

UNCLASSIFIED



# **SAMSUNG ANDROID OS 8 WITH KNOX 3.X STIG SUPPLEMENTAL PROCEDURES**

**Version 1, Release 4**

**25 October 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

	<b>Page</b>
<b>1. SECURITY READINESS REVIEW .....</b>	<b>1</b>
1.1 General .....	1
1.2 Mobile Policy Registration .....	1
<b>2. KNOX 3.X CHANGES.....</b>	<b>2</b>
2.1 Unification.....	2
2.2 What Happens to Existing Knox 2.x Containers?.....	2
2.3 How Are Knox 3.x Workspaces Created? .....	3
<b>3. CONFIGURATION OF THE PERSONAL SPACE.....</b>	<b>4</b>
<b>4. CONFIGURATION OF COBO .....</b>	<b>6</b>
<b>5. CONFIGURATION OF COPE CONTAINER.....</b>	<b>7</b>
5.1 Overview .....	7
5.2 Container Isolation .....	7
<b>6. INFRASTRUCTURE .....</b>	<b>8</b>
6.1 Knox SDK.....	8
6.2 Knox Licensing .....	8
6.3 Knox On-Premise Servers.....	8
<b>7. DEVICE SECURITY .....</b>	<b>10</b>
7.1 Biometric Authentication .....	10
7.2 Data-at-Rest Encryption.....	10
7.3 Trusted Boot and Warranty Fuse .....	11
7.4 Samsung Android Device Disposal .....	11
<b>8. DOD PKI PUREBRED.....</b>	<b>12</b>
<b>9. SAMSUNG KNOX FOR ANDROID USER-BASED ENFORCEMENT .....</b>	<b>13</b>
9.1 Calendar Alarm .....	13
9.2 Content Transferring and Screen Mirroring.....	13
9.3 Report Diagnostic Information .....	14
9.4 Google Usage and Diagnostics .....	14
9.5 Certificate Removal .....	14
9.6 Samsung DeX Station .....	14
9.7 Smart Call.....	15
9.8 Samsung Wi-Fi Sharing .....	15
9.9 VPN Profiles .....	15
<b>10. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES .....</b>	<b>16</b>
10.1 Public Cloud Backup Applications.....	16
10.2 Content Sharing Applications.....	16
10.3 Mobile Printing .....	16
10.4 Core and Preinstalled Applications.....	17

10.5	Auditing/Reviewing Device Applications .....	21
<b>11.</b>	<b>ADDITIONAL SAMSUNG FEATURES .....</b>	<b>23</b>
11.1	Samsung Wearables .....	23
11.2	Google Location Tracking on Samsung Devices.....	23
11.3	Tactical Use Case.....	24

## LIST OF TABLES

	<b>Page</b>
Table 10-1: Mandatory Disablements – Personal Area .....	17
Table 10-2: Mandatory Disablements – Work Environment.....	17
Table 10-3: Optional Disablements .....	18
Table 11-1: List of Tactical Changes to STIG Requirements with Recommended Mitigations..	25



## **1. SECURITY READINESS REVIEW**

### **1.1 General**

When conducting a Samsung Android 8.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 8.x platform, its associated network infrastructure, and the individual devices that make up the system.

