

UNCLASSIFIED



SAMSUNG ANDROID OS 7 WITH KNOX 2.x STIG CONFIGURATION TABLES

Version 1, Release 6

25 October 2019

Developed by Samsung and DISA for the DoD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: Configuration Policy Rules for Non-Work Environment.....	1
Table 2: Configuration Policy Rules for Work Environment Container	14
Table 3: Samsung API for Each MDM Policy Rule.....	20

Note: The logic of some of the configuration settings in the following tables may differ from one MDM product to another. For example, the policy rule "Disable Manual Date Time Changes" may appear as "Allow Manual Date Time Changes" in some MDM consoles. In this case the rule should be set to "Disable" instead of "Enable" as indicated on page 2 below.

Table 1: Configuration Policy Rules for Non-Work Environment

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Advanced Restrictions	Enable CC Mode	Enable/Disable	X		Enable	KNOX-07-006600, KNOX-07-011600	Puts the devices in (Common Criteria) CC Mode as defined by the Samsung Galaxy Device MDFPP Security Target. If the configuration is not available on the MDM console, install the Samsung CC Mode Android Application Package File (APK) and enable CC Mode. The APK is available on Google Play.
Android Restrictions	Allow Developer Mode	Select/Not Select	X		Not Select	KNOX-07-003700	
Android Restrictions	Allow Location	Enable/Disable		X	Enable (GPS, Wi-Fi, Cellular)		
Android Restrictions	Allow Camera	Select/Not Select		X	Not Select		
Android Restrictions	Allow Microphone	Select/Not Select		X	Not Select		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Advanced Restrictions	Prevent New Admin Install	Select/Not Select	X		Select	KNOX-07-012400	
Android Date Time	Date Time Change Enabled	Select/Not Select	X		Not Select	KNOX-07-013100	
Android Applications	Disable Android Market	Enable/Disable	X		Enable	KNOX-07-001100	This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Restrictions	Allow Install Non Market App	Select/Not Select	X		Not Select	KNOX-07-001200	
Android Applications	Package Name White List	Configure	X		Add Approved Packages	KNOX-07-001400	This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Applications	Signature White List	Configure	X		Add Approved Signatures	KNOX-07-001400	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Applications	Package Name Black List	Configure	X		Add All Packages	KNOX-07-012500	All packages specified by wildcard (.*). When all apps are blacklisted, only apps on the whitelist are allowed. This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Applications	Signature Black List	Configure	X		Add All Signatures	KNOX-07-012500	All signatures specified by wildcard (.*). When all apps are blacklisted, only apps on the whitelist are allowed. This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Applications	Application uninstallation disable list	Configure		X	Add Packages		List of applications that the user cannot uninstall. This list is site specific.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Applications	Application disable list	Configure	X		Add Unapproved Packages	KNOX-07-018400	The systems administrator should identify all pre-installed applications that are not approved and disable them (see Tables 6-1 through 6-3 in the STIG Supplemental document). In addition, applications with features included in KNOX-07-001600/001700/1800/1900/2000/2200 should be disabled. KNOX-07-001600/1800/1900/2000/2200 are Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Browser	Allow Cookies	Select/Not Select		X	Select		Native browser application only
Android Browser	Allow Auto-Fill	Select/Not Select		X	Select		Native browser application only
Android Browser	Allow Java Script	Select/Not Select		X	Select		Native browser application only
Android Browser	Allow Popups	Select/Not Select		X	Not Select		Native browser application only

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restrictions	Enable CAC authentication for browser	Enable/Disable		X	Enable		Native browser application only
Android Restrictions	Allow Google Accounts Auto Sync	Select/Not Select	X		Not Select	KNOX-07-004900	
Android Restrictions	Allow Google Crash Report	Select/Not Select	X		Not Select	KNOX-07-005700	
Android Restrictions	Enable CAC authentication for email	Enable/Disable		X	Enable		This affects non-container email only.
Android Security	Storage Encryption	Enable/Disable	X		Enable	KNOX-07-002800	Encrypt all user and enterprise data at rest.
Android Security	External Storage Encryption	Enable/Disable	X		Enable	KNOX-07-003000	Encrypt all external media cards.
Android Restrictions	Copy contacts to SIM	Enable/Disable		X	Disable		
Android VPN	VPN	Configure	X		See Comments	KNOX-07-017100, KNOX-07-017120	Configure in one of the following configurations: -Disabled -Configured for per app use for the personal side
Android VPN	Add Packages To VPN	Configure	X		See Comments	KNOX-07-017120	Required if “Configured for per app use for the personal side” option is selected
Android Password Restrictions	Maximum Failed Attempts for wipe	0-	X		10	KNOX-07-000600	Unsuccessful logon attempts before device wipe

