SAMSUNG ANDROID OS 5 WITH KNOX 2.x STIG CONFIGURATION TABLE

Version 1, Release 3

22 April 2016

Developed by Samsung and DISA for the DoD

UNCLASSIFIED

Samsung Android OS 5 with Knox 2.x STIG Configuration Table, V1R3   DISA
22 April 2016   Developed by Samsung and DISA for the DoD

LIST OF TABLES

Samsung Android OS 5 with Knox 2.x STIG Configuration Table, V1R3   DISA
22 April 2016   Developed by Samsung and DISA for the DoD

1

UNCLASSIFIED

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 rule should be set to "Disable" instead of "Enable" as indicated on page 2 below.

Table 1: Configuration Policy Rules for Non-Work Environment

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Advanced Restriction	Enable CC Mode	Enable/Disable	X		Enable	KNOX-39-015600	Puts the devices in (Common Criteria) CC Mode as defined by the Samsung Galaxy Device MDFPP Security Target. If the configuration is not available on the MDM console, install the Samsung CC Mode Android Application Package File (APK) and enable CC Mode. The APK is available on Google Play.
Android Restriction	Disable Developer Mode	Enable/Disable	X		Enable	KNOX-35-020000	
Android Restriction	Allow Location	Enable/Disable		X	Enable (GPS, Wi-Fi, Cellular)		
Android Restriction	Disable Camera	Enable/Disable		X	Enable		
Android Restriction	Disable Microphone	Enable/Disable		X	Enable		

2

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restriction	Allow new admin	Enable/Disable	X		Disable	KNOX-35-021000	
Android Restriction	Disable Manual Date Time Changes	Enable/Disable	X		Enable	KNOX-38-012600	
Android Restriction	Enable Google Play	Enable/Disable	X		Disable	KNOX-35-009000	
Android Restriction	Allow Unknown Sources	Enable/Disable	X		Disable	KNOX-35-009010	
Application	Application White List	Configure	X		Add Approved Packages	KNOX-35-009100	
Application	Application Black List	Configure	X		Add All Packages	KNOX-35-021100	All packages specified by wildcard (.*). When all apps are blacklisted, then only apps on the white list are allowed.
Application	Required List	Configure		X	Add Packages		List of applications that the user cannot uninstall. This list is site specific.
Application	Disable Applications	Configure	X		Add Unapproved Packages	KNOX-35-021200	The systems administrator should identify all pre-installed applications that are not approved and disable them.
Android Restriction	Allow cookies	Enable/Disable		X	Enable		Native browser application only
Android Restriction	Enable auto-fill	Enable/Disable		X	Enable		Native browser application only

3

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restriction	Enable JavaScript	Enable/Disable		X	Enable		Native browser application only
Android Restriction	Enable popups	Enable/Disable		X	Disable		Native browser application only
Android Restriction	Enable CAC authentication for browser	Enable/Disable		X	Enable		Native browser application only
Accounts	Google auto sync	Enable/Disable	X		Disable	KNOX-35-021300	
Accounts	Google crash report	Enable/Disable	X		Disable	KNOX-35-021400	
Android Restriction	Enable CAC authentication for email	Enable/Disable		X	Enable		This affects non-container email only.
Android Restriction	Storage Encryption	Enable/Disable	X		Enable	KNOX-30-004400	Encrypt all user and enterprise data at rest.
Android Restriction	External Storage Encryption	Enable/Disable	X		Enable	KNOX-30-004410	Encrypt all external media cards.
Android Restriction	Copy contacts to SIM	Enable/Disable		X	Disable		
Android VPN	VPN	Configure	X		Add VPN Profile	KNOX-35-024500	Configure organization VPN profile.
Password Restriction	Maximum Failed Attempts for wipe	0-	X		10	KNOX-34-008900	Unsuccessful login attempts before device wipe
Password Restriction	Minimum Length	0-	X		6	KNOX-34-008700	Minimum device password length