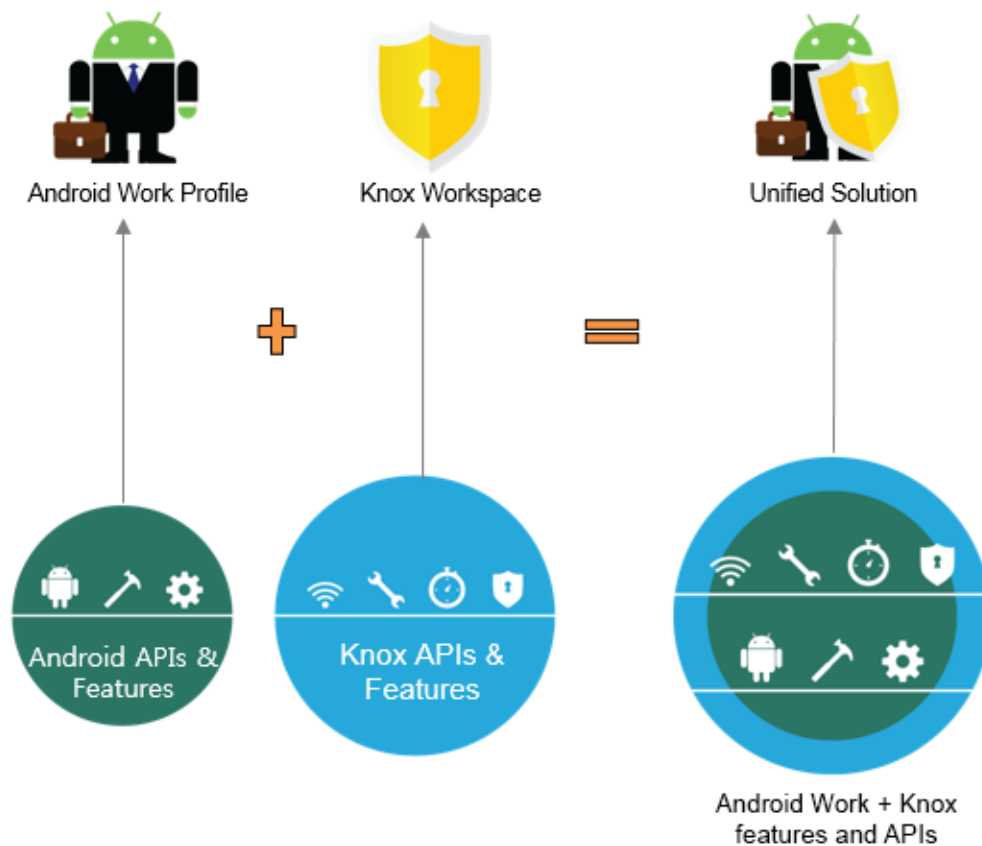
### **1.2 Mobile Policy Registration**

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 Mobile Policy STIG to review the General Wireless Policy asset and the CMD Policy STIG to review the Smartphone Handheld asset.

## 2. KNOX 3.X CHANGES

### 2.1 Unification

The most important improvement introduced in Knox 3.x is Android Enterprise Unification. Samsung and Google have collaborated to combine Android Enterprise and Samsung Knox into one unified solution. As part of unification, enterprises can leverage Samsung Knox features and application program interfaces (APIs) on Android Enterprise Work Profile and Managed Device modes by simply activating a Samsung Knox License. This enables Enterprise Mobile Management (EMM) agents to apply both Android and Samsung Knox APIs on one solution.



#### 2.1.1 Deprecated Containers

Knox 2.x containers are now considered legacy and will be deprecated once the unified solution is adopted and supported by EMM partners. Until then, all legacy containers will continue to be available and supported in Knox 3.x.

### 2.2 What Happens to Existing Knox 2.x Containers?

All legacy Samsung Knox containers will continue to be available in Knox 3.x. For Corporate Liable (CL)/B2B Workspaces implemented using the previous STIG, the only noticeable changes when upgrading to Knox 3.x will be:



- The container name changes from “Knox” to “Workspace”; and
- If biometric data (Fingerprint, IRIS) has been registered, the user will be asked to reregister the biometric data (user may postpone registration).

## **2.3 How Are Knox 3.x Workspaces Created?**

Once the unified solution is adopted and supported by EMM partners, the Mobile Device Management (MDM) will create Knox 3.x workspaces through the Android Enterprise Work Profile and Managed Device modes. Until then, legacy containers will be used.

### **2.3.1 Default Apps**

Android Enterprise enables the following default apps (Knox does not enable additional apps):

- Contacts
- My Files
- Google Play Store

### **2.3.2 Default Policies**

In Knox 3.x, a newly set up device is permissive by default. The following are examples of functions that are no longer restricted by default:

- USB debugging
- Screen capture
- Bluetooth
- NFC
- Copy/paste from profile to device
- Password enablement

### 3. CONFIGURATION OF THE PERSONAL SPACE

Section 1.1 of the Overview document states that the scope of this STIG includes the Corporate Owned Personally Enabled (COPE) use case where both a personal space and work container are set up on the Samsung Android 8 device.

DoD mobile service providers may allow users full access to the Google Play app store for the personal space, including downloading and installing Google Play apps and syncing personal data on the device with personal cloud data storage accounts when ALL of the following conditions have been met:

- The site Authorizing Official (AO) has approved full access to the Google Play app store for the personal space, including downloading and installing Google Play apps into the personal space and syncing personal data on the device with personal cloud data storage accounts<sup>1</sup>. Written approval must be available for any system compliance review.
- The site AO has provided guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.) in the Samsung device personal space (guidance can be added to user training or the User Agreement).
- Site mobile devices are configured with a work-only container technology or application that is NIAP certified. Currently Samsung Knox is the only NIAP-certified container technology or application for Samsung mobile devices.
- The site MDM is configured to restrict the download of apps from all third-party app stores.
- The MDM or user to restrict the use of DoD VPN profiles within the personal space configures site mobile devices.
- Site mobile device users receive training on known Google Play application risks and required STIG controls that must be enabled by the user (User Based Enforcement)<sup>2</sup>. See STIG requirement KNOX-08-008100 for more information.

This STIG assumes all of the conditions above have been met and allows full user access to the personal space. If the AO has not approved unrestricted use of the personal space, the AO should consider implementing the following COPE Configuration Policy Rules for Non-Work Environment policy controls:

- Android Market/Google Play (disable)
- Application White list (Package Name/Signature White List) (configure)
- Application Black List (Package Name/Signature Black List) (configure)
- Google Accounts Auto Sync (disable)
- Bixby Vision (disable)

---

<sup>1</sup> It is recommended that the AO provide guidance on types of apps that should be avoided in the Google app store due to known risky functions or behaviors.

