

UNCLASSIFIED



SAMSUNG ANDROID OS 8 WITH KNOX 3.X STIG CONFIGURATION TABLES

Version 1, Release 4

25 October 2019

Developed by Samsung and DISA for the DoD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: COPE Configuration Policy Rules for Non-Work Environment	1
Table 2: COPE Configuration Policy Rules for Work Environment Container	9
Table 3: COBO Configuration Policy Rules for Device-Wide Work Environment	16
Table 4: Optional Controls.....	26

For the “personally enabled” device use case (COPE), apply Tables 1 and 2.

For “business only” devices (COBO), apply Table 3.

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”.

Table 1: COPE Configuration Policy Rules for Non-Work Environment

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Restrictions	Allow Install Non Market App	True/False	False	KNOX-08-002900	MDM API: <u>setAllowNonMarketApps(boolean)</u>
Android Applications	Battery optimizations modes Whitelist	Configure	Add MDM Client	KNOX-08-003200	MDM API: <u>addPackageToBatteryOptimizationWhiteList(AppIdentity appIdentity)</u>
Android Application	Application disable list	Configure	Add Unapproved Packages	KNOX-08-000700, KNOX-08-002100	The systems administrator should identify all pre-installed applications that are not approved and disable them (see Tables 10-1 through 10-3 in the STIG Supplemental document). MDM API: <u>setDisableApplication(String packageName)</u>
Android Audit Log	Enable Audit Log	True/False	True	KNOX-08-004000	MDM API: <u>enableAuditLog()</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Password Restrictions	Minimum Length	0+	6	KNOX-08-008300	Minimum device password length. MDM API: <u>setPasswordMinimumLength(Component Name admin, int length)</u>
Android Password Restrictions	Maximum Sequential Characters	0+	2	KNOX-08-008600	Max number of sequential characters in password. MDM API: <u>setMaximumCharacterSequenceLength(int length)</u>
Android Password Restrictions	Maximum Sequential Numbers	0+	2	KNOX-08-008600	Max number of sequential numbers in password. MDM API: <u>setMaximumNumericSequenceLength(int length)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Password Restrictions	Minimum Password Complexity	None Pattern PIN Alphabetic Alphanumeric Complex Biometric	PIN Alphabetic Alphanumeric or Complex	KNOX-08-008800	<p>Password complexity. PIN is recommended</p> <p>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 these selections will cause the user to select a complex password, which is not required by the STIG.</p> <p>MDM API: <u>setPasswordQuality(ComponentName admin, int quality)</u></p>
Android Password Restrictions	Maximum Time to Lock	0+	5	KNOX-08-009100	<p>This value defines the amount of time from when the screen turns off until the device locks. Since the maximum screen timeout a user can select on Android 8 is 10 minutes, a 5-minute or less lock time value fulfills this requirement.</p> <p>MDM API: <u>setMaximumTimeToLock(ComponentName admin, long timeMs)</u></p>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Password Restrictions	Maximum Failed Attempts for wipe	0+	10	KNOX-08-009400	Unsuccessful logon attempts before device wipe. MDM API: <u>setMaximumFailedPasswordsForWipe(ComponentName admin, int num)</u>
Android Password Restrictions	Disable Face Recognition	True/False	True	KNOX-08-011000	MDM API: <u>setBiometricAuthenticationEnabled(int bioAuth, boolean enable)</u>
Android Password Restrictions	Disable Intelligent Scanning	True/False	True	KNOX-08-010800	This policy is indirectly configured by disabling face or iris scanning. MDM API: Use the same APIs as for Disable Face Recognition rule or Disable Iris rule
Android Password Restrictions	Disable Keyguard Trust Agents	True/False	True	KNOX-08-010300	MDM API: <u>setKeyguardDisabledFeatures(ComponentName admin, int which)</u>
