

UNCLASSIFIED



SAMSUNG ANDROID OS 6 WITH KNOX 2.x SUPPLEMENTAL PROCEDURES

Version 1, Release 3

26 April 2019

Developed by Samsung and DISA for the DoD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. SECURITY READINESS REVIEW	1
1.1 General	1
1.2 Mobile Policy Registration	1
2. SAMSUNG ANDROID WITH KNOX IMPLEMENTATION CONSIDERATIONS ...	2
2.1 Compliance via Third-Party Applications and Components.....	2
2.2 Indirect Compliance	2
2.3 Logic of STIG Requirements	3
3. SAMSUNG KNOX FOR ANDROID DUAL-PERSONA CAPABILITY	4
3.1 Overview	4
3.2 Container Applications.....	4
3.3 Container Isolation	5
3.4 Container Data-at-Rest Encryption	6
3.5 Trusted Boot and Warranty Fuse-Based Container Protection	6
3.6 Data-in-Transit Protection.....	6
3.7 Container Access Control	7
3.8 Container Configuration and Management	8
3.8.1 Container Management Policies	8
3.8.2 Container Application Management Policies	8
3.8.3 Container Password Policies.....	9
3.8.4 Container Email and Browser Policies	9
3.9 Container Activation	10
3.10 KNOX On-Premise Servers	10
4. SAMSUNG KNOX FOR ANDROID IA FEATURES	12
4.1 Samsung Android Device Disposal	12
4.2 Samsung Device Encryption Guidelines.....	12
5. SAMSUNG KNOX FOR ANDROID USER-BASED ENFORCEMENT	13
5.1 Calendar Alarm	13
5.2 Content Transferring and Screen Mirroring.....	13
5.3 Content Sharing	13
5.4 Report Diagnostic Information	14
6. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES	15
6.1 Public Cloud Backup Applications	15
6.2 Social Networking Applications	15
6.3 Data Uploading Applications	15
6.4 Content-Sharing Applications	16
6.5 Mobile Printing	16
6.6 Core and Preinstalled Applications	16
6.6.1 Introduction.....	16

6.6.2 Disabled Core and Preinstalled Applications	16
6.6.3 Approved Core and Preinstalled Applications	19
6.7 Auditing/Reviewing Device Applications	21
7. SAMSUNG WEARABLES.....	22
8. PLAY FOR WORK INSIDE KNOX CONTAINER.....	22

LIST OF TABLES

	Page
Table 6-1: Disabled Applications – Personal Area.....	16
Table 6-2: Disabled Applications – Container.....	19
Table 6-3: Applications Recommended for Approval – Personal Area	19
Table 6-4: Applications Recommended for Approval – Container	20

1. SECURITY READINESS REVIEW

1.1 General

When conducting a Samsung Android 6.x (with KNOX 2.x) Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the Samsung Android 6.x platform, its associated network infrastructure, and the individual devices composing the system.

1.2 Mobile Policy Registration

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website at: <http://iase.disa.mil/stigs/mobility/Pages/policies.aspx>. Use the Mobility Policy Security Technical Implementation Guide (STIG) to review the General Wireless Policy asset and the Commercial Mobile Device (CMD) Policy STIG to review the smartphone handheld asset.

2. SAMSUNG ANDROID WITH KNOX IMPLEMENTATION CONSIDERATIONS

2.1 Compliance via Third-Party Applications and Components

The Samsung Android with KNOX platform provides various application program interfaces (APIs) for third-party solution vendors to develop KNOX security components that can be used to implement several Mobile Device Fundamentals Protection Profile (MDFPP) STIG Template Information Assurance (IA) controls. This allows for the integration of any third-party applications and components to achieve compliance with the Samsung Android OS 6 (with KNOX 2.x) STIG. The APIs provided by the Samsung Android with KNOX platform are as follows:

- The Samsung MDM API includes more than 600 policies and 1500 interfaces designed to be called by any MDM agent. Using these policies and interfaces, the MDM solution vendor can implement an MDM solution that can meet or exceed the STIG Template requirements. Examples of MDM vendors that implement the Samsung MDM API include Mobile Iron, AirWatch, BlackBerry, SOTI, MasS360, Centrify, and SAP.
- The Samsung MDM API includes advanced virtual private network (VPN) policies and interfaces that allow an MDM admin to configure any third-party IPsec VPN solution that implements the MDM interfaces. The VPN enables the Samsung Android with KNOX device to connect to DoD networks and uses a FIPS 140-2 validated cryptographic module to protect data in transit. Examples of solutions that implement the MDM interface include Mocana KeyVPN, strongSwan, and Inside Secure VPN.
- The Samsung Smart Card API provides an interface that allows any third-party vendor to implement smart card reader functionality for the Samsung Android with KNOX device. Solutions implementing this interface enable Samsung Android with KNOX to support applications leveraging the DoD Common Access Card (CAC) for public key infrastructure (PKI)-related transactions, including user authentication to DoD networks and websites, S/MIME digital signatures, and, if desired, device unlock. Examples of solutions that implement this interface include the Biometrics Associates Bluetooth Smart Card Reader.

