

UNCLASSIFIED



## **SAMSUNG ANDROID 12 WITH KNOX 3.X STIG CONFIGURATION TABLES**

**24 July 2024**

**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 ..... | 4           |
| Table 3: KPE Equivalent APIs .....                 | 8           |
| Table 4: KSP App Separation .....                  | 10          |

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 policies listed in the document are implemented using AE APIs. If your 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 your management tool, or via KSP. In this situation, look for an “\*” next to the AE API in the comment of the associated policy row – an “\*” 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. Please 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-12-110010      | Enroll device as an Android Enterprise device.                                                                                                                                   |
| <b>Device User Agreement</b>           | User agreement            |                                                                                                  | Include DOD-mandated warning banner text in User Agreement | KNOX-12-110020      | Include the warning banner text in the User Agreement.<br><br>Alternatively, but not preferred, include on the lock screen information:<br><br>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-12-110030, KNOX-12-110040 | This allows for PIN code.<br><br>API: setPasswordQuality *<br><br>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”.             |
| <b>Device Password Policies</b> | Minimum password length              | 0+ characters                                                                        | Six characters   | KNOX-12-110050                 | API: setPasswordMinimumLength *                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Device Password Policies</b> | Max password failures for local wipe | 0+                                                                                   | 10 attempts      | KNOX-12-110060                 | API: setMaximumFailedPasswordsForWipe *                                                                                                                                                                                                                                                                                                                                                                |
| <b>Device Password Policies</b> | Max time to screen lock              | 0+ minutes                                                                           | 15 minutes       | KNOX-12-110070                 | API: setMaximumTimeToLock *                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Device Restrictions</b>      | Face                                 | Enable/Disable                                                                       | Disable          | KNOX-12-110080                 | API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE<br><br>This policy is included to allow a Samsung Android device to be deployed as an AE device without an activated KPE premium license. If a license is activated, Facial Recognition will be automatically disabled. In this case, this policy does not need to be configured for STIG compliance, as Face as a biometric will be disabled. |
| <b>Device Restrictions</b>      | Trust agents                         | Enable/Disable                                                                       | Disable          | KNOX-12-110090                 | API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS                                                                                                                                                                                                                                                                                                                                        |
| <b>Device Restrictions</b>      | Backup service                       | Enable/Disable                                                                       | Disable          | KNOX-12-110100                 | API: setBackupServiceEnabled *                                                                                                                                                                                                                                                                                                                                                                         |

| Policy Group        | Policy Rule          | Options        | Settings    | Related Requirement            | Comment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|----------------------|----------------|-------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Restrictions | Debugging features   | Allow/Disallow | Disallow    | KNOX-12-110110                 | API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Device Restrictions | Bluetooth            | Allow/Disallow | AO decision | KNOX-12-110120                 | Guidance is provided for AO to approve Bluetooth.<br><br>API: addUserRestriction, DISALLOW_BLUETOOTH *                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Device Restrictions | Mount physical media | Allow/Disallow | Disallow    | KNOX-12-110130                 | Not applicable for devices that do not support removable storage media.<br><br>Disables use of all removable storage, e.g., SD cards, USB thumb drives.<br><br>API: addUserRestriction, DISALLOW_MOUNT_PHYSICAL_MEDIA *<br><br>If your 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 “enable”. |
| Device Restrictions | USB file transfer    | Allow/Disallow | Disallow    | KNOX-12-110140, KNOX-12-110150 | DeX drag and drop file transfer capabilities will be prohibited, but all other DeX capabilities remain useable.<br><br>API: addUserRestriction, DISALLOW_USB_FILE_TRANSFER *                                                                                                                                                                                                                                                                                                                                                             |
| Device Restrictions | Config tethering     | Allow/Disallow | Disallow    | KNOX-12-110160                 | API: addUserRestriction, DISALLOW_CONFIG_TETHERING *<br><br>If deployment requires the use of Mobile Hotspot & Tethering, 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) “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 | Config date/time     | Allow/Disallow | Disallow    | KNOX-12-110170                 | API: addUserRestriction, DISALLOW_CONFIG_DATE_TIME *                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Policy Group                    | Policy Rule                                         | Options        | Settings                                 | Related Requirement            | Comment                                                                                                    |
|---------------------------------|-----------------------------------------------------|----------------|------------------------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Device Policy Management</b> | Certificates                                        |                | Include DOD certificates in Work Profile | KNOX-12-110180                 | API: installCaCert *                                                                                       |
| <b>Device Restrictions</b>      | List of approved apps listed in managed Google Play | List of apps   | List only approved work apps             | KNOX-12-110190, KNOX-12-110200 | *                                                                                                          |
| <b>Device Restrictions</b>      | Unredacted notifications                            | Allow/Disallow | Disallow                                 | KNOX-12-110210                 | API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS                                |
| <b>Device Restrictions</b>      | Security logging                                    | Enable/Disable | Enable                                   | KNOX-12-110220                 | Management tool must provide means to read the Log in the console.<br><br>API: setSecurityLoggingEnabled * |
| <b>Device Restrictions</b>      | Modify accounts                                     | Allow/Disallow | Disallow                                 | KNOX-12-110230, KNOX-12-110240 | API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *                                                        |
| <b>Device Restrictions</b>      | Config credentials                                  | Allow/Disallow | Disallow                                 | KNOX-12-110250                 | API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *                                                     |
| <b>Device Restrictions</b>      | Install from unknown sources globally               | Allow/Disallow | Disallow                                 | KNOX-12-110260                 | API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *                                       |
| <b>Device Restrictions</b>      | CC mode                                             | Enable/Disable | Enable                                   | KNOX-12-110270, KNOX-12-110280 | 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 | Work Profile for company-owned devices | KNOX-12-210010      | Enroll device as an Android Enterprise device. |

