SAMSUNG ANDROID OS 11 WITH KNOX 3.X AE STIG CONFIGURATION TABLES

Version 1, Release 1

20 November 2020

Developed by Samsung and DISA for the DoD

LIST OF TABLES

Page

Unified Endpoint Management (UEM) empowers enterprise IT administrators with powerful tools to centrally set up, deploy, secure, control, and maintain desktops, laptops, smartphones, tablets, wearables, and Internet of Things (IoT) devices. Samsung has collaborated with the leading UEM providers to ease the management of Samsung devices, which feature the Knox Platform for Enterprise. To set up Samsung devices using popular UEM platforms, go to: https://docs.samsungknox.com/admin/uem/index.htm

All APIs used to implement the policies are listed in the comment column in the following tables.

If there is an "*" below "AE" in the "Vendor" cell, it means:

- There is a KPE alternative policy that may be used for compliance if your management tool does not implement the AE policy.
- If your management tool also does not implement the KPE policy, then KSP should be used to provide full coverage.
- KSP implements all STIG listed KPE policies and all the listed alternatives to AE policies.
- The appendix section of this document includes cross-references for KSP.

Table 01: Configuration Policy Rules for COPE

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	**Device** Password Requirements	Minimum password length	0+	6	KNOX-11-000100	setPasswordMinimumLength
AE	**Device** Password Requirements	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric	KNOX-11-000100, KNOX-11-000500, KNOX-11-000700	**This allows for PIN code.** setPasswordQuality PASSWORD_QUALITY_NUMERIC (minimum)
KPE	**Device** Password Requirements	Maximum sequential numbers	0+	2	KNOX-11-000300	**This policy is not applicable if the password quality is set to Numeric (complex) or better.** PasswordPolicy setMaximumNumericSequenceLength

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	**Device** Password Requirements	Max time to screen lock	0 minutes	15 minutes	KNOX-11-000500	setMaximumTimeToLock
AE	**Device** Password Requirements	Max password failures for local wipe	0+	10	KNOX-11-000700	setMaximumFailedPasswordsForWipe
AE *	**Device** Restrictions	Installs from unknown sources globally	Allow/Disallow	Disallow	KNOX-11-001300	addUserRestriction DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY
AE	**Device** Restrictions	Trust agents	Disable/Enable	Disable	KNOX-11-003900	setKeyguardDisabledFeatures KEYGUARD_DISABLE_TRUST_AGENTS
AE *	**Device** Restrictions	Face	Disable/Enable	Disable	KNOX-11-004100	setKeyguardDisabledFeatures KEYGUARD_DISABLE_FACE
AE *	**Device** Restrictions	Debugging features	Allow/Disallow	Disallow	KNOX-11-005100	addUserRestriction DISALLOW_DEBUGGING_FEATURES
AE *	**Device** Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-11-006500, KNOX-11-006900	addUserRestriction DISALLOW_USB_FILE_TRANSFER
KPE	**Device** Wi-Fi	Unsecured hotspot	Allow/Disallow	Disallow	KNOX-11-008100	allowOpenWifiAp
KPE	**Device** Restrictions	CC mode	Enable/Disable	Enable	KNOX-11-013900, KNOX-11-020100	**Refer to Supplemental section 6.4 Common Criteria (CC) Settings.** setCCMode
AE *	**Device** Restrictions	Mount physical media	Allow/Disallow	Disallow	KNOX-11-003500	**Disable SD cards.** addUserRestriction

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
						DISALLOW_MOUNT_PHYSICAL_MEDIA
KPE	**Device** 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-11-020900	**This allows the use of DEX capabilities.** setUsbExceptionList allowUsbHostStorage (must be toggled off/on for USB exception list to take effect)
KPE	**Device** Bluetooth	Bluetooth UUID allowlist	A2DP, AVRCP, BNEP, BPP, DUN, FTP, HFP, HSP, NAP, OBEXOBJECTPUSH, PANU, PBAP,	HFP, HSP, SPP, A2DP, AVRCP, PBAP	KNOX-11-002300	addBluetoothUUIDsToWhiteList addBluetoothUUIDsToBlackList activateBluetoothUUIDRestriction

