SAMSUNG ANDROID OS 10 WITH KNOX 3.X SUPPLEMENTAL PROCEDURES

Version 1, Release 1

20 March 2020

Developed by Samsung and DISA for the DoD

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

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. GLOSSARY

Throughout this documentation a number of terms and acronyms are used. Please refer to the following link for the definition of terms used throughout this STIG:
https://support.samsungknox.com/hc/en-us/articles/360041379213

2. HARMONIZATION

Samsung has been supporting businesses to secure and manage millions of Android devices around the world by pioneering advanced security with its Knox enterprise platform, building a deep set of features on the Android framework. Over the past few years, Samsung has worked with Google to simplify mobility for customers and reduce duplication. With the introduction of Knox Platform for Enterprise (KPE) in Android 8.0 Oreo, Knox features are now built on top of the core Android Enterprise (AE) framework to meet mandatory security requirements for Government and regulated deployments. This enables Mobile Device Management (MDM) vendors to offer a single foundation for customers to deploy Android Enterprise while adding necessary Samsung Knox features on top to comply with their security requirements.

3. ANDROID ENTERPRISE

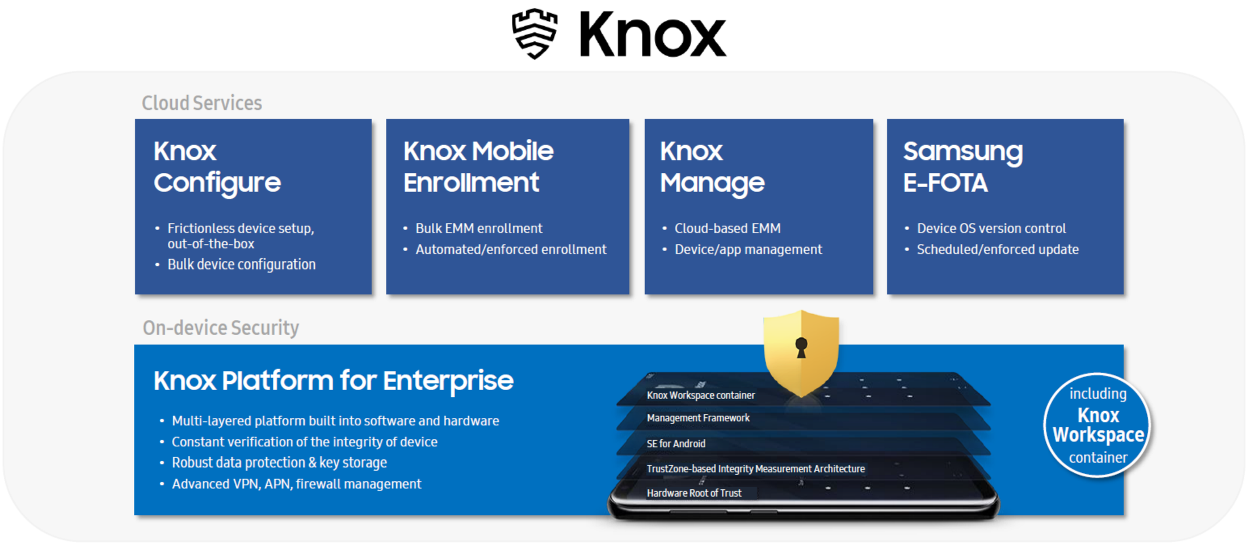
AE provides basic security protections, management policies, and network functions. However, the Samsung Android mobile device leverages Samsung-specific security features and hardware to enhance security and comply with the configuration standards for DoD Information Assurance (IA).

4. KNOX PLATFORM FOR ENTERPRISE

KPE provides defense-grade security supporting every aspect of mobile device operation. KPE resolves pain points identified by enterprises and meets the strict requirements of highly regulated industries.

With KPE, a Samsung Android mobile device can be deployed to meet the configuration standards for DoD IA.

