

UNCLASSIFIED



SAMSUNG ANDROID OS 14 WITH KNOX 3.X STIG CONFIGURATION TABLES

30 January 2025

Developed by Samsung and DISA for the DOD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: Configuration Policy Rules for COBO	1
Table 2: Configuration Policy Rules for COPE	7
Table 3: KPE Equivalent APIs	13
Table 4: KSP App Separation	15

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 (KPE). To set up Samsung devices using popular UEM platforms, go to: <https://docs.samsungknox.com/admin/uem/index.htm>.

All policies listed in the document are implemented using Android Enterprise (AE) APIs. If the management tool does not implement the AE policy, a KPE API may be available to use as a substitute either directly by the management tool or via Knox Service Plugin (KSP). In this situation, look for an “*” next to the AE API in the comment of the associated policy row, which indicates a KPE substitute is available. To keep these tables as simple as possible, substitute KPE APIs will not be listed in the tables here. Refer to [Table 3](#) in this document for the full list of available substitutions.

In some cases, a KPE API could be used to allow additional features while remaining STIG compliant. Details of this are provided in the comment of the associated policy row.

Table 1: Configuration Policy Rules for COBO

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Device Enrollment Configuration	Default device enrollment	Fully managed, Work Profile for company-owned devices, Work Profile for personally owned devices	Fully managed	KNOX-14-110010	Enroll device as an Android Enterprise device.
Device User Agreement	User agreement		Include DOD-mandated warning banner text in User Agreement	KNOX-14-110020	Include the warning banner text in the User Agreement. Alternatively, but not preferred, include on the lock screen information: API: setDeviceOwnerLockScreenInfo
Device Password Policies	Minimum password quality	Unspecified, Something, Numeric,	Numeric(Complex)	KNOX-14-110030,	This allows for PIN code. API: setPasswordQuality *

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
		Numeric(Complex), Alphabetic, Alphanumeric, Complex		KNOX-14-110040	Or setRequiredPasswordComplexity If the management tool does not support Numeric(Complex) but does support Numeric , KPE can be used to achieve STIG compliance. In this case, configure this policy with value Numeric and use an additional KPE policy, (innately by management tool or via KSP) Maximum Numeric Sequence Length with value 4 .
Device Password Policies	Minimum password length	0+ characters	Six characters	KNOX-14-110050	API: setPasswordMinimumLength *
Device Password Policies	Max password failures for local wipe	0+ attempts	10 attempts	KNOX-14-110060	API: setMaximumFailedPasswordsForWipe *
Device Password Policies	Max time to screen lock	0+ minutes	15 minutes	KNOX-14-110070	API: setMaximumTimeToLock *
Device Restrictions	Face recognition	Enable/Disable	Disable	KNOX-14-110080	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
Device Restrictions	Trust agents	Enable/Disable	Disable	KNOX-14-110090	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS Or

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					setTrustAgentConfiguration
Device Restrictions	Backup service	Enable/Disable	Disable	KNOX-14-110100	API: setBackupServiceEnabled *
Device Restrictions	Debugging features	Allow/Disallow	Disallow	KNOX-14-110110	API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *
Device Restrictions	Bluetooth	Allow/Disallow	AO decision	KNOX-14-110120	Guidance is provided for Authorizing Official (AO) to approve Bluetooth. API: addUserRestriction, DISALLOW_BLUETOOTH *
Device Restrictions	Mount physical media	Allow/Disallow	Disallow	KNOX-14-110130	Not applicable for devices that do not support removable storage media. Disables use of all removable storage, e.g., SD cards, USB thumb drives. API: addUserRestriction, DISALLOW_MOUNT_PHYSICAL_MEDIA * If deployment requires the use of SD cards, KPE can be used to allow its usage in a STIG-approved configuration. In this case, do not configure this policy and instead replace with KPE policy (innately by management tool or via KSP) Enforce external storage encryption with value <code>enable</code>.
Device Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-14-110140,	DeX drag and drop file transfer capabilities will be prohibited, but all other DeX capabilities remain usable.

