SAMSUNG ANDROID OS 9 WITH KNOX 3.X CORPORATE OWNED BUSINESS ONLY (COBO) USE CASE KPE (AE) DEPLOYMENT STIG CONFIGURATION TABLE

24 July 2020

Developed by Samsung and DISA for the DoD

LIST OF TABLES

Page

Note: The logic of some of the configuration settings in the following table 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 “Unselect” instead of “Select”.

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 9 API table" page (https://support.samsungknox.com/hc/en-us/articles/360021444993). To filter the API details on the page to display only the policies in the following table, select only the "COBO KPE(AE)" checkbox.

For these deployments, a number of KPE APIs which have been used in previous STIGs have now been replaced by AE APIs. Full details of the mapping between old KPE APIs and new AE APIs can be found on the Samsung Knox portal "Knox 3.x STIG Implementation Guide - Samsung Android OS 9 API mapping table" page (https://support.samsungknox.com/hc/en-us/articles/360021444873).

Table Error! No text of specified style in document.**1: COBO Configuration Policy Rules for Device-Wide Work Environment**

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	Android account	account management	Configure	Disable for the work email app	KNOX-09-000010	Refer to MDM documentation to determine how to provision user’s work email accounts for the work email app.
AE	Android certificate	install a CA certificate	Configure	Install the DoD root and intermediate certificates	KNOX-09-001080	Select PEM encoded representations of the DoD root and intermediate certificates.
AE	Android device owner management	enable backup service	Select/Unselect	Unselect	KNOX-09-000860	
AE	Android lock screen restrictions	disable face	Select/Unselect	Select	KNOX-09-000500	

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	Android lock screen restrictions	disable trust agents	Select/Unselect	Select	KNOX-09-000470	
AE	Android lock screen restrictions	disable unredacted notifications	Select/Unselect	Select	KNOX-09-000280	
AE	Android lock screen restrictions	max password failures for local wipe	0+	10	KNOX-09-000430	Unsuccessful logon attempts before device wipe
AE	Android lock screen restrictions	max time to screen lock	0+	15	KNOX-09-000400	
AE	Android password constraints	minimum password length	0+	6	KNOX-09-000370	Minimum device password length
AE	Android password constraints	minimum password quality	None, Pattern, PIN, Alphabetic, Alphanumeric, Complex, Biometric	PIN Alphabetic Alphanumeric or Complex	KNOX-09-001440	Device password complexity PIN recommended Some MDM consoles may display “Numeric” and “Numeric-Complex” instead of “PIN”. Either selection is acceptable but “Numeric-Complex” is recommended. Alphabetic, Alphanumeric, and Complex are also acceptable selections but

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						these selections will cause the user to select a complex password, which is not required by the STIG.
AE	Android password constraints	password history length	0+	0	KNOX-09-001390	
KPE	Android user restrictions	disallow autofill	Select/Unselect	Select	KNOX-09-000610	
AE	Android user restrictions	disallow config date time	Select/Unselect	Select	KNOX-09-000730	
AE	Android user restrictions	disallow debugging features	Select/Unselect	Select	KNOX-09-000920	
AE	Android user restrictions	disallow install unknown sources	Select/Unselect	Select	KNOX-09-000130	Disallow unknown app installation sources.
AE	Android user restrictions	disallow mount physical media	Select/Unselect	Select	KNOX-09-000980	For KNOX-09-000980, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #1: Disallow mount physical media.
AE	Android user restrictions	disallow outgoing beam	Select/Unselect	Select	KNOX-09-000800	

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	Android user restrictions	disallow usb file transfer	Select/Unselect	Select	KNOX-09-000680, KNOX-09-000840	Disabling USB Media Player will also disable USB MTP, USB mass storage, and USB vendor protocol (KIES).
KPE	Knox Bluetooth	allowed profiles	HSP, HFP, PBAP, A2DP, AVRCP, SPP, NAP, BNEP, HID, BPP, DUN, SAP	HFP, HSP, SPP, A2DP, AVRCP, PBAP	KNOX-09-000660	Disables all Bluetooth profiles except for those specified in the settings.
KPE	Knox Wifi	allow unsecured hotspot	Select/Unselect	Unselect	KNOX-09-000940	Disallow unsecured hotspots.
KPE	Knox application	application installation whitelist	Configure	Add each AO-approved package	KNOX-09-000070	For KNOX-09-000070, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2: Refer to the “System Apps that must not be disabled” table within the Supplemental document, which must be included in the “application installation whitelist” to allow updates. Refer to the MDM documentation to determine if an “application installation blacklist” is also required