<sup>2</sup> UBE controls cannot be managed by the site MDM server and, therefore, must be managed by the mobile device user. See Section titled *Configuration of COPE Container* in this document for more information.

- S Voice (disable)
- Samsung Accounts (disable)
- Back up MD data to non-DoD cloud servers (disable)
- Voice assistant application if available when MD is locked (disable)
- Voice dialing application if available when MD is locked (disable)
- Applications that allow synchronization of data or applications between devices associated with user (disable or remove)
- Applications that allow unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers (disable or remove)
- Display of notifications when screen is locked (disable)
- Application disable list (core and preinstalled apps not approved by AO)

#### **4. CONFIGURATION OF COBO**

In the COBO use case, a container is not required to provide isolation from personal applications, and the Managed Device mode provides a secure environment for enterprise applications and data.

## 5. CONFIGURATION OF COPE CONTAINER

### 5.1 Overview

The container provides an isolated and independent workspace for enterprise applications and data when implementing the COPE use case. Enterprise data and applications are placed inside the container, while personal applications and data reside outside the container. The user of the device has separate resources inside and outside of the container.

### 5.2 Container Isolation

The Knox container provides a completely separated Android environment with its own home screen, launcher, applications, and data. 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. Upon provisioning, the device is configured to not restrict the user's ability to allow data to pass through the container barrier. An administrator must explicitly restrict this behavior through APIs as indicated in the STIG configuration table.

## 6. INFRASTRUCTURE

### 6.1 Knox SDK

The Samsung Knox 3.x SDK provides various APIs for third-party MDM solution vendors to configure Knox security components that can be used to implement several Mobile Device Fundamentals Protection Profile (MDFPP) STIG Template Information Assurance (IA) controls. These APIs can be used to configure restrictions on the device and a container. The Knox container can be fully managed by MDM using a variety of policies that are independent of the device policies.

Some policies, such as application whitelist and password requirements, must be applied separately for the personal area and container. Others, such as disabling Wi-Fi, can only be applied at a device-wide level. This behavior is reflected in the STIG configuration table for mandatory policies.

### 6.2 Knox Licensing

MDM is required to activate a Knox Workspace license prior to getting access to the full range of Samsung Knox features and APIs. Knox licenses are purchased by the enterprise from a Knox reseller and are managed using MDM. An agent running on the device will validate the license with the Samsung Knox License Management (KLM) server.

### 6.3 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):** The license management and compliance system for Samsung Knox. KLM is used to activate Knox services on supported devices.
- **Global Server Load Balancing (GSLB):** 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 endpoints (URL) for the various services to the device agents.

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.

## 7. DEVICE SECURITY

### 7.1 Biometric Authentication

Selected Samsung Android 8 devices incorporate fingerprint, facial, and iris biometric authentication mechanisms that can be configured to allow users to authenticate to unlock the device and also the Knox Workspace Container (as part of two-step authentication). Fingerprint authentication and iris scan are the only DoD-approved Samsung biometric authentication mechanisms because facial biometric authentication has not been certificated by NIAP as compliant with the Protection Profile for Mobile Device Fundamentals (MDF).

The user must first register a fingerprint and iris with the system. In order to use fingerprint and iris for device authentication, the user must also create a password, which is used as the authentication factor at first boot prior to first use of fingerprint and iris scan authentication.

### 7.2 Data-at-Rest Encryption

The Data at Rest Encryption mechanism provides two levels of data protection:

- Protected Data – Data marked as “protected” is encrypted when the device is powered off.
- Sensitive Data – Data marked as “sensitive” is encrypted when the device is in the Locked state in addition to the powered-off state protection.

#### 7.2.1 Protected Data

Since Android 6.x, device encryption is turned on by default. A function called Secure Startup allows the encryption keys to be derived from the user password and must be turned on for CC (Common Criteria) compliance. DoD policy requires CC mode to be enabled. When Secure Startup is turned on, the user will be required to enter their device unlock password as part of the boot process and again at the device lock screen. 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.

#### 7.2.2 Sensitive Data

Files can be optionally marked as “sensitive” using Knox APIs and are then provided protection when the device is on but the container is in the locked state. In addition, users can store files in the container’s “Chamber” directory, in which all files are automatically marked as “sensitive” by the system. Chamber is only available in the container; therefore, data must be marked as sensitive via the provided APIs in the COBO use case.



### 7.3 Trusted Boot and Warranty Fuse

Samsung Android OS 8 with Knox 3.x also implements security mechanisms that protect the container and On Device Encryption (ODE) when an invalid image is detected during the device boot process. If an invalid image is detected, the Knox Warranty Fuse (a one-time eFuse) is blown. A blown fuse will permanently block container creation and access to existing container. The ODE mechanism will not decrypt the data partition upon detection of invalid images, and the device must be factory reset to recover.

### 7.4 Samsung Android Device Disposal

For Samsung Android devices that have been exposed to classified data, follow this procedure prior to disposing of (or transferring to another user) a mobile device via site property disposal procedures.

