SAMSUNG ANDROID OS 9 WITH KNOX 3.X CORPORATE OWNED PERSONALLY ENABLED (COPE) USE CASE KPE (LEGACY) DEPLOYMENT STIG CONFIGURATION TABLES

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 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 “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 "COPE KPE(LEGACY)" checkbox.

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

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	Android lock screen restrictions	disable trust agents	Select/Unselect	Select	KNOX-09-000475	
AE	Android lock screen restrictions	max password failures for local wipe	0+	10	KNOX-09-000435	Unsuccessful logon attempts before device wipe
AE	Android lock screen restrictions	max time to screen lock	0+	15	KNOX-09-000405	
AE	Android password constraints	minimum password length	0+	6	KNOX-09-000375	Minimum device password length
AE	Android password constraints	minimum password quality	None, Pattern, PIN, Alphabetic, Alphanumeric, Complex, Biometric	PIN Alphabetic Alphanumeric or Complex	KNOX-09-001445	Device password complexity PIN recommended Some MDM consoles may display “Numeric” and “Numeric-Complex” instead

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						of "PIN". Either selection is acceptable but "Numeric-Complex" is recommended. Alphabetic, Alphanumeric, and Complex are also acceptable selections but 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-09-001395	
KPE	Knox Bluetooth	allowed profiles	HSP, HFP, PBAP, A2DP, AVRCP, SPP, NAP, BNEP, HID, BPP, DUN, SAP	HFP, HSP, SPP, A2DP, AVRCP, PBAP	KNOX-09-000665	Disables all Bluetooth profiles except for those specified in the settings.
KPE	Knox Date Time	date time change enabled	Select/Unselect	Unselect	KNOX-09-000735	
KPE	Knox Wifi	allow unsecured hotspot	Select/Unselect	Unselect	KNOX-09-000945	Disallow unsecured hotspots.
KPE	Knox Workspace	create legacy Knox Workspace	Configure	Create legacy Knox Workspace	KNOX-09-000265	Create a legacy Knox Workspace.
KPE	Knox application	system application disable list	Configure	Add all non-AO-approved system app packages, add	KNOX-09-000045,	Refer to the "System Apps for disablement (other characteristics)" and "System

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
				all system app packages that have been identified to transmit MD diagnostic data to non-DoD servers	KNOX-09-000115	Apps that must not be disabled" tables within the Supplemental document. Refer to the "System Apps for disablement (non-DoD-approved characteristics)" and "System Apps that must not be disabled" tables within the Supplemental document. Only system apps that are identified with characteristic "transmit MD diagnostic data to non-DoD servers" need to be added the "system application disable list".
KPE	Knox audit log	enable audit log	Select/Unselect	Select	KNOX-09-000175	This simultaneously enables audit logging for Workspace events.
KPE	Knox banner	banner text	Configure	DoD-mandated warning banner text	KNOX-09-001165	For KNOX-09-001165, 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.

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	Knox certificate	Certificate	Configure	Install the DoD root and intermediate certificates	KNOX-09-001085	Select PEM encoded representations of the DoD root and intermediate certificates.
KPE	Knox certificate	OCSP check	Configure	Enable for all apps	KNOX-09-001345	Refer to the MDM documentation to determine how to configure OCSP checking to “enable for all apps”. Some may, for example, allow a wildcard string: “*” (asterisk).
KPE	Knox certificate	revocation check	Configure	Enable for all apps	KNOX-09-001055	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-09-000985	Encrypt all external media cards.
KPE	Knox multiuser	allow multi-user mode	Select/Unselect	Unselect	KNOX-09-000645	
KPE	Knox password constraints	disable face	Select/Unselect	Select	KNOX-09-000505	
KPE	Knox password constraints	maximum sequential characters	0+	2	KNOX-09-000395	

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	Knox password constraints	maximum sequential numbers	0+	2	KNOX-09-000395	
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-09-000755	
KPE	Knox restrictions	allow developer mode	Select/Unselect	Unselect	KNOX-09-000925	
KPE	Knox restrictions	allow install unknown sources	Select/Unselect	Unselect	KNOX-09-000135	Disallow unknown app installation sources.
KPE	Knox restrictions	disable USB media player	Select/Unselect	Select	KNOX-09-000685, KNOX-09-000845	Disabling USB Media Player will also disable USB MTP, USB mass storage, and USB vendor protocol (KIES).
KPE	Knox restrictions	enable CC mode	Select/Unselect	Select	KNOX-09-000715	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

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						of operation: KNOX-09-001445: minimum password quality, KNOX-09-000505: disable face, KNOX-09-000435/(KNOX-09-000445): max password failures for local wipe, KNOX-09-001375/(KNOX-09-001365): password recovery, KNOX-09-001395/(KNOX-09-001405): password history length, KNOX-09-001055/(KNOX-09-001045): revocation check, KNOX-09-001345/(KNOX-09-001335): OCSP check, KNOX-09-001425: Secure Startup, KNOX-09-000985: enable external storage encryption, or disallow mount physical media.
KPE	Microsoft Exchange ActiveSync	password recovery	Enable/Disable	Disable	KNOX-09-001375	The DoD mobile service provider should verify the Exchange server is configured to disable Microsoft Exchange ActiveSync (EAS) password recovery.