2.2 Indirect Compliance

In some cases, the Samsung Android with KNOX solution MDFPP STIG Template compliance is achieved through means other than direct implementation of the required IA control:

- Neither Android nor Samsung Android with KNOX authenticate applications through digital signature verification, but Samsung Android with KNOX uses an application quarantine capability that provides equivalent protection when system administrators correctly identify which applications should be permitted to exit the quarantine.
- Samsung Android with KNOX does not directly enforce STIG Template Bluetooth requirements in its native Bluetooth stack, but Samsung Android with KNOX uses a Bluetooth whitelisting capability to assure that only Bluetooth peripherals that comply

with the requirements are permitted to pair with the Samsung Android with KNOX device.

- Samsung Android with KNOX meets the requirement for having a capability to log privileged text-based commands by disabling the ability to perform such commands, thereby rendering the requirement inapplicable.

2.3 Logic of STIG Requirements

The logic of some of the STIG configuration settings 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 in STIG requirement KNOX-38-012600 and the Configuration Table document.

3. SAMSUNG KNOX FOR ANDROID DUAL-PERSONA CAPABILITY

3.1 Overview

Samsung Android with KNOX supports a dual-persona capability using "container" technology. The container provides a secure and isolated workspace for enterprise applications and data. Enterprise applications and data are placed inside the container. General productivity and morale applications and data reside outside the container. The device user has a separate home screen, launcher, and widgets for resources inside and outside the container. The container supports several security-related features:

- Separate home screen, launcher, applications, and widgets
- AES 256 encryption of all container data using a FIPS 140-2 validated cryptographic module
- No interaction between applications and data inside and outside the container
- Password-based access control mechanism that is independent of the device lock screen
- Data-in-transit protection of all container network traffic using a VPN employing FIPS 140-2 validated cryptographic modules
- Container-only configuration and management policies, including application management, password complexity, CAC configurations for browser and email, and remote wipe of only the container

MDM software can set security policies for the entire device or target them for the container only. In some deployment scenarios, organizations may implement relaxed security policies outside the container where users are prohibited from performing DoD mission activities or storing DoD sensitive data outside the container. While DoD organizations, at their discretion, may permit limited personal activity outside the container, in all cases the entire device is subject to the terms of the DoD Information Systems User Agreement. Users do not have an expectation of privacy for activity outside the container.

3.2 Container Applications

Most wireless carriers add applications to mobile devices that are in addition to core applications included with the Android operating system. These additional applications are sometimes referred to as "bloatware". Bloatware applications have been found to track mobile device user activities, download usage statistics and other device data to third-party servers, and provide additional revenue opportunities for carriers. Unfortunately, it is very difficult or impossible to remove bloatware applications from Android devices. The Samsung Android with KNOX container is used to create a work environment on the Samsung mobile device to separate DoD applications and data from the main device environment where the bloatware applications reside. When Samsung Android devices are used in the DoD, all applications used by the DoD must be installed in the KNOX container, and all DoD data must be saved in the KNOX container.

In KNOX 2.x, applications no longer need to be containerized in order to be installed into the container. Any application from Google Play can be installed without modifications as long as application development follows guidelines specified here:

<http://developer.android.com/about/versions/android-4.2.html#MultipleUsers>

Several applications are installed by default during container creation and include basic applications needed for work (calendar, contacts, browser, email, file viewer). These default applications cannot be removed by the user.

In KNOX 2.x, in addition to the Samsung KNOX application store and MDM application push, the administrator can configure the container to allow the user to install applications from Google Play select from a list of applications installed outside the container and install them inside the container. By default, these two policies are disabled.

If the enterprise allows users to install applications inside the container, the enterprise must use MDM policies to whitelist container applications, as well as to enable and disable container applications.

3.3 Container Isolation

The KNOX container provides a completely separated Android environment with its own home screen, launcher, applications, and widgets. Various security mechanisms, such as Security Enhancements (SE) for Android policies, provide isolation of container applications and data from applications and data outside the container, thereby blocking interaction between the two personas.

KNOX container also provides other features to prevent enterprise data leakage.