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

## 8. DOD PKI PUREBRED

Purebred is a key management server and set of apps for mobile devices and provides a secure, scalable method of distributing software certificates for DoD PKI subscribers' use on commercial mobile devices.

Requirements for Samsung devices credentialed using DoD PKI Purebred are as follows:

- Users are responsible for maintaining positive control of their credentialed devices. The DoD PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and to report any loss of control so the credentials can be revoked.
- Upon device retirement, turn in, or reassignment, ensure a factory data reset is performed prior to device handoff. Follow Mobility Service Provider decommissioning procedures as applicable.

More information is available at <http://iase.disa.mil/pki-pke/Pages/purebred.aspx>.

## 9. SAMSUNG KNOX FOR ANDROID USER-BASED ENFORCEMENT

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

### 9.1 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.

### 9.2 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” and “Samsung Connect” features (device model dependent) are accessed from the notification bar and display 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.

Screen mirroring can also be initiated by selecting the file and then selecting “Share” and “Smart View” or by enabling “Smart View” in the Quick Settings panel.

The user can enable “MirrorLink” to allow integration of the device with car infotainment systems, connected over USB. This provides the user with the ability to access and control applications on the device via the car’s infotainment system. This is enabled by selecting “Connections”, “More Connections”, and “MirrorLink” in the Settings application.

The “Phone Visibility” option allows a user to make the device visible to other devices via wireless interfaces such as Bluetooth or Wi-Fi Direct, meaning other devices can attempt to initiate data transfers.

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.

**Note:** The administrator can also restrict the underlying connection method (Bluetooth, Wi-Fi Direct, etc.) via MDM controls, or the administrator can explicitly disable the application package that implements the service.

### 9.3 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.

Settings >> General Management >> Report Diagnostic Info

Users should be trained to not enable this option. See STIG requirements KNOX-08-013300, KNOX-08-013500, and KNOX-08-013700.

### 9.4 Google Usage and Diagnostics

Android devices include the “Usage & Diagnostics” feature, which allows the device to collect diagnostic and usage data and automatically transmit this data to Google servers. The purpose is to allow Google to analyze the data to improve product and service quality and address unexpected shutdowns or system errors.

Settings >> Google >> Overflow Menu >> Usage & Diagnostics

Users should be trained to disable this option on the device and in the container, if one exists. See STIG requirements KNOX-08-013300, KNOX-08-013500, and KNOX-08-013700.

### 9.5 Certificate Removal

The administrator may install DoD PKI certificates on the device both directly and via MDM.

Installed certificates can be deleted manually by the user via the Settings application (Lock Screen and Security >> Other Security Settings >> User Certificates).

Users should be trained to not remove DoD root and intermediate PKI certificates. See STIG requirements KNOX-08-019400 and KNOX-08-019500.

### 9.6 Samsung DeX Station

The Samsung DeX Station provides a desktop experience for select Samsung devices that have the capability to include the DeX mode. The dock provides the capability to connect the Samsung device to an external monitor, keyboard, mouse, and Ethernet cable.

Users should be trained to not connect the DeX Station to a DoD network via an Ethernet cable. See STIG requirement KNOX-08-008200.

## **9.7 Smart Call**

The Smart Call feature provides Caller ID and spam protection but requires the DoD user's name and phone number to be uploaded into an online service.

Users should be trained to disable the "Share name and number" within "Smart Call" built into the native dialer for both the COBO use case and in the container for the COPE use case. See STIG requirements KNOX-08-016500 and KNOX-08-016600.

## **9.8 Samsung Wi-Fi Sharing**

Wi-Fi Sharing is a new option included in the Samsung tethering feature. It allows a Samsung device user to share their Wi-Fi connection with other Wi-Fi-enabled devices but could allow unauthorized devices to access a DoD network.

Users should be trained to disable Samsung Wi-Fi Sharing. See STIG requirement KNOX-08-016800.

## **9.9 VPN Profiles**

The cybersecurity risk of a DoD network could be elevated when a Samsung mobile device with an unmanaged personal space connects to a DoD network via a VPN client in the device personal space.

Users should be trained to not configure a DoD network (work) VPN profile in any third-party VPN client installed in the personal space on a Samsung device. See STIG requirement KNOX-08-023300.

## 10. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES

The Samsung Knox for Android supports application disable policies that allow administrators to disable core and preinstalled applications<sup>3</sup> by specifying package names. As each device and operator variant will be pre-installed with different sets of applications, the administrator must identify any application that could pose a threat to sensitive information on the device and disable such applications by configuring application disable policies.

