SAMSUNG ANDROID OS 10 WITH KNOX 3.X STIG CONFIGURATION TABLES

Version 1, Release 1

20 March 2020

Developed by Samsung and DISA for the DoD

LIST OF TABLES

Page

Full details of the APIs used to implement the policies in the following table can be found on the Samsung Knox portal "Knox 3.x STIG Implementation Guide - Samsung Android OS 10 API table" page (https://support.samsungknox.com/hc/en-us/articles/360041379213).

Table Error! No text of specified style in document.**1: Configuration Policy Rules for Device/Asset**

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
Password Requirements	Minimum password length	0+	6	KNOX-10-000100	
#1: Password Requirements #2: Password Requirements KPE Password Requirements	#1: Minimum password quality #2: Minimum password quality Maximum sequential numbers	#1: Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex #2: Password quality options as #1 0+	#1: Numeric(Complex) #2: Numeric 2	KNOX-10-000200, KNOX-10-000300	**Choose Method #1 or #2**. Alphabetic, Alphanumeric, and Complex are also acceptable selections but will cause the user to select a complex password, which is not required by the STIG.
Password Requirements	Max time to screen lock	0 minutes	15 minutes	KNOX-10-000400	
Password Requirements	Max password failures for local wipe	0+	10	KNOX-10-000500	
Restrictions	Installs from unknown sources	Allow/Disallow	Disallow	KNOX-10-000800	Google play must not be disabled. Disabling Google play will cause system instability

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
					and critical updates will not be received. Users will not be able to log into Google play in the Work Environment with personal accounts when applying KNOX-10-003900.
Restrictions	Trust Agents	Enable/Disable	Disable	KNOX-10-002100	
Restrictions	Face	Enable/Disable	Disable	KNOX-10-002200	
Restrictions	Debugging features	Allow/Disallow	Disallow	KNOX-10-002700	For KPE(LEGACY) COPE deployments this configuration is the default configuration. If the management tool does not provide the capability to enable/disable “debugging features”, there is NO finding because the default setting cannot be changed.
Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-10-003400, KNOX-10-003600	For KPE(AE) deployments this configuration is the default

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
					configuration. If the management tool does not provide the capability to configure "USB file transfer", there is NO finding because the default setting cannot be changed.
KPE Wifi	Unsecured hotspot	Allow/Disallow	Disallow	KNOX-10-004200	
KPE Multiuser	Multi-user mode	Allow/Disallow	Disallow	KNOX-10-005000	**KPE(LEGACY) deployed Samsung Tablets ONLY.**
KPE Restrictions	CC mode	Enable/Disable	Enable	KNOX-10-007300, KNOX-10-010800	
#1: Restrictions #2: KPE Encryption	#1: SD Card #2: External storage encryption	#1: Enable/Disable #2: Enable/Disable	#1: Disable #2: Enable	KNOX-10-001900	**Choose Method #1 or #2**. Method #1: Disable SD card (if not using SD card). Method #2: Enable Data-at-Rest protection.

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
#1: Policy Management #2: KPE Application	#1: Core app white list #2: System app disable list	#1: List of apps #2: List of apps	#1: List approved core apps #2: List non-AO-approved system app packages	KNOX-10-009200	**COPE Personal Environment ONLY.** **Choose Method #1 or #2**. Method #1: Fully managed device with work profile enrollment. Method #2: KPE system app disable list.
#1: KPE audit log #2: Restrictions Restrictions	#1: Audit Log #2: Security logging Network logging	#1: Enable/Disable #2: Enable/Disable Enable/Disable	#1: Enable #2: Enable Enable	KNOX-10-009500	**Choose Method #1 or #2**. Method #1: KPE Audit Logging KPE audit log Method #2: AE Audit Logging Restrictions

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
#1: KPE Restrictions #2: KPE Restrictions	#1: USB host mode exception list #2: USB host mode	#1: APP AUD CDC COM CON CSC HID HUB MAS MIS PER PHY PRI STI VEN VID WIR #2: Enable/Disable	#1: HID #2: Disable	KNOX-10-011200	**Choose Method #1 or #2**. Method #1: Use USB exception list (preferred), which allows DeX usage. Method #2: Disable USB host mode (fall back if exception list policy cannot be applied).

