

UNCLASSIFIED



APPLE IOS/IPADOS 17 BRING YOUR OWN DEVICE (BYOAD) STIG CONFIGURATION TABLES

02 July 2025

Developed by Apple and DISA for the DOD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: COPE Required Controls – Supervised and Nonsupervised	1

Table 1: COPE Required Controls – Supervised and Nonsupervised

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Passcode	Allow Simple Value	Enable/Disable	X		Disable	AIOS-17-706600	Simple value passcodes include repeating, ascending, and descending character sequences. Configuration Profile Key: allowSimple
Passcode	Minimum passcode length	1–16	X		6	AIOS-17-706500	Configuration Profile Key: minLength
Passcode	Maximum auto-lock	1–15, or None	X		1–5 recommended; 15 maximum allowable	AIOS-17-706700, AIOS-17-706800	Device automatically locks when minutes elapse. If maximum auto-lock equals 15, the grace period must be set to “Immediately”. 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-17-706700, AIOS-17-706800	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”.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
							Configuration Profile Key: maxGracePeriod
Passcode	Maximum number of failed attempts	2–10	X		10	AIOS-17-706900	Configuration Profile Key: maxFailedAttempts
Passcode	Require passcode	Enable/Disable	X		Enable	AIOS-17-010400	Configuration Profile Key: forcePIN
Passcode	Passcode history	None, 1-50	X		2 or more	AIOS-17-706950	Configuration Profile Key: pinHistory
Restrictions	Allow managed apps to store data in iCloud	Enable/Disable	X		Disable	AIOS-17-703600	Configuration Profile Key: allowManagedAppsCloudSync
Restrictions	Allow backup of enterprise books	Enable/Disable	X		Disable	AIOS-17-703700	Configuration Profile Key: allowEnterpriseBookBackup
Restrictions	Force encrypted backups	Enable/Disable	X		Enable	AIOS-17-710700	Configuration Profile Key: forceEncryptedBackup
Restrictions	Allow Trusting New Enterprise App Authors	Enable/Disable	X		Disable	AIOS-17-707000, AIOS-17-800060	Configuration Profile Key: allowEnterpriseAppTrust

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Allow documents from managed sources in unmanaged destinations	Enable/Disable	X		Disable	AIOS-17-709700	Configuration Profile Key: allowOpenFromManagedToUnmanaged
Restrictions	Treat AirDrop as unmanaged destination	Enable/Disable	X		Enable	AIOS-17-711500	Configuration Profile Key: forceAirDropUnmanaged
Restrictions	Allow sending diagnostic and usage data to Apple	Enable/Disable	X		Disable	AIOS-17-713400	Configuration Profile Key: allowDiagnosticSubmission
Restrictions	Force Apple Watch wrist detection	Enable/Disable	X		Enable	AIOS-17-711800	Configuration Profile Key: forceWatchWristDetection
Restrictions	Require passcode on first AirPlay pairing (outgoing request)	Enable/Disable	X		Enable	AIOS-17-710900	Configuration Profile Key: forceAirPlayOutgoingRequestsPairingPassword
Restrictions	Require passcode on first AirPlay pairing (incoming request)	Enable/Disable	X		Enable	AIOS-17-710950	Configuration Profile Key: forceAirPlayIncomingRequestsPairingPassword
Restrictions	Show Notification in Lock screen	Enable/Disable	X		Disable	AIOS-17-707500	Configuration Profile Key: allowLockScreenNotificationView

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Restrictions	Show Today view in Lock screen	Enable/Disable	X		Disable	AIOS-17-707600	Configuration Profile Key: allowLockScreenTodayView
Restrictions	Allow managed apps to write contacts to unmanaged contacts accounts	Enable/Disable	X		Disable	AIOS-17-712300	Configuration Profile Key: allowManagedToWriteUnmanagedContacts 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-17-712400	Configuration Profile Key: allowunmanagedToReadManagedContacts This payload can only be installed via an MDM.
Restrictions	Require Managed pasteboard	Enable/Disable	X		Enable	AIOS-17-714600	Configuration Profile Key: requireManagedPasteboard
Restrictions	Allow unmanaged apps to open managed apps	Enable/Disable	X		Enable	AIOS-17-714900	Configuration Profile Key: allowOpenFromUnmanagedToManaged
Exchange ActiveSync	Use SSL	Enable/Disable	X		Enable	AIOS-17-711300	Configuration Profile Key: SSL
Exchange ActiveSync	Allow messages to be moved	Enable/Disable	X		Disable	AIOS-17-711400	Configuration Profile Key: PreventMove

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
MDM Server Option	App must be deleted when the MDM enrollment profile is removed	Enable/Disable	X		Enable	AIOS-17-709900, AIOS-17-710000	Must be configured on the MDM server for each managed app.
MDM Server Option	Allow backup in Managed Apps	Enable/Disable	X		Disable	AIOS-17-709200	Must be configured on the MDM server for each managed app.