Android Multi User	Allow multi-user mode	True/False	False	KNOX-08-013000	MDM API: <u>allowMultipleUsers(boolean allow)</u>
Android Restrictions	Allow Google Crash Report	True/False	False	KNOX-08-013200	MDM API: <u>allowGoogleCrashReport(boolean allow)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Bluetooth	Allowed Bluetooth Profiles	HSP HFP PBAP A2DP AVRCP SPP NAP BNEP HID BPP DUN SAP	HFP HSP SPP	KNOX-08-013900	Disables all Bluetooth profiles except for those specified in the settings. MDM API: <u>enableSecureMode(BluetoothSecureMode Config configObj, ListwhiteList)</u>
Android Advanced Restrictions	Prevent New Admin Install	True/False	True	KNOX-08-014100	MDM API: <u>preventNewAdminInstallation(boolean prevent)</u>
Android Restrictions	Allow Admin Remove	True/False	False	KNOX-08-014200	Only applicable to legacy configurations. MDM API: <u>setAdminRemovable(boolean removable)</u>
Android Restrictions	Disable USB Media Player	True/False	True	KNOX-08-015000, KNOX-08-017300	Disabling USB Media Player will also disable USB MTP, USB mass storage, and USB vendor protocol (KIES). MDM API: <u>setUsbMediaPlayerAvailability(boolean enable)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Advanced Restrictions	Enable CC Mode	True/False	True	KNOX-08-015300	<p>CC mode is fundamental to MDFPP compliance and is a top-level requirement.</p> <p>Puts the devices in CC (Common Criteria) mode as defined by the Samsung Galaxy Device MDFPP Security Target.</p> <p>All cryptography will be configured to be in FIPS 140-2 validated mode.</p> <p>Encryption for information at rest on built-in storage media must be enabled.</p> <p>MDM API: <u>setInternalStorageEncryption(boolean isEncrypt)</u> <u>setCCMode(Boolean)</u> </p>
Android Date Time	Date Time Change Enabled	True/False	False	KNOX-08-015500	MDM API: <u>setDateTimeChangeEnabled(boolean)</u>
Android Restrictions	Allow Google Backup	True/False	False	KNOX-08-017400	MDM API: <u>setBackup(boolean)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Restrictions	USB Host Modes Whitelist	APP AUD CDC COM CON CSC HID HUB MAS MIS PER PHY PRI STI VEN VID WIR	HID	KNOX-08-015700	USB MAS host mode allows the device to mount external USB drives. MDM API: <u>SetUsbExceptionList(int exceptionList)</u> allowUsbHostStorage(boolean allow)
Android Restrictions	Allow Developer Mode	True/False	False	KNOX-08-017900	MDM API: <u>allowDeveloperMode(boolean allow)</u>
Android WiFi	Allow Unsecured Hotspot	True/False	False	KNOX-08-018100	MDM API: <u>allowOpenWifiAp(boolean allow)</u>
Android Security	External Storage Encryption	True/False	True	KNOX-08-018500	Encrypt all external media cards. MDM API: <u>setExternalStorageEncryption(boolean isEncrypt)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Certificate	Certificate Revocation Check (CRL)	True/False	True	KNOX-08-019100	Enable revocation check on all packages using the string: "*" (asterisk). MDM API: <u>enableRevocationCheck(String pkgName, boolean enable)</u>
Android Certificate	Certificate	Configure	Add Certificates	KNOX-08-019400	Select PEM encoded representations of the DoD root and intermediate certificates. MDM API: <u>installCertificateToKeystore(String type, byte[] value, String name, String password, int keystore)</u>
Android VPN	VPN	Configure	See Comments	KNOX-08-023000, KNOX-08-023200	Configure in one of the following configurations: - Disabled - Configured for per app use for the personal side MDM API: <u>allowVpn(boolean allow)</u> <u>createVpnProfile(String profileInfo)</u>
Android VPN	Add packages to VPN	Configure	See Comments	KNOX-08-023200	Required if "Configured for per app use for the personal side" option is selected. MDM API: <u>addPackagesToVpn(String[] packageList, String profileName)</u>