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
#1: Restrictions #2: Restrictions #3: KPE Bluetooth	#1: Bluetooth #2: Bluetooth #3: Bluetooth UUID Whitelist	#1: Allow/Disallow #2: Allow/Disallow #3: A2DP_ADVAUDIODIST_UUID A2DP_AUDIOSINK_UUID A2DP_AUDIOSOURCE_UUID AVRCP_CONTROLLER_UUID AVRCP_TARGET_UUID BNEP_UUID BPP_UUID DUN_UUID FTP_UUID HFP_AG_UUID HFP_UUID HSP_AG_UUID HSP_UUID NAP_UUID OBEXOBJECTPUSH_UUID PANU_UUID PBAP_PSE_UUID PBAP_UUID SAP_UUID SPP_UUID	#1: Allow #2: Disallow #3: HFP_AG_UUID HFP_UUID HSP_AG_UUID HSP_UUID SPP_UUID A2DP_ADVAUDIODIST_UUID A2DP_AUDIOSINK_UUID A2DP_AUDIOSOURCE_UUID AVRCP_CONTROLLER_UUID AVRCP_TARGET_UUID PBAP_PSE_UUID PBAP_UUID	KNOX-10-001300	**Choose Method #1, #2 or #3**. Method #1: AO decision: Allow Bluetooth and train users. Training is covered in KNOX-10-009900. Method #2: AO decision: Disallow use of Bluetooth. Method #3: Use KPE Bluetooth UUID Whitelisting to allow only DoD-approved profiles.

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
#1: User Agreement #2: Restrictions #3: KPE Banner	#1: User Agreement #2: Lock Screen Message #3: Banner text	#1: User Agreement #2: Enable/Disable #3: Configure	#1: Include DoD-mandated Warning banner text in User Agreement #2: DoD-mandated Warning banner text #3: DoD-mandated Warning banner text	KNOX-10-003300	**Choose Method #1, #2 or #3**. Method #1: Put the DoD Warning banner text in the User Agreement (preferred method). Method #2: Put the DoD Warning banner in the Lock Screen message. Method #3: Enable the KPE Reboot Banner.
#1: Restrictions #2: Restrictions #3: KPE Date Time	#1: Config Date Time #2: Set auto (network) time required #3: Date Time Change	#1: Allow/Disallow #2: Require/Do not require #3: Enable/Disable	#1: Disallow #2: Require #3: Disable	KNOX-10-011000	**Choose Method #1, #2 or #3**. Each method uses a different API to accomplish the same result. Any of the methods are acceptable. Method #1: Restrict User from configuring time. Method #2: Require

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
					Auto Time. Method #3: Disable Date/Time change (KPE).
Enrollment Configuration	Default device enrollment	Fully managed, Fully managed with work profile, Device admin managed, Device admin managed with Legacy Workspace	#1: Fully managed with work profile [KPE(AE) COPE deployment] #2: Device admin managed with Legacy Workspace [KPE(LEGACY) COPE deployment] #3: Fully managed [KPE(AE) COBO deployment] #4: Device admin managed [KPE(LEGACY) COBO deployment]	KNOX-10-009600	**COPE deployment**: **Choose Method #1 or #2**. **COBO deployment**: **Choose Method #3 or #4.**

Table 2: Configuration Policy Rules for Work Environment

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
Restrictions	Outgoing beam	Allow/Disallow	Disallow	KNOX-10-011600	**COBO ONLY.**
KPE Restrictions	Share Via List	Allow/Disallow	Disallow	KNOX-10-011400	Disabling "Share Via List" will also disable functionality such as "Gallery Sharing" and "Direct Sharing".
Restrictions	Backup service	Allow/Disallow	Disallow	KNOX-10-003800	**COBO ONLY.**
KPE RCP	Move files to personal	Allow/Disallow	Disallow	KNOX-10-004600	**COPE ONLY.** This configuration is the default configuration. If the management tool does not provide the capability to configure "Move files to personal", there is NO finding because the default setting cannot be changed.
KPE RCP	Sync calendar to personal	Allow/Disallow	Disallow	KNOX-10-004800	**COPE ONLY.**
Restrictions	Autofill services	Allow/Disallow	Disallow	KNOX-10-010600	**KPE(AE) deployments ONLY.**

