

UNCLASSIFIED



SAMSUNG ANDROID OS 6 (WITH KNOX 2.x) STIG CONFIGURATION TABLES

Version 1, Release 2

27 January 2017

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 | 10 |
| Table 3: Configuration Policy Rules for Play for Work Inside KNOX Container | 15 |

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 Restriction | Enable CC Mode | Enable/Disable | X | | Enable | KNOX-39-015600 | 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 Restriction | Disable Developer Mode | Enable/Disable | X | | Enable | KNOX-35-020000 | |
| Android Restriction | Allow Location | Enable/Disable | | X | Enable (GPS, Wi-Fi, Cellular) | | Local site can change setting based on mission needs. |
| Android Restriction | Disable Camera | Enable/Disable | | X | Enable | | Local site can change setting based on mission needs. |
| Android Restriction | Disable Microphone | Enable/Disable | | X | Enable | | Local site can change setting based on mission needs. |
| Android Restriction | Allow New Admin | Enable/Disable | X | | Disable | KNOX-35-021000 | |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|---------------------|----------------------------------|----------------|----------|----------|-------------------------|----------------------------|---|
| Android Restriction | Disable Manual Date Time Changes | Enable/Disable | X | | Enable | KNOX-38-012600 | |
| Android Restriction | Enable Google Play | Enable/Disable | X | | Disable | KNOX-35-009000 | |
| Android Restriction | Allow Unknown Sources | Enable/Disable | X | | Disable | KNOX-35-009010 | |
| Application | Application White List | Configure | X | | Add Approved Packages | KNOX-35-009100 | |
| Application | Application Blacklist | Configure | X | | Add All Packages | KNOX-35-021100 | All packages specified by wildcard (.*). When all apps are blacklisted, only apps on the whitelist are allowed. |
| Application | Required List | Configure | | X | Add Packages | | List of applications the user cannot uninstall. This list is site specific. Local site can change setting based on mission needs. |
| Application | Disable Applications | Configure | X | | Add Unapproved Packages | KNOX-35-021200 | The systems administrator should identify all pre-installed applications that are not approved and disable them. |
| Android Restriction | Allow Cookies | Enable/Disable | | X | Enable | | Native browser application only. Local site can change setting based on mission needs. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|---------------------|---------------------------------------|----------------|----------|----------|----------|----------------------------|--|
| Android Restriction | Enable Auto-fill | Enable/Disable | | X | Enable | | Native browser application only. Local site can change setting based on mission needs. |
| Android Restriction | Enable JavaScript | Enable/Disable | | X | Enable | | Native browser application only. Local site can change setting based on mission needs. |
| Android Restriction | Enable Pop-ups | Enable/Disable | | X | Disable | | Native browser application only. Local site can change setting based on mission needs. |
| Android Restriction | Enable CAC Authentication for Browser | Enable/Disable | | X | Enable | | Native browser application only. Local site can change setting based on mission needs. |
| Accounts | Google Auto Sync | Enable/Disable | X | | Disable | KNOX-35-021300 | |
| Accounts | Google Crash Report | Enable/Disable | X | | Disable | KNOX-35-021400 | |
| Android Restriction | Enable CAC Authentication for Email | Enable/Disable | | X | Enable | | This affects non-container email only. Local site can change setting based on mission needs. |
| Android Restriction | Storage Encryption | Enable/Disable | X | | Enable | KNOX-30-004400 | Encrypt all user and enterprise data at rest. |
| Android Restriction | External Storage Encryption | Enable/Disable | X | | Enable | KNOX-30-004410 | Encrypt all external media cards. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|----------------------|----------------------------------|---|----------|----------|-----------------|----------------------------|---|
| Android Restriction | Copy Contacts to SIM | Enable/Disable | | X | Disable | | Local site can change setting based on mission needs. |
| Android VPN | VPN | Configure | X | | Add VPN Profile | KNOX-35-024500 | Configure organization VPN profile. |
| Password Restriction | Maximum Failed Attempts for Wipe | 0- | X | | 10 | KNOX-34-008900 | Unsuccessful logon attempts before device wipe |
| Password Restriction | Minimum Length | 0- | X | | 6 | KNOX-34-008700 | Minimum device password length. |
| Password Restriction | Password Complexity | None Pattern Pin Alphabetic Alphanumeric Complex | X | | Alphanumeric | KNOX-35-024600 | Device password complexity. |
| Password Restriction | Maximum Password Lifetime | 0- | | X | 0 | | Days after which password must be changed. Local site can change setting based on mission needs. |
| Password Restriction | Max Time to Lock | 0- | X | | 15 | KNOX-34-012100 | Minutes of inactivity after which device will lock |
| Password Restriction | Min Uppercase | 0- | | X | 0 | | Minimum number of uppercase alphabetic characters in device password. Local site can change setting based on mission needs. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|----------------------|--|----------------|----------|----------|----------|----------------------------|--|