Table 2: COPE Configuration Policy Rules for Work Environment Container

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container Account	Account whitelist	Configure	Approved accounts	KNOX-08-000300	MDM API: <u>addAccountsToAdditionWhiteList(String type, List accounts)</u>
Container Account	Account blacklist	Configure	.* (wildcard)	KNOX-08-000400	Configure by blacklisting all domains. When all apps are blacklisted, only accounts on the whitelist are allowed. MDM API: <u>addAccountsToAdditionBlackList(String type, List accounts)</u>
Container Application	Application disable list	Configure	Add Unapproved Packages	KNOX-08-000800, KNOX-08-002200, KNOX-08-002300, KNOX-08-002400, KNOX-08-002500, KNOX-08-002600, KNOX-08-002700	The Systems Administrator should identify all pre-installed applications that are not approved and disable them (see Tables 10-1 through 10-3 in the STIG Supplemental document). MDM API: <u>setDisableApplication(String packageName)</u>
Container Application	Package Name or Signature Blacklist	Configure	Add All Packages or Signatures	KNOX-08-001100	All packages or signatures specified by wildcard (.*). MDM API: <u>addAppPackageNameToBlackList(String packageName)</u> <u>addAppSignatureToBlackList(String appSignature)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container Application	Package Name or Signature Whitelist	Configure	Add Approved Packages or Signatures	KNOX-08-001400	<p>Configure by setting the list of only DoD-approved packages or signatures. The following app packages must be included in the app whitelist so that Google Play services can be updated:</p> <ul style="list-style-type: none"> • com.android.vending • com.google.android.finsky • com.google.android.gm • com.google.android.gms • com.google.android.gsf.login • com.google.android.setupwizard • com.google.android.gsf <p>MDM API: <u>addAppPackageNameToWhiteList(String packageName, boolean defaultBlackList)</u> <u>addAppPackageNameToWhiteList(String packageName)</u> <u>addAppSignatureToWhiteList(String appSignature)</u> <u>addAppSignatureToWhiteList(String appSignature, boolean defaultBlackList)</u> </p>
Container Application	Battery optimizations modes Whitelist	Configure	Add MDM Client	KNOX-08-003300	<p>MDM API: <u>addPackageToBatteryOptimizationWhiteList(AppIdentity appIdentity)</u> </p>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container Application	Disable Bixby Vision	True/False	True	KNOX-08-003600	This policy is implemented using Disable Application policies. See STIG requirement for more information. MDM API: Use the same APIs as for rule Application Disable List
Container Management	Enable container	True/False	True	KNOX-08-006600, KNOX-08-007000, KNOX-08-007100	MDM API: <u>startActivity(DevicePolicyManager.ACTION_PROVISION_MANAGED_PROFILE)</u> <u>createContainer(CreationParams params)</u> <u>createContainer(String type, String adminPackageName)</u>
Container Restrictions	Allow Show detailed notifications	True/False	False	KNOX-08-007500	Display details of container application notifications when user is outside container. MDM API: <u>setAllowChangeDataSyncPolicy(List appNames, String syncProperty, boolean value)</u>
Container Password Restrictions	Minimum Length	0+	4	KNOX-08-008400	Minimum container password length. MDM API: <u>setPasswordMinimumLength(ComponentName admin, int length)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container Password Restrictions	Maximum Sequential Characters	0+	2	KNOX-08-008700	Max number of sequential characters in password. MDM API: <u>setMaximumCharacterSequenceLength(int length)</u>
Container Password Restrictions	Maximum Sequential Numbers	0+	2	KNOX-08-008700	Max number of sequential numbers in password. MDM API: <u>setMaximumNumericSequenceLength(int length)</u>