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Password Restriction	Password Complexity	None Pattern Pin Alphabetic Alphanumeric Complex	X		Alphanumeric	KNOX-35-024600	Device password complexity
Password Restriction	Maximum Password Lifetime	0-		X	0		Days after which password must be changed
Password Restriction	Max Time to Lock	0-	X		15	KNOX-34-012100	Minutes of inactivity after which device will lock
Password Restriction	Min Uppercase	0-		X	0		Minimum number of uppercase alphabetic characters in device password.
Password Restriction	Min Lowercase	0-		X	0		Minimum number of lowercase alphabetic characters in device password
Password Restriction	Min Numeric	0-		X	0		Minimum number of numeric characters in device password
Password Restriction	Min Mutation on Change	0-		X	0		Minimum number of characters that must be changed when device password is changed
Password Restriction	Max Sequential Characters	0-	X		2	KNOX-35-021900	Max number of sequential characters in device password

5

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Password Restriction	Max Sequential Numbers	0-	X		2	KNOX-35-021900	Max number of sequential numbers in device password
Password Restriction	Fingerprint for Lock screen authentication	Enable/Disable	X		Disable	KNOX-35-024600	
Password Restriction	Smart Lock	Enable/Disable	X		Disable	KNOX-35-030000	
Android Restriction	DoD Banner	Enable/Disable	X		Enable	KNOX-36-009700	The administrator can configure enterprise specific banner text. If the enabled without configuring any text, the device will display a default text which matches the required DoD banner.
Android Certificate	Certificate	Configure	X		Add Certificates	KNOX-35-020600	Select PEM encoded representations of the DoD root and intermediate certificates
Android Certificate	Certificate Revocation Check (CRL)	Enable/Disable	X		Enable	KNOX-35-028500	
Android Restriction	Disable USB Media Player	Select/Not Select	X		Select	KNOX-35-023600	Disabling USB Media Player will also disable USB MTP, USB mass storage, USB vendor protocol (KIES).
Android Restrictions	Allowed Bluetooth Profiles		X		HFP HSP SPP	KNOX-39-015700	Disables all Bluetooth profiles except for those specified in the settings

6

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restriction	Disable Wi-Fi Tethering	Select/Not Select		X	Select		The systems administrator shall select the setting based on local policy.
Android Restriction	Disable Bluetooth Tethering	Select/Not Select		X	Select		The systems administrator shall select the setting based on local policy.
Android Restriction	Disable USB host storage	Select/Not Select	X		Select	KNOX-35-021600	USB host storage allows the device to mount external USB drives.
Android Restriction	Allow screen capture	Enable/Disable		X	Enable		
Android Restriction	Allow Google backup	Enable/Disable	X		Disable	KNOX-35-021300	
Knox Restriction	Knox License	Configure	X		Enterprise issued Knox license	KNOX-35-030100	Proper configuration of the Knox license ensures reporting information is sent to the correct enterprise servers.
Android Restriction	Allow multi-user mode	Enable/Disable	X		Disable	KNOX-35-022500	
Android Restriction	Allow Cloud backup	Enable/Disable	X		Disable	KNOX-35-021200	This policy is implemented using Disable Application policies. See STIG requirement for more information.
Android Restriction	Allow S Voice	Enable/Disable	X		Disable	KNOX-35-022800	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restriction	Allow mobile payment	Enable/Disable	X		Disable	KNOX-35-021250	This policy is implemented using Disable Application policies. See STIG requirement for more information.
Android Restriction	Allow NFC	Enable/Disable	X		Disable	KNOX-35-023100	
Accounts	Account whitelist	Configure		X	Approved accounts		The idea is to use combination of Account whitelist and Account Blacklist policies to control what email accounts a user is allowed to configure on the device in the non-work environment. Configure by adding the domain of email accounts.
Accounts	Account blacklist			X	.* (wildcard)		Configure by blacklisting all domains. Then only accounts on the white list are allowed.
Android Restriction	Allow Samsung Accounts	Enable/Disable	X		Disable	KNOX-35-021275	This policy is implemented using Disable Application policies. See STIG requirement for more information.
Android Restriction	Allow FOTA	Enable/Disable	X		Disable	KNOX-35-023700	Disables automatic firmware updates.

