SAMSUNG ANDROID OS 14 BRING YOUR OWN APPROVED DEVICE (BYOAD) CONFIGURATION TABLES

13 March 2024

Developed by Samsung and DISA for the DOD

LIST OF TABLES

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 AE APIs. If the management tool does not implement the AE policy, it may be possible there is a KPE API that could be used as a substitute – either directly by the management tool, or via 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. In an effort 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 Work Profile for Employee-Owned Devices (BYOD)

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 employee-owned devices	Work Profile for employee-owned devices	KNOX-14-710010	Android work profile for employee-owned devices (BYOD).
Device User Agreement	User agreement		Include DOD-mandated warning banner text in User Agreement	KNOX-14-710020	Include the warning banner text in the User Agreement.
Device Password Policies	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic,	Numeric(Complex)	KNOX-14-710030	This allows for PIN code. API: setPasswordQuality Or

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
		Alphanumeric, Complex			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 - natively by management tool or via KSP - **Maximum Numeric Sequence Length** with value **4**.
Device Password Policies	Minimum password length	0+ characters	Six characters	KNOX-14-710050	API: setPasswordMinimumLength
Device Password Policies	Max password failures for local wipe	0+	10 attempts	KNOX-14-710060	API: setMaximumFailedPasswordsForWipe
Device Password Policies	Max time to screen lock	0+ minutes	15 minutes	KNOX-14-710070	API: setMaximumTimeToLock
Device Restrictions	Face recognition	Enable/Disable	Disable	KNOX-14-710080	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
Device Restrictions	Trust agents	Enable/Disable	Disable	KNOX-14-710090	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS Or setTrustAgentConfiguration
Work Profile Policy Management	Certificates	Enable/Disable	Enable	KNOX-14-725010	*

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					KPE provides an API to check for Certificate revocation: CertificatePolicy enableRevocationCheck
Work Profile Policy Management	Certificates		Include DOD certificates in work profile	KNOX-14-710180	API: installCaCert *
Work Profile Restrictions	List of approved apps listed in managed Google Play	List of apps	List only approved work apps	KNOX-14-710190, KNOX-14-710200	*
Work Profile Restrictions	Hide Certain Preinstalled Apps	App package name	Only allowed work apps	KNOX-14-725030	API: setApplicationHidden
Work Profile Restrictions	Configure Chrome Autofill	ON/OFF	“PasswordManager Enabled”=”OFF” "AutofillAddressEnabled"=”OFF” "AutofillCreditCard Enabled"=”OFF”	KNOX-14-725050	API: setApplicationRestrictions
Work Profile Restrictions	Configure Autofill	Allow/Disallow	Disallow	KNOX-14-725060	API: addUserRestriction, DISALLOW_AUTOFILL
Work Profile Restrictions	Input Methods	List of packages	List only approved Input Method Editor apps	KNOX-14-725070	API: setPermittedInputMethods
Work Profile Restrictions	Unredacted notifications	Allow/Disallow	Disallow	KNOX-14-710210	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
Work Profile Restrictions	Modify accounts	Allow/Disallow	Disallow	KNOX-14-710230, KNOX-14-710240	API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Work Profile Restrictions	Cross profile copy/paste	Allow/Disallow	Disallow	KNOX-14-710250	API: addUserRestriction, DISALLOW_CROSS_PROFILE_COPY_PASTE
Work Profile Restrictions	Configure credentials	Allow/Disallow	Disallow	KNOX-14-710260	API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *
Work Profile Restrictions	Install from unknown sources globally	Allow/Disallow	Disallow	KNOX-14-710270	API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *

Table 2: KPE Equivalent APIs

STIG LISTED AE API	Values	Available KPE Substitute API Available in Case of Management Tool Not Supporting AE API
addUserRestriction	DISALLOW_CONFIG_CREDENTIALS	CertificatePolicy allowUserRemoveCertificates
	DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY	RestrictionPolicy setAllowNonMarketApps
	DISALLOW_MODIFY_ACCOUNTS	DeviceAccountPolicy addAccountsToAdditionBlackList
N/A	N/A	CertificatePolicy enableRevocationCheck
installCaCert	DOD Root and Intermediate Certs	CertificateProvisioning installCertificateToKeystore
managed Google Play	List only approved work apps	ApplicationPolicy addAppPackageNameToWhiteList, ApplicationPolicy addAppPackageNameToBlackList, ApplicationPolicy addAppSignatureToWhiteList,

STIG LISTED AE API	Values	Available KPE Substitute API Available in Case of Management Tool Not Supporting AE API
		ApplicationPolicy addAppSignatureToBlackList
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.