SAMSUNG ANDROID OS 11 WITH KNOX 3.X LEGACY 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.

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

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Device** Password Requirements	Minimum password length	0+	6	KNOX-11-000200	setPasswordMinimumLength
KPE	**Device** Password Requirements	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric	KNOX-11-000200, KNOX-11-000600, KNOX-11-000800	**This allows for PIN code.** setPasswordQuality PASSWORD_QUALITY_NUMERIC (minimum)
KPE	**Device** Password Requirements	Maximum sequential numbers	0+	2	KNOX-11-000400	**This policy 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-11-000600	setMaximumTimeToLock
AE	**Device** Password Requirements	Max password failures for local wipe	0+	10	KNOX-11-000800	setMaximumFailedPasswordsForWipe

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Device** Restrictions	Installs from unknown sources	Allow/Disallow	Disallow	KNOX-11-001400	setAllowNonMarketApps
KPE	**Device** Restrictions	Trust agents	Disable/Enable	Disable	KNOX-11-004000	setKeyguardDisabledFeatures KEYGUARD_DISABLE_TRUST_AGENTS
KPE	**Device** Restrictions	Face	Disable/Enable	Disable	KNOX-11-004200	setBiometricAuthenticationEnabled BIOMETRIC_AUTHENTICATION_FACE
KPE	**Device** Restrictions	Debugging features	Allow/Disallow	Disallow	KNOX-11-005200	allowDeveloperMode
KPE	**Device** Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-11-006600, KNOX-11-007000	setUsbMediaPlayerAvailability
KPE	**Device** Wi-Fi	Unsecured hotspot	Allow/Disallow	Disallow	KNOX-11-008200	allowOpenWifiAp
KPE	**Device** Restrictions	CC mode	Enable/Disable	Enable	KNOX-11-014000, KNOX-11-020200	**Refer to Supplemental Section 6.4 Common Criteria (CC) Settings.** setCCMode
KPE	**Device** Restrictions	SD Card	Enable/Disable	Disable	KNOX-11-003600	**Disable SD cards.** setSdCardState

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
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-11-021000	**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, SAP,	HFP, HSP, SPP, A2DP, AVRCP, PBAP	KNOX-11-002400	addBluetoothUUIDsToWhiteList addBluetoothUUIDsToBlackList activateBluetoothUUIDRestriction

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
			SPP			
N/A	User Agreement	User Agreement		Include DoD-mandated warning banner text in User Agreement	KNOX-11-006400	**Put the DoD Warning banner text in the User Agreement.** Alternative: KPE enableRebootBanner
KPE	**Device** Multiuser	Multi-user mode	Allow/Disallow	Disallow	KNOX-11-009800	**Tablet devices only.** allowMultipleUsers
KPE	**Device** Application	System app disable list	Configure	List non-AO-approved system app packages	KNOX-11-017800	setDisableApplication
KPE	**Device** Audit log	Audit Log	Enable/Disable	Enable	KNOX-11-018400	enableAuditLog
KPE	**Device** Restrictions	Date Time Change	Enable/Disable	Disable	KNOX-11-020600	setDateTimeChangeEnabled
AE	**Device** Enrollment Configuration	Default device enrollment	Legacy managed, Legacy managed with Legacy Workspace	Legacy managed with Legacy Workspace	KNOX-11-018600	
KPE	**Workspace** Restrictions	Share Via List	Allow/Disallow	Disallow	KNOX-11-021400	allowShareList
KPE	**Workspace** RCP	Move files to personal	Allow/Disallow	Disallow	KNOX-11-009000	allowMoveFilesToOwner
KPE	**Workspace** RCP	Sync calendar to personal	Allow/Disallow	Disallow	KNOX-11-009400	setAllowChangeDataSyncPolicy CALENDAR, EXPORT, FALSE

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Workspace** Account	Account Addition Denylist	Account types, Enable/Disable	Deny for: Work email app, Samsung Accounts, Google Accounts	KNOX-11-007600, KNOX-11-017400	addAccountsToAdditionBlackList
KPE	**Workspace** Restrictions	Revocation check **OR** OCSP check	Enable/Disable	Enable	KNOX-11-022600	enableRevocationCheck enableOcspCheck
KPE	**Workspace** Certificate	Certificates	Configure	Include DoD certificates in Workspace	KNOX-11-023000	installCertificateToKeystore
KPE	**Workspace** Restrictions	User Remove Certificates	Allow/Disallow	Disallow	KNOX-11-023200	allowUserRemoveCertificates
KPE	**Workspace** Application	App installation alllowlist	List of apps	List only approved work apps	KNOX-11-001800, KNOX-11-002000	addAppPackageNameToWhiteList, addAppPackageNameToBlackList
KPE	**Workspace** Application	System app disable list	Configure	List non-AO-approved system app packages	KNOX-11-018000	setDisableApplication
KPE	**Workspace** RCP	Show detailed notifications	Allow/Disallow	Disallow	KNOX-11-002800	setAllowChangeDataSyncPolicy NOTIFICATIONS
KPE	**Workspace** RCP	Sharing clipboard to personal	Allow/Disallow	Disallow	KNOX-11-009200	allowShareClipboardDataToOwner