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
			SAP, SPP			
N/A	User Agreement	User Agreement		Include DoD-mandated warning banner text in User Agreement	KNOX-11-006300	**Put the DoD Warning banner text in the User Agreement** Alternative: AE* setDeviceOwnerLockScreenInfo
AE *	**Device** Restrictions	Config Date Time	Allow/Disallow	Disallow	KNOX-11-020500	addUserRestriction DISALLOW_CONFIG_DATE_TIME
AE	**Device** Enrollment Configuration	Default device enrollment	Full managed, Work profile for company-owned devices	Work profile for company-owned devices	KNOX-11-017700, KNOX-11-017900, KNOX-11-018500	
KPE	**Work profile** Restrictions	Share Via List	Allow/Disallow	Disallow	KNOX-11-021300	allowShareList
KPE	**Work profile** RCP	Move files to personal	Allow/Disallow	Disallow	KNOX-11-008900	allowMoveFilesToOwner
KPE	**Work profile** RCP	Sync calendar to personal	Allow/Disallow	Disallow	KNOX-11-009300	setAllowChangeDataSyncPolicy CALENDAR, EXPORT, FALSE
AE	**Work profile** Restrictions	Autofill services	Allow/Disallow	Disallow	KNOX-11-019700	addUserRestriction DISALLOW_AUTOFILL
AE *	**Work profile** Restrictions	Account management	Account types, Enable/Disable	Disable for: Work email app, Samsung Accounts, Google	KNOX-11-007500, KNOX-11-017300	setAccountManagementDisabled

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
				Accounts, and each AO-approved app that uses accounts for data backup/sync		
KPE	**Work profile** Restrictions	Revocation check **OR** OCSP check	Enable/Disable	Enable	KNOX-11-022500	enableRevocationCheck enableOcspCheck
AE *	**Work profile** Policy Management	Certificates	Configure	Include DoD certificates in work profile	KNOX-11-022900	installCaCert
AE *	**Work profile** Restrictions	Config credentials	Allow/Disallow	Disallow	KNOX-11-023100	addUserRestriction DISALLOW_CONFIG_CREDENTIALS
AE *	**Work profile** Restrictions	List of approved apps listed in managed Google Play	List of apps	List only approved work apps in managed Google Play	KNOX-11-001700, KNOX-11-001900	Configure managed Google Play with approved work apps.
AE *	**Work profile** Restrictions	Unredacted Notifications	Allow/Disallow	Disallow	KNOX-11-002700	setKeyguardDisabledFeatures KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
AE *	**Work profile** Restriction	Cross profile copy/paste	Allow/Disallow	Disallow	KNOX-11-009100	addUserRestriction DISALLOW_CROSS_PROFILE_COPY_PASTE
AE *	**Work profile** Restrictions	Security logging	Enable/Disable	Enable	KNOX-11-018300	setSecurityLoggingEnabled (MDM must also provide means to read the Log in the console.)

Table 2: Configuration Policy Rules for COBO

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE *	**Device** Password Requirements	Minimum password length	0+	6	KNOX-11-000100	setPasswordMinimumLength
AE *	**Device** Password Requirements	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric	KNOX-11-000100, KNOX-11-000500, KNOX-11-000700	**This allows for PIN code.** setPasswordQuality PASSWORD_QUALITY_NUMERIC (minimum)
KPE	**Device** Password Requirements	Maximum sequential numbers	0+	2	KNOX-11-000300	**This requirement is not applicable if the password quality is set to Numeric (complex), or better.** PasswordPolicy setMaximumNumericSequenceLength
AE *	**Device** Password Requirements	Max time to screen lock	0 minutes	15 minutes	KNOX-11-000500	setMaximumTimeToLock
AE *	**Device** Password Requirements	Max password failures for local wipe	0+	10	KNOX-11-000700	setMaximumFailedPasswordsForWipe
AE *	**Device** Restrictions	Installs from unknown sources globally	Allow/Disallow	Disallow	KNOX-11-001300	addUserRestriction DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY
AE *	**Device** Restrictions	Trust agents	Enable/Disable	Disable	KNOX-11-003900	setKeyguardDisabledFeatures KEYGUARD_DISABLE_TRUST_AGENTS

