Disable	X		Disable	AIOS-15-012300	Configuration Profile Key: allowManagedToWrite UnmanagedContacts This payload can only be installed via an MDM.
Restrictions	Allow unmanaged apps to read contacts from managed contacts accounts	Enable/Disable	X		Disable	AIOS-15-012400	Configuration Profile Key allowunmanagedToRead ManagedContacts This payload can only be installed via an MDM.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Disable connections to Siri servers for the purpose of dictation	Enable/Disable	X		Enable	AIOS-15-014400	Configuration Profile Key: forceOnDeviceOnlyDictation
Restrictions	Disable connections to Siri servers for the purpose of translation	Enable/Disable	X		Enable	AIOS-15-014500	Configuration Profile Key: forceOnDeviceOnlyTranslation
Restrictions – Apps	Enable Safari autofill	Enable/Disable	X		Disable	AIOS-15-010600	Supervised only. Disables Safari autofill. Configuration Profile Key: safariAllowAutoFill
Exchange ActiveSync	Use SSL	Enable/Disable	X		Enable	AIOS-15-011300	Configuration Profile Key: SSL
Exchange ActiveSync	Allow messages to be moved	Enable/Disable	X		Disable	AIOS-15-011400	Configuration Profile Key: PreventMove
Exchange ActiveSync	Allow MailDrop	Enable/Disable	X		Disable	AIOS-15-011000	Prevents users from using the iOS MailDrop feature.
MDM Server Option	App must be deleted when the MDM enrollment profile is removed	Enable/Disable	X		Enable	AIOS-15-004900, AIOS-15-005000	Must be configured on the MDM server for each managed app.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
MDM Server Option	Allow backup in Managed Apps	Enable/Disable	X		Disable	AIOS-15-009200	Must be configured on the MDM server for each managed app.

Table 2: Optional Controls – Supervised and Non-Supervised

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Passcode	Require alphanumeric value	Enable/Disable		X	Disable		
Passcode	Minimum number of complex characters	1–4, – –		X	– –		
Passcode	Maximum passcode age	1–730, or None		X	None		
Passcode	Passcode history	1–50, or None		X	None		
Restrictions	Allow use of camera	Enable/Disable		X	Enable		
Restrictions	Allow FaceTime	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow screenshots and screen recording	Enable/Disable		X	Enable		
Restrictions	Allow AirPlay, view Screen by Classroom, and Screen Sharing	Enable/Disable		X	Enable		
Restrictions	Allow Classroom to perform AirPlay and View Screen without prompting	Enable/Disable		X	Disable	Restrictions	Supervised only.
Restrictions	Allow iMessage	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Apple Music	Enable/Disable		X	Enable		Supervised only.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions	Allow Radio	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Siri	Enable/Disable		X	Enable		
Restrictions	Enable Siri Profanity Filter	Enable/Disable		X	Disable		Supervised only.
Restrictions	Show user-generated content in Siri	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Siri Suggestions	Enable/Disable		X	Enable		Supervised only. Also called "Allow Spotlight Internet Results".
Restrictions	Allow Apple Books	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow installing apps using App Store	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow automatic app downloads	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow removing apps	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow removing system apps	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow App Clips	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow in-app purchase	Enable/Disable		X	Enable		