| Password Restriction | Min Lowercase | 0- | | X | 0 | | Minimum number of lowercase alphabetic characters in device password. Local site can change setting based on mission needs. |
| Password Restriction | Min Numeric | 0- | | X | 0 | | Minimum number of numeric characters in device password. Local site can change setting based on mission needs. |
| Password Restriction | Min Mutation on Change | 0- | | X | 0 | | Minimum number of characters that must be changed when device password is changed. Local site can change setting based on mission needs. |
| Password Restriction | Max Sequential Characters | 0- | X | | 2 | KNOX-35-021900 | Max number of sequential characters in device password. |
| Password Restriction | Max Sequential Numbers | 0- | X | | 2 | KNOX-35-021900 | Max number of sequential numbers in device password. |
| Password Restriction | Fingerprint for Lock screen Authentication | Enable/Disable | X | | Disable | KNOX-35-024600 | |
| Password Restriction | Smart Lock | Enable/Disable | X | | Disable | KNOX-35-030000 | |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|----------------------|------------------------------------|-------------------|----------|----------|-------------------|----------------------------|--|
| Android Restriction | DoD Banner | Enable/Disable | X | | Enable | KNOX-36-009700 | The administrator can configure enterprise-specific banner text. If the banner is 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-35-020600 | Select PEM encoded representations of the DoD root and intermediate certificates. |
| Android Certificate | Certificate Revocation Check (CRL) | Enable/Disable | X | | Enable | KNOX-35-028500 | |
| Android Restriction | Disable USB Media Player | Select/Not Select | X | | Select | KNOX-35-023600 | Disabling USB Media Player will also disable USB MTP, USB mass storage, USB vendor protocol (KIES). |
| Android Restrictions | Allowed Bluetooth Profiles | | X | | HFP HSP SPP | KNOX-39-015700 | Disables all Bluetooth profiles except for those specified in the settings. |
| Android Restriction | Disable Wi-Fi Tethering | Select/Not Select | | X | Select | | The systems administrator must select the setting based on local policy. Local site can change setting based on mission needs. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|---------------------|-----------------------------|-------------------|----------|----------|--------------------------------|----------------------------|--|
| Android Restriction | Disable Bluetooth Tethering | Select/Not Select | | X | Select | | The systems administrator must select the setting based on local policy. Local site can change setting based on mission needs. |
| Android Restriction | Disable USB Host Storage | Select/Not Select | X | | Select | KNOX-35-021600 | USB host storage allows the device to mount external USB drives. |
| Android Restriction | Allow Screen Capture | Enable/Disable | | X | Enable | | Local site can change setting based on mission needs. |
| Android Restriction | Allow Google Backup | Enable/Disable | X | | Disable | KNOX-35-021300 | |
| Knox Restriction | Knox License | Configure | X | | Enterprise issued Knox license | KNOX-35-030100 | Proper configuration of the Knox license ensures reporting information is sent to the correct enterprise servers. |
| Android Restriction | Allow Multi-user Mode | Enable/Disable | X | | Disable | KNOX-35-022500 | |
| Android Restriction | Allow Cloud Backup | Enable/Disable | X | | Disable | KNOX-35-021200 | This policy is implemented using Disable Application policies. See STIG requirement for more information. |
| Android Restriction | Allow S Voice | Enable/Disable | X | | Disable | KNOX-35-022800 | |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|---------------------|----------------------|----------------|----------|----------|-------------------|----------------------------|---|
| Android Restriction | Allow Mobile Payment | Enable/Disable | X | | Disable | KNOX-35-021250 | This policy is implemented using Disable Application policies. See STIG requirement for more information. |
| Android Restriction | Allow NFC | Enable/Disable | X | | Disable | KNOX-35-023100 | |
| 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. Local site can change setting based on mission needs. |
| Accounts | Account Blacklist | | | X | .*(wildcard) | | Configure by blacklisting all domains. Then only accounts on the whitelist are allowed. Local site can change setting based on mission needs. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|---------------------|------------------------------|---|----------|----------|--|----------------------------|---|
| Android Restriction | Allow Samsung Accounts | Enable/Disable | X | | Disable | KNOX-35-021275 | This policy is implemented using Disable Application policies. See STIG requirement for more information. |
| Android Restriction | Allow FOTA | Enable/Disable | X | | Disable | KNOX-35-023700 | Disables automatic firmware updates. |
| Android Restriction | Notifications on Lock Screen | Show content Hide content Do not show notifications | X | | Hide content or Do not show notifications | KNOX-35-024000 | |
| Android Restriction | Allow Admin Remove | Enable/Disable | X | | Disable | KNOX-35-028400 | |
| Android Restriction | Enable Audit Log | Enable/Disable | X | | Enable | KNOX-35-027300 | |