Table 2: COPE Configuration Policy Rules for Work Environment Workspace

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	Knox RCP	allow move applications to workspace	Select/Unselect	Unselect	KNOX-09-000245	
KPE	Knox RCP	allow move files to personal	Select/Unselect	Unselect	KNOX-09-000245	
KPE	Knox RCP	allow sharing clipboard to personal	Select/Unselect	Unselect	KNOX-09-000245	
KPE	Knox RCP	allow show detailed notifications	Select/Unselect	Unselect	KNOX-09-000305	Display details of Work application notifications when user is outside Workspace.
KPE	Knox RCP	sync calendar to personal	Select/Unselect	Unselect	KNOX-09-000245	
KPE	Knox RCP	sync contact to personal	Select/Unselect	Unselect	KNOX-09-000245	
KPE	Knox account	account addition blacklist	Configure	All email domains	KNOX-09-000025	For KNOX-09-000025, 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 MDM documentation to determine how to provision user's work email accounts for the work email app.

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	Knox account	account addition whitelist	Configure	All DoD-approved email domains	KNOX-09-000025	For KNOX-09-000025, 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 MDM documentation to determine if an “account addition blacklist” is also required to be configured when enforcing an “account addition whitelist” and how to provision user’s work email accounts for the work email app.
KPE	Knox application	application installation whitelist	Configure	Add each AO-approved package	KNOX-09-000085	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 to be configured when enforcing an “application installation whitelist” and if the MDM

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						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-09-000055, KNOX-09-000125, KNOX-09-000875	Refer to the "System Apps for disablement (other characteristics)" and "System Apps that must not be disabled" tables within the Supplemental document. Refer to the "System Apps for disablement (non-DoD-approved characteristics)" and "System Apps that must not be disabled" tables within the Supplemental document.
KPE	Knox certificate	Certificate	Configure	Install the DoD root and intermediate certificates	KNOX-09-001075	Select PEM encoded representations of the DoD root and intermediate certificates.
KPE	Knox certificate	OCSP check	Configure	Enable for all apps	KNOX-09-001335	Refer to the MDM documentation to determine how to configure OCSP checking to "enable for all apps". Some may, for example, allow a wildcard string: "*" (asterisk).

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	Knox certificate	revocation check	Configure	Enable for all apps	KNOX-09-001045	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 password constraints	max password failures for local wipe	0+	10	KNOX-09-000445	Unsuccessful logon attempts before Workspace wipe
KPE	Knox password constraints	maximum sequential characters	0+	2	KNOX-09-001465	
KPE	Knox password constraints	maximum sequential numbers	0+	2	KNOX-09-001465	
KPE	Knox password constraints	maximum time to lock	0+	15	KNOX-09-000415	
KPE	Knox password constraints	minimum password length	0+	4	KNOX-09-001455	Minimum Workspace password length
KPE	Knox password constraints	minimum password quality	None, Pattern, PIN, Alphabetic, Alphanumeric, Complex, Biometric	PIN Alphabetic Alphanumeric or Complex	KNOX-09-001475	Workspace password complexity PIN recommended Some MDM consoles may display “Numeric” and “Numeric-Complex” instead

Policy Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						of "PIN". Either selection is acceptable but "Numeric-Complex" is recommended. Alphabetic, Alphanumeric, and Complex are also acceptable selections but these selections will cause the user to select a complex password, which is not required by the STIG.
KPE	Knox password constraints	password history length	0+	0	KNOX-09-001405	
KPE	Knox restrictions	Disallow share via list	Select/Unselect	Select	KNOX-09-000785	Note: Disabling "Share Via List" will also disable functionality such as "Gallery Sharing" and "Direct Sharing".
KPE	Knox restrictions	allow auto-fill	Select/Unselect	Unselect	KNOX-09-000595	
KPE	Knox restrictions	allow google accounts auto sync	Select/Unselect	Unselect	KNOX-09-000875	
KPE	Microsoft Exchange ActiveSync	password recovery	Enable/Disable	Disable	KNOX-09-001365	The DoD mobile service provider should verify the Exchange server is configured to disable Microsoft Exchange ActiveSync (EAS) password recovery.