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions	Require iTunes Store password for all purchases	Enable/Disable		X	Disable		
Restrictions	Allow notes and highlights sync for enterprise books	Enable/Disable		X	Enable		
Restrictions	Allow automatic sync while roaming	Enable/Disable		X	Enable		
Restrictions	Allow Erase All Content and Settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow users to accept untrusted TLS certificates	Enable/Disable		X	Enable		
Restrictions	Allow Automatic Updates to certificate trust settings	Enable/Disable		X	Enable		Also called "Allow OTA PKI Updates".
Restrictions	Allow Installing configuration profiles	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow adding VPN configurations	Enable/Disable		X	Enable		Supervised only.
Restrictions	Force Automatic date and time	Enable/Disable		X	Enable		Supervised only.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions	Allow Classroom to lock to an app and lock the device without prompting	Enable/Disable		X	Disable		Supervised only.
Restrictions	Automatically join Classroom classes without prompting	Enable/Disable		X	Disable		Supervised only.
Restrictions	Require teacher permission to leave Classroom unmanaged classes	Enable/Disable		X	Disable		Supervised only.
Restrictions	Force Wi-Fi power on	Enable/Disable		X	Disable		Supervised only.
Restrictions	Allow modifying account settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying Bluetooth settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying cellular data app settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying cellular plan settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying eSim settings	Enable/Disable		X	Enable		Supervised only.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions	Allow modifying device name	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying notifications settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying passcode	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying Touch ID fingerprints/ Face ID faces	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Screen Time	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying Wallpaper	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow modifying Personal Hotspot settings	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Find My Device	Enable/Disable		X	Allow		Supervised only.
Restrictions	Allow pairing with non-Configurator hosts	Enable/Disable		X	Enable		Supervised only.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions	Allow documents from unmanaged sources in managed destinations	Enable/Disable		X	Enable		
Restrictions	Allow modifying diagnostics settings	Enable/Disable		X	Disable		Supervised only.
Restrictions	Allow Touch ID/Face ID to unlock device	Enable/Disable		X	Enable		
Restrictions	Require Touch ID/ Face ID authentication before Autofill	Enable/Disable		X	Enable		Supervised only.
Restrictions	Join only Wi-Fi networks installed by a Wi-Fi payload	Enable/Disable		X	Enable		Supervised only. (Wi-Fi whitelisting)
Restrictions	Allow AirPrint	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow discovery of AirPrint printers using iBeacons	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow storage of AirPrint credentials in Keychain	Enable/Disable		X	Enable		Supervised only.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions	Disallow AirPrint to destinations with untrusted certificates	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow predictive keyboard	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow keyboard shortcuts	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow continuous path keyboard	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow auto correction	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow spell check	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Define	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow dictation	Enable/Disable		X	Enable		Supervised only.
Restrictions	Allow Wallet notifications in Lock screen	Enable/Disable		X	Enable		
Restrictions	Show Control Center in Lock Screen	Enable/Disable		X	Enable		
Restrictions	Defer software updates for _____ days	value		X	AO defined		Supervised only.
Restrictions – Apps	Allow use of iTunes Store	Enable/Disable		X	Enable		Supervised only.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions – Apps	Allow use of News	Enable/Disable		X	Enable		Supervised only.
Restrictions – Apps	Allow use of Podcasts	Enable/Disable		X	Enable		Supervised only.
Restrictions – Apps	Allow use of Game Center	Enable/Disable		X	Disable		Supervised only.
Restrictions – Apps	Allow multiplayer gaming	Enable/Disable		X	Disable		Supervised only.
Restrictions – Apps	Allow adding Game Center friends	Enable/Disable		X	Disable		Supervised only.
Restrictions – Apps	Allow use of Safari	Enable/Disable		X	Enable		Supervised only.
Restrictions – Apps	Force fraud warning	Enable/Disable		X	Enable		
Restrictions – Apps	Enable JavaScript	Enable/Disable		X	Enable		
Restrictions – Apps	Safari Block pop-ups	Enable/Disable		X	Enable		
Restrictions – Apps	Safari Accept Cookies	0, 1, 1.5, 2		X	2		"2-Prevent Cross-Site Tracking" is enabled and "Block All Cookies" is not enabled.

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
							Note: Options changed in iOS 11. Some MDMs may still use the old settings. In that case, recommend "Always" be selected.
Restrictions – Media Content	Ratings region	- Australia - Canada - France - Germany - Ireland - Japan - New Zealand - United Kingdom - United States		X	United States		
Restrictions – Media Content	Allowed Content Ratings (Movies)	Varies by country		X	Allow All Movies		
Restrictions – Media Content	Allowed Content Ratings (TV Shows)	Varies by country		X	Allow All TV Shows		
Restrictions – Media Content	Allowed Content Ratings (Apps)	4+/9+/12+/17+		X	Allow All Apps		

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
Restrictions – Media Content	Allow playback of explicit music, podcasts, and iTunes U media	Enable/Disable		X	Disable		Supervised only.
Restrictions – Media Content	Allow explicit sexual content in iBooks Store	Enable/Disable		X	Disable		
Domains	Unmarked Email Domains	Add/Remove		X	Enterprise email domain		
Domains	Managed Safari Web Domains	Add/Remove		X	List of .mil domains		A configuration profile may be set up by listing DoD web domains (obtain a list of DoD domains from the DoD NIC at https://www.nic.mil).
Exchange ActiveSync	Enable S/MIME signing	Enable/Disable		X	Enable		
Exchange ActiveSync	Allow recent addresses to be synced	Enable/Disable		X	Enable		
Exchange ActiveSync	Use only in Mail	Enable/Disable		X	Disable		Prevents third-party apps from sending messages using the Exchange email account.
Certificates	NA	NA		X	NA		It is not required to add certificates. If certificates are

Policy Group	Policy Rule	Options	Required	Optional	Suggested Settings	Related Requirement Number	Comments
							added, they must be DoD-approved certificates.
NA	Wi-Fi Assist	Enable/Disable		X	Disable		User-Based Enforcement (UBE) control. User must implement configuration setting (Settings >> Cellular >> Wi-Fi Assist).