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Password Restrictions	Minimum Length	0-	X		6	KNOX-07-000100	Minimum device password length
Android Password Restrictions	Minimum Password Complexity	None Pattern PinAlphabetic Alphanumeric ComplexBiometric	X		PIN Alphabetic Alphanumeric or Complex	KNOX-07-018600	Device password complexity PIN recommended Some MDM consoles may display “Numeric” and “Numeric-Complex” instead of “PIN”. Either selection is acceptable but “Numeric-Complex” is recommended. Alphabetic, Alphanumeric, and Complex are also acceptable selections but these selections will cause the user to select a complex password, which is not required by the STIG.
Android Password Restrictions	Password Expires (days)	0-		X	0		Days after which password must be changed Value 0 will reset this policy and no expiry will be applied.
Android Password Restrictions	Maximum Time to Lock	0-	X		15	KNOX-07-000500	Minutes of inactivity after which device will lock

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Password Restrictions	Minimum Uppercase	0-		X	0		Minimum number of uppercase alphabetic characters in device password
Android Password Restrictions	Minimum Lowercase	0-		X	0		Minimum number of lowercase alphabetic characters in device password
Android Password Restrictions	Minimum Numeric	0-		X	0		Minimum number of numeric characters in device password
Android Password Restrictions	Minimum Mutation on Change	0-		X	0		Minimum number of characters that must be changed when device password is changed
Android Password Restrictions	Maximum Sequential Characters	0-	X		2	KNOX-07-000200	Max number of sequential characters in device password
Android Password Restrictions	Maximum Sequential Numbers	0-	X		2	KNOX-07-000200	Max number of sequential numbers in device password
Android Password Restrictions	Fingerprint	Select/Not Select		X	Select		Fingerprint for Lock screen authentication
Android Password Restrictions	Disable Keyguard Trust Agents	Select/Not Select	X		Select	KNOX-07-003300	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Applications	Disable Face Recognition	Enable/Disable	X		Disable	KNOX-07-017400	This policy is implemented using Disable Application policies. See STIG requirement for more information.
Android Password Restrictions	Iris	Select/Not Select		X	Select		Iris scan for Lock screen authentication
Android Security	DoD Banner	Enable/Disable	X		Enable	KNOX-07-004300	The administrator can configure enterprise-specific banner text. If enabled without configuring any text, the device will display a default text that matches the required DoD banner.
Android Certificate	Certificate	Configure	X		Add Certificates	KNOX-07-012300	Select PEM encoded representations of the DoD root and intermediate certificates.
Android Certificate	Certificate Revocation Check (CRL)	Enable/Disable	X		Enable	KNOX-07-013000	Enable revocation check on all packages using the string: "*" (asterisk).
Android Restrictions	Disable USB Media Player	Select/Not Select	X		Select	KNOX-07-004500, KNOX-07-004700	Disabling USB Media Player will also disable USB MTP, USB mass storage, USB vendor protocol (KIES).

