FIRST DRAFT

APPLE iOS 10
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG)
CONFIGURATION TABLE

Version 1, Release 0.1

23 September 2016

Developed by Apple and DISA for the DoD

LIST OF TABLES

Page

Table 1: Non-Supervised Controls

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
General - Security	Removal of configuration profile	-Always -Never -With Authentication	X		Never	AIOS-10-080103	
Passcode	Allow Simple Value	Enable/Disable	X		Disable	AIOS-01-080007	Simple value passcodes include repeating, ascending, and descending character sequences.
Passcode	Require Alphanumeric value	Enable/Disable		X	Disable		
Passcode	Minimum passcode length	1 – 16	X		6	AIOS-01-080004	
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		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Passcode	Maximum auto-lock	1 – 15, or None	X		1 - 5 recommended, 15 maximum allowable	AIOS-01-080002	Device automatically locks when minutes elapse. If maximum auto-lock equals 15, the grace period shall be set to "Immediately".
Passcode	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-01-080002	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".
Passcode	Maximum number of failed attempts	2 – 10	X		10	AIOS-01-080005	
Restrictions - Functionality	Allow use of camera	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow FaceTime	Enable/Disable		X	Disable		"Disable" is a non-default value.
Restrictions - Functionality	Allow screenshots	Enable/Disable		X	Disable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Allow AirDrop	Enable/Disable	X		Disable	AIOS-05-080001	An iOS management tool can only enforce this setting on a Supervised iOS device. It is not required that iOS devices be Supervised. For devices that are not Supervised, users must manually enforce the setting on each device.
Restrictions - Functionality	Allow voice dialing	Enable/Disable	X		Disable	AIOS-02-080012	
Restrictions - Functionality	Allow Siri	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Siri while device is locked	Enable/Disable	X		Disable	AIOS-02-080011	
Restrictions - Functionality	Allow installing apps	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow in-app purchase	Enable/Disable		X	Disable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Require iTunes Store password for all purchases	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow iCloud backup	Enable/Disable	X		Disable	AIOS-02-080002	
Restrictions – Functionality	Allow iCloud documents & data	Enable/Disable	X		Disable	AIOS-02-080003	
Restrictions - Functionality	Allow iCloud keychain	Enable/Disable	X		Disable	AIOS-02-080004	
Restrictions - Functionality	Allow managed apps to store data in iCloud	Enable/Disable	X		Disable	AIOS-02-080103	
Restrictions - Functionality	Allow backup of enterprise books	Enable/Disable	X		Disable	AIOS-02-080101	
Restrictions - Functionality	Allow notes and highlights sync for enterprise books	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow iCloud photo sharing	Enable/Disable	X		Disable	AIOS-02-080006	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Allow My Photo Stream	Enable/Disable	X		Disable	AIOS-02-080005	
Restrictions - Functionality	Allow automatic sync while roaming	Enable/Disable		X	Disable		
Restrictions - Functionality	Force encrypted backups	Enable/Disable	X		Enable	AIOS-02-080017	
Restrictions – Functionality	Force limited ad tracking	Enable/Disable	X		Enable	AIOS-02-080008	
Restrictions - Functionality	Allow users to accept untrusted TLS certificates	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow automatic updates to certificate trust settings	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow documents from managed apps in unmanaged apps	Enable/Disable	X		Disable	AIOS-02-080014	
Restrictions – Functionality	Allow documents from unmanaged apps in managed apps	Enable/Disable		X	Disable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Allow Handoff	Enable/Disable	X		Disable	AIOS-02-080102	
Restrictions - Functionality	Allow Internet search results in Spotlight	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow sending diagnostic and usage data to Apple	Enable/Disable	X		Disable	AIOS-02-080007	
Restrictions – Functionality	Allow Touch ID to unlock device	Enable/Disable	X	X	Disable	AIOS-02-080013	Based on AO determination
Restrictions - Functionality	Require passcode on first AirPlay pairing	Enable/Disable	X		Enable	AIOS-02-080104	
Restrictions - Functionality	Allow access when unlocked-Passbook	Enable/Disable		X	Disable		
Restrictions – Functionality	Show Control Center in Lock screen	Enable/Disable		X	Disable		
Restrictions – Functionality	Show Notification Center in Lock screen	Enable/Disable	X		Disable	AIOS-02-080009	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Show Today view in Lock screen	Enable/Disable	X		Disable	AIOS-02-080010	
Restrictions - Applications	Allow installing apps using App Store and Apple Configurator	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow adding Game Center friends	Enable/Disable		X	Disable		
Restrictions - Functionality	Force Apple Watch wrist detection	Enable/Disable	X		Enable	AIOS-11-080203	
Restrictions – Apps	Allow use of Safari	Enable/Disable		X	Enable		
Restrictions - Apps	Enable autofill	Enable/Disable	X		Disable	AIOS-02-080016	
Restrictions - Apps	Force fraud warning	Enable/Disable		X	Enable		
Restrictions - Apps	Enable JavaScript	Enable/Disable		X	Enable		
Restrictions - Apps	Block pop-ups	Enable/Disable		X	Enable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Apps	Accept Cookies	-Never -From visited sites -Always		X	From visited sites		
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	Settings	Related Requirement Number	Comments
Restrictions – Media Content	Allow playback of explicit, music, podcasts, and iTunes U media	Enable/Disable		X	Disable		
Restrictions – Media Content	Allow explicit sexual content in iBooks Store	Enable/Disable		X	Disable		
Domains	Unmarked Email Domains	Add/Remove		X	Enterprise email domain		
Exchange Active Sync	Enable S/MIME	Enable/Disable		X	Enable		
Exchange Active Sync	Use SSL	Enable/Disable	X		Enable	AIOS-03-080101	
Exchange Active Sync	Past Days of Mail to Sync	-No limit -1 day -3 days -1 week -2 weeks -1 month		X	No limit		"No limit" is not a default setting.
Exchange Active Sync	Allow messages to be moved	Enable/Disable	X		Disable	AIOS-03-080102	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Exchange Active Sync	Allow recent addresses to be synced	Enable/Disable		X	Enable		
Exchange Active Sync	Use only in Mail	Enable/Disable		X	Disable		Prevents third-party apps from sending messages using the Exchange email account.
Exchange Active Sync	Allow MailDrop	Enable/Disable	**X**		Disable	AIOS-02-090100	Prevents users from using the iOS MailDrop feature. Control is New in iOS 9
Certificates	NA	NA		X	NA		It is not required to add certificates. If certificates are added, they must be DoD-approved certificates.
MDM Server Option	App must be deleted when the MDM enrollment profile is removed	Enable/Disable	X		Enable	AIOS-11-080202	Must be configured on the MDM server for each Managed App.
MDM Server Option	Allow backup in Managed Apps	Enable/Disable	X		Disable	AIOS-11-080201	Must be configured on the MDM server for each Managed App.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Managed Domains	Managed Safari Web Domains	Add/Remove		X	List of .mil domains		An example configuration profile listing .mil domains will be provided as PKI-protected content at the IASE website (http://iase.disa.mil). Authorized individuals should visit the site for the latest guidance on appropriate use of managed domains.
VPN	Per App VPN	Enable/Disable		X	Enable	AIOS-11-080200	Not required if the Always-on VPN profile is enabled, or a DoD-approved VPN profile is installed, or if the App has VPN functions already included in the App.
VPN	Always-on VPN	Enable/Disable		X	Enable	AIOS-11-080200	This setting is only available if managed devices are supervised. Not required if the Per App VPN is enabled, or a DoD-approved VPN profile is installed, or the App has VPN functions already included in the App.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
VPN	VPN Function included in App	NA		X		AIOS-11-080200	Not required if the Always-on VPN profile is enabled, or the Per App VPN is enabled, or a DoD-approved VPN profile is installed.
Restrictions - Functionality	Allow iCloud Photo Library	Enable/Disable	X		Disable	AIOS-02-090101	
Restrictions - Functionality	Treat AirDrop as unmanaged destination	Enable/Disable	X		Enable	AIOS-05-080001	
NA	Wi-Fi Assist	Enable/Disable		X	Disable		User-Based Enforcement (UBE) control. User must implement configuration setting (Settings >> Cellular >> Wi-Fi Assist)