Table 2: Configuration Policy Rules for Work Environment Container

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|--------------------------------|----------------------------------|----------------------|----------|----------|--------------|----------------------------|---|
| Container Password Restriction | Min Mutation on Change | 0- | | X | 0 | | Minimum number of characters that must be changed when container password is changed. Local site can change setting based on mission needs. |
| Container Password Restriction | Minimum Length | 0- | X | | 4 | KNOX-39-014900 | Minimum container password length. |
| Container Password Restriction | Max Time to Lock | 0- | X | | 15 | KNOX-34-012110 | Minutes of inactivity after which container will lock. |
| Container Password Restriction | Maximum Failed Attempts for Wipe | 0- | X | | 10 | KNOX-39-015200 | Unsuccessful logon attempts before container wipe. |
| Container Password Restriction | Maximum Password Lifetime | 0- | | X | 0 | | Days after which password must be changed. Local site can change setting based on mission needs. |
| Container Password Restriction | Max Sequential Numbers | 0- | X | | 2 | KNOX-39-021100 | Max number of sequential numbers in device password. |
| Container Password Restriction | Password Complexity | Alphanumeric Complex | X | | Alphanumeric | KNOX-39-022000 | |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|-----------------------|---------------------------------------|----------------|----------|----------|-------------------|----------------------------|--|
| Container Restriction | Allow Camera | Enable/Disable | | X | Disable | | Camera use inside container. In KNOX 2.0, disabling the camera outside will also disable the camera inside. Local site can change setting based on mission needs. |
| Container Accounts | Account Whitelist | Configure | X | | Approved accounts | KNOX-39-021200 | 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-39-021300 | Configure by blacklisting all domains. When all apps are blacklisted, then only accounts on the whitelist are allowed. |
| Container Restriction | Allow Account Addition | Enable/Disable | | X | Enable | | Allows user to add email accounts inside container. Configuration determined by local policy. Local site can change setting based on mission needs. |
| Container Restriction | Allow Calendar Info Outside Container | Enable/Disable | X | | Disable | KNOX-39-015100 | Sharing of container calendar events to outside calendar. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|-----------------------|--------------------------------------|----------------|----------|----------|-----------------------|----------------------------|---|
| Container Restriction | Allow Contact Info Outside Container | Enable/Disable | X | | Disable | KNOX-39-015250 | Sharing of container contacts to outside contacts. |
| Container Restriction | Allow Notification Details | Enable/Disable | X | | Disable | KNOX-39-015300 | Display details of container application notifications when user is outside container. |
| Container Restriction | Allow Cookies | Enable/Disable | | X | Disable | | Container native browser application only. Local site can change setting based on mission needs. |
| Container Restriction | Enable Auto-Fill | Enable/Disable | X | | Disable | KNOX-39-021000 | Container native browser application only. |
| Container Restriction | Enable JavaScript | Enable/Disable | | X | Enable | | Container native browser application only. Local site can change setting based on mission needs. |