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE *****	**Device** Restrictions	Face	Enable/Disable	Disable	KNOX-11-004100	setKeyguardDisabledFeatures KEYGUARD_DISABLE_FACE
AE *****	**Device** Restrictions	Debugging features	Allow/Disallow	Disallow	KNOX-11-005100	addUserRestriction DISALLOW_DEBUGGING_FEATURES
AE *****	**Device** Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-11-006500, KNOX-11-006900	addUserRestriction DISALLOW_USB_FILE_TRANSFER
KPE	**Device** Wi-Fi	Unsecured hotspot	Allow/Disallow	Disallow	KNOX-11-008100	allowOpenWifiAp
KPE	**Device** Restrictions	CC mode	Enable/Disable	Enable	KNOX-11-013900, KNOX-11-020100	**Refer to Supplemental section 6.4 Common Criteria (CC) Settings.** setCCMode
AE *****	**Device** Restrictions	Mount physical media	Allow/Disallow	Disallow	KNOX-11-003500	**Disable SD card.** addUserRestriction DISALLOW_MOUNT_PHYSICAL_MEDIA
AE *****	**Device** Restrictions	Security logging	Enable/Disable	Enable	KNOX-11-018300	setSecurityLoggingEnabled (MDM must also provide means to read the Log in the console)
KPE	**Device** Restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON, CSC, HID, HUB, MAS, MIS, PER,	HID	KNOX-11-020900	**This allows the use of DEX capabilities.** setUsbExceptionList allowUsbHostStorage (must be toggled off/on for USB exception list to take effect)

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
			PHY, PRI, STI, VEN, VID, WIR			
KPE	**Device** Bluetooth	Bluetooth UUID allowlist	A2DP, AVRCP, BNEP, BPP, DUN, FTP, HFP, HSP, NAP, OBEXOBJECTPUSH, PANU, PBAP, SAP, SPP	HFP, HSP, SPP, A2DP, AVRCP, PBAP	KNOX-11-002300	addBluetoothUUIDsToWhiteList addBluetoothUUIDsToBlackList activateBluetoothUUIDRestriction
N/A	User Agreement	User Agreement		Include DoD-mandated warning banner text in User Agreement	KNOX-11-006300	**Put the DoD Warning banner text in the User Agreement** Alternative: AE* setDeviceOwnerLockScreenInfo
AE *	**Device** Restrictions	Config Date Time	Allow/Disallow	Disallow	KNOX-11-020500	addUserRestriction DISALLOW_CONFIG_DATE_TIME

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE	**Device** Enrollment Configuration	Default device enrollment	Full managed, Work profile for company-owned devices	Fully managed	KNOX-11-017900, KNOX-11-018500	Enroll device as an Android Enterprise device (DO).
AE *	**Device** Restrictions	Outgoing beam	Allow/Disallow	Disallow	KNOX-11-021700	addUserRestriction DISALLOW_OUTGOING_BEAM
KPE	**Device** Restrictions	Share Via List	Allow/Disallow	Disallow	KNOX-11-021300	allowShareList
AE *	**Device** Restrictions	Backup service	Allow/Disallow	Disallow	KNOX-11-007300	setBackupServiceEnabled
AE	**Device** Restrictions	Autofill services	Allow/Disallow	Disallow	KNOX-11-019700	addUserRestriction DISALLOW_AUTOFILL
AE *	**Device** Restrictions	Account management	Account types, Enable/Disable	Disable for: Work email app, Samsung Accounts, Google Accounts, and each AO-approved app that uses accounts for data backup/sync	KNOX-11-007500, KNOX-11-017300	setAccountManagementDisabled
KPE	**Device** Restrictions	Revocation check **OR** OCSP check	Enable/Disable	Enable	KNOX-11-022500	enableRevocationCheck enableOcspCheck

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
AE *	**Device** Policy Management	Certificates	Configure	Include DoD certificates in work profile	KNOX-11-022900	installCaCert
AE *	**Device** Restrictions	Config credentials	Allow/Disallow	Disallow	KNOX-11-023100	addUserRestriction DISALLOW_CONFIG_CREDENTIALS
AE *	**Device** Restrictions	List of approved apps listed in managed Google Play	List of apps	List only approved work apps in managed Google Play	KNOX-11-001700, KNOX-11-001900	Configure managed Google Play with approved work apps.
AE	**Device** Restrictions	Unredacted Notifications	Allow/Disallow	Disallow	KNOX-11-002700	setKeyguardDisabledFeatures KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS

APPENDIX

Table 1: KSP Cross-Reference

The instructions contained in the following tables are based on the latest KSP version available at time of writing: Version: [1.2.45].