- Container application access to external storage is blocked by SE for Android policies.
- Device screenshot functions are disabled when inside the container.
- Full content of notifications (received emails) are not shown in the notification bar when outside the container. In KNOX 2.x, MDM policy or user settings can be configured to show full content of notifications.
- Contact and calendar information from outside the container are accessible inside the container. MDM policy or user settings can be configured to show container contacts and calendar events outside the container.
- Container applications are blocked from sharing data with applications outside the container.
- In KNOX 2.x, MDM policy can be configured to allow movement of files between the container and outside the container. Each direction can be configured independently.
Note: The STIG requires movement of files from inside the container to outside the container to be disabled.

3.4 Container Data-at-Rest Encryption

All container data is stored encrypted in a separate file system. Access to the file system is limited to container applications and is enforced by SE for Android policies. Files are encrypted by default using the AES256-CBC cipher, a feature that cannot be turned off. Storage is shared between inside the container and outside the container, so storage for container applications is only limited by the amount of space available on the device.

During container creation, the user is required to enter a container password that will be used to control access into the container. This password is used to generate the container Key Encryption Key (KEK), which is stored securely in TrustZone. The KEK encrypts the per-file Data Encryption Keys (DEKs).

On a device reboot, the container file system is auto-mounted if an email account has been configured inside the container. This is to allow email synchronization to continue in the background even when the user is not using the container in the foreground. The container is allowed to retrieve the KEK from TrustZone in order to auto-mount the file system. However, the user must still enter the password in order to access the container.

3.5 Trusted Boot and Warranty Fuse-Based Container Protection

Samsung Android with KNOX also implements security mechanisms that protect the container when an invalid image is detected during the device boot process. This process works by blocking container creation or by blocking access to the container if a container has already been created.

The primary bootloader (in ROM) does signature verification of the secondary bootloader using public keys fused into the hardware at manufacture (hardware root-of-trust). The secondary bootloader also does signature verification of the kernel image. If the kernel image verification fails (indicating an invalid image has been loaded), then the KNOX Warranty Fuse (a one-time eFuse) is blown. A blown fuse will block container creation and access.

Trusted Boot works by taking cryptographic measurements of the bootloaders and kernel image during device boot and storing these measurements in TrustZone secure memory. A TrustZone secure world application compares these measurements with expected valid measurements. The valid measurements are generated during binary compile time and are signed and stored as a file on the device. A failed measurement check results in container creation and access being blocked.

3.6 Data-in-Transit Protection

The KNOX Enterprise VPN can be configured by MDM to be for full device, for the container, and also for specified applications (per-app). The per-app configuration allows an MDM to select applications (inside or outside the container) to connect to the network via a specified VPN profile. When a VPN profile is configured to be for the container, all outbound traffic from applications inside the container is blocked from leaving the device. When connected, traffic

from applications inside the container is routed via the VPN. Similarly, when a VPN profile is configured as per app, traffic for those specified applications is routed to the network.

3.7 Container Access Control

The KNOX container has a separate authentication mechanism, which is implemented and configured independent of the device lock screen. PIN, password, or pattern or fingerprint can be used to configure the container's authentication factor; however, DoD policy requires either a password or fingerprint to be used.

When the KNOX container is configured with a password and is locked, the user is required to enter the correct password to gain access into the container. The container is locked after a defined idle period of time, on device reboot, or manually by the user from the notification bar. Idle time can be configured by the MDM. This lock mechanism cannot be disabled by the user or the MDM.

If the user enters the wrong password more than a configured number of consecutive attempts, the container will go into an admin locked state. With KNOX 2.x, the MDM can configure the container to wipe in this situation. Only the MDM can reset the container password and unlock the container. The maximum number of failed password attempts can be configured by MDM.

Container password complexity can be configured using MDM policies that are independent of the device lock screen password policies. The policy includes password length, complexity, and expiry.

The MDM can apply specific password policies for the KNOX container password. This is independent of the device password policy. The policy includes password length and complexity, disabling or wiping the container following a configurable number of failed logon attempts, password expiry time, etc.

On devices running Android 5.x or earlier, when the device encryption is turned on, the user is required to configure a device unlock password. The device unlock password is also used as the device encryption password. However, on Android 6.x, a password does not need to be configured when device encryption is turned on and once turned on there is an option that allows the user to enable encryption password. DoD policy requires CC mode to be enabled, which in turn forces password encryption. Also, device encryption is turned on by default on the Galaxy S7. Once enabled, device encryption cannot be turned off on Android 6.x devices.

When the device is rebooted, the user will be required to enter the following sequence of passwords:

- Encryption password: Only needs to be entered on device reboot. Same as the device unlock password.
- Device unlock password: Needs to be entered to unlock the device (personal environment). Device goes into locked state after defined period of user inactivity. Device also boots into a locked state. Length and complexity can be controlled by the

MDM.

