

UNCLASSIFIED



APPLE iOS 11 STIG CONFIGURATION TABLES

Version 1, Release 1

11 December 2017

Developed by Apple and DISA for the DoD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: Non-Supervised Controls.....	1
Table 2: Optional Supervised Controls.....	12

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-11-012400	
Passcode	Allow Simple Value	Enable/Disable	X		Disable	AIOS-11-000200	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-11-000100	
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		

UNCLASSIFIED

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-11-000300	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-11-000300	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-11-000400	
Restrictions – Functionality	Allow use of camera	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow FaceTime	Enable/Disable		X	Enable		“Disable” is a non-default value.
Restrictions – Functionality	Allow screenshots	Enable/Disable		X	Enable		Default
Restrictions – Functionality	Allow voice dialing while device is locked	Enable/Disable	X		Disable	AIOS-11-001300	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Allow Siri	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow Siri while device is locked	Enable/Disable	X		Disable	AIOS-11-001200	
Restrictions – Functionality	Allow Siri Suggestions	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow installing apps	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow in-app purchase	Enable/Disable		X	Enable		
Restrictions – Functionality	Require iTunes Store password for all purchases	Enable/Disable		X	Disable		
Restrictions – Functionality	Allow iCloud backup	Enable/Disable	X	X	Disable	AIOS-11-004100	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store.
Restrictions – Functionality	Allow iCloud Documents & Data	Enable/Disable	X	X	Disable	AIOS-11-004200	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store.

UNCLASSIFIED

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Allow iCloud Keychain	Enable/Disable	X	X	Disable	AIOS-11-004300	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store.
Restrictions – Functionality	Allow managed apps to store data in iCloud	Enable/Disable	X		Disable	AIOS-11-004600	
Restrictions – Functionality	Allow backup of enterprise books	Enable/Disable	X		Disable	AIOS-11-011200	
Restrictions – Functionality	Allow notes and highlights sync for enterprise books	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow iCloud photo sharing	Enable/Disable	X	X	Disable	AIOS-11-004500	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store.
Restrictions – Functionality	Allow iCloud Photo Library	Enable/Disable	X	X	Disable	AIOS-11-011700	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Allow My Photo Stream	Enable/Disable	X	X	Disable	AIOS-11-004400	This requirement is Not Applicable if the AO has approved unrestricted download of unmanaged apps from the Apple App Store.
Restrictions – Functionality	Allow automatic sync while roaming	Enable/Disable		X	Enable		
Restrictions – Functionality	Force encrypted backups	Enable/Disable	X		Enable	AIOS-11-011100	
Restrictions – Functionality	Force limited ad tracking	Enable/Disable	X		Enable	AIOS-11-010900	
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 Trusting New Enterprise App Authors	Enable/Disable	X		Disable	AIOS-11-000900	

UNCLASSIFIED

Apple iOS 11 STIG Configuration Tables, V1R1
11 December 2017

DISA
Developed by Apple and DISA for the DoD

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Allow documents from managed sources in unmanaged destinations	Enable/Disable	X		Disable	AIOS-11-005210	
Restrictions – Functionality	Allow documents from unmanaged sources in managed destinations	Enable/Disable		X	Disable		
Restrictions – Functionality	Treat AirDrop as unmanaged destination	Enable/Disable	X		Enable	AIOS-11-012100	
Restrictions – Functionality	Allow Handoff	Enable/Disable	X		Disable	AIOS-11-011300	
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-11-005400	
Restrictions – Functionality	Allow Touch ID/Face ID to unlock device	Enable/Disable	X	X	Disable	AIOS-11-002400 AIOS-11-002500	Based on AO determination for Touch ID only.
Restrictions – Functionality	Force Apple Watch wrist detection	Enable/Disable	X		Enable	AIOS-11-080203	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Require passcode on first AirPlay pairing	Enable/Disable	X		Enable	AIOS-11-011500	
Restrictions – Functionality	Allow setting up new nearby devices	Enable/Disable		X	Disable		
Restrictions – Functionality	Allow Wallet notifications in Lock screen	Enable/Disable		X	Enable		
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-11-001700	
Restrictions – Functionality	Show Today view in Lock screen	Enable/Disable	X		Disable	AIOS-11-001800	
Restrictions – Apps	Allow use of iTunes Store	Enable/Disable		X	Enable		
Restrictions – Apps	Allow adding Game Center friends	Enable/Disable		X	Disable		
Restrictions – Apps	Allow use of Safari	Enable/Disable		X	Enable		
Restrictions – Apps	Enable autofill	Enable/Disable	X		Disable	AIOS-11-011000	

UNCLASSIFIED

Apple iOS 11 STIG Configuration Tables, V1R1
11 December 2017

DISA
Developed by Apple and DISA for the DoD

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
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		
Restrictions – Apps	Accept Cookies	- Never - From visited sites - Always		X	Always		
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		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
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		
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-11-011900	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
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-11-012000	
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-11-011600	Prevents users from using the iOS MailDrop feature.
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-11-007200, AIOS-11-008700	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-11-003900	Must be configured on the MDM server for each managed app.
Managed Domains	Managed Safari Web Domains	Add/Remove		X	List of .mil domains		A configuration profile may be developed by listing DoD web domains (obtain a list of DoD domains from the DoD NIC at https://www.nic.mil).
VPN	Per App VPN	Enable/Disable		X	Enable		
VPN	Always-on VPN	Enable/Disable		X	Enable		
VPN	Device VPN	NA		X	Enable		
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		
Restrictions – Functionality	Allow removal of apps	Enable/Disable		X	Disable		
Restrictions – Functionality	Allow pairing to computers for content sync	Enable/Disable		X	Disable		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
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		
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		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions – Functionality	Allow modifying Touch ID fingerprints	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow modifying restrictions	Enable/Disable		X	Enable		
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 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 modifying Bluetooth settings	Enable/Disable		X	Enable		
Restrictions – Functionality	Allow modifying notifications settings	Enable/Disable		X	Disable		