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
				KNOX-14-110150	API: addUserRestriction, DISALLOW_USB_FILE_TRANSFER *
Device Restrictions	Configure tethering	Allow/Disallow	Disallow	KNOX-14-110160	API: addUserRestriction, DISALLOW_CONFIG_TETHERING * If deployment requires the use of Mobile Hotspot & Tethering, KPE can be used to allow its use in a STIG-approved configuration. In this case, do not configure this policy and instead replace with KPE policy (innately by management tool or via KSP) Allow open Wi-Fi connection with value disable and add Training Topic Don't use Wi-Fi Sharing . (Refer to Supplemental document for additional information.)
Device Restrictions	Configure date/time	Allow/Disallow	Disallow	KNOX-14-110170	API: addUserRestriction, DISALLOW_CONFIG_DATE_TIME *
Device Policy Management	Certificate revocation checks	Enable/Disable	Enable	KNOX-14-125010	* KPE provides an API to check for Certificate revocation.
Device Policy Management	Certificates		Include DOD certificates in Work Profile	KNOX-14-110180	API: installCaCert *
Device Restrictions	List of approved	List of apps	List only approved work apps	KNOX-14-110190,	*

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
	apps listed in managed Google Play			KNOX-14-110200	
Device Restrictions	Hide Certain Preinstalled Apps	App package name	Only allowed work apps	TBC	API: setApplicationHidden
Device Restrictions	Input Methods	List of packages	List only approved Input Method Editor apps	TBC	API: setPermittedInputMethods
Device Restrictions	USB Data Signaling	Enable/Disable	Disable	TBC	API: setUsbDataSignalingEnabled
Device Restrictions	Nearby Notification Streaming	Policy Option	NEARBY_STREAMING_DISABLED	TBC	API: setNearbyNotificationStreamingPolicy
Device Restrictions	Nearby App Streaming	Policy Option	NEARBY_STREAMING_DISABLED	TBC	API: setNearbyAppStreamingPolicy
Device Restrictions	Unredacted notifications	Allow/Disallow	Disallow	KNOX-14-110210	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
Device Restrictions	Security logging	Enable/Disable	Enable	KNOX-14-110220	Management tool must provide means to read the log in the console. API: setSecurityLoggingEnabled *
Device Restrictions	Modify accounts	Allow/Disallow	Disallow	KNOX-14-110230, KNOX-14-110240	API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Device Restrictions	Configure credentials	Allow/Disallow	Disallow	KNOX-14-110260	API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *
Device Restrictions	Install from unknown sources globally	Allow/Disallow	Disallow	KNOX-14-110270	API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *
Device Restrictions	Common Criteria mode	Enable/Disable	Enable	KNOX-14-110280, KNOX-14-110290	API: setCommonCriteriaModeEnabled *

Table 2: Configuration Policy Rules for COPE

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Device Enrollment Configuration	Default device enrollment	Fully managed, Work Profile for company-owned devices, Work Profile for personally owned devices	Work Profile for company-owned devices	KNOX-14-210010	Enroll device as an Android Enterprise device.
Device User Agreement	User agreement		Include DOD-mandated warning banner text in User Agreement	KNOX-14-210020	<p>Include the warning banner text in the User Agreement.</p> <p>Alternatively, but not preferred, include on the Lock screen information:</p> <p>API: <code>setDeviceOwnerLockScreenInfo</code></p>
Device Password Policies	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric(Complex)	KNOX-14-210030, KNOX-14-210040	<p>This allows for PIN code.</p> <p>API: <code>setPasswordQuality</code></p> <p>Or</p> <p><code>setRequiredPasswordComplexity</code></p> <p>If the management tool does not support Numeric(Complex) but does support Numeric, KPE can be used to achieve STIG compliance. In this case, configure this policy with value Numeric and use an additional KPE policy (natively by management tool or via KSP)</p>