- Container password: Unlocks the container, which enables access to the container home screen, applications, and data. Length and complexity can be controlled by the MDM. The STIG allows the use of fingerprint authentication for unlocking the container.

In the current version of KNOX, unlocking the device will not unlock the container. However, for enhanced usability, an MDM-controlled configuration to combine the device unlock and container unlock will be made available in the next upgrade of KNOX. Even though the encryption password is the same, the user will still be required to enter the device encryption password once on every device reboot.

3.8 Container Configuration and Management

The KNOX container can be fully managed by MDM using a variety of policies that are independent of the device policies. The MDM agent is installed outside the container, and therefore the administrator has the option to manage both the entire device and the container. All device-level policies in the Samsung Android OS 6 (with KNOX 2.x) STIG are available, as well as the following container policies:

- Container management policies
- Container application management policies
- Container password policies
- Container email and browser policies

3.8.1 Container Management Policies

Samsung Android with KNOX includes the following MDM controls for container management.

- Create container: KNOX 2.x supports up to two container creations on the device.
- Remove container: Deletes the container and all data and applications inside the container.
- Lock/unlock container: Determines whether the MDM administrator has the ability to lock/unlock the container.

3.8.2 Container Application Management Policies

Users can be allowed to download and install applications into the container from the Samsung KNOX application store, Google Play (KNOX 2.x only), or from applications that are installed outside the container (KNOX 2.x only). However, the MDM can further control container applications using the following policies.

- Package whitelist: MDM can add and remove packages in the whitelist. If configured,

only applications in the whitelist can be installed into the container.

- Install/uninstall packages in the container.
- Enable/disable packages: A user is blocked from using disabled applications. Disabled applications are not uninstalled from the container.
- Start/stop applications: MDM can remotely start and stop applications inside the container.

3.8.3 Container Password Policies

Samsung Android includes the following MDM controls to manage container passwords.

- Set max number of failed password attempts after which the container will be disabled.
- Set expiration (specified in days) for container password.
- Set minimum password length.
- Set idle time after which container will be locked.
- Set the number of passwords to be stored as history. The user will not be able to reuse any of these when changing the password.
- Set the minimum number of changed characters when changing the password.
- Set password to be alphanumeric or complex (i.e., requiring characters other than alphanumeric characters).

3.8.4 Container Email and Browser Policies

Samsung Android with KNOX includes the following MDM controls to configure the native email and browser applications inside the container.

- Set the browser HTTP proxy.
- Enable/disable browser JavaScript.
- Enable/disable browser cookies.
- Enable/disable smart card authentication in the browser: This configures the browser to use CAC. This is the same CAC specified in the Samsung Android 6.0 (with KNOX 2.x) STIG.
- Whitelist/blacklist accounts allowed in email: Accounts can be specified by domain name (e.g., ".@test.com").
- Enable/disable smart card credentials for a specified email account.

Samsung Android with KNOX also includes MDM controls to provision Exchange accounts to be used with the native email client. The following parameters can be configured:

- Email address

- User name
- Domain name
- Sync interval
- Server address
- Use SSL/TLS

3.9 Container Activation

MDM is required to activate the container using a KNOX license during container creation. KNOX licenses are purchased by the enterprise from a KNOX reseller and are managed using MDM. Prior to pushing a container-create policy; the MDM needs to push a KNOX license to the device. On receiving the KNOX license, the MDM agent will trigger the license activation process. An agent running on the device will validate the license with the Samsung KNOX License Management server. Container creation can only proceed if the KNOX license validation succeeds.

3.10 KNOX On-Premise Servers

All services necessary to enable KNOX services on the device are hosted on the cloud. However, the Samsung KNOX On-Premise server is also available for enterprises wanting to deploy and manage KNOX services on premise. DoD implementations are expected to install, configure, and manage the KNOX On-Premise servers on enterprise-managed servers. Samsung provides the On-Premise server install packages, which are available for both Windows and Linux.

The KNOX On-Premise server includes the following components:

- KNOX License Management (KLM) — KLM is the license management and compliance system for Samsung KNOX. KLM is used to activate KNOX services on supported devices.
- Global Server Load Balancing (GSLB) — GSLB is a dictionary server for the various services (e.g., KLM server). The URL for the GSLB server is coded into the enterprise-provided KNOX license. During activation, the GSLB server will return the end points (URL) for the various services to the device agents.

The KNOX On-Premise server can be installed on both Windows and Linux distributions. Current versions supported are RHEL 6.4 64bit, CentOS 6.4 64bit, Windows 2008 R2, and Windows 2012 R2.