| Policy Group                    | Policy Rule                          | Options                                                                              | Settings                                                   | Related Requirement            | Comment                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|--------------------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                      | for personally-owned devices                                                         |                                                            |                                |                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Device User Agreement</b>    | User agreement                       |                                                                                      | Include DOD-mandated warning banner text in User Agreement | KNOX-12-21002                  | <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: setDeviceOwnerLockScreenInfo</p>                                                                                                                                                                                                                       |
| <b>Device Password Policies</b> | Minimum password quality             | Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex | Numeric(Complex)                                           | KNOX-12-210030, KNOX-12-210040 | <p>This allows for PIN code.</p> <p>API: setPasswordQuality</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 - “Maximum Numeric Sequence Length” with value “4”.</p>             |
| <b>Device Password Policies</b> | Minimum password length              | 0+ characters                                                                        | Six characters                                             | KNOX-12-210050                 | API: setPasswordMinimumLength                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Device Password Policies</b> | Max password failures for local wipe | 0+                                                                                   | 10 attempts                                                | KNOX-12-210060                 | API: setMaximumFailedPasswordsForWipe                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Device Password Policies</b> | Max time to screen lock              | 0+ minutes                                                                           | 15 minutes                                                 | KNOX-12-210070                 | API: setMaximumTimeToLock                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Device Restrictions</b>      | Face                                 | Enable/Disable                                                                       | Disable                                                    | KNOX-12-210080                 | <p>API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE</p> <p>This policy is included to allow a Samsung Android device to be deployed as an AE device without an activated KPE premium license. If a license is activated, Facial Recognition will be automatically disabled. In this case, this policy does not need to be configured for STIG compliance, as Face as a biometric will be disabled.</p> |

| Policy Group               | Policy Rule          | Options        | Settings    | Related Requirement            | Comment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|----------------------|----------------|-------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Device Restrictions</b> | Trust agents         | Enable/Disable | Disable     | KNOX-12-210090                 | API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Device Restrictions</b> | Debugging features   | Allow/Disallow | Disallow    | KNOX-12-210100                 | API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Device Restrictions</b> | Bluetooth            | Allow/Disallow | AO decision | KNOX-12-210110                 | Guidance is provided for AO to approve Bluetooth.<br><br>API: addUserRestriction, DISALLOW_BLUETOOTH *                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Device Restrictions</b> | Mount physical media | Allow/Disallow | Disallow    | KNOX-12-210120                 | Not applicable for devices that do not support removable storage media.<br><br>Disables use of all removable storage, e.g., SD cards and USB thumb drives.<br><br>API: addUserRestriction, DISALLOW_MOUNT_PHYSICAL_MEDIA *<br><br>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”. |
| <b>Device Restrictions</b> | USB file transfer    | Allow/Disallow | Disallow    | KNOX-12-210130, KNOX-12-210140 | DeX drag & drop file transfer capabilities will be prohibited, but all other DeX capabilities remain useable.<br><br>API: addUserRestriction, DISALLOW_USB_FILE_TRANSFER *                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Device Restrictions</b> | Config tethering     | Allow/Disallow | Disallow    | KNOX-12-210150                 | API: addUserRestriction, DISALLOW_CONFIG_TETHERING *<br><br>If deployment requires the use of Mobile Hotspot & Tethering, 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) “Allow open Wi-Fi connection” with value “disable” and add Training Topic “Don’t use Wi-Fi Sharing” (see supplemental document for additional information)                                                     |

