

UNCLASSIFIED



GOOGLE ANDROID 13 BYOAD SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) CONFIGURATION TABLES

24 April 2024

Developed by Google and DISA for the DOD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: Configuration Policy Rules for Work Profile for Employee-Owned Devices (BYOD)	1

Note: The logic of some of the configuration settings in the following table may differ from one EMM product to another. For example, the policy rule “Disable Manual Date Time Changes” may appear as “Allow Manual Date Time Changes” in some EMM consoles. In this case, the setting should be configured to “False” instead of “True”.

Table 1: Configuration Policy Rules for Work Profile for Employee-Owned Devices (BYOD)

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Password Requirements	Minimum password length (Work Profile)	0+	6	GOOG-13-706000	Applies only to the Work Profile. Minimum work profile password length Configuration API: setPasswordMinimumLength(int) Int = 6 (or more)
Password Requirements	Password Quality (Device)	High, Medium, Low	High	GOOG-13-706000	Applies only to the Work Profile. Configuration API: setRequiredPasswordComplexity(int) int = PASSWORD_COMPLEXITY_HIGH
Password Requirements	OneLock	Enable, Disable	Enable/Disable	GOOG-13-706000	This is an optional setting. Configuration setting depends on whether OneLock will be allowed at the site and the logic of the MDM configuration policy setting. Configuration API: DISALLOW_UNIFIED_PASSWORD
Password Requirements	Minimum password quality (Work Profile)	Unspecified, Something, Numeric, Numeric (Complex), Alphabetic,	Numeric (Complex), Alphabetic, Alphanumeric, or Complex	GOOG-13-706000	Applies only to the Work Profile. Configuration API: setRequiredPasswordComplexity

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
		Alphanumeric, Complex			
Password Requirements	Device lock timeout	0+	15	GOOG-13-706200, GOOG-13-706300	Configuration API: setMaximumTimeToLock
Password Requirements	Maximum number of failed attempts	0+	10	GOOG-13-706400	Configuration API: setMaximumFailedPasswordsForWipe()
Restrictions	Nonmarket App installation	Select/unselect	Select	GOOG-13-706500	Configuration API: DISALLOW_INSTALL_UNKNOWN_SOURCES
Restrictions	List of approved apps listed in managed Google Play	List of approved apps	List only approved workspace apps in managed Google Play	GOOG-13-706600, GOOG-13-706700	Managed Google Play is always an allowlisted App Store.
Restrictions	Unredacted notifications	Select/unselect	Select	GOOG-13-706800	Configuration API: KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
Restrictions	Disable trust agents	Select/unselect	Select	GOOG-13-707200	Configuration API: KEYGUARD_DISABLE_TRUST_AGENTS
Restrictions	Lock screen message	Enable/disable	Enable, Disable	GOOG-13-707700	If the DOD warning banner is not placed in the user agreement, configure on the Google device via the MDM console and enter required text. Configuration API: setDeviceOwnerLockScreenInfo
Restrictions	Disallow backup service (remote)	Select/unselect	Select	GOOG-13-008600	Configuration API: setBackupServiceEnabled

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Restrictions	Disallow cross-profile copy/paste	Select/unselect	Select	GOOG-13-708900	Configuration API: DISALLOW_CROSS_PROFILE_COPY_PASTE
Restrictions	Disallow sharing data into the profile	Select/unselect	Select	GOOG-13-708900	Configuration API: DISALLOW_SHARE_INTO_MANAGED_PROFILE
Policy Management	Certificates	Include DOD certificates in work profile		GOOG-13-710000	Configuration API: installCaCert()
Restrictions	Disallow config credentials	Select/unselect	Select	GOOG-13-712300	Configuration API: DISALLOW_CONFIG_CREDENTIALS
Restrictions	Disallow modify accounts in work profile	Select/unselect	Select	GOOG-13-710100	Blocks user from adding personal accounts to a work profile. Configuration API: DISALLOW_MODIFY_ACCOUNTS
Policy Management	Core app allowlist	Select/unselect	Select	GOOG-13-710200	Enforce system app “disable” list with this control. Configuration API: enableSystemApp and setApplicationHidden
Enrollment Configuration	Default device enrollment	Fully Managed/use for work and personal/ Android work profile for employee-owned devices (BYOD)	Android work profile for employee-owned devices (BYOD)	GOOG-13-710300	Android work profile for employee-owned devices (BYOD)

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Restrictions	Disallow autofill on web browser	Enable/Disable	Disable	GOOG-13-710400	Workspace browser auto completion Chrome Browser configuration: SearchSuggestEnabled = Disabled
Restrictions	Disallow autofill in work profile apps	Select/unselect	Select	GOOG-13-710500	System autofill: Configuration API: DISALLOW_AUTOFILL
Restrictions	Set input method to only default keyboard	List of approved keyboards in device-side Google Play	Do not approve any third-party keyboard applications	GOOG-13-710900	Google Play on personal side of device can be allowlist or blocklist. Configure with an allowlist of approved apps and do not approve any third-party keyboard apps.