An enterprise that decides to deploy the KNOX On-Premise server will request the appropriate KNOX license from the KNOX reseller. The enterprise will provide its on-premise GSLB server URL, which will be encoded into the KNOX license.

The MDM agent will pass the KNOX license to a KLM agent running off the device. This agent will connect to the GSLB server, which will return the KLM server URL. The agent then connects to the KLM server to get KNOX license validation.

4. SAMSUNG KNOX FOR ANDROID IA FEATURES

The Samsung Android with KNOX platform builds on top of the Android platform to provide strong guarantees for the protection of enterprise data by constructing a hardware-rooted trusted environment. This was accomplished by adding security features across the full software stack, from the bootloaders, kernel, TrustZone, and Android framework.

Key IA features found in Samsung Android with KNOX that are not present in typical Android devices are:

- Mobile application quarantine
- Container support
- Smart card support
- Host-based firewall
- Ability to revoke mobile application permissions
- Over-the-air (OTA) audit log retrieval
- Support for PKI authentication and certificate verification in native browser

4.1 Samsung Android Device Disposal

For Samsung Android devices never exposed to classified data, follow this procedure prior to disposing of (or transferring to another user) a mobile device via site property disposal procedures:

- Follow device manufacturer's instructions for wiping all user data and installed applications from the device memory.

4.2 Samsung Device Encryption Guidelines

When device encryption is enabled for the first time, the user is given the option of doing a fast encryption. Users should be guided to enable fast encryption before starting the initial encryption process. The difference between a full encryption (fast encryption disabled) and fast encryption is the following:

- Full encryption encrypts the entire disk, including slack.
- Fast encryption encrypts only the files on the device but not slack, so the initial encryption time can be considerably less than full encryption.

Future files are encrypted regardless of the full or fast encryption.

5. SAMSUNG KNOX FOR ANDROID USER-BASED ENFORCEMENT

There are various features available on the device that, when enabled by the user, could result in unauthorized persons gaining access to sensitive information on the device. For those features that cannot be disabled by MDM, the mitigation must include proper training of individual users.

5.1 Calendar Alarm

The default Samsung pre-installed Calendar application allows users to create events that include event title, location, date and time, and also notification alarms for the event. When the alarm is configured, at the specified time the event details will be shown on the device screen, even when the device is in a locked state. Users should be trained to not configure this option, or to not include any sensitive information in the event title and location.

5.2 Content Transferring and Screen Mirroring

Samsung devices include various ways that allow the user to transfer files on their device to other devices and to display content from their device on select Samsung Smart TVs.

The "Quick Connect" feature is accessed from the notification bar and displays a list of scanned devices that the user's device can connect to. The user can select a device from this list to transfer selected files to (either via Wi-Fi direct or Bluetooth), or to do screen mirroring. Depending on the selected device's capabilities, either Miracast or DLNA technology will be used to provide screen mirroring. Both Miracast and DLNA will work over a Wi-Fi direct connection or with devices connected to the same Wi-Fi access point. Whereas Miracast renders whatever is on the device screen to the target device, DLNA requires the playback on the target device.

The user can also transfer a file by selecting the file and then selecting "Share" and "Nearby sharing".

Screen mirroring can also be initiated by selecting the file and then selecting "Share" and "Smart View".

Users should be trained to not enable these options unless they are authorized to do so and they visually verify the recipient device. Users should be trained to not enable these options unless using an approved DoD screen mirroring technology with FIPS 140-2 validated Wi-Fi. Miracast must only be used with TVs, monitors, and Miracast dongles with FIPS 140-2 validated Wi-Fi clients.

5.3 Content Sharing

Select Samsung devices include the "Nearby devices" feature. This allows the user to share files on their device with other devices over a Wi-Fi connection by allowing other devices to connect to the user's device and download selected files (videos, photos, music) to their own device. This is disabled by default but can be enabled by the user from the following setting:

Device settings >> More connection settings >> (Media share) Nearby devices

5.4 Report Diagnostic Information

Samsung devices include the "Report diagnostic info" feature, which allows the device to collect diagnostic and usage data and automatically transmit this data to Samsung servers. The purpose is to allow Samsung to analyze the data to improve product and service quality and address unexpected shutdowns or system errors.

Device settings >> Privacy and safety >> Report diagnostic info

Device settings >> Privacy and safety >> About device

Users should be trained to not enable this option.

6. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES

The Samsung KNOX for Android supports application disable policies that allow administrators to disable core and preinstalled applications¹ by specifying package names. Because each device and operator variant will be pre-installed with different sets of applications, the administrator must identify any applications that could pose a threat to sensitive information on the device and disable such applications by configuring application disable policies.