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Bluetooth	Allowed Bluetooth Profiles	HSP HFP PBAP A2DP AVRCP SPP NAP BNEP HID BPP DUN SAP	X		HFP HSP SPP	KNOX-07-002400	Disables all Bluetooth profiles except for those specified in the settings.
Android Restrictions	Allow Wi-Fi Tethering	Select/Not Select		X	Not Select		The systems administrator shall select the setting based on local policy.
Android Restrictions	Allow Bluetooth Tethering	Select/Not Select		X	Not Select		The systems administrator shall select the setting based on local policy.
Android Restrictions	Allow USB host storage	Select/Not Select	X		Not Select	KNOX-07-012600	USB host storage allows the device to mount external USB drives.
Android Restrictions	Allow Screen Capture	Select/Not Select		X	Select		
Android Restrictions	Allow Google Backup	Select/Not Select	X		Not Select	KNOX-07-004900	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Knox Management	Knox License	Configure		X	Enterprise issued Knox license		Proper configuration of the Knox license ensures reporting information is sent to the correct enterprise servers.
Android MultiUser	Allow multi-user mode	Select/Not Select	X		No Select	KNOX-07-006100	
Android Applications	Allow Cloud backup	Select/Not Select	X		Not Select	KNOX-07-001600	This policy is implemented using Disable Application policies. See STIG requirement for more information. This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Restrictions	Allow S Voice	Enable/Disable	X		Disable	KNOX-07-012700	This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Applications	Allow mobile payment	Enable/Disable		X	Disable		This policy is implemented using Disable Application policies. See STIG requirement for more information.
Android Restrictions	Allow NFC	Select/Not Select		X	Not Select		

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Accounts	Account whitelist	Configure		X	Approved accounts		The idea is to use combination of Account Whitelist and Account Blacklist policies to control what email accounts a user is allowed to configure on the device in the non-work environment. Configure by adding the domain of email accounts.
Android Accounts	Account blacklist			X	.* (wildcard)		Configure by blacklisting all domains. Then only accounts on the whitelist are allowed.
Android Applications	Allow Samsung Accounts	Enable/Disable	X		Disable	KNOX-07-001600	This policy is implemented using Disable Application policies. See STIG requirement for more information. This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Restrictions	Allow FOTA	Select/Not Select	X		Not Select	KNOX-07-006300	Disables automatic firmware updates.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Restrictions	Notifications on lock screen	Show content Hide content Do not show notifications	X		Hide content or Do not show notifications	KNOX-07-002600	This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android Restrictions	Allow Admin Remove	Select/Not Select	X		Not Select	KNOX-07-012900	
Android Restrictions	Allow Google Accounts Auto Sync	Select/Not Select	X		Not Select	KNOX-07-004950	This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android AuditLog	Enable Audit Log	Select/Not Select	X		Select/Not Select	KNOX-07-018800	
Android Applications	Disable Bixby	Enable/Disable	X		Disable	KNOX-07-017800	This policy is implemented using Disable Application policies. See STIG requirement for more information. This requirement is Not Applicable if the AO has approved unmanaged personal space/container (COPE use case).
Android WiFi	Allow Unsecured Hotspot	Select/Not Select	X		Not Select	KNOX-07-005100	

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Android Applications	Battery optimizations modes Whitelist	Configure	X		Add MDM Client	KNOX-07-018200	
Android Applications	Allow Share Via List	Select / Not Select		X	Select		

Table 2: Configuration Policy Rules for Work Environment Container

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Password Restrictions	Minimum Mutation on Change	0-		X	0		Minimum number of characters that must be changed when container password is changed.
Container Password Restrictions	Minimum Length	0-	X		4	KNOX-07-013200	Minimum container password length
Container Password Restrictions	Maximum Time to Lock	0-	X		15	KNOX-07-012200	Minutes of inactivity after which container will lock
Container Password Restrictions	Maximum Failed Attempts for wipe	0-	X		10	KNOX-07-013400	Unsuccessful logon attempts before container wipe
Container Password Restrictions	Password Expires (days)	0-		X	0		Days after which password must be changed
Container Password Restrictions	Maximum Sequential Characters	0-	X		2	KNOX-07-000300	Max number of sequential characters in device password
Container Password Restrictions	Maximum Sequential Numbers	0-	X		2	KNOX-07-000300	Max number of sequential numbers in device password