Table 2: Optional Supervised Controls

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Allow manual install of configuration profiles	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow account modification	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow Game Center	Enable/Disable		X	Disable		
Restrictions - Functionality	Multiplayer gaming	Enable/Disable		X	Disable		
Restrictions - Functionality	Adding Game Center Friends	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow AirDrop	Enable/Disable		X	Enable		This setting can be set in conjunction with treating AirDrop as unmanaged.
Restrictions - Functionality	Allow Find my friends	Enable/Disable		X	Disable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Allow removal of apps	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow pairing to computers for content sync	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow iMessage	Enable/Disable		X	Enable		
Restrictions - Functionality	Enable Siri Profanity Filter	Enable/Disable		X	Enable		
Restrictions - Functionality	Show User Generated content in Siri	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow iBooks Store	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow installing apps using App Store	Enable/Disable		X	Enable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Allow automatic app downloads	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow Erase All Content and Settings	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow modifying cellular data app settings	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow modifying device name	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow modifying passcode	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow modifying Touch ID fingerprints	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow modifying restrictions	Enable/Disable		X	Enable		.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Functionality	Allow modifying Wallpaper	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow pairing with Apple Watch	Enable/Disable		X	Enable (if approved by AO)		
Restrictions - Functionality	Allow Predictive keyboard	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow keyboard shortcuts	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow auto correction	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Spell check	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Define	Enable/Disable		X	Enable		
Restrictions - Apps	Allow use of News	Enable/Disable		X	Enable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions - Apps	Allow use of Podcasts	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Trusting new Enterprise App Authors	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow Screen Observation by Classroom App	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Apple Music	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Radio	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow Siri Suggestions	Enable/Disable		X	Disable		
Restrictions - Functionality	Allow modifying bluetooth settings	Enable/Disable		X	Enable		
Restrictions - Functionality	Allow modifying notifications settings	Enable/Disable		X	Disable		