

UNCLASSIFIED



SAMSUNG ANDROID OS 5 WITH KNOX 2.x SUPPLEMENTAL PROCEDURES

Version 1, Release 4

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	9
3.10 Knox On-Premise Servers.....	10
4. SAMSUNG KNOX FOR ANDROID IA FEATURES	11
4.1 Samsung Android Device Disposal	11
4.2 Samsung Device Encryption Guideline	11
5. SAMSUNG KNOX FOR ANDROID USER BASED ENFORCEMENT	12
5.1 Calendar Alarm	12
5.2 Content Sharing.....	12
5.3 Screen Mirroring	12
5.4 Report diagnostic information.....	12
6. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES	14
6.1 Public cloud backup applications.....	14
6.2 Social networking applications	14
6.3 Data uploading applications	14
6.4 Content sharing applications	15
6.5 Mobile Printing	15
6.6 Core and Preinstalled Applications	15
6.6.1 Introduction.....	15

6.6.2 Disabled Core and Preinstalled Applications	15
6.6.3 Approved Core and Preinstalled Applications	18
6.7 Auditing/Reviewing Device Applications	20
7. SAMSUNG WEARABLES.....	21

LIST OF TABLES

	Page
Table 6-1: Disabled Applications - Personal Area	15
Table 6-2: Disabled Applications - Container	18
Table 6-3: Applications Recommended for Approval - Personal Area.....	18
Table 6-4: Applications Recommended for Approval - Container.....	19

1. SECURITY READINESS REVIEW

1.1 General

When conducting an Samsung Android 5.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 5.x platform, its associated network infrastructure, and the individual devices comprising the system.

1.2 Mobile Policy Registration

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at: <http://iase.disa.mil/stigs/mobility/Pages/policies.aspx>. Use the Mobility Policy STIG to review the General Wireless Policy asset and the 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 APIs for third-party solution vendors to develop Knox security components that can be used to implement several MDFPP STIG Template IA controls. This allows for the integration of any third-party applications and components to achieve compliance to the Samsung Android OS 5 (with Knox 2.x) STIG. The APIs that are provided by the Samsung Android with Knox platform are:

- The Samsung MDM API includes over 600 policies and 1300 interfaces that are 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 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 enables Samsung Android with Knox to support applications leveraging the DoD Common Access Card (CAC) for PKI related transactions, including user authentication to DoD networks and website, 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 Knox for Android solution MDFPP STIG Template compliance is achieved through means other than direct implementation of the required IA control:

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

- Samsung Knox for Android 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 Knox for Android supports a dual-persona capability using "container" technology. The container provides a secure and isolated workspace for enterprise applications and data. Enterprise data and applications are placed inside the container. General productivity and morale applications and data reside outside the container. The user of the device has a separate home screen, launcher and widgets for resources inside and outside of 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 of the container where users are prohibited from performing DoD mission activities or storing DoD sensitive data outside of the container. While DoD organizations, at their discretion, may permit limited personal activity outside of 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 Knox for Android 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 or allow the user to 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 in the container, the enterprise can 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 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 in each direction 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 (KEK).

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 Knox for Android 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 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 password-based authentication mechanism, which is implemented and configured independent of the device lock screen. When the Knox container 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 MDM. This lock mechanism cannot be disabled by user or 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, which 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 login attempts, password expiry time, etc.

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. 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 MDM. However, device encryption can only be enabled if the password is at least six characters long (alphanumeric). Note that DoD policy requires the device unlock password to be only four characters when not used to protect sensitive DoD data, but the Samsung Knox for Android platform will force a 6-character password when device encryption is enabled.
- Container password: Unlocks the container, which enables access to the container home screen, applications, and data. Length and complexity can be controlled by MDM.

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. However, 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, which are independent of the device policies. The MDM agent is installed outside the container, and as such, the administrator has the option to manage both the entire device and the container. All device-level policies in the Samsung Android OS 5 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 Knox for Android 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 install 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 Knox for Android 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 Smartcard authentication in the browser: This configures the browser to use CAC. This is the same CAC specified in the Samsung Knox for Android STIG.
- Whitelist/blacklist accounts allowed in email: Accounts can be specified by domain name (e.g., ".@test.com").
- Enable/disable Smartcard credentials for a specified email account.

Samsung Knox for Android 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 (KLM) 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)**
Global Server Load Balancing 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 their 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 Knox for Android platform builds on top of the Android platform to provide strong guarantees for the protection of enterprise data by building 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 Knox for Android 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 Guideline

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 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 Sharing

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

Device settings >> Nearby device
Pull down the notification bar >> Quick connect

5.3 Screen Mirroring

Samsung devices also include the "Screen mirroring" feature that allows the user's device to display the device screen to another device (e.g., TV) that supports Samsung Link. This is by default disabled but can be enabled by the user from the following setting.