### 10.1 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 Knox for Android supports policy to disable Google backup, but other third-party services are disabled using application disable policies. The administrator must identify any such service pre-installed on the Knox container and disable these applications unless use is approved by the AO. This list includes:

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

### 10.2 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 in the Knox container and disable these applications unless use is approved by the AO. This list includes:

- Group Play
- Samsung Connect (Quick Connect)

### 10.3 Mobile Printing

Mobile printing applications provide the capability for wireless printing from a Samsung Android device. Setting up wireless printing from a mobile device to a DoD network-connected printer is problematic due to the print server requirements listed in the MultiFunction Device STIG and the DoD Wi-Fi network requirements listed in the Network Infrastructure STIG. If a mobile device is directly connected to a DoD network via a VPN or Wi-Fi connection, it may be able to print to network printers if the printer drivers or a printer app is installed. Android 8.x

---

<sup>3</sup> A core app is defined as an app bundled by the operating system vendor (e.g., Google). A preinstalled app is included on the device by a third-party integrator, including the device manufacturer or cellular service provider (e.g., Samsung, Verizon Wireless, or AT&T).

comes with a built-in print service that allows communication with most commercial printers. This package is covered in the disabled applications table.

## 10.4 Core and Preinstalled Applications

### 10.4.1 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' operating system (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.

### 10.4.2 Disabled Core and Preinstalled Applications

Tables 10-1 and 10-2 list core and pre-installed applications that must be disabled for STIG compliance unless the AO has approved the use of the application. Table 10-1 is applicable to the personal area in the COPE use case, while Table 10-2 is applicable to the container for COPE and the device for COBO. Table 10-3 lists applications that may be disabled at the AO's discretion. DoD Commands and Agencies should fully vet these apps using the Application Software Protection Profile (APPSWPP) prior to approving their use. Note that depending on many factors, including how the device was provisioned, Android upgrade path, and carrier modifications, many of these applications may be already disabled or not installed.

**Table 10-1: Mandatory Disablements – Personal Area**

Application Package Name	Application Name
net.aetherpal.device	AT&T Remote Support
com.samsung.oh	Samsung+
com.asurion.android.verizon.vms	Support & Protection

**Table 10-2: Mandatory Disablements – Work Environment**

Application Package Name	Application Name
com.att.mobilesecurity	AT&T Mobile Security
com.asurion.android.mobilerecovery.att	AT&T Protect Plus
net.aetherpal.device	AT&T Remote Support
com.wssnps	Backup and Restore Manager
com.vcast.mediamanager	Cloud
com.samsung.android.slinkcloud	CloudGateway
com.android.bips	Default Print Service
com.samsung.android.scloud	Samsung Cloud
com.sec.app.samsungprintservice	Samsung Print Service Plugin
com.samsung.oh	Samsung+

Application Package Name	Application Name
com.synchronoss.dcs.att.r2g	Setup & Transfer
com.sec.android.easyMover	Smart Switch
com.sec.android.easyMover.Agent	Smart Switch Agent
com.asurion.android.verizon.vms	Support & Protection
com.samsung.android.visionintelligence	Bixby Vision
com.samsung.android.visionprovider	Bixby Vision

Table 10-3: Optional Disablements

Application Package Name	Application Name
com.sec.android.mimage.gear360editor	360 Photo Editor
com.amazon.mShop.android	Amazon
com.amazon.fv	Amazon App Suite
com.amazon.mShop.android.install	Amazon Installation Status
com.amazon.mShop.android.shopping	Amazon Shopping
com.android.egg	Android Easter Egg
com.google.android.apps.walletnfcrel	Android Pay
com.sec.providers.assistedddialing	Assisted Dialing
com.dti.att	AT&T App Select
com.att.callprotect	AT&T Call Protect
com.wavemarket.waplauncher	AT&T FamilyMap
com.matchboxmobile.wisp	AT&T Hot Spots
com.att.android.digitallocker	AT&T Locker
com.yahoo.mobile.client.android.mail.att	AT&T Mail
com.samsung.android.bixby.agent.dummy	Bixby
com.samsung.android.bixby.agent	Bixby
com.samsung.android.es.globalaction	Bixby Global Action
com.samsung.android.bixby.plmsync	Bixby service
com.samsung.android.visionprovider	Bixby Vision
com.samsung.android.visionintelligence	Bixby Vision
com.samsung.android.widgetapp.briefing	Briefing Feed
com.uscc.ecid	Call Guardian
com.android.calllogbackup	Call Log Backup/Restore
com.sprint.ecid	Caller ID
com.vzw.ecid	Caller Name ID
com.cequint.ecid	Caller Name ID
com.sec.sprint.wfc	Calling Plus
com.samsung.sprint.chameleon	Chameleon
com.cnn.mobile.android.phone.edgepanel	CNN for Edge Panel