Container Password Restrictions	Minimum Password Complexity	None Pattern PIN Alphabetic Alphanumeric Complex Biometric	PIN Alphabetic Alphanumeric or Complex	KNOX-08-008900	Password complexity. PIN is 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 these selections will cause the user to select a complex password, which is not required by the STIG. MDM API: <u>setPasswordQuality(ComponentName admin, int quality)</u>
Container Password Restrictions	Maximum Time to Lock	0+	15	KNOX-08-009200	MDM API: <u>setMaximumTimeToLock(ComponentName admin, long timeMs)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container Password Restrictions	Maximum Failed Attempts for wipe	0+	10	KNOX-08-009500	Unsuccessful logon attempts before container wipe. MDM API: <u>setMaximumFailedPasswordsForWipe(ComponentName admin, int num)</u>
Container Password Restrictions	Disable Keyguard Trust Agents	True/False	True	KNOX-08-010500	MDM API: <u>setKeyguardDisabledFeatures(ComponentName admin, int which)</u>
Container Restrictions	Allow Auto-Fill	True/False	False	KNOX-08-012800	MDM API: <u>setAutoFillSetting(boolean enable)</u>
Container Restrictions	Allow Google Crash Report	True/False	False	KNOX-08-013400	MDM API: <u>allowGoogleCrashReport(boolean allow)</u>
Android Advanced Restrictions	Prevent New Admin Install	True/False	True	KNOX-08-014300	MDM API: <u>preventNewAdminInstallation(boolean prevent)</u>
Container Restrictions	Allow S Voice	True/False	False	KNOX-08-014800	MDM API: <u>allowSVoice(boolean allow)</u>
Container Restrictions	Disable Share Via List	True/False	True	KNOX-08-015955	Note: Disabling “Share Via List” will also disable functionality such as “Gallery Sharing” and “Direct Sharing”. MDM API: <u>allowShareList(boolean allow)</u>
Container Restrictions	Allow Google Accounts Auto Sync	True/False	False	KNOX-08-017200	MDM API: <u>allowGoogleAccountsAutoSync(boolean allow)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container Certificate	Certificate Revocation Check (CRL)	True/False	True	KNOX-08-019200	Enable revocation check on all packages using the string: "*" (asterisk). MDM API: <u>enableRevocationCheck(String pkgName, boolean enable)</u>
Container Certificate	Certificate	Configure	Add Certificates	KNOX-08-019500	Select PEM encoded representations of the DoD root and intermediate certificates. MDM API: <u>installCertificateToKeystore(String type, byte[] value, String name, String password, int keystore)</u>
Container RCP	Move Files from Container to Personal	True/False	False	KNOX-08-021800	Blocks users from moving files from container. MDM API: <u>allowMoveFilesToOwner(boolean allow)</u>
Container RCPSync	Allow Calendar Info Outside Container	True/False	False	KNOX-08-022000	Sharing of container calendar events to outside container. MDM API: <u>setAllowChangeDataSyncPolicy(List appNames, String syncProperty, boolean value)</u>
Container RCP	Allow Sharing Clipboard Outside Container	True/False	False	KNOX-08-022200	Sharing of container clipboard to outside container. MDM API: <u>allowShareClipboardDataToOwner(boolean allow)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Container RCPSync	Allow Contact Info Outside Container	True/False	False	KNOX-08-022400	Sharing of container contacts to outside container. MDM API: <u>setAllowChangeDataSyncPolicy(List appNames, String syncProperty, boolean value)</u>
Container RCP	Move Applications to Container	True/False	False	KNOX-08-022600	Blocks users from moving installed applications (outside container) to the container. MDM API: <u>allowMoveAppsToContainer(boolean allow)</u>
Container VPN	VPN	Configure	See Comments	KNOX-08-023100	Configured for container use only. MDM API: <u>addContainerPackagesToVpn(int mContainerId, String[] packageList, String profileName)</u>