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Password Restrictions	Minimum Password Complexity	Alphanumeric Complex	X		PIN PIN Alphabetic Alphanumeric or Complex	KNOX-07-914500	Workspace password complexity PIN recommended Some MDM consoles may display “Numeric” and “Numeric-Complex” instead of “PIN”. Either selection is acceptable but “Numeric-Complex” is recommended. Alphabetic, Alphanumeric, and Complex are also acceptable selections but these selections will cause the user to select a complex password, which is not required by the STIG.
Container Restrictions	Allow camera	Select/Not Select		X	Not Select		Camera use inside container. In KNOX 2.0, disabling the camera outside will also disable the camera inside.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Accounts	Account whitelist	Configure	X		Approved accounts	KNOX-07-014300	The idea is to use a combination of these policies to control what accounts a user is allowed to configure on the device. Configure by adding the domain of agency email accounts.
Container Accounts	Account blacklist		X		.* (wildcard)	KNOX-07-014400	Configure by blacklisting all domains. When all apps are blacklisted, only accounts on the whitelist are allowed.
Container Restrictions	Allow account addition	Enable/Disable		X	Enable		Allows user to add email accounts inside container. Configuration determined by local policy.
Container Restrictions	Allow calendar info outside container	Enable/Disable	X		Disable	KNOX-07-013300	Sharing of container calendar events to outside calendar
Container Restrictions	Allow contact info outside container	Enable/Disable	X		Disable	KNOX-07-013500	Sharing of container contacts to outside contacts
Container Restrictions	Allow Show detailed notifications	Enable/Disable	X		Disable	KNOX-07-013600	Display details of container application notifications when user is outside container.
Container Restrictions	Allow cookies	Select/Not Select		X	Not Select		Container native browser application only
Container Restrictions	Allow Auto-Fill	Select/Not Select	X		Not Select	KNOX-07-014200	Container native browser application only

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Restrictions	Allow JavaScript	Select/Not Select		X	Not Select		Container native browser application only
Container Restrictions	Allow popups	Select/Not Select		X	Not Select		Container native browser application only
Container Application	Application White List	Configure	X		Add Approved Packages	KNOX-07-001500	Configure by setting the list of only DoD-approved applications.
Container Application	Signature White List	Configure	X		Add Approved Signatures	KNOX-07-001500	
Container Application	Application Black List	Configure	X		Add All Packages	KNOX-07-013700	All packages specified by wildcard (*.*)
Container Application	Application uninstallation disable list	Configure		X	Add Packages		List of applications that the user cannot uninstall
Container Application	Move Applications to Container	Enable/Disable	X		Disable	KNOX-07-013800	Blocks users from moving installed applications (outside container) to the container. By default this is disabled and can only be enabled by the admin.
Container Application	Move Files from Container to Personal	Enable/Disable	X		Disable	KNOX-07-013900	Blocks users from moving files from container. By default "from" is disabled and can only be changed by the admin.

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Container Application	Application disable list	Configure	X		Add Packages	KNOX-07-014100	The systems administrator should identify all pre-installed applications that are not approved and disable them.
Container Management	Enable container	Enable/Disable	X		Enable	KNOX-07-005500, KNOX-07-012800	
Container VPN	VPN	Configure		X	See Comments	KNOX-07-017110	Configured for container use only
Container VPN	Add All Container Packages To VPN	Select/Unselect	X		Select		Required when device VPN is configured for container use only.
Android Container Firewall	Proxy	Configure		X	Add Proxy		Configure a proxy to force all container traffic to be routed to the proxy. The system administrator should configure only if needed by local network.
Container Restrictions	Allow screen capture	Select/Not Select		X	Select		
Container Application	Allow Samsung Accounts	Enable/Disable	X		Disable	KNOX-07-014100	This policy is implemented using Disable Application policies. See STIG requirement for more information.

The following table lists the Samsung management APIs for each Policy Rule listed in Tables 1 and 2 above.