6.1 Public Cloud Backup Applications

Android allows users to back up and sync application data, user files, and settings to Google servers or other third-party cloud services, such as Samsung accounts and Dropbox. Samsung Android with KNOX supports policy to disable Google backup, but other third-party services must be disabled using application disable policies. The administrator must identify any such service pre-installed on the device and disable these applications. This list includes:

- Samsung account
- Dropbox
- Drive (Google)
- OneDrive (Microsoft)

6.2 Social Networking Applications

Many social networking services allow users to upload files, as well as synchronize contacts information to their servers. The administrator must identify any such service pre-installed on the device and disable these applications. This list includes:

- Google+
- Facebook
- Twitter
- Instagram

6.3 Data Uploading Applications

Various applications will upload information to the service provider's servers. The administrator must identify any such service pre-installed on the device and disable these applications. This list includes:

- S Voice

¹ A core app is defined as an app bundled by the operating system vendor (for example, Google). A preinstalled app is included on the device by a third-party integrator, including the device manufacturer or cellular service provider (for example Samsung, Verizon Wireless, or AT&T).

6.4 Content-Sharing Applications

Samsung devices include various methods that allow a device to share content with or send content to other devices nearby. The administrator must identify any such service pre-installed on the device and disable these applications. This list includes:

- Group Play

6.5 Mobile Printing

Mobile printing applications provide the capability for wireless printing from a Samsung Android device. Information, including security requirements, for setting up mobile printing services on a DoD network will be included in the MultiFunction Device STIG in the near future. DoD Samsung Android devices should connect to only approved DoD-managed mobile printing services.

6.6 Core and Preinstalled Applications

6.6.1 Introduction

The core and preinstalled application lists below may not reflect the exact list on any specific device that is being reviewed. Small modifications to app names or app package names can be expected between various carriers' OS builds. Also, additional apps not on the lists may be included in an OS build, or the OS build may not include all apps on a list. The app lists below should be compared to the list of apps installed on a device being reviewed.

It is the responsibility of the Authorizing Official's (AO's) designated representative to update the following tables as new Samsung KNOX 2.x devices and firmware are deployed in the DoD inventory.

6.6.2 Disabled Core and Preinstalled Applications

Tables 6-1 and 6-2 list core and preinstalled applications that should be disabled. Risk in using these apps in the DoD environment is considered to be high. DoD Commands and Agencies should fully vet these apps, using the Application Software protection Profile (APPSWPP), prior to approving their use.

Table 6-1: Disabled Applications – Personal Area

Application Package Name	Application Name
com.amazon.fv	Amazon App Suite
com.amazon.mp3	Amazon Music
com.amazon.mShop.android	Amazon
com.android.vending	Google Play Store
com.asurion.android.mobilerecovery.att	AT&T Mobile Locate AT&T Protect Plus

Application Package Name	Application Name
com.asurion.android.verizon.vms	Verizon Support & Protection
com.att.android.digitallocker	AT&T Locker
com.att.android.mobile.attmessages	AT&T Messages
com.att.myWireless com.m.att	myAT&T
com.google.android.apps.books	Google Play Books
com.google.android.apps.docs	Drive
com.google.android.gm	Gmail
com.google.android.music	Google Play Music
com.google.android.talk	Hangouts
com.google.android.videos	Google Play Movies & TV
com.google.android.youtube	YouTube
com.gotv.nflgamecenter.us.lite	NFL Mobile
com.hancom.office.editor com.hancom.office.editor.hidden	Hancom Office 2014
com.imdb.mobile	IMDb
com.infracore.polarisoffice5	POLARIS Office 5
com.matchboxmobile.wisp	AT&T Hot Spots
com.mobitv.client.tv	Mobile TV
com.osp.app.signin	Samsung account
com.sec.app.samsungprintservice	Samsung Print Service Plugin
com.sec.penup	PEN.UP
com.slacker.radio	Slacker Radio
com.vcast.mediamanager	Cloud
com.verizon.messaging.vzmsgs	Message+
com.vzw.hss.myverizon com.vzw.hss.myverizontabletlt	My Verizon Mobile
com.wavemarket.waplauncher	AT&T FamilyMap
com.sec.android.app.samsungapps	Galaxy Apps
com.google.android.play.games	Google Play Games
com.facebook.katana	Facebook
com.yahoo.mobile.client.android.yahoo.att	AT&T Live
com.locationlabs.cni.att	Smart Limits
net.aetherpal.device	AT&T Remote Support
com.sec.att.usagemanager3	Usage Manager
com.att.mobiletransfer	AT&T Mobile Transfer
com.yellowpages.android.yppmobile	YP
com.yahoo.mobile.client.android.mail.att	AT&T Mail
com.samsung.android.service.peoplestripe	PeopleStripe
com.locationlabs.sparkle.blue	Family Utility
com.ubercab	Uber
com.microsoft.office.onenote	OneNote