Device settings >> Screen mirroring

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. Samsung Link must only be used with FIPS 140-2 validated Wi-Fi clients.

5.4 Report diagnostic information

Samsung devices include the "Report diagnostic info" feature that 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. As 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 backup and sync application data, user files, and settings to Google servers or other third party cloud services, such as Samsung accounts and Dropbox. Samsung Knox for Android 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:

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).

- S Health
- S Voice

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 Approving Official'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

Application Package Name	Application Name
com.amazon.mShop.android	Amazon
com.amazon.venezia	Appstore
com.android.vending	Google Play Store
com.asurion.android.mobilerecovery.att	AT&T Mobile Locate
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.beatsmusic.android.client	Beats Music
com.drivemode	DriveMode
com.google.android.apps.books	Google Play Books
com.google.android.apps.docs	Drive
com.google.android.apps.maps	Maps
com.google.android.gm	Gmail
com.google.android.googlequicksearchbox	Google Search
com.google.android.music	Google Play Music
com.google.android.street	Street View
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	Hancom Office 2014
com.hp.android.printservice	HP Print Service Plugin
com.imdb.mobile	IMDb
com.infracore.polarisoffice5	POLARIS Office 5
com.intsig.camdict	CamDictionary
com.isis.mclient.atnt.activity	Wallet
com.isis.mclient.verizon.activity	Isis Wallet
com.matchboxmobile.wisp	AT&T Hot Spots
com.mobitv.client.tv	Mobile TV
com.osp.app.signin	Samsung account
com.samsung.everglades.video	Video
com.sec.android.app.popupcalculator	Calculator
com.sec.android.widgetapp.SPlannerAppWidget	Calendar
com.sec.app.samsungprintservice	Samsung Print Service Plugin
com.sec.chaton	ChatON
com.sec.penup	PEN.UP
com.slacker.radio	Slacker Radio
com.telenav.app.android.cingular	AT&T Navigator
com.vcast.mediamanager	Cloud
com.verizon.familybase.companion	FamilyBase Companion

Application Package Name	Application Name
com.verizon.messaging.vzmsgs	Message+
com.vznavigator.Generic com.vznavigator.Tablet	VZ Navigator
com.vzw.hss.myverizon com.vzw.hss.myverizontabletlte	My Verizon Mobile
com.wavemarket.waplauncher	AT&T FamilyMap
com.dropbox.android	Dropbox
com.sec.android.app.samsungapps	Galaxy Apps
com.samsung.milk.milkvideo	Milk Video
com.google.android.play.games	Google Play Games
com.facebook.katana	Facebook
com.facebook.orca	Messenger
com.yahoo.mobile.client.android.yahoo.att	AT&T Live
com.locationlabs.cni.att	Smart Limits
com.att.digitallife.android.phone22	Digital Life
net.aetherpal.device	AT&T Remote Support
com.sec.att.usagemanager3	Usage Manager
com.att.mobiletransfer	AT&T Mobile Transfer
com.yellowpages.android.ypmobile	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
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.callpod.android_apps.keeper	Keeper
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

Application Package Name	Application Name
com.google.android.apps.photos	Photos
com.amazon.windowshop	Amazon
com.att.android.tablet.attmessages	Messages
com.directv.navigator	DIRECTV
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.android.app.watchmanager	Samsung Gear
com.samsung.helphub	Help

Table 6-2: Disabled Applications - Container

Application Package Name	Application Name
com.hancom.office.editor	Hancom Office 2014
com.infracore.polarisoffice5	POLARIS Office 5
com.osp.app.signin	Samsung account
com.sec.android.app.samsungapps	Galaxy Apps
com.hancom.office.viewer	Hancom Office Viewer
com.hancom.androidpc.viewer.launcher	

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	Calendar
com.android.chrome	Chrome
com.android.contacts	Contacts
com.android.email	Email
com.android.exchange	Exchange services
com.android.mms	Messaging
com.android.phone	Phone
com.android.providers.downloads.ui	Downloads
com.drivemode	DriveMode
com.google.android.apps.maps	Maps
com.google.android.gm	Gmail
com.google.android.googlequicksearchbox	Google Search
com.google.android.street	Street View

Application Package Name	Application Name
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.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.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

Table 6-4: Applications Recommended for Approval - Container

Application Package Name	Application Name
com.android.calendar	Calendar
com.android.chrome	Chrome
com.android.contacts	Contacts
com.android.email	Email
com.android.exchange	Exchange services
com.samsung.android.app.memo	Memo
com.samsung.android.app.pinboard	Scrapbook
com.samsung.android.snote	S Note
com.samsung.verglades.video	Video

Application Package Name	Application Name
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.samsung.android.email.ui	Email

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 Approving Official (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 that 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 Authorizing Official (AO). As 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 incumbent MAM/MDM solution. Please contact your local Samsung representative to obtain the needed APK file.