8

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restriction	Notifications on lock screen	Show content Hide content Do not show notifications	X		Hide content or Do not show notifications	KNOX-35-024000	
Android Restriction	Allow Admin Remove	Enable/Disable	X		Disable	KNOX-35-028400	

UNCLASSIFIED

Samsung Android OS 5 with Knox 2.x STIG Configuration Table, V1R3   DISA
22 April 2016   Developed by Samsung and DISA for the DoD

Table 2: Configuration Policy Rules for Work Environment Container

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Password Restriction	Min Mutation on Change	0-		X	0		Minimum number of characters that must be changed when container password is changed
Container Password Restriction	Minimum Length	0-	X		4	KNOX-39-014900	Minimum container password length
Container Password Restriction	Max Time to Lock	0-	X		15	KNOX-34-012110	Minutes of inactivity after which container will lock
Container Password Restriction	Maximum Failed Attempts for wipe	0-	X		10	KNOX-39-015200	Unsuccessful login attempts before container wipe
Container Password Restriction	Maximum Password Lifetime	0-		X	0		Days after which password must be changed
Container Password Restriction	Max Sequential Numbers	0-	X		2	KNOX-39-021100	Max number of sequential numbers in device password
Container Password Restriction	Password complexity	Alphanumeric Complex	X		Alphanumeric	KNOX-39-022000	
Container Restriction	Allow camera	Enable/Disable		X	Disable		Camera use inside container. In KNOX 2.0, disabling the camera outside will also disable the camera inside.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Accounts	Account whitelist	Configure	X		Approved accounts	KNOX-39-021200	The idea is to use combination of these policies to control what accounts a user is allowed to configure on the device. Configure by adding the domain of agency email accounts.
Container Accounts	Account blacklist		X		.* (wildcard)	KNOX-39-021300	Configure by blacklisting all domains. When all apps are blacklisted, then only accounts on the white list are allowed.
Container Restriction	Allow account addition	Enable/Disable		X	Enable		Allows user to add email accounts inside container. Configuration determined by local policy.
Container Restriction	Allow calendar info outside container	Enable/Disable	X		Disable	KNOX-39-015100	Sharing of container calendar events to outside calendar
Container Restriction	Allow contact info outside container	Enable/Disable	X		Disable	KNOX-39-015250	Sharing of container contacts to outside contacts
Container Restriction	Allow notification details	Enable/Disable	X		Disable	KNOX-39-015300	Display details of container application notifications when user is outside container
Container Restriction	Allow cookies	Enable/Disable		X	Disable		Container native browser application only

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Restriction	Enable auto-fill	Enable/Disable	X		Disable	KNOX-39-021000	Container native browser application only
Container Restriction	Enable JavaScript	Enable/Disable		X	Enable		Container native browser application only
Container Restriction	Enable popups	Enable/Disable		X	Disable		Container native browser application only
Container Application	Application White List	Configure	X		Add Approved Packages	KNOX-39-020100	Configure by setting the list of only DoD approved applications.
Container Application	Application Black List	Configure	X		Add All Packages	KNOX-39-020300	All packages specified by wildcard (.*).
Container Application	Required List	Configure		X	Add Packages		List of applications that the user cannot uninstall
Container Application	Enable Move Applications to Container	Enable/Disable	X		Disable	KNOX-39-020400	Blocks users from moving installed applications (outside container) to the container. By default this is disabled, and can only be enabled by the admin.
Container Application	Enable Move Files from Container	Enable/Disable	X		Disable	KNOX-39-020500	Blocks users from moving files from container. By default "from" is disabled and can only be changed by the admin.

12

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Application	Disable Applications	Configure	X		Add Packages	KNOX-39-020700	The systems administrator should identify all pre-installed applications that are not approved and disable them.
Container Management	Enable container	Enable/Disable	X		Enable	KNOX-39-015400	
Android Container VPN	VPN	Configure		X	Add VPN Profile		Configure organization VPN profile for the container only. Use the container-VPN configuration.
Android Container Firewall	Proxy	Configure		X	Add Proxy		Configure a proxy to force all container traffic to be routed to the proxy. The system administrator should configure only if needed by local network.
Container Restriction	Allow screen capture	Enable/Disable		X	Disable		
Container Restriction	Allow Samsung Accounts	Enable/Disable	X		Disable	KNOX-39-020700	This policy is implemented using Disable Application policies. See STIG requirement for more information.