Application Package Name	Application Name
com.microsoft.office.powerpoint	PowerPoint
com.microsoft.office.word	Word
com.microsoft.office.excel	Excel
com.microsoft.skydrive	OneDrive
com.skype.raider	Skype
com.samsung.mdl.radio	Milk
com.instagram.android	Instagram
com.google.android.apps.plus	Google+
com.whatsapp	WhatsApp
com.lookout	Lookout
com.audible.application	Audible
com.google.android.apps.magazines	Google Play Newsstand
com.sec.android.sidesync30	SideSync
com.hancom.office.viewer com.hancom.androidpc.viewer.launcher	Hancom Office Viewer
com.facebook.pages.app	Pages Manager
com.google.android.apps.walletnfcrel	Android Pay
com.samsung.android.spay	Samsung Pay
com.wildtangent.android	Games
com.americanexpress.plenti	Plenti
com.google.android.apps.photos	Photos
com.amazon.windowshop	Amazon
com.att.android.tablet.attmessages	Messages
com.directv.navigator com.directv.dvrscheduler	DIRECTV
com.directv.promo.shade	Remote
com.synchronoss.dcs.att.r2g	AT&T Ready2Go
tv.peel.smartremote	Smart Remote
com.smartcom	AT&T AllAccess
com.att.android.attsmartwifi	AT&T Smart Wi-Fi
com.samsung.helphub	Help
com.dti.att com.LogiaGroup.LogiaDeck	DT Ignite
<i>Note: The following applications are not included in 6.0 firmware. However, devices with 5.x firmware will retain these installed applications on upgrading to 6.0 firmware; therefore, these must be kept on the disabled application list.</i>	
com.amazon.venezia	Appstore
com.att.digitallife.android.phone22	Digital Life
com.beatsmusic.android.client	Beats Music
com.callpod.android_apps.keeper	Keeper
com.dropbox.android	Dropbox
com.facebook.orca	Messenger
com.hp.android.printservice	HP Print Service Plugin

Application Package Name	Application Name
com.intsig.camdict	CamDictionary
com.isis.mclient.atnt.activity	Wallet
com.isis.mclient.verizon.activity	Isis Wallet
com.samsung.milk.milkvideo	Milk Video
com.sec.chaton	ChatON
com.verizon.familybase.companion	FamilyBase Companion

Table 6-2: Disabled Applications – Container

Application Package Name	Application Name
com.hancom.office.editor com.hancom.office.editor.hidden	Hancom Office 2014
com.infraware.polarisoffice5	POLARIS Office 5
com.osp.app.signin	Samsung Account
com.sec.android.app.samsungapps	Galaxy Apps
com.hancom.office.viewer com.hancom.androidpc.viewer.launcher	Hancom Office Viewer
com.google.android.gm	GMail

6.6.3 Approved Core and Preinstalled Applications

Tables 6-3 and 6-4 list core and preinstalled applications that are recommended for approval. DoD Commands and Agencies should consider vetting these apps using the Application Software Protection Profile (APPSWPP).

Table 6-3: Applications Recommended for Approval – Personal Area

Application Package Name	Application Name
com.amazon.kindle	Amazon Kindle
com.android.calendar com.samsung.android.calendar	Calendar
com.android.chrome	Chrome
com.android.contacts com.samsung.android.contacts	Contacts
com.android.email (5.x only) com.samsung.android.email.provider (6.x)	Email
com.android.exchange	Exchange Services
com.android.mms com.samsung.android.messaging	Messaging
com.android.phone	Phone
com.android.providers.downloads.ui	Downloads
com.drivemode	DriveMode
com.google.android.apps.maps	Maps
com.google.android.googlequicksearchbox	Google Search

Application Package Name	Application Name
com.google.android.street	Street View
com.matchboxmobile.wisp	AT&T Hot Spots
com.samsung.android.app.memo	Memo
com.samsung.android.app.pinboard	Scrapbook
com.samsung.android.snote	S Note
com.samsung.android.app.notes	
com.samsung.verglades.video	Video
com.sec.android.app.camera	Camera
com.sec.android.app.clockpackage	Clock
com.sec.android.app.dictionary	Dictionary
com.sec.android.app.music	Music
com.sec.android.app.myfiles	My Files
com.sec.android.app.popupcalculator	Calculator
com.sec.android.app.sbrowser	Internet
com.sec.android.app.shealth	S Health
com.sec.android.app.videoplayer	Video Player
com.sec.android.app.voicenote	Voice Recorder
com.sec.android.automotive.drivelink	Car mode
com.sec.android.gallery3d	Gallery
com.sec.android.GeoLookout	Geo News
com.sec.android.widgetapp.ap.hero.accuweather	Weather
com.sec.android.widgetapp.SPlannerAppWidget	Calendar
com.telenav.app.android.cingular	AT&T Navigator
com.vznavigator.Generic	VZ Navigator
com.vznavigator.Tablet	
com.yahoo.mobile.client.android.liveweather	Live weather
flipboard.app	Flipboard
flipboard.boxer.app	Briefing
tv.peel.smartremote	Smart Remote
com.samsung.android.video	Video
com.samsung.android.email.ui	Email
tv.peel.app	Smart Remote
com.samsung.android.app.watchmanager	Samsung Gear