Application Package Name	Application Name
com.tmobile.pr.adapt	com.tmobile.pr.adapt
com.smithmicro.netwise.director.cricket	Cricket Wi-Fi Manager
com.samsung.android.app.camera.sticker.facear3d.preload	Default 3D live stickers
com.samsung.android.app.camera.sticker.facearframe.preload	Default frames
com.samsung.android.app.camera.sticker.facear.preload	Default live stickers
com.samsung.android.app.camera.sticker.stamp.preload	Default stamps
com.aetherpal.attdh.se	Device Help
com.tmobile.simlock	Device Unlock
com.metro.simlock	Device Unlock
com.directv.dvrscheduler	DIRECTV
com.att.dtv.shaderemote	DIRECTV Remote
com.google.android.apps.docs	Drive
com.LogiaGroup.LogiaDeck	DT Ignite
com.facebook.katana	Facebook
com.facebook.system	Facebook App Installer
com.facebook.appmanager	Facebook App Manager
com.facebook.services	Facebook Services
com.samsung.android.widgetapp.yahooedge.finance	Finance
com.sec.android.app.samsungapps	Galaxy Apps
com.sec.android.widgetapp.samsungapps	Galaxy Essentials Widget
com.samsung.android.game.gamehome	Game Launcher
com.enhance.gameservice	Game Optimizing Service
com.samsung.android.game.gametools	Game Tools
com.ampsvc.android	Games Assistant
com.samsung.android.hmt.vrsvc	Gear VR Service
com.samsung.android.app.vrsetupwizardstub	Gear VR SetupWizardStub
com.samsung.android.hmt.vrshell	Gear VR Shell
com.google.android.gm	Gmail
com.google.android.apps.books	Google Play Books
com.google.android.play.games	Google Play Games
com.google.android.videos	Google Play Movies
com.google.android.music	Google Play Music
com.google.android.apps.magazines	Google Play Newsstand
com.android.vending	Google Play Store
com.google.android.apps.plus	Google+
com.hancom.office.editor.hidden	Hancom Office Editor
com.google.android.talk	Hangouts
com.samsung.android.app.spage	Hello Bixby

Application Package Name	Application Name
com.samsung.helphub	Help
com.imdb.mobile	IMDb
com.instagram.android	Instagram
com.samsung.android.app.simplesharing	Link Sharing
com.linkedin.android	LinkedIn
com.verizon.llkagent	LLKAgent
com.lookout	Lookout
com.google.android.feedback	Market Feedback Agent
com.verizon.messaging.vzmsgs	Message+
com.facebook.orca	Messenger
com.handmark.metro.launcher	Metro App Store
com.metropcs.metrozone	metroZONE
com.samsung.android.app.mhswrapperusc	Mobile Hotspot
com.dti.cricket	Mobile Services
com.sec.android.app.camera.avatarauth	My Emoji Maker
com.vzw.hss.widgets.infozone	My InfoZone
com.sprint.zone	My Sprint Launcher
com.att.myWireless	myAT&T
com.mizmowireless.acctmgt	myCricket
com.nuance.nmc.sihome.metropcs	myMetro
com.privacystar.android.metro	name iD
com.samsung.android.nearby.mediaserver	Nearby Devices
com.samsung.android.allshare.service.mediashare	Nearby Service
com.samsung.android.widgetapp.yahooedge.news	News
com.gotv.nflgamecenter.us.lite	NFL Mobile
com.verizon.v4b	One Talk
com.microsoft.office.onenote	OneNote
com.samsung.android.service.peoplestripe	PeopleStripe
com.sec.android.mimage.photoretouching	Photo Editor
com.android.dreams.phototable	Photo Screensavers
com.americanexpress.plenti	Plenti
com.amazon.avod.thirdpartyclient	Prime Video
com.samsung.android.oneconnect	Quick Connect
com.directv.promo.shade	Remote
com.samsung.android.controltv	Remote Control
com.osp.app.signin	Samsung account
com.sec.android.app.sns3	Samsung Galaxy
com.samsung.android.mateagent	Samsung Galaxy Friends

Application Package Name	Application Name
com.samsung.android.app.mirrorlink	Samsung MirrorLink 1.1
com.samsung.android.spay	Samsung Pay
com.samsung.android.themestore	Samsung Themes
com.samsung.android.bixby.voiceinput	Samsung voice input
com.samsung.android.svoiceime	Samsung voice input
com.samsung.knox.securefolder	Secure Folder
com.samsung.knox.securefolder.setuppage	Secure your stuff
com.slacker.radio	Slacker Radio
com.samsung.android.smartcallprovider	Smart Call
com.locationlabs.cni.att	Smart Limits
com.samsung.android.smartmirroring	Smart View
com.samsung.android.easysetup	SmartThings
com.samsung.android.beaconmanager	SmartThings
com.samsung.android.widgetapp.yahooedge.sport	Sports
com.tmobile.pr.mymobile	T-Mobile
com.tmobile.services.nameid	T-Mobile Name ID
com.ubercab	Uber
com.telecomsys.directedsms.android.SCG	Verizon Location Agent
com.motricity.verizon.ssodownloadable	Verizon Login
com.customermobile.preload.vzw	Verizon Store Demo Mode
com.samsung.android.visioncloudagent	VisionCloudAgent
com.samsung.visionprovider	VisionProvider
com.samsung.tmovvm	Visual Voicemail
com.samsung.android.app.talkback	Voice Assistant
com.samsung.android.bixby.wakeup	Voice wake-up
com.samsung.vzwapiservice	VzwApiService
com.whatsapp	WhatsApp
com.samsung.android.allshare.service.fileshare	Wi-Fi Direct
com.samsung.android.app.withtv	withTV
com.samsung.android.widgetapp.yahooedge	Yahoo! Edge
com.google.android.youtube	YouTube
com.yellowpages.android.ypmobile	YP

### 10.5 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 installing 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 pre-installed applications

are added to the whitelist so that updates can be installed. Application disable is used to disable undesirable/unapproved core and pre-installed applications. Core and pre-installed applications listed on the “disable” list are not removed from the device but cannot be seen and/or launched by the user. In the COPE use case, these controls apply independently in the personal area and the container.