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					Maximum Numeric Sequence Length with value 4 .
Device Password Policies	Minimum password length	0+ characters	Six characters	KNOX-14-210050	API: setPasswordMinimumLength
Device Password Policies	Max password failures for local wipe	0+	10 attempts	KNOX-14-210060	API: setMaximumFailedPasswordsForWipe
Device Password Policies	Max time to screen lock	0+ minutes	15 minutes	KNOX-14-210070	API: setMaximumTimeToLock
Device Restrictions	Face recognition	Enable/Disable	Disable	KNOX-14-210080	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
Device Restrictions	Trust agents	Enable/Disable	Disable	KNOX-14-210090	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS Or setTrustAgentConfiguration
Device Restrictions	Debugging features	Allow/Disallow	Disallow	KNOX-14-210110	API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *
Device Restrictions	Bluetooth	Allow/Disallow	AO decision	KNOX-14-210120	Guidance is provided for AO to approve Bluetooth. API: addUserRestriction, DISALLOW_BLUETOOTH *

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Device Restrictions	Mount physical media	Allow/Disallow	Disallow	KNOX-14-210130	<p>Not applicable for devices that do not support removable storage media.</p> <p>Disables use of all removable storage, e.g., SD cards and USB thumb drives.</p> <p>API: addUserRestriction, DISALLOW_MOUNT_PHYSICAL_MEDIA *</p> <p>If deployment requires the use of SD cards, KPE policy can be used to allow its usage in a STIG-approved configuration. In this case, do not configure this policy and instead replace with KPE policy (innately by management tool or via KSP) Enforce external storage encryption with value enable.</p>
Device Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-14-210140, KNOX-14-210150	<p>DeX drag-and-drop file transfer capabilities will be prohibited, but all other DeX capabilities remain usable.</p> <p>API: addUserRestriction, DISALLOW_USB_FILE_TRANSFER *</p>
Device Restrictions	Configure tethering	Allow/Disallow	Disallow	KNOX-14-210160	<p>API: addUserRestriction, DISALLOW_CONFIG_TETHERING *</p> <p>If deployment requires the use of Mobile Hotspot & Tethering, KPE policy can be</p>

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					used to allow its usage in a STIG-approved configuration. In this case, do not configure this policy, and instead replace with KPE policy (innately by management tool or via KSP) Allow open Wi-Fi connection with value disable and add Training Topic Don't use Wi-Fi Sharing (see supplemental document for additional information)
Device Restrictions	Configure date/time	Allow/Disallow	Disallow	KNOX-14-210170	API: addUserRestriction, DISALLOW_CONFIG_DATE_TIME *
Work Profile Policy Management	Certificates		Include DOD certificates in work profile	KNOX-14-210180	API: installCaCert *
Work Profile Policy Management	Certificate revocation checks	Enable/Disable	Enable	KNOX-14-225010	* KPE provides an API to check for Certificate revocation.
Work Profile Restrictions	List of approved apps listed in managed Google Play	List of apps	List only approved work apps	KNOX-14-210190, KNOX-14-210200	*
Work Profile Restrictions	Hide Certain Preinstalled Apps	App package name	Only allowed work apps	TBC	API: setApplicationHidden
Work Profile Restrictions	Configure Chrome Autofill	ON/OFF	"PasswordManager Enabled"="OFF"	TBC	API: setApplicationRestrictions

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
			"AutofillAddressEnabled"="OFF" "AutofillCreditCardEnabled"="OFF"		
Work Profile Restrictions	Configure Autofill	Allow/Disallow	Disallow	TBC	API: addUserRestriction, DISALLOW_AUTOFILL
Work Profile Restrictions	Input Methods	List of packages	List only approved Input Method Editor apps	TBC	API: setPermittedInputMethods
Work Profile Restrictions	USB Data Signaling	Enable/Disable	Disable	TBC	API: setUsbDataSignalingEnabled
Work Profile Restrictions	Nearby Notification Streaming	Policy Option	NEARBY_STREAMING_DISABLED	TBC	API: setNearbyNotificationStreamingPolicy
Work Profile Restrictions	Nearby App Streaming	Policy Option	NEARBY_STREAMING_DISABLED	TBC	API: setNearbyAppStreamingPolicy
Work Profile Restrictions	Unredacted notifications	Allow/Disallow	Disallow	KNOX-14-210210	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
Work Profile Restrictions	Security logging	Enable/Disable	Enable	KNOX-14-210220	Management tool must provide means to read the Log in the console. API: setSecurityLoggingEnabled *
Work Profile Restrictions	Modify accounts	Allow/Disallow	Disallow	KNOX-14-210230, KNOX-14-210240	API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *
Work Profile Restrictions	Cross profile copy/paste	Allow/Disallow	Disallow	KNOX-14-210250	API: addUserRestriction, DISALLOW_CROSS_PROFILE_COPY_PASTE