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						to be configured when enforcing an "application installation whitelist" and if the MDM supports adding packages to the application installation whitelist by package name and/or digital signature or supports a combination of the two.
KPE	Knox application	system application disable list	Configure	Add all non-AO-approved system app packages, add all system app packages that have been identified as having non-DoD-approved characteristics, add all preinstalled public cloud backup system apps	KNOX-09-000040, KNOX-09-000100, KNOX-09-000860	For KNOX-09-000040, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2: Refer to the "System Apps for disablement (other characteristics)" and "System Apps that must not be disabled" tables within the Supplemental document. For KNOX-09-000100, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2: Refer to the "System Apps for disablement (non-DoD-approved characteristics)"

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						and "System Apps that must not be disabled" tables within the Supplemental document. For KNOX-09-000860, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2.
KPE	Knox audit log	enable audit log	Select/Unselect	Select	KNOX-09-000170	This simultaneously enables audit logging for Workspace events.
KPE	Knox banner	banner text	Configure	DoD-mandated warning banner text	KNOX-09-001160	For KNOX-09-001160, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2: The Administrator can configure enterprise-specific banner text. If enabled without configuring any text, the device will display a default text that matches the required DoD banner.
KPE	Knox certificate	OCSP check	Configure	Enable for all apps	KNOX-09-001340	Refer to the MDM documentation to determine how to configure OCSP checking to "enable

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						for all apps". Some may, for example, allow a wildcard string: "*" (asterisk).
KPE	Knox certificate	revocation check	Configure	Enable for all apps	KNOX-09-001050	Refer to the MDM documentation to determine how to configure revocation checking to "enable for all apps". Some may, for example, allow a wildcard string: "*" (asterisk).
KPE	Knox encryption	enable external storage encryption	Select/Unselect	Select	KNOX-09-000980	For KNOX-09-000980, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2: Encrypt all external media cards.
KPE	Knox password constraints	maximum sequential characters	0+	2	KNOX-09-000390	
KPE	Knox password constraints	maximum sequential numbers	0+	2	KNOX-09-000390	
KPE	Knox restrictions	Disallow share via list	Select/Unselect	Select	KNOX-09-000770	Note: Disabling "Share Via List" will also disable functionality such as "Gallery Sharing" and "Direct Sharing".

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	Knox restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON, CSC, HID, HUB, MAS, MIS, PER, PHY, PRI, STI, VEN, VID, WIR	HID	KNOX-09-000750	
KPE	Knox restrictions	allow auto-fill	Select/Unselect	Unselect	KNOX-09-000580	
KPE	Knox restrictions	allow google accounts auto sync	Select/Unselect	Unselect	KNOX-09-000860	
KPE	Knox restrictions	enable CC mode	Select/Unselect	Select	KNOX-09-000710	Common Criteria (CC) Mode is fundamental to MDFPP compliance and is a top-level requirement. Puts the devices in CC Mode as defined by the Samsung Galaxy Device MDFPP Security Target. The following configuration must also be implemented for the Samsung Android device to be operating in the NIAP-certified complaint CC mode of operation: KNOX-09-001440: minimum password quality, KNOX-09-000500: disable face, KNOX-09-000430/(KNOX-09-

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						000440): max password failures for local wipe, KNOX-09-001370/(KNOX-09-001360): password recovery, KNOX-09-001390/(KNOX-09-001400): password history length, KNOX-09-001050/(KNOX-09-001040): revocation check, KNOX-09-001340/(KNOX-09-001330): OCSP check, KNOX-09-001420: Secure Startup, KNOX-09-000980: enable external storage encryption, or disallow mount physical media.
KPE	Microsoft Exchange ActiveSync	password recovery	Enable/Disable	Disable	KNOX-09-001370	The DoD mobile service provider should verify the Exchange server is configured to disable Microsoft Exchange ActiveSync (EAS) password recovery.
AE	managed Google Play	application installation whitelist	Configure	Add each AO-approved package	KNOX-09-000070	For KNOX-09-000070, confirm if Method #1 or Method #2 is used at the Samsung device site. This

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						configuration is only required for Method #1: Refer to the "System Apps that must not be disabled" table within the Supplemental document, which must be included in the "application installation whitelist" to allow updates.
AE	managed Google Play	system application disable list	Configure	Add all non-AO-approved system app packages, add all system app packages that have been identified as having non-DoD-approved characteristics, add all preinstalled public cloud backup system apps	KNOX-09-000040, KNOX-09-000100, KNOX-09-000860	For KNOX-09-000040, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #1: Refer to the "System Apps for disablement (other characteristics)" and "System Apps that must not be disabled" tables within the Supplemental document. For KNOX-09-000100, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #1: Refer to the "System Apps for disablement (non-DoD-approved characteristics)" and "System Apps that

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						must not be disabled" tables within the Supplemental document. For KNOX-09-000860, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #1.