## 11. ADDITIONAL SAMSUNG FEATURES

### 11.1 Samsung Wearables

The use of Samsung Wearables with a DoD-owned Samsung device is prohibited. Samsung Wearables is considered a personal use product with no DoD mission requirement.

### 11.2 Google Location Tracking on Samsung Devices

DoD policy memorandum “Use of Geolocation-Capable Devices, Applications, and Services,” 03 August 2018, prohibits the use of geolocation-capable devices, applications, and services on DoD mobile devices in designated operational areas (OAs). Independent researchers and DISA analysis has determined that even when “Location History” is disabled Google continues to store location data on the mobile device<sup>4</sup>. Therefore, AOs should consider additional actions to limit Google tracking mobile devices when these devices are operated in OAs.

The following actions are recommended to disable Google location tracking:

1. For Samsung Android Knox 3.2 or later devices (Galaxy Note 9, Tab S4, and later):
  - a. Have the user log on to the Google Account associated with the Android device and disable “Location History”.
  - b. Implement the following new MDM APIs to disable Wi-Fi and Bluetooth scanning<sup>5</sup>:
    - allowWifiScanning()<sup>6</sup>
    - allowBLE()<sup>7</sup>
  - c. Disable GPS in the optional STIG rule “Allow Location” on MDM for the device.
  - d. Review all Google services and apps that may track device location and determine if the risk in using these apps in a designated OA is acceptable<sup>8</sup>.

**Note:** Operational Impact of recommended STIG controls:

- Few MDM products support these APIs at this time (September 2018).  
Impact: Site will need to use procedures for Knox 3.1 devices until its MDM supports the new APIs.

---

<sup>4</sup> A copy of DISA’s “Google Location Tracking on Samsung Devices” white paper can be requested by sending an email to [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil).

<sup>5</sup> When Wi-Fi or Bluetooth Low Energy (BLE) scanning is disabled (using the API allowWifiScanning or allowBLE), the device declines location accuracy and does not allow apps and services to scan for and connect to nearby devices automatically via Wi-Fi or Bluetooth.

<sup>6</sup> When Wi-Fi scanning is disabled either by the user changing the setting in “Settings” on the mobile device or the Administrator (MDM) enforcing by policy, the device user can still use the device Wi-Fi radio to connect to Wi-Fi networks.

<sup>7</sup> When the Administrator (MDM) disables Bluetooth scanning by enforcing the MDM policy, all Bluetooth functionality on the device is disabled. Alternately, the UBE control can be used to disable Bluetooth scanning and the Bluetooth radio can still be used. See footnote 9 for additional information.

<sup>8</sup> See DoD CIO memo “Mobile Application Security Requirements”, 06 Oct 2017, for information on reviewing mobile applications.

- Wi-Fi control disables apps and services from connecting to nearby devices.  
Impact: None expected. Connecting to nearby devices is a STIG-prohibited feature. There are no known tactical use cases for this feature at this time.
  - When Bluetooth is disabled by the “allowBLE” MDM control, all Bluetooth functionality is disabled.  
Impact: Connecting the mobile device to Bluetooth peripherals and sensors or to a computer via Bluetooth will be disabled.
2. For older Samsung devices (Knox 3.1 and earlier):
- a. Have the user log on to the Google Account associated with the Android device and disable “Location History”.
  - b. Disable Wi-Fi/Bluetooth Scanning (User-Based Enforcement [UBE] Control): Go to Settings >> Google >> Location >> Improve Accuracy. Set “Wi-Fi scanning” to “Off” and set “Bluetooth scanning” to “Off”.<sup>9</sup>
  - c. Disable GPS in the optional STIG rule “Allow Location” on MDM for the device.
  - d. Review all Google services and apps that may track device location and determine if the risk in using these apps in a designated OA is acceptable<sup>10</sup>.

**Note:** Operational Impact of recommended STIG controls:

- Wi-Fi control disables apps and services from connecting to nearby devices.  
Impact: None expected. Connecting to nearby devices is a STIG-prohibited feature. There are no known tactical use cases for this feature at this time.

### 11.3 Tactical Use Case

Not all STIG requirements are appropriate for tactical use cases. Approving Officials (AOs) have the authority to POAM STIG requirements and accept risks after considering mitigation strategies. See Table 11-1 for recommended mitigations for specific STIG controls.