Table 3: COBO Configuration Policy Rules for Device-Wide Work Environment

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Account	Account whitelist	Configure	Approved accounts	KNOX-08-000100	<p>The idea is to use a combination of these policies to control what accounts a user is allowed to configure on the device.</p> <p>Configure by adding the domain of agency email accounts.</p> <p>MDM API: <u>addAccountsToAdditionWhiteList(String type, List accounts)</u></p>
Android Account	Account blacklist	Configure	.* (wildcard)	KNOX-08-000200	<p>Configure by blacklisting all domains. When all apps are blacklisted, only accounts on the whitelist are allowed.</p> <p>MDM API: <u>addAccountsToAdditionBlackList(String type, List accounts)</u></p>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Application	Application disable list	Configure	Add Unapproved Packages	KNOX-08-000700, KNOX-08-001600, KNOX-08-001700, KNOX-08-001800, KNOX-08-001900, KNOX-08-002000, KNOX-08-002100	The Systems Administrator should identify all pre-installed applications that are not approved and disable them (see Tables 10-1 through 10-3 in the STIG Supplemental document). MDM API: <u>setDisableApplication(String packageName)</u>
Android Applications	Package Name or Signature Blacklist	Configure	Add All Packages	KNOX-08-001000	All packages or signatures specified by wildcard (*.*). When all apps are blacklisted, only apps on the whitelist are allowed. MDM API: <u>addAppPackageNameToBlackList(String packageName)</u> <u>addAppSignatureToBlackList(String appSignature)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Applications	Package Name or Signature Whitelist	Configure	Add Approved Packages or Signatures	KNOX-08-001300	<p>Configure by setting the list of only DoD-approved packages or signatures. The following app packages must be included in the app whitelist so that Google Play services can be updated:</p> <ul style="list-style-type: none"> • com.android.vending • com.google.android.finsky • com.google.android.gm • com.google.android.gms • com.google.android.gsf.login • com.google.android.setupwizard • com.google.android.gsf <p>MDM API: <u>addAppPackageNameToWhiteList(String packageName, boolean defaultBlackList)</u> <u>addAppPackageNameToWhiteList(String packageName)</u> <u>addAppSignatureToWhiteList(String appSignature)</u> <u>addAppSignatureToWhiteList(String appSignature, boolean defaultBlackList)</u> </p>
Android Restrictions	Allow Install Non Market App	True/False	False	KNOX-08-002900	MDM API: <u>setAllowNonMarketApps(boolean)</u>
Android Applications	Battery optimizations modes Whitelist	Configure	Add MDM Client	KNOX-08-003200	MDM API: <u>addPackageToBatteryOptimizationWhiteList(AppIdentity appIdentity)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Applications	Disable Bixby Vision	True/False	True	KNOX-08-003500	This policy is implemented using Disable Application policies. See STIG requirement for more information. MDM API: Use the same APIs as for rule Application Disable List
Android Audit Log	Enable Audit Log	True/False	True	KNOX-08-004000	MDM API: <u>enableAuditLog()</u>
Android Restrictions	Notifications on lock screen	Show content, Hide content, Do not show notifications	Hide content or Do not show notifications	KNOX-08-007300	MDM API: <u>setKeyguardDisabledFeatures(ComponentName admin, int which)</u>
Android Password Restrictions	Minimum Length	0+	6	KNOX-08-008300	Minimum device password length. MDM API: <u>setPasswordMinimumLength(ComponentName admin, int length)</u>
Android Password Restrictions	Maximum Sequential Characters	0+	2	KNOX-08-008600	Max number of sequential characters in password. MDM API: <u>setMaximumCharacterSequenceLength(int length)</u>
Android Password Restrictions	Maximum Sequential Numbers	0+	2	KNOX-08-008600	Max number of sequential numbers in password. MDM API: <u>setMaximumNumericSequenceLength(int length)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Password Restrictions	Minimum Password Complexity	None Pattern PIN Alphabetic Alphanumeric Complex Biometric	PIN Alphabetic Alphanumeric or Complex	KNOX-08-008800	<p>Password complexity. PIN is recommended.</p> <p>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 these selections will cause the user to select a complex password, which is not required by the STIG.</p> <p>MDM API: <u>setPasswordQuality(ComponentName admin, int quality)</u></p>