Table 3: Samsung API for Each MDM Policy Rule

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
AdvancedRestrictionPolicy	setCCMode(boolean)		TRUE	X		
RestrictionPolicy	allowDeveloperMode(boolean allow)		FALSE	X		
LocationPolicy	setLocationProviderState(String provider, boolean enable)		provider=gps,network,passive? Enable=TRUE	X		
RestrictionPolicy	setCameraState(boolean enable)		FALSE	X		
RestrictionPolicy	setMicrophoneState(boolean enable)		FALSE	X		
AdvancedRestrictionPolicy	preventNewAdminInstallation(boolean prevent)		TRUE	X		
DateTimePolicy	setDateTimeChangeEnabled(boolean)		FALSE	X		
ApplicationPolicy	disableAndroidMarket()		NA	X		
RestrictionPolicy	setAllowNonMarketApps(boolean)		FALSE	X		
ApplicationPolicy	addAppPackageNameToWhiteList(String packageName)	X		X		
ApplicationPolicy	addAppPackageNameToWhiteList(String packageName, boolean defaultBlackList)	X	If 'defaultBlackList' is TRUE, then it is the same as applying "Package Name Black List :: Android Applications" configuration.	X		
ApplicationPolicy	addAppSignatureToWhiteList(String appSignature)	X		X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
ApplicationPolicy	addAppSignatureToWhiteList(String appSignature, boolean defaultBlackList)	X	If 'defaultBlackList' is TRUE, then it is the same as applying "Signature Black List :: Android Applications" configuration.	X		
ApplicationPolicy	addAppPackageNameToBlackList(String packageName)			X		
ApplicationPolicy	addAppSignatureToBlackList(String appSignature)			X		
ApplicationPolicy	setApplicationUninstallationDisabled(String packageName)			X		
ApplicationPolicy	setDisableApplication(String packageName)			X		
BrowserPolicy	setCookiesSetting(boolean enable)		TRUE	X		
BrowserPolicy	setAutoFillSetting(boolean enable)		TRUE	X		
BrowserPolicy	setJavaScriptSetting(boolean enable)		TRUE	X		
BrowserPolicy	setPopupsSetting(boolean enable)		FALSE	X		
SmartCardBrowserPolicy	enableAuthentication()			X		
RestrictionPolicy	allowGoogleAccountsAutoSync(boolean allow)		FALSE	X		
RestrictionPolicy	allowGoogleCrashReport(boolean allow)		FALSE	X		
SmartCardEmailPolicy	requireCredentials(String emailAddress, boolean require)			X		
SecurityPolicy	setInternalStorageEncryption(boolean isEncrypt)		TRUE	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
SecurityPolicy	setExternalStorageEncryption(boolean isEncrypt)		TRUE	X		
PhoneRestrictionPolicy	allowCopyContactToSim(boolean allow)		FALSE	X		
GenericVpnPolicy	createVpnProfile(String profileInfo)			X		
GenericVpnPolicy	addPackagesToVpn(String[] packageList, String profileName)			X		
GenericVpnPolicy	addContainerPackagesToVpn(int mContainerId, String[] packageList, String profileName)			X		
GenericVpnPolicy	addAllContainerPackagesToVpn(int mContainerId, String profileName)			X		
RestrictionPolicy	allowVpn(boolean allow)		FALSE	X		
DevicePolicyManager	setMaximumFailedPasswordsForWipe(ComponentName admin, int num)		num=10		X	
DevicePolicyManager	setPasswordMinimumLength(ComponentName admin, int length)		length=6		X	
DevicePolicyManager	setPasswordQuality(ComponentName admin, int quality)		quality=PASSWORD_QUALITY_ALPHANUMERIC		X	
PasswordPolicy	setPasswordExpires(ComponentName admin, int value)		0	X		
DevicePolicyManager	setMaximumTimeToLock(ComponentName admin, long timeMs)		convert 15 minutes to MS		X	
DevicePolicyManager	setPasswordMinimumUpperCase(ComponentName admin, int length)		0		X	

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
DevicePolicyManager	setPasswordMinimumLowerCase(ComponentName admin, int length)		0		X	
DevicePolicyManager	setPasswordMinimumNumeric(ComponentName admin, int length)		0		X	
PasswordPolicy	setMinimumCharacterChangeLength(int length)		0	X		
PasswordPolicy	setMaximumCharacterSequenceLength(int length)		2	X		
PasswordPolicy	setMaximumNumericSequenceLength(int length)		2	X		
PasswordPolicy	setBiometricAuthenticationEnabled(int bioAuth, boolean enable)		bioAuth=BIOMETRIC_AUTHENTICATION_FINGERPRINT enable=TRUE	X		
DevicePolicyManager	setKeyguardDisabledFeatures(ComponentName admin, int which)		which=KEYGUARD_DISABLE_TRUST_AGENTS	X		
NA	NA		NA			This policy is implemented using Disable Application policies. See STIG requirement for more information.