Policy Group	Policy Rule	KSP Policy Mapping
Device Password Requirements	Minimum password length	**COPE: Use MDM native capability** **COBO:** 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Password policy 4. Enable password policy controls with KSP [enable] 5. Password Restriction 6. Minimum Password Length [6] **API:** BasePasswordPolicy setPasswordMinimumLength
Device Password Requirements	Minimum password quality	**COPE: Use MDM native capability** **COBO:** 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Password policy 4. Enable password policy controls with KSP [enable] 5. Define Password Quality [numeric]" **API:** BasePasswordPolicy setPasswordQuality
Device Password Requirements	Maximum sequential numbers	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Password policy

Policy Group	Policy Rule	KSP Policy Mapping
		4. Enable password policy controls with KSP [enable] 5. Password Restriction 6. Maximum Numeric Sequence Length [2] **API:** PasswordPolicy setMaximumNumericSequenceLength
Device Password Requirements	Max time to screen lock	**COPE: Use MDM native capability** **COBO:** 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Password policy 4. Enable password policy controls with KSP [enable] 5. Allowed Time for User Activity before Device Locks [900] **API:** BasePasswordPolicy setMaximumTimeToLock
Device Password Requirements	Max password failures for local wipe	**COPE: Use MDM native capability** **COBO:** 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Password policy 4. Enable password policy controls with KSP [enable] 5. Maximum Failed Password Attempt to Wipe Data [10] **API:** BasePasswordPolicy setMaximumFailedPasswordsForWipe
Device Restrictions	Installs from unknown sources	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions

Policy Group	Policy Rule	KSP Policy Mapping
		4. Enable device restriction controls [enable] 5. Allow installation of non-Google Play apps [disable] **API:** RestrictionPolicy setAllowNonMarketApps
Device Restrictions	Trust agents	**Use MDM native capability**
Device Restrictions	Face	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Password policy 4. Enable password policy controls with KSP [enable] 5. Biometric authentication 6. Enable Face recognition [disable] **API:** PasswordPolicy setBiometricAuthenticationEnabled
Device Restrictions	Debugging features	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Allow developer mode [disable] **API:** RestrictionPolicy allowDeveloperMode
Device Restrictions	USB file transfer	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Allow USB media player [disable] **API:** RestrictionPolicy setUsbMediaPlayerAvailability
Device Wi-Fi	Unsecured hotspot	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted)

Policy Group	Policy Rule	KSP Policy Mapping
		2. Enable device policy controls [enable] 3. Device Controls 4. Wi-Fi Policy 5. Enable Wi-Fi policy controls [enable] 6. Allow open Wi-Fi connection [disable] **API:** WiFiPolicy allowOpenWifiAp
Device Restrictions	CC mode	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Advanced Restriction policies (Premium) 4. Enable Advanced Restriction controls [enable] 5. Enable Common Criteria (CC) mode [enable] **API:** AdvancedRestrictionPolicy setCCMode
Device Restrictions	Mount physical media	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Allow SD card access [disable] **API:** RestrictionPolicy setSdCardState
Device Restrictions	USB host mode exception list	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Setup USB exception list [Human Interface Device] **API:** RestrictionPolicy allowUsbHostStorage + setUsbExceptionList

Policy Group	Policy Rule	KSP Policy Mapping
Device Bluetooth	Bluetooth UUID allowlist	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Controls 4. Bluetooth Policy 5. Enable Bluetooth policy controls [enable] 6. Allowlist Bluetooth Service by UUID [configure] **API:** BluetoothPolicy addBluetoothUUIDsToWhiteList/BlackList + activateBluetoothUUIDRestriction
User Agreement	User Agreement	**Put the DoD Warning banner text in the User Agreement** Alternative: 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Controls 4. Boot banner 5. Enable banner on device reboot [enable] **API:** BootBanner enableRebootBanner
Device Restrictions	Config Date Time	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Date Time Change 4. Enable Date Time Policy controls [enable] 5. Allow Date Time change [disable] **API:** DateTimePolicy setDateTimeChangeEnabled
Device Enrollment Configuration	Default device enrollment	**Use MDM native capability**