Android Password Restrictions	Maximum Time to Lock	0+	5	KNOX-08-009100	<p>This value defines the amount of time from when the screen turns off until the device locks. Since the maximum screen timeout a user can select on Android 8 is 10 minutes, a 5-minute or less lock time value fulfills this requirement.</p> <p>MDM API: <u>setMaximumTimeToLock(ComponentName admin, long timeMs)</u></p>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Password Restrictions	Maximum Failed Attempts for wipe	0+	10	KNOX-08-009400	Unsuccessful logon attempts before device wipe. MDM API: <u>setMaximumFailedPasswordsForWipe(ComponentName admin, int num)</u>
Android Password Restrictions	Disable Face Recognition	True/False	True	KNOX-08-011000	MDM API: <u>setBiometricAuthenticationEnabled(int bioAuth, boolean enable)</u>
Android Password Restrictions	Disable Intelligent Scanning	True/False	True	KNOX-08-010800	This policy is indirectly configured by disabling face or iris scanning. MDM API: Use the same APIs as for Disable Face Recognition rule or Disable Iris rule
Android Password Restrictions	Disable Keyguard Trust Agents	True/False	True	KNOX-08-010300	MDM API: <u>setKeyguardDisabledFeatures(ComponentName admin, int which)</u>
Android Restrictions	Allow Auto-Fill	True/False	False	KNOX-08-012700	MDM API: <u>setAutoFillSetting(boolean enable)</u>
Android Multi User	Allow multi-user mode	True/False	False	KNOX-08-013000	MDM API: <u>allowMultipleUsers(boolean allow)</u>
Android Restrictions	Allow Google Crash Report	True/False	False	KNOX-08-013200	MDM API: <u>allowGoogleCrashReport(boolean allow)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Bluetooth	Allowed Bluetooth Profiles	HSP HFP PBAP A2DP AVRCP SPP NAP BNEP HID BPP DUN SAP	HFP HSP SPP	KNOX-08-013900	Disables all Bluetooth profiles except for those specified in the settings. MDM API: <u>enableSecureMode(BluetoothSecureModeConfig configObj, ListwhiteList)</u>
Android Advanced Restrictions	Prevent New Admin Install	True/False	True	KNOX-08-014100	MDM API: <u>preventNewAdminInstallation(boolean prevent)</u>
Android Restrictions	Allow Admin Remove	True/False	False	KNOX-08-014200	Only applicable to legacy configurations. MDM API: <u>setAdminRemovable(boolean removable)</u>
Android Restrictions	Allow S Voice	True/False	False	KNOX-08-014700	MDM API: <u>allowSVoice(boolean allow)</u>
Android Restrictions	Disable USB Media Player	True/False	True	KNOX-08-015000, KNOX-08-017300	Disabling USB Media Player will also disable USB MTP, USB mass storage, and USB vendor protocol (KIES). MDM API: <u>setUsbMediaPlayerAvailability(boolean enable)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Advanced Restrictions	Enable CC Mode	True/False	True	KNOX-08-015300	<p>CC mode is fundamental to MDFPP compliance and is a top-level requirement.</p> <p>Puts the devices in CC (Common Criteria) mode as defined by the Samsung Galaxy Device MDFPP Security Target.</p> <p>All cryptography will be configured to be in FIPS 140-2 validated mode.</p> <p>Encryption for information at rest on built-in storage media must be enabled.</p> <p>MDM API: <u>setInternalStorageEncryption(boolean isEncrypt)</u> <u>setCCmode(boolean enable)</u></p>
Android Date Time	Date Time Change Enabled	True/False	False	KNOX-08-015500	MDM API: <u>setDateTimeChangeEnabled(boolean)</u>
Android Restrictions	USB Host Modes Whitelist	APP AUD CDC COM CON CSC HID HUB MAS MIS PER	HID	KNOX-08-015700	<p>USB MAS host mode allows the device to mount external USB drives.</p> <p>MDM API: <u>SetUsbExceptionList(int exceptionList)</u> <u>allowUsbHostStorage(boolean allow)</u></p>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
		PHY PRI STI VEN VID WIR			
Android Restrictions	Disable Share Via List	True/False	True	KNOX-08-015950	Note: Disabling “Share Via List” will also disable functionality such as “Gallery Sharing” and “Direct Sharing”. MDM API: <u>allowShareList(boolean allow)</u>
Android Restrictions	Disable Android Beam	True/False	True	KNOX-08-016000	MDM API: <u>allowAndroidBeam(boolean allow)</u>
Android Restrictions	Allow Google Backup	True/False	False	KNOX-08-017400	MDM API: <u>setBackup(boolean)</u>
Android Restrictions	Allow Google Accounts Auto Sync	True/False	False	KNOX-08-017100	MDM API: <u>allowGoogleAccountsAutoSync(boolean allow)</u>
Android Restrictions	Allow Developer Mode	True/False	False	KNOX-08-017900	MDM API: <u>allowDeveloperMode(boolean allow)</u>
Android WiFi	Allow Unsecured Hotspot	True/False	False	KNOX-08-018100	MDM API: <u>allowOpenWifiAp(boolean allow)</u>
Android Security	External Storage Encryption	True/False	True	KNOX-08-018500	Encrypt all external media cards. MDM API: <u>setExternalStorageEncryption(boolean isEncrypt)</u>