| Container Restriction | Enable Pop-ups | Enable/Disable | | X | Disable | | Container native browser application only. Local site can change setting based on mission needs. |
| Container Application | Application Whitelist | Configure | X | | Add Approved Packages | KNOX-39-020100 | Configure by setting the list of only DoD-approved applications. |
| Container Application | Application Blacklist | Configure | X | | Add All Packages | KNOX-39-020300 | All packages specified by wildcard (.*) |
| Container Application | Required List | Configure | | X | Add Packages | | List of applications the user cannot uninstall. Local site can change setting based on mission needs. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|-----------------------|---------------------------------------|----------------|----------|----------|-----------------|----------------------------|---|
| Container Application | Enable Move Applications to Container | Enable/Disable | X | | Disable | KNOX-39-020400 | 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 | Enable Move Files from Container | Enable/Disable | X | | Disable | KNOX-39-020500 | Blocks users from moving files from container. By default, "from" is disabled and can only be changed by the admin. |
| Container Application | Disable Applications | Configure | X | | Add Packages | KNOX-39-020700 | 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-39-015400 | |
| Android Container VPN | VPN | Configure | | X | Add VPN Profile | | Configure organization VPN profile for the container only. Use the container-VPN configuration. Local site can change setting based on mission needs. |

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|----------------------------|------------------------|----------------|----------|----------|-----------|----------------------------|--|
| 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. Local site can change setting based on mission needs. |
| Container Restriction | Allow Screen Capture | Enable/Disable | | X | Disable | | Local site can change setting based on mission needs. |
| Container Restriction | Allow Samsung Accounts | Enable/Disable | X | | Disable | KNOX-39-020700 | This policy is implemented using Disable Application policies. See STIG requirement for more information. |

Table 3: Configuration Policy Rules for Play for Work Inside KNOX Container

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|-----------------------|-------------------------------|----------------|----------|----------|------------------------|----------------------------|--|
| Container Restriction | Enable Google Play | Enable/Disable | | X | Enable | KNOX-35-009005 | Enabling this results in Play showing up inside the KNOX container. |
| Container Application | Disable Applications | Configure | X | | com.google.android.gms | KNOX-39-020700 | This disables Gmail inside the container. Policy is only required if Play for Work Inside KNOX is used. |
| Container Application | Application Install Whitelist | Configure | X | | com.android.vending | KNOX-39-020100 | This allows Play to install apps inside the container. Policy is only required if Play for Work Inside KNOX is used. |
| Container Accounts | Account Whitelist | Configure | X | | Approved accounts | KNOX-39-021200 | This is to allow only DoD-approved Play for Work Inside KNOX account configuration. |
| Container Accounts | Account Blacklist | Configure | X | | .* (wildcard) | KNOX-39-021300 | |

Note: Enterprises that configure Play for Work Inside KNOX must configure all of the above controls. Use of Play for Work Inside KNOX requires Authorizing Official (AO) approval.