**Note:** Not all STIG controls listed in Table 11-1 are appropriate for every tactical use case.

**Note:** Specific MDM/EMM products may not support some of the risk mitigations listed in Table 11-1. Recommend DoD organizations consult with their MDM/EMM vendor and Samsung on how best to implement recommended mitigations.

---

<sup>9</sup> When BLE scanning is disabled by the user changing the setting in “Settings” on the mobile device, the device user can still use the device Bluetooth radio to connect to Bluetooth devices. See footnote 7 for Wi-Fi scanning information.

<sup>10</sup> See DoD CIO memo “Mobile Application Security Requirements”, 06 Oct 2017, for information on reviewing mobile applications.

**Table 11-1: List of Tactical Changes to STIG Requirements with Recommended Mitigations**

<b>STIG Requirement Identifier</b>	<b>STIG Required Configuration</b>	<b>Tactical Use case Configuration</b>	<b>Tactical Application Notes</b>	<b>DoD Recommended Risk Mitigations</b>
V-80331/KNOX-08-009400	Protect wipe after 10 consecutive failed authentication attempts	Disable device after 10 consecutive failed authentication attempts and disable further authentication attempts; device can only be re-enabled by MDM	Administrator maintains control of the device. Assets remains provisioned, until the user authentication can be reconfigured. Administrator must implement "Lock device on Failed Passcode Attempts" or similar MDM control.	None
V-80315/KNOX-08-008300	Device unlock password length set to 6 or more characters	-Minimum password length = 4 -Minimum password complexity = PIN	Unlocking the device with Alphanumeric password on a keyboard can be problematic in battle gear. PIN pad use required for many tactical use cases. In addition, there is an emphasis on reducing Head Down time.	Decrease allowed number of authentication failures to 5 or less (V-80331/KNOX-08-009400).
V-80327/KNOX-08-009100	Device screen must lock after 15 minutes of inactivity	Two options: -Device screen must lock after 2 hours of inactivity Or -Configure Smart Lock (Trust Agent) to use Trusted Device	Longer screen inactivity timeouts needed for some battlefield situations or quick screen unlock needed	-Require COBO deployment mode. -Enable Trust Agent whitelist on MDM so only approved trust agent can be used (for example, Samsung API setTrustAgentConfiguration()).
V-000000/Knox-08-002900	Disable Unknown Sources	Enable Unknown Sources	Change required so apps can be downloaded from SD cards or sources other than	-Require COBO deployment mode -Require apps be downloaded from other AO-approved app

STIG Requirement Identifier	STIG Required Configuration	Tactical Use case Configuration	Tactical Application Notes	DoD Recommended Risk Mitigations
			Google Play and an MDM app catalog.	repository (for example, DoD app store) -Use “APP Installer Whitelist”, to only allow whitelisted applications to act as application installers. This enforces the user capability: Lock Screen and Security   Install unknown apps   <<<select an app to act as installer>>>   Allow from this source << ON (for example, Samsung API addPackageToWhiteList with type "TYPE APPROVED APP INSTALLER".
V-80357/KNOX-08-013900	All Bluetooth profiles except for HSP, HFP, and SPP are disabled.	Enable other Bluetooth profiles based on mission need.	Other Bluetooth profiles required for connection to tactical equipment: examples - Laser path/range finder, medical sensor, airfield survey sensor, data passing, cockpit headset, video displays, and control interfaces.	Disable additional Bluetooth profiles when no longer needed.
V-80335/KNOX-08-010300	Disable Trust Agents	Enable Trust Agents and configure a list of trusted devices using “Trusted Device”.	The user authentication mechanism would be bypassed so that the user need not unlock the device while flying or on patrol. The device would lock	Enable Trust Agent whitelist on MDM so only approved trust agent can be used (for example, Samsung API setTrustAgentConfiguration()).



STIG Requirement Identifier	STIG Required Configuration	Tactical Use case Configuration	Tactical Application Notes	DoD Recommended Risk Mitigations
			automatically when separated from the Trusted Device, enabling user authentication mechanisms.	
V-80367/KNOX-08-017900	Disable Developer Mode	Enable Developer Mode.	Mock Locations and USB Debugging is required for some tactical use cases.	Require COBO deployment mode.
V-80387/KNOX-08-015000 V-80383/KNOX-08-017300	Disable USB Media Player	Enable USB Media Player.	Required to side-load tactical apps and data and to allow backup of data to locally connected systems after return from mission.	-For V-80387/KNOX-08-015000, disable control “USB Mass Storage Mode”.
V-80371/KNOX-08-015500	Disable Manual Date Time Changes	Enable Manual Date Time Changes.	In some tactical situations, the user needs to be able to change the device time so it is different from the time of the local wireless carrier.	None
V-80373/KNOX-08-015700	USB host mode whitelist must be restricted to only HID host	Add MAS (mass storage device) to the USB host mode whitelist.	MAS is required to connect laptops and mission planning computers to side-load data such as military imagery and map data.	Implement policy to enable only during pre-mission device configuration and set to disable prior to mission deployment.