Policy Group	Policy Rule	Options	Settings	Related Requirement Number	Comments
Android Certificate	Certificate Revocation Check (CRL)	True/False	True	KNOX-08-019100	Enable revocation check on all packages using the string: "*" (asterisk). MDM API: <u>enableRevocationCheck(String pkgName, boolean enable)</u>
Android Certificate	Certificate	Configure	Add Certificates	KNOX-08-019400	Select PEM encoded representations of the DoD root and intermediate certificates. MDM API: <u>installCertificateToKeystore(String type, byte[] value, String name, String password, int keystore)</u>

DoD Wireless service providers should consider including the following optional controls, if warranted, based on the operational environment and use case implemented.

Table 4: Optional Controls

Policy Group	Policy Rule	Options	Comments
Android Restrictions	Allow Location	Passive Network GPS	An administrator can enable or disable specific location providers (i.e., passive, network, gps). MDM API: <u>setLocationProviderState(String provider, boolean enable)</u>
Container Restrictions	Allow Location	Passive Network GPS	An administrator can enable or disable specific location providers (i.e., passive, network, gps). MDM API: <u>setLocationProviderState(String provider, boolean enable)</u>
Android Restrictions	Allow Microphone	True/False	MDM API: <u>setMicrophoneState(boolean enable)</u>
Container Restrictions	Allow Microphone	True/False	MDM API: <u>setMicrophoneState(boolean enable)</u>
Android Restrictions	Allow Camera	True/False	MDM API: <u>setCameraState(boolean enable)</u>
Container Restrictions	Allow Camera	True/False	MDM API: <u>setCameraState(boolean enable)</u>
Android Restrictions	Allow Bluetooth tethering	True/False	This setting also applies in the container if one exists. MDM API: <u>setBluetoothTethering(boolean enable)</u>
Android Restrictions	Allow WiFi tethering	True/False	This setting also applies in the container if one exists. MDM API: <u>setWifiTethering(boolean)</u>
Android NFC	Allow NFC	True/False	This setting also applies to the container if one exists. MDM API: <u>startNFC (boolean start)</u> <u>allowNFCStateChange (boolean allow)</u>
Android Password Restrictions	Allow Fingerprint Unlock	True/False	MDM API: <u>setBiometricAuthenticationEnabled(int bioAuth, boolean enable)</u>

Policy Group	Policy Rule	Options	Comments
Container Password Restrictions	Allow Fingerprint Unlock	True/False	MDM API: <u>setBiometricAuthenticationEnabled(int bioAuth, boolean enable)</u>
Android Password Restrictions	Allow Iris Scan Unlock	True/False	MDM API: setBiometricAuthenticationEnabled()
Container Password Restrictions	Allow Iris Scan Unlock	True/False	MDM API: setBiometricAuthenticationEnabled()