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
PasswordPolicy	setBiometricAuthenticationEnabled(int bioAuth, boolean enable)		bioAuth=BIOMETRIC_AUTHENTICATION_IRIS enable=FALSE	X		
SecurityPolicy	enableRebootBanner(boolean enable, String bannerText)	X	enable=TRUE bannerText=DoD Defined Text	X		
SecurityPolicy	enableRebootBanner(boolean enable)	X	enable=TRUE	X		This is specifically implemented for STIG compliance requirement for DoD-US (Department of Defense). Banner Text will be DoD Defined Text.
SecurityPolicy	installCertificateToKeystore(String type, byte[] value, String name, String password, int keystore)			X		
CertificatePolicy	enableRevocationCheck(String pkgName, boolean enable)		pkgName="*" enable=TRUE	X		
RestrictionPolicy	setUsbMediaPlayerAvailability(boolean enable)		FALSE	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
BluetoothPolicy	setProfileState(boolean enable, int profile)		TRUE, BLUETOOTH_HFP_PROFILE TRUE, BLUETOOTH_HSP_PROFILE TRUE, BLUETOOTH_SPP_PROFILE FALSE, BLUETOOTH_A2DP_PROFILE FALSE, BLUETOOTH_AVRCP_PROFI LE FALSE, BLUETOOTH_BPP_PROFILE FALSE, BLUETOOTH_DUN_PROFILE FALSE, BLUETOOTH_FTP_PROFILE FALSE, BLUETOOTH_PBAP_PROFILE FALSE, BLUETOOTH_SAP_PROFILE	X		
RestrictionPolicy	setWiFiTethering(boolean)		FALSE	X		
RestrictionPolicy	setBluetoothTethering(boolean enable)		FALSE	X		
RestrictionPolicy	allowUsbHostStorage(boolean allow)		FALSE	X		
RestrictionPolicy	setScreenCapture(boolean)		TRUE	X		
RestrictionPolicy	setBackup(boolean)		FALSE	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
EnterpriseLicenseManager	activateLicense(String licenseKey, String pkgName)			X		
EnterpriseLicenseManager	activateLicense(String licenseKey)			X		
MultiUserManager	allowMultipleUsers(boolean allow)		FALSE	X		
NA	NA		NA			This policy is implemented using Disable Application policies. See STIG requirement for more information.
RestrictionPolicy	allowSVoice(boolean allow)		FALSE	X		
NA	NA		NA			This policy is implemented using Disable Application policies. See STIG requirement for more information.
RestrictionPolicy	setEnabledNFC(boolean enable)		FALSE	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
DeviceAccountPolicy	addAccountsToAdditionWhiteList(String type, List<String> accounts)	X		X		Use getSupportedAccountTypes() for values to pass to 'type'
DeviceAccountPolicy	addAccountsToAdditionWhiteList(String type, List<String> accounts, boolean defaultBlackList)	X	If “defaultBlackList” is TRUE, then it is the same as applying “Account Black List :: Android Accounts” configuration.	X		Use getSupportedAccountTypes() for values to pass to 'type'
DeviceAccountPolicy	addAccountsToAdditionBlackList(String type, List<String> accounts)			X		Use getSupportedAccountTypes() for values to pass to 'type'
NA	NA		NA			This policy is implemented using Disable Application policies. See STIG requirement for more information.
RestrictionPolicy	allowOTAUpgrade(boolean allow)		FALSE	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
DevicePolicyManager	setKeyguardDisabledFeatures(ComponentName admin, int which)		which: KEYGUARD_DISABLE_SECURITY_NOTIFICATIONS OR KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS		X	
EnterpriseDeviceManager	setAdminRemovable(boolean removable)		FALSE	X		
AuditLog	enableAuditLog()			X		
NA	NA		NA			This policy is implemented using Disable Application policies. See STIG requirement for more information.
WiFiPolicy	allowOpenWiFiAp(boolean allow)		FALSE	X		
ApplicationPolicy	addPackageToBatteryOptimizationWhiteList(AppIdentity appIdentity)			X		AppIdentity only needs Package Name. Signature is optional.
RestrictionPolicy	allowShareList(boolean allow)		FALSE	X		
PasswordPolicy	setMinimumCharacterChangeLength(int length)		0	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