Policy Group	Policy Rule	KSP Policy Mapping
Device Restrictions	Share Via List	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Allow Share Via option [disable] **API:** RestrictionPolicy allowShareList
Device Restrictions	Autofill services	**Use MDM native capability**
Device Restrictions	Account management	Step 1: 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Account Policy 4. Enable Device Account Policy controls [enable] 5. Enable Device Account policies (Configure profiles below) [enable] Step 2: 1. Device Account Policy Configurations 2. Add setting 3. Device Account Policy Configuration 4. Add Account Type to Addition Blacklist [choose types] 5. Add Accounts to Addition Blacklist [configure ""*""] **API:** DeviceAccountPolicy addAccountsToAdditionBlackList
Device Restrictions	Revocation check	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Certificate revocation 6. Enable revocation check [Enable for all apps]

Policy Group	Policy Rule	KSP Policy Mapping
		API: CertificatePolicy enableRevocationCheck
Device Restrictions	**OR** OCSP check	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Certificate revocation 6. Enable revocation check [Enable for all apps] 7. Enable OCSP check before CRL [enable] **API:** CertificatePolicy enableRevocationCheck + enableOcspCheck
Device Policy Management	Certificates	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Install Certificate in keystore(s) silently [configure] **API:** CertificateProvisioning installCertificateToKeystore
Device Restrictions	Config credentials	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Block User from removing Certificate [enable] **API:** CertificatePolicy allowUserRemoveCertificates
Device Restrictions	List of approved apps listed in managed Google Play	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Application management policies

Policy Group	Policy Rule	KSP Policy Mapping
		4. Enable application management controls [enable] 5. Application Allowlist by Pkg Name [configure comma-separated package list] **API:** ApplicationPolicy addAppPackageNameToWhiteList
		1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Application management policies 4. Enable application management controls [enable] 5. Application Blocklist by Pkg Name [configure ""*""] **API:** ApplicationPolicy addAppPackageNameToBlackList
		1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Application management policies 4. Enable application management controls [enable] 5. Application Allowlist by Signature used [configure comma-separated package hash list] **API:** ApplicationPolicy addAppSignatureToWhiteList
		1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Application management policies 4. Enable application management controls [enable] 5. Application Blocklist by Signature used [configure ""*""] **API:** ApplicationPolicy addAppSignatureToBlackList
Device Restrictions	Unredacted Notifications	**Use MDM native capability**

Policy Group	Policy Rule	KSP Policy Mapping
Device Restrictions	Security logging	**Use KPE Audit logging feature** 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Audit Log (Premium) 4. Enable Audit Log [enable] 5. Log Path [configure] **API:** AuditLog enableAuditLog
Device Restrictions	Outgoing beam	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Allow Android Beam on device [disable] **API:** RestrictionPolicy allowAndroidBeam
Device Restrictions	Backup service	1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Device Restrictions 4. Enable device restriction controls [enable] 5. Allow backup on Google Server [disable] **API:** RestrictionPolicy setBackup
Work profile Restrictions	Share Via List	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Restrictions in work profile (Premium) 4. Enable work profile restriction controls [enable] 5. Allow Share Via option [disable]

Policy Group	Policy Rule	KSP Policy Mapping
		API: RestrictionPolicy allowShareList
Work profile RCP	Move file to personal	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. RCP policy (Premium) 4. Enable RCP Policy Controls [enable] 5. Allow moving files from work profile to personal space [disable] **API:** RCPPolicy allowMoveFilesToOwner
Work profile RCP	Sync calendar to personal	Step 1: 1. RCP Data Sync profile Configurations (Premium) 2. Add setting 3. RCP Data Sync profile Configuration 4. Select Application to Data Sync >> Name of the Application [calendar] 5. Select Data Sync Property >> Data Sync Property [export data] 6. Enable user to data sync on selective applications [enable] Step 2: 1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. RCP policy (Premium) 4. Enable RCP Policy Controls [enable] 5. Enable RCP data sync policy (Configure profiles below) [enable] **API:** RCPPolicy setAllowChangeDataSyncPolicy CALENDAR, EXPORT, FALSE
Work profile Restrictions	Autofill services	**Use MDM native capability**
Work profile Restrictions	Account management	Step 1: 1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Device Account Policy 4. Enable Device Account Policy Controls [enable]