Table 6-4: Applications Recommended for Approval – Container

Application Package Name	Application Name
com.android.calendar	Calendar
com.samsung.android.calendar	
com.android.chrome	Chrome
com.android.contacts	Contacts
com.samsung.android.contacts	
com.android.email (5.x only)	Email

Application Package Name	Application Name
com.samsung.android.email.ui	
com.samsung.android.email.provider (6.x)	
com.android.exchange	Exchange Services
com.samsung.android.app.memo	Memo
com.samsung.android.app.pinboard	Scrapbook
com.samsung.android.snote	
com.samsung.android.app.notes	S Note
com.samsung.everglades.video	Video
com.sec.android.app.camera	Camera
com.sec.android.app.music	Music
com.sec.android.app.myfiles	My Files
com.sec.android.app.sbrowser	Internet
com.sec.android.app.videoplayer	Video Player
com.sec.android.gallery3d	Gallery
com.samsung.android.video	Video
com.android.vending	Play for Work Inside KNOX

6.7 Auditing/Reviewing Device Applications

Applications are controlled by three APIs: application whitelist, application blacklist, and application disable. The application whitelist and blacklist are used to control installed applications. All applications are added to the blacklist using the "."* wildcard so that only applications listed on the whitelist can be installed. Approved core and preinstalled applications are added to the whitelist so that updates can be installed. Application disable is used to disable undesirable/unapproved core and preinstalled applications. Core and preinstalled applications listed on the "disable" list are not removed from the device but cannot be seen and/or launched by the user. There are two sets of these controls, one for applications in the personal area of the device and one for applications in the container.

The following procedures are recommended for performing an audit/review of applications on the Samsung KNOX 2.0 for Android devices:

1. Installed applications (these steps are performed separately for personal area and container):
 - Review the list of applications listed on the whitelist on the MDM Administration console.
 - Verify all apps on the list have been approved by the AO.

Note: Core and preinstalled applications included in Tables 6-3 and 6-4 are considered approved for DoD use unless expressly disapproved by the AO.

2. Core and preinstalled applications (these steps are performed separately for personal area and container):
 - View the list of "disable" core and preinstalled apps on the MDM Administration console. Tap the "Apps" menu button to view all installed apps. Verify all apps on the "disabled" list are either not shown on the Apps menu or cannot be launched.
 - Generate a list of applications installed on the Samsung device:
 - o Tap the "Apps" menu button to view all installed apps.
 - o Remove any app on the whitelist from this list.

Note: The whitelist may include approved core and preinstalled apps.

Verify all apps remaining on the list have been approved by the AO.

7. SAMSUNG WEARABLES

The use of Samsung Wearables is based on the approval of the AO. Because the Samsung Wearables do not have access to the KNOX container, no further configuration is required. The Samsung Gear Manager Application Package File (APK) would be required to integrate the wearable to the Samsung smartphone.

This APK is available upon request from Samsung and can be deployed using the incumbent MAM/MDM solution. Please contact your local Samsung representative to obtain the needed APK file.

8. PLAY FOR WORK INSIDE KNOX CONTAINER

Google Play for Work Inside KNOX is an enterprise-controlled application store for enterprises using Android for Work. The enterprise administrator controls all applications that are available to their users and can use Google Play for Work Inside KNOX to securely push application installs to their users. Applications that are made available on the enterprise's Google Play for Work Inside KNOX application store can be selected from the public Google Play application store or can be private applications developed by the enterprise.

The Play for Work Inside KNOX container feature allows enterprises to make Play for Work available inside the KNOX container without having to create an Android for Work profile on the device. However, the enterprise administrator will have to set up and manage the enterprise's Play for Work application store.

This feature provides an alternative to using MDM to manage application installs. Not only can the administrator push application installs to users for mandatory applications, the administrator can also make a set of vetted applications available for their users to install at any time.

Play for Work Inside KNOX can be implemented when approved by the AO. Table 3 in the Configuration Tables document lists the required security policy controls when using Play for Work Inside KNOX.