Table 2: Configuration Policy Rules for COBO

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Device** Password Requirements	Minimum password length	0+	6	KNOX-11-000200	setPasswordMinimumLength
KPE	**Device** Password Requirements	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric	KNOX-11-000200, KNOX-11-000600, KNOX-11-000800	**This allows for PIN code.** setPasswordQuality PASSWORD_QUALITY_NUMERIC (minimum)
KPE	**Device** Password Requirements	Maximum sequential numbers	0+	2	KNOX-11-000400	**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-11-000600	setMaximumTimeToLock
AE	**Device** Password Requirements	Max password failures for local wipe	0+	10	KNOX-11-000800	setMaximumFailedPasswordsForWipe
KPE	**Device** Password Requirements	Installs from unknown sources	Allow/Disallow	Disallow	KNOX-11-001400	setAllowNonMarketApps
KPE	**Device** Password Requirements	Trust agents	Enable/Disable	Disable	KNOX-11-004000	setKeyguardDisabledFeatures KEYGUARD_DISABLE_TRUST_AGENTS

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Device** Password Requirements	Face	Enable/Disable	Disable	KNOX-11-004200	setBiometricAuthenticationEnabled BIOMETRIC_AUTHENTICATION_FACE
KPE	**Device** Password Requirements	Debugging features	Allow/Disallow	Disallow	KNOX-11-005200	allowDeveloperMode
KPE	**Device** Password Requirements	USB file transfer	Allow/Disallow	Disallow	KNOX-11-006600, KNOX-11-007000	setUsbMediaPlayerAvailability
KPE	**Device** Wi-Fi	Unsecured hotspot	Allow/Disallow	Disallow	KNOX-11-008200	allowOpenWifiAp
KPE	**Device** Restrictions	CC mode	Enable/Disable	Enable	KNOX-11-014000, KNOX-11-020200	**Refer to Supplemental section 6.4 Common Criteria (CC) Settings.** setCCMode
KPE	**Device** Restrictions	SD Card	Enable/Disable	Disable	KNOX-11-003600	**Disable SD cards.** setSdCardState
KPE	**Device** Audit Log	Audit Log	Enable/Disable	Enable	KNOX-11-018400	enableAuditLog

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
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-11-021000	**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
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-11-002400	addBluetoothUUIDsToWhiteList addBluetoothUUIDsToBlackList activateBluetoothUUIDRestriction
N/A	User Agreement	User Agreement		Include DoD-mandated warning banner text in User Agreement	KNOX-11-006400	**Put the DoD Warning banner text in the User Agreement.** Alternative: KPE enableRebootBanner
KPE	**Device** Multiuser	Multi-user mode	Allow/Disallow	Disallow	KNOX-11-009800	**Tablet devices only** allowMultipleUsers
KPE	**Device** Application	System app disable list	Configure	List non-AO-approved system app packages	KNOX-11-018000	setDisableApplication

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Device** Restrictions	Date Time Change	Enable/Disable	Disable	KNOX-11-020600	setDateTimeChangeEnabled
AE	**Device** Enrollment Configuration	Default device enrollment	Legacy managed, Legacy managed with Legacy Workspace	Legacy managed	KNOX-11-018600	
KPE	**Device** Restrictions	Outgoing beam	Allow/Disallow	Disallow	KNOX-11-021800	allowAndroidBeam
KPE	**Device** Restrictions	Share Via List	Allow/Disallow	Disallow	KNOX-11-021400	allowShareList
KPE	**Device** Restrictions	Backup service	Allow/Disallow	Disallow	38b	setBackup
KPE	**Device** Account	Account Addition Denylist	Account types, Enable/Disable	Deny for: Work email app, Samsung Accounts, Google Accounts	KNOX-11-007600, KNOX-11-017400	addAccountsToAdditionBlackList
KPE	**Device** Restrictions	Revocation check **OR** OCSP check	Enable/Disable	Enable	KNOX-11-022600	enableRevocationCheck enableOcspCheck
KPE	**Device** Certificate	Certificates	Configure	Include DoD certificates in Workspace	KNOX-11-023000	installCertificateToKeystore

Vendor	Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
KPE	**Device** Restrictions	User Remove Certificates	Allow/Disallow	Disallow	KNOX-11-023200	allowUserRemoveCertificates
KPE	**Device** Application	App installation allowlist	List of apps	List only approved work apps	KNOX-11-001800, KNOX-11-002000	addAppPackageNameToWhiteList, addAppPackageNameToBlackList