| Policy Group                          | Policy Rule                                         | Options        | Settings                                 | Related Requirement            | Comment                                                                                                    |
|---------------------------------------|-----------------------------------------------------|----------------|------------------------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Device Restrictions</b>            | Config date/time                                    | Allow/Disallow | Disallow                                 | KNOX-12-210160                 | API: addUserRestriction, DISALLOW_CONFIG_DATE_TIME *                                                       |
| <b>Work Profile Policy Management</b> | Certificates                                        |                | Include DOD certificates in work profile | KNOX-12-210170                 | 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-12-210180, KNOX-12-210190 | *                                                                                                          |
| <b>Work Profile Restrictions</b>      | Unredacted notifications                            | Allow/Disallow | Disallow                                 | KNOX-12-210200                 | API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS *                              |
| <b>Work Profile Restrictions</b>      | Security logging                                    | Enable/Disable | Enable                                   | KNOX-12-210210                 | Management tool must provide means to read the Log in the console.<br><br>API: setSecurityLoggingEnabled * |
| <b>Work Profile Restrictions</b>      | Modify accounts                                     | Allow/Disallow | Disallow                                 | KNOX-12-210220, KNOX-12-210230 | API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *                                                        |
| <b>Work Profile Restrictions</b>      | Cross profile copy/paste                            | Allow/Disallow | Disallow                                 | KNOX-12-210240                 | API: addUserRestriction, DISALLOW_CROSS_PROFILE_COPY_PASTE *                                               |
| <b>Work Profile Restrictions</b>      | Config credentials                                  | Allow/Disallow | Disallow                                 | KNOX-12-210250                 | API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *                                                     |
| <b>Work Profile Restrictions</b>      | Install from unknown sources globally               | Allow/Disallow | Disallow                                 | KNOX-12-210260                 | API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *                                       |
| <b>Work Profile Restrictions</b>      | CC mode                                             | Enable/Disable | Enable                                   | KNOX-12-210270, KNOX-12-210280 | API: setCommonCriteriaModeEnabled *                                                                        |

## APPENDIX

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<br><br>Alternatively: WiFiPolicy allowOpenWifiAp                             |
|                           | DISALLOW_CROSS_PROFILE_COPY_PASTE         | RCPolicy allowShareClipboardDataToOwner                                                                     |
|                           | DISALLOW_DEBUGGING_FEATURES               | RestrictionPolicy allowDeveloperMode                                                                        |
|                           | DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY | RestrictionPolicy setAllowNonMarketApps                                                                     |
|                           | DISALLOW_MODIFY_ACCOUNTS                  | DeviceAccountPolicy<br>addAccountsToAdditionBlackList                                                       |
|                           | DISALLOW_MOUNT_PHYSICAL_MEDIA             | RestrictionPolicy setSdCardState<br><br>Alternatively: DeviceSecurityPolicy<br>setExternalStorageEncryption |
|                           | DISALLOW_USB_FILE_TRANSFER                | RestrictionPolicy setUsbMediaPlayerAvailability                                                             |
| <b>installCaCert</b>      | DOD Root and Intermediate Certs           | CertificateProvisioning<br>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<br>addAppPackageNameToWhiteList,<br>ApplicationPolicy<br>addAppPackageNameToBlackList,<br>ApplicationPolicy addAppSignatureToWhiteList,<br>ApplicationPolicy addAppSignatureToBlackList |
| <b>setBackupServiceEnabled</b>          | FALSE                                     | RestrictionPolicy setBackup                                                                                                                                                                               |
| <b>setCommonCriteriaModeEnabled</b>     | TRUE                                      | AdvancedRestrictionPolicy setCCMode                                                                                                                                                                       |
| <b>setKeyguardDisabledFeatures</b>      | KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS | RCPPolicy setAllowChangeDataSyncPolicy<br>NOTIFICATIONS, SANITIZE_DATA, FALSE                                                                                                                             |
| <b>setMaximumFailedPasswordsForWipe</b> | 10                                        | BasePasswordPolicy<br>setMaximumFailedPasswordsForWipe                                                                                                                                                    |
| <b>setMaximumTimeToLock</b>             | 900                                       | BasePasswordPolicy setMaximumTimeToLock                                                                                                                                                                   |
| <b>setPasswordMinimumLength</b>         | 6                                         | BasePasswordPolicy setPasswordMinimumLength                                                                                                                                                               |
| <b>setPasswordQuality</b>               | Numeric(Complex)                          | BasePasswordPolicy setPasswordQuality<br><br>Alternatively:<br>PasswordPolicy<br>setMaximumNumericSequenceLength(2) with<br>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    | <div>1. App Sep Policies</div> <div>2. Enable App Sep Policies [enable]</div> <div>3. Allow Listing Policies</div> <div>4. Set Location [inside or outside]</div>       |
| App Separation | App List    | <div>1. App Sep Policies</div> <div>2. Enable App Sep Policies [enable]</div> <div>3. Allow Listing Policies</div> <div>4. Configure Apps List [list of packages]</div> |