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
#1: Restrictions #2: KPE Account	#1: Account Management #2: Account Addition Blacklist	#1: Account types, Enable/Disable #2: Account types, Blacklist	#1: Disable for: Work email app, Samsung accounts, Google accounts, and each AO-approved app that uses accounts for data backup/sync #2: "Blacklist all" for: Work email app, Samsung accounts, and Google accounts	KNOX-10-003900, KNOX-10-009000	**Choose Method #1 or #2.** Method #1: AE Account management Method #2: KPE Account Addition Blacklist
#1: Policy Management #2: KPE Application	#1: Core app whitelist #2: System app disable list	#1: List of apps #2: List of apps	#1: List approved core apps #2: List non-AO-approved system app packages	KNOX-10-009300	**Choose Method #1 or #2.** Method #1: KPE(AE) enrollment Method #2: KPE system app disable list
#1: KPE Restrictions #2: KPE Restrictions	#1: Revocation check #2: OCSP check (with revocation check fallback)	#1: Enable/Disable #2: Enable/Disable	#1: Enable for all apps #2: Enable for all apps	KNOX-10-012000	**Choose Method #1 or #2.** Method #1: Certificate Revocation List (CRL) checking

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
					Method #2: Online Certificate Status Protocol (OCSP), with CRL fallback
#1: Policy Management #2: KPE Certificate	#1: Certificates #2: KPE Certificates	#1: Configure #2: Configure	#1: Include DoD certificates in work profile #2: Include DoD certificates in work profile	KNOX-10-012300	**Choose Method #1 or #2.** Method #1: Use AE Key management Policy Management. Method #2: Use KPE Key management KPE Certificate.
#1: Restrictions #2: KPE Restrictions	#1: Config credentials #2: User Remove Certificates	#1: Allow/Disallow #2: Allow/Disallow	#1: Disallow #2: Disallow	KNOX-10-012400	**Choose Method #1 or #2.** #1: Disallow User from configuring any credential. #2: Disallow User from removing certificates.

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
#1: Restrictions #2: KPE Application	#1: List of approved apps listed in managed Google Play #2: App installation whitelist	#1: List of apps #2: List of apps	#1: List only approved work apps in managed Google Play #2: List only approved work apps	KNOX-10-001000, KNOX-10-001100	**Choose Method #1 or #2.** Method #1: Use managed Google Play [not available for KPE(LEGACY) deployments]. Method #2: Use KPE app installation whitelist. Refer to the management tool documentation to determine the following: - If an application installation blacklist is also required to be configured when enforcing an “app installation whitelist”; and - If the management tool supports adding apps to the “app installation whitelist” by

Policy Group	Policy Name	Options	Settings	Related Requirement	Comment
					package name and/or digital signature or supports a combination of the two.
#1: Restrictions #2: KPE RCP	#1: Unredacted Notifications #2: Show detailed notifications	#1: Allow/Disallow #2: Allow/Disallow	#1: Disallow #2: Disallow	KNOX-10-001500	**Choose Method #1 or #2.** Method #1: Disable unredacted notifications on Keyguard (**COBO or COPE**). Method #2: Use KPE notification sanitization for notifications (**COPE ONLY**).
#1: KPE RCP #2: Restrictions	#1: Sharing clipboard to personal #2: Cross profile copy/paste	#1: Allow/Disallow #2: Allow/Disallow	#1: Disallow #2: Disallow	KNOX-10-004700	**COPE ONLY.** **Choose Method #1 or #2.** Method #1: KPE RCP Method #2: AE Restriction