Policy Group	Policy Rule	KSP Policy Mapping
		5. Enable Device Account policies (Configure profiles below) [enable] Step 2: 1. Device Account Policy Configurations 2. Add setting 3. Device Account Policy Configuration 4. Add Account Type to Addition Blacklist [choose types] 5. Add Accounts to Addition Blacklist [configure ""*""] **API:** DeviceAccountPolicy addAccountsToAdditionBlackList
Work profile Restrictions	Revocation check	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Certificate revocation 6. Enable revocation check [enable for all apps] **API:** CertificatePolicy enableRevocationCheck
Work profile Restrictions	**OR** OCSP check	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Certificate revocation 6. Enable revocation check [enable for all apps] 7. Enable OCSP check before CRL [enable] **API:** CertificatePolicy enableRevocationCheck + enableOcspCheck
Work profile Policy Management	Certificates	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Install Certificate in keystore(s) silently [configure]

Policy Group	Policy Rule	KSP Policy Mapping
		API: CertificateProvisioning installCertificateToKeystore
Work profile Restrictions	Config credentials	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Certificate management policies (Premium) 4. Enable certificate management controls [enable] 5. Block user from removing Certificate [enable] **API:** CertificatePolicy allowUserRemoveCertificates
Work profile Restrictions	List of approved apps listed in managed Google Play	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Application management policies (Premium) 4. Enable application management controls [enable] 5. Application Allowlist by Pkg Name [configure comma-separated package list] **API:** ApplicationPolicy addAppPackageNameToWhiteList
		1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Application management policies 4. Enable application management controls [enable] 5. Application Blocklist by Pkg Name [configure "*"] **API:** ApplicationPolicy addAppPackageNameToBlackList
		1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Application management policies 4. Enable application management controls [enable] 5. Application Allowlist by Signature used [configure comma-separated package hash list] **API:** ApplicationPolicy addAppSignatureToWhiteList

Policy Group	Policy Rule	KSP Policy Mapping
		1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Application management policies 4. Enable application management controls [enable] 5. Application Blocklist by Signature used [configure "*"] **API:** ApplicationPolicy addAppSignatureToBlackList
Work profile Restrictions	Unredacted Notifications	Step 1: 1. RCP Data Sync profile Configurations (Premium) 2. Add setting 3. Select Application to Data Sync >> Name of Application [notifications] 4. Select Data Sync Property >> Data Sync Property [sanitize data] 5. Enable user to data sync on selective applications [enable] Step 2: 1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. RCP policy (Premium) 4. Enable RCP Policy Controls [enable] 5. Enable RCP data sync policy (Configure profiles below) [enable] **API:** RCPPolicy setAllowChangeDataSyncPolicy NOTIFICATIONS, SANITIZE_DATA, FALSE
Work profile RCP	Cross profile copy/paste	1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. RCP policy (Premium) 4. Enable RCP Policy Controls [enable] 5. Enable Sharing of Clipboard Data to Owner [disable] **API:** RCPPolicy allowShareClipboardDataToOwner

Policy Group	Policy Rule	KSP Policy Mapping
Work profile Audit Log	Security logging	**Use KPE Audit logging feature.** 1. Work profile policies (Profile Owner) 2. Enable work profile policies [enable] 3. Audit Log (Premium) 4. Enable Audit Log [enable] 5. Log Path [configure] When enabling KPE Audit logging feature for the Work profile, it must also be enabled for the device: 1. Device-wide policies (Selectively applicable to Fully Manage Device [DO] or Work Profile on company-owned devices [WP-C] mode as noted) 2. Enable device policy controls [enable] 3. Audit Log (Premium) 4. Enable Audit Log [enable] 5. Log Path [configure] **API:** AuditLog enableAuditLog

Table 2: KSP App Separation

To implement the Knox app separation feature, the policies listed in "Table 2: Configuration Policy Rules for COBO" must be used in conjunction with the policies listed in the following table:

Policy Group	Policy Rule	KSP Policy Mapping
App Separation	Location	1. App Sep Policies 2. Enable App Sep Policies [enable] 3. Allow Listing Policies 4. Set Location [inside or outside]
App Separation	App List	1. App Sep Policies 2. Enable App Sep Policies [enable] 3. Allow Listing Policies 4. Configure Apps List [list of packages]