

UNCLASSIFIED



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

**10 November 2023**

**Developed by Samsung and DISA for the DOD**

UNCLASSIFIED

## LIST OF TABLES

	<b>Page</b>
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
<b>Device Enrollment Configuration</b>	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.
<b>Device User Agreement</b>	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

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
<b>Device Password Policies</b>	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric(Complex)	KNOX-14-110030, KNOX-14-110040	This allows for PIN code.  API: setPasswordQuality *  Or  setRequiredPasswordComplexity  If the management tool does not support <b>Numeric(Complex)</b> but does support <b>Numeric</b> , KPE can be used to achieve STIG compliance. In this case, configure this policy with value <b>Numeric</b> and use an additional KPE policy, (innately by management tool or via KSP) <b>Maximum Numeric Sequence Length</b> with value <b>4</b> .
<b>Device Password Policies</b>	Minimum password length	0+ characters	Six characters	KNOX-14-110050	API: setPasswordMinimumLength *
<b>Device Password Policies</b>	Max password failures for local wipe	0+ attempts	10 attempts	KNOX-14-110060	API: setMaximumFailedPasswordsForWipe *
<b>Device Password Policies</b>	Max time to screen lock	0+ minutes	15 minutes	KNOX-14-110070	API: setMaximumTimeToLock *
<b>Device Restrictions</b>	Face recognition	Enable/Disable	Disable	KNOX-14-110080	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
<b>Device Restrictions</b>	Trust agents	Enable/Disable	Disable	KNOX-14-110090	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					Or  setTrustAgentConfiguration
<b>Device Restrictions</b>	Backup service	Enable/Disable	Disable	KNOX-14-110100	API: setBackupServiceEnabled *
<b>Device Restrictions</b>	Debugging features	Allow/Disallow	Disallow	KNOX-14-110110	API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *
<b>Device Restrictions</b>	Bluetooth	Allow/Disallow	AO decision	KNOX-14-110120	Guidance is provided for Authorizing Official (AO) to approve Bluetooth.  API: addUserRestriction, DISALLOW_BLUETOOTH *
<b>Device Restrictions</b>	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) <b>Enforce external storage encryption with value enable.</b>

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Device Restrictions	USB file transfer	Allow/Disallow	Disallow	KNOX-14-110140, KNOX-14-110150	DeX drag and drop file transfer capabilities will be prohibited, but all other DeX capabilities remain usable.  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) <b>Allow open Wi-Fi connection</b> with value <b>disable</b> and add Training Topic <b>Don't use Wi-Fi Sharing</b> . (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	Certificates		Include DOD certificates in Work Profile	KNOX-14-110180	API: installCaCert *
Device Restrictions	List of approved apps listed	List of apps	List only approved work apps	KNOX-14-110190,	*

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
	in managed Google Play			KNOX-14-110200	
<b>Device Restrictions</b>	Hide Certain Preinstalled Apps	App package name	Only allowed work apps	TBC	API: setApplicationHidden
<b>Device Restrictions</b>	Input Methods	List of packages	List only approved Input Method Editor apps	TBC	API: setPermittedInputMethods
<b>Device Restrictions</b>	USB Data Signaling	Enable/Disable	Disable	TBC	API: setUsbDataSignalingEnabled
<b>Device Restrictions</b>	Nearby Notification Streaming	Policy Option	NEARBY_STREAMING_DISABLED	TBC	API: setNearbyNotificationStreamingPolicy
<b>Device Restrictions</b>	Nearby App Streaming	Policy Option	NEARBY_STREAMING_DISABLED	TBC	API: setNearbyAppStreamingPolicy
<b>Device Restrictions</b>	Unredacted notifications	Allow/Disallow	Disallow	KNOX-14-110210	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
<b>Device Restrictions</b>	Security logging	Enable/Disable	Enable	KNOX-14-110220	Management tool must provide means to read the log in the console.  API: setSecurityLoggingEnabled *
<b>Device Restrictions</b>	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
<b>Device Enrollment Configuration</b>	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.
<b>Device User Agreement</b>	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>
<b>Device Password Policies</b>	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 <b>Numeric(Complex)</b> but does support <b>Numeric</b>, KPE can be used to achieve STIG compliance. In this case, configure this policy with value <b>Numeric</b> and use an additional KPE policy (natively by management tool or via KSP)</p>