BasePasswordPolicy	setPasswordMinimumLength(ComponentName admin, int length)		length=4	X		
BasePasswordPolicy	setMaximumTimeToLock(ComponentName admin, long timeMs)		convert 15 minutes to MS	X		
BasePasswordPolicy	setMaximumFailedPasswordsForWipe(ComponentName admin, int num)		num=10	X		
PasswordPolicy	setPasswordExpires(ComponentName admin, int value)		0	X		
PasswordPolicy	setMaximumCharacterSequenceLength(int length)		2	X		
PasswordPolicy	setMaximumNumericSequenceLength(int length)		2	X		
BasePasswordPolicy	setPasswordQuality(ComponentName admin, int quality)		quality=PASSWORD_QUALITY_ALPHANUMERIC	X		
RestrictionPolicy	setCameraState(boolean enable)		FALSE	X		
DeviceAccountPolicy	addAccountsToAdditionWhiteList(String type, List<String> accounts)	X		X		Use getSupportedAccountTypes() for values to pass to 'type'
DeviceAccountPolicy	addAccountsToAdditionWhiteList(String type, List<String> accounts, boolean defaultBlackList)	X	If “defaultBlackList” is TRUE, then it is the same as applying “Account Black List :: Container Accounts” configuration.	X		Use getSupportedAccountTypes() for values to pass to 'type'
DeviceAccountPolicy	addAccountsToAdditionBlackList(String type, List<String> accounts)			X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
EmailPolicy	allowAccountAddition(boolean allowed)		TRUE	X		
RCPPolicy	setAllowChangeDataSyncPolicy(List<String> appNames, String syncProperty, boolean value)		Sync Provider Name: CALENDAR Sync Property Name: EXPORT_DATA Sync Property Value: false	X		
RCPPolicy	setAllowChangeDataSyncPolicy(List<String> appNames, String syncProperty, boolean value)		Sync Provider Name: CONTACTS Sync Property Name: EXPORT_DATA Sync Property Value: false	X		
RCPPolicy	setAllowChangeDataSyncPolicy(List<String> appNames, String syncProperty, boolean value)		Sync Provider Name: NOTIFICATIONS Sync Property Name: EXPORT_DATA Sync Property Value: false	X		
BrowserPolicy	setCookiesSetting(boolean enable)		FALSE	X		
BrowserPolicy	setAutoFillSetting(boolean enable)		FALSE	X		
BrowserPolicy	setJavaScriptSetting(boolean enable)		FALSE	X		
BrowserPolicy	setPopupsSetting(boolean enable)		FALSE	X		
ApplicationPolicy	addAppPackageNameToWhiteList(String packageName)	X		X		
ApplicationPolicy	addAppPackageNameToWhiteList(String packageName, boolean defaultBlackList)	X	If “defaultBlackList” is TRUE, then it is the same as applying “Package Name Black List ::	X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
			Android Applications” configuration.			
ApplicationPolicy	addAppSignatureToWhiteList(String appSignature)	X		X		
ApplicationPolicy	addAppSignatureToWhiteList(String appSignature, boolean defaultBlackList)	X	If 'defaultBlackList' is TRUE, then it is the same as applying "Signature Black List :: Android Applications" configuration.	X		
ApplicationPolicy	addAppPackageNameToBlackList(String packageName)			X		
ApplicationPolicy	addAppSignatureToBlackList(String appSignature)			X		
ApplicationPolicy	setApplicationUninstallationDisabled(String packageName)			X		
RCPPolicy	allowMoveAppsToContainer(boolean allow)		FALSE	X		
RCPPolicy	allowMoveFilesToOwner(boolean allow)		FALSE	X		
ApplicationPolicy	setDisableApplication(String packageName)			X		
KnoxContainerManager	createContainer(String type)			X		
KnoxContainerManager	createContainer(CreationParams params)			X		
KnoxContainerManager	createContainer(String type, String adminPackageName)			X		
BrowserPolicy	setHttpProxy(String proxySetting)			X		

Implementation API						
<i>Class</i>	<i>Method</i>	<i>Alternatives</i>	<i>Parameters</i>	<i>Samsung</i>	<i>Google</i>	<i>Notes</i>
RestrictionPolicy	setScreenCapture(boolean)		FALSE	X		
NA	NA		NA			This policy is implemented using Disable Application policies. See STIG requirement for more information.