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Work Profile Restrictions	Configure credentials	Allow/Disallow	Disallow	KNOX-14-210260	API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *
Work Profile Restrictions	Install from unknown sources globally	Allow/Disallow	Disallow	KNOX-14-210270	API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *
Work Profile Restrictions	Common Criteria mode	Enable/Disable	Enable	KNOX-14-210280 KNOX-14-210290	API: setCommonCriteriaModeEnabled *

Table 3: KPE Equivalent APIs

STIG LISTED AE API	Values	Available KPE Substitute API Available in Case of Management Tool Not Supporting AE API
addUserRestriction	DISALLOW_BLUETOOTH	RestrictionPolicy allowBluetooth
	DISALLOW_CONFIG_CREDENTIALS	CertificatePolicy allowUserRemoveCertificates
	DISALLOW_CONFIG_DATE_TIME	DateTimePolicy setDateTimeChangeEnabled
	DISALLOW_CONFIG_TETHERING	RestrictionPolicy setTethering Alternatively: WiFiPolicy allowOpenWifiAp
	DISALLOW_DEBUGGING_FEATURES	RestrictionPolicy allowDeveloperMode
	DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY	RestrictionPolicy setAllowNonMarketApps
	DISALLOW_MODIFY_ACCOUNTS	DeviceAccountPolicy addAccountsToAdditionBlackList
	DISALLOW_MOUNT_PHYSICAL_MEDIA	RestrictionPolicy setSdCardState Alternatively: DeviceSecurityPolicy setExternalStorageEncryption
	DISALLOW_USB_FILE_TRANSFER	RestrictionPolicy setUsbMediaPlayerAvailability
N/A	N/A	CertificatePolicy enableRevocationCheck
installCaCert	DOD Root and Intermediate Certs	CertificateProvisioning installCertificateToKeystore

STIG LISTED AE API	Values	Available KPE Substitute API Available in Case of Management Tool Not Supporting AE API
managed Google Play	List only approved work apps	ApplicationPolicy addAppPackageNameToWhiteList, ApplicationPolicy addAppPackageNameToBlackList, ApplicationPolicy addAppSignatureToWhiteList, ApplicationPolicy addAppSignatureToBlackList
setBackupServiceEnabled	FALSE	RestrictionPolicy setBackup
setCommonCriteriaModeEnabled	TRUE	AdvancedRestrictionPolicy setCCMode
setMaximumFailedPasswordsForWipe	10	BasePasswordPolicy setMaximumFailedPasswordsForWipe
setMaximumTimeToLock	900	BasePasswordPolicy setMaximumTimeToLock
setPasswordMinimumLength	6	BasePasswordPolicy setPasswordMinimumLength
setPasswordQuality	Numeric(Complex)	BasePasswordPolicy setPasswordQuality Alternatively: PasswordPolicy setMaximumNumericSequenceLength(2) with password quality of Numeric.
setSecurityLoggingEnabled	TRUE	AuditLog enableAuditLog

To implement the Knox app separation feature, the policies listed in Table 1: Configuration Policy Rules for COBO must be used in conjunction with the policies listed in the following table:

Table 4: KSP App Separation

Policy Group	Policy Rule	KSP Policy Mapping
App Separation	Location	<ol style="list-style-type: none">1. App Sep Policies.2. Enable App Sep Policies [enable].3. Allow Listing Policies.4. Set Location [inside or outside].
App Separation	App List	<ol style="list-style-type: none">1. App Sep Policies.2. Enable App Sep Policies [enable].3. Allow Listing Policies.4. Configure Apps List [list of packages].