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					<b>Maximum Numeric Sequence Length</b> with value <b>4</b> .
<b>Device Password Policies</b>	Minimum password length	0+ characters	Six characters	KNOX-14-210050	API: setPasswordMinimumLength
<b>Device Password Policies</b>	Max password failures for local wipe	0+	10 attempts	KNOX-14-210060	API: setMaximumFailedPasswordsForWipe
<b>Device Password Policies</b>	Max time to screen lock	0+ minutes	15 minutes	KNOX-14-210070	API: setMaximumTimeToLock
<b>Device Restrictions</b>	Face recognition	Enable/Disable	Disable	KNOX-14-210080	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
<b>Device Restrictions</b>	Trust agents	Enable/Disable	Disable	KNOX-14-210090	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS  Or  setTrustAgentConfiguration
<b>Device Restrictions</b>	Debugging features	Allow/Disallow	Disallow	KNOX-14-210110	API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *
<b>Device Restrictions</b>	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
<b>Device Restrictions</b>	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) <b>Enforce external storage encryption</b> with value <b>enable</b>.</p>
<b>Device Restrictions</b>	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>
<b>Device Restrictions</b>	Configure tethering	Allow/Disallow	Disallow	KNOX-14-210160	<p>API: addUserRestriction, DISALLOW_CONFIG_TETHERING *</p> <p>If deployment requires the use of Mobile Hotspot &amp; 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) <b>Allow open Wi-Fi connection</b> with value <b>disable</b> and add Training Topic <b>Don't use Wi-Fi Sharing</b> (see supplemental document for additional information)
<b>Device Restrictions</b>	Configure date/time	Allow/Disallow	Disallow	KNOX-14-210170	API: addUserRestriction, DISALLOW_CONFIG_DATE_TIME *
<b>Work Profile Policy Management</b>	Certificates		Include DOD certificates in work profile	KNOX-14-210180	API: installCaCert *
<b>Work Profile Restrictions</b>	List of approved apps listed in managed Google Play	List of apps	List only approved work apps	KNOX-14-210190, KNOX-14-210200	*
<b>Work Profile Restrictions</b>	Hide Certain Preinstalled Apps	App package name	Only allowed work apps	TBC	API: setApplicationHidden
<b>Work Profile Restrictions</b>	Configure Chrome Autofill	ON/OFF	"PasswordManager Enabled"="OFF" "AutofillAddressEnabled"="OFF" "AutofillCreditCard Enabled"="OFF"	TBC	API: setApplicationRestrictions

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
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
Work Profile Restrictions	Configure credentials	Allow/Disallow	Disallow	KNOX-14-210260	API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
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
<b>addUserRestriction</b>	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
<b>installCaCert</b>	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
<b>managed Google Play</b>	List only approved work apps	ApplicationPolicy addAppPackageNameToWhiteList, ApplicationPolicy addAppPackageNameToBlackList, ApplicationPolicy addAppSignatureToWhiteList, ApplicationPolicy addAppSignatureToBlackList
<b>setBackupServiceEnabled</b>	FALSE	RestrictionPolicy setBackup
<b>setCommonCriteriaModeEnabled</b>	TRUE	AdvancedRestrictionPolicy setCCMode
<b>setMaximumFailedPasswordsForWipe</b>	10	BasePasswordPolicy setMaximumFailedPasswordsForWipe
<b>setMaximumTimeToLock</b>	900	BasePasswordPolicy setMaximumTimeToLock
<b>setPasswordMinimumLength</b>	6	BasePasswordPolicy setPasswordMinimumLength
<b>setPasswordQuality</b>	Numeric(Complex)	BasePasswordPolicy setPasswordQuality  Alternatively: PasswordPolicy setMaximumNumericSequenceLength(2) with password quality of Numeric.
<b>setSecurityLoggingEnabled</b>	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"><li>1. App Sep Policies.</li><li>2. Enable App Sep Policies [enable].</li><li>3. Allow Listing Policies.</li><li>4. Set Location [inside or outside].</li></ol>
App Separation	App List	<ol style="list-style-type: none"><li>1. App Sep Policies.</li><li>2. Enable App Sep Policies [enable].</li><li>3. Allow Listing Policies.</li><li>4. Configure Apps List [list of packages].</li></ol>