GOOGLE ANDROID 10.x SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) CONFIGURATION TABLE

Version 1, Release 2

24 January 2020

Developed by Google and DISA for the DoD

LIST OF TABLES

Page

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

The configuration for this STIG assumes the Corporate Owned Personally Enabled (COPE) use case is deployed.

Table 1: Configuration Policy Rules

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Password Requirements	Minimum password length	0+	6	GOOG-10-000100	Minimum device password length Configuration API: setPasswordMinimumLength()
Password Requirements	Minimum password quality	Unspecified, Something, Numeric, Numeric (Complex), Alphabetic, Alphanumeric, Complex	Numeric (Complex), Alphabetic, Alphanumeric, or Complex	GOOG-10-000200	Numeric (Complex) recommended Configuration API: setPasswordQuality()
Password Requirements	Device lock timeout	0+	15	GOOG-10-000300, GOOG-10-000400	Configuration API: setMaximumTimeToLock()
Password Requirements	Maximum number of failed attempts	0+	10	GOOG-10-000500	Configuration API: setMaximumFailedPasswordsForWipe()
Restrictions	Non-Market App Installation	Allow/Disallow	Disallow	GOOG-10-000800	Configuration API: DISALLOW_INSTALL_UNKNOWN_SOURCES()
Restrictions	List of approved apps listed in	List of approved apps	List only approved workspace	GOOG-10-001000,	Managed Google Play is always a Whitelisted App Store

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
	managed Google Play		apps in managed Google Play	GOOG-10-001100	
Restrictions	Bluetooth	Allow/ Disallow	Allow, Disallow	GOOG-10-001400	Setting of control depends on AO decision Configuration API: DISALLOW_BLUETOOTH()
Restrictions	Unredacted Notifications	Allow/ Disallow	Disallow	GOOG-10-001600	Configuration API: KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
Restrictions	Disable trust agents	Select/ unselect	Select	GOOG-10-002300	Configuration API: KEYGUARD_DISABLE_TRUST_AGENTS()
Restrictions	Debugging features	Allow/ Disallow	Disallow	GOOG-10-002800	Configuration API: DISALLOW_DEBUGGING_FEATURES()
Restrictions	Lock Screen Message	Enable/ Disable	Enable, Disable	GOOG-10-003400	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 USB file transfer	Select/ unselect	Select	GOOG-10-003500, GOOG-10-003700	Configuration API: DISALLOW_MOUNT_PHYSICAL_MEDIA()
Restrictions	Disallow backup servicer	Select/ unselect	Select	Optional setting	Since personal accounts cannot be added (GOOG-10-009200), this control only impacts personal profile accounts. Site can allow backup based on local policy. Configuration API: setBackupServiceEnabled()
Restrictions	Disallow cross profile copy/paste	Enable/ disable	Select	GOOG-10-004500	Configuration API: DISALLOW_CROSS_PROFILE_COPY_PASTE()

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Restrictions	Disallow sharing data into the profile	Enable/ disable	Select	GOOG-10-004500	Configuration API: DISALLOW_SHARE_INTO_MANAGED_PROFILE()
Restrictions	Disallow Add User	Select/ unselect	Select	GOOG-10-004700	Multi-user mode Configuration API: DISALLOW_ADD_USER()
Restrictions	Enable security logging	Select/ unselect	Select	GOOG-10-005505, GOOG-10-006100	Configuration API: setSecurityLoggingEnabled
Restrictions	Enable network logging	Select/ unselect	Select	GOOG-10-005505	Configuration API: setNetworkLoggingEnabled()
Restrictions	Disallow config tethering	Select/ unselect	Select	GOOG-10-008800	Configuration API: DISALLOW_CONFIG_TETHERING()
Policy Management	Certificates	Include DoD certificates in work profile		GOOG-10-009000	Configuration API: installCaCert()
Restrictions	Disallow config credentials	Select/ unselect	Select	GOOG-10-009100	Configuration API: DISALLOW_CONFIG_CREDENTIALS()
Restrictions	Disallow modify accounts in work profile	Select/ unselect	Select	GOOG-10-009200	Blocks adding personal accounts to a work profile by user Configuration API: DISALLOW_MODIFY_ACCOUNTS()
Policy Management	Core app white list	List approved core apps		GOOG-10-009400	Enforce system app “disable” list with this control Configuration API: enableSystemApp()

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Enrollment Configuration	Default device enrollment	Fully Managed/ Fully Managed Devices with Work Profiles	Fully Managed Devices with Work Profiles	GOOG-10-009600	COPE enrollment
Restrictions	Disallow autofill	Select/ unselect	Select	GOOG-10-009800,GOOG-10-010000	Workspace browser and app auto completion Configuration API: DISALLOW_AUTOFILL()
Restrictions	Set auto (network) time required	Select/ unselect	Select	GOOG-10-010200	Configuration API: setAutoTimeRequired()
Restrictions	Set input method to only default Keyboard	Set default list	Set default list	GOOG-10-011000	Disable the use of a third-party keyboard Configuration API: setPermittedInputMethods()
Restrictions	Cross-profile calendar	Allow all packages/Set allowed packages	Disabled	Optional	Enables the capability of the personal profile calendar for viewing events on the work profile calendar Configuration API: setCrossProfileCalendarPackages()
Restrictions	Set Private DNS Mode	Off, Automatic, Specified Host, Unknown	Select	Optional	Forces the use of DNS over TLS Configuration API: setGlobalPrivateDnsModeOpportunistic() or setGlobalPrivateDnsModeSpecifiedHost()