Figure 4-1: Knox Platform Diagram


Knox
Cloud Services
Knox Configure
• Frictionless device setup, out-of-the-box
• Bulk device configuration
Knox Mobile Enrollment
• Bulk EMM enrollment
• Automated/enforced enrollment
Knox Manage
• Cloud-based EMM
• Device/app management
Samsung E-FOTA
• Device OS version control
• Scheduled/enforced update
On-device Security
Knox Platform for Enterprise
• Multi-layered platform built into software and hardware
• Constant verification of the integrity of device
• Robust data protection & key storage
• Advanced VPN, APN, firewall management
Knox Workspace container
Management Framework
SE for Android
TrustZone-based Integrity Measurement Architecture
Hardware Root of Trust
including Knox Workspace container

For additional information, visit:

- https://www.samsungknox.com/en/solutions/it-solutions/knox-platform-for-enterprise
- https://www.samsungknox.com/en/secured-by-knox

4.1 KPE Security Highlights

4.1.1 Hardware-Backed Security

4.1.1.1 Trusted Environment

KPE defends against threats and protects enterprise data through layers of security built on top of a hardware-backed trusted environment.

The trusted environment integrity checks the trusted processes prior to execution and, if successful, executes them in isolation from each other and the rest of the system. Only trusted processes can perform sensitive operations, such as data encryption and decryption.

Knox features that use the trusted environment include:

- Real-time Kernel Protection (RKP)
- Knox Verified Boot
- Device Attestation
- Certificate Management
- Sensitive Data Protection (SDP)
- Network Platform Analytics (NPA)

4.1.1.2 Knox Verified Boot

Starting with Samsung Galaxy S10, KPE introduced Knox Verified Boot (KVB). KVB is a Samsung-specific implementation of Android Verified Boot (AVB) v2, which enhances the AVB concept, extending the chain of trust to Kernel, system, vendor, product file system images, and other partitions, providing integrity, authenticity, and assurance that an aligned set of binaries is used. While AVB only checks the integrity of the kernel and platform components, KVB extends those checks to also cover the earlier bootloaders. This provides a more comprehensive guarantee that the device is booting using trusted components that are all from an aligned set of binaries.

KVB will be enabled by default on new devices released with Knox 3.3 onward but will not be available to older devices launched with Knox versions prior to 3.3, with firmware updates to Knox 3.3 or later. These devices will continue to use Knox Trusted Boot instead.

4.1.1.3 Hardware Fuses

KPE uses a one-time programmable fuse that signifies whether the Samsung Android device has ever booted into an unapproved state. If the Trusted Boot process detects that non-approved components are used, or if certain critical security features such as Security Enhancements (SE) for Android are disabled, this sets the fuse. When the fuse is set, the following security measures take place:

- Device Health Attestation checks fail.
- KPE Keystore removes the cryptographic keys used by SDP, preventing access to data marked as “sensitive”.
- KPEWorkspace/Work profile no longer operates, preventing access to the secure enterprise apps and “protected” data within.

4.1.2 App Isolation

Android provides both app isolation and group of app isolation.

The core app isolation technology is called SE for Android, which is an integration of SELinux and Android.

Apps are isolated from each other in the Android Sandbox.

With Workspace/Work profile on Samsung Android mobile devices, KPE provides additional features to enhance app security, such as:

- RKP
- Secure enterprise apps
- Hardware-backed integrity checks specific to Samsung Galaxy devices (requires KPE license)

- SDP for whitelisted apps (Samsung Email and Work Environment apps; KPE also provides an Application Programming Interface (API) for use in any app [requires KPE license])

4.1.3 Data Protection

KPE protects personal and enterprise data on Samsung Android devices using a rich set of features:

- User authentication:
  - Device password: This STIG enforces that the user configures a strong password that meets the standards for DoD IA: a PIN code, with a minimum length of six numeric digits and a maximum of two sequential or repeating numbers. On first boot, any NIAP-certified biometric authentication mechanism enabled will not function until the user successfully authenticates with the device password.
  - Work Environment password: This STIG does not require a separate password for the Work Environment.
  - Biometric authentication: Fingerprint and iris authentication are NIAP certified as compliant with the Protection Profile for Mobile Device Fundamentals (MDFPP) and available for use in this STIG. The Galaxy S10 (and newer) devices do not have an iris scanner but have face recognition authentication. Face recognition is not currently NIAP certified as compliant with MDFPP; therefore, the STIG requires this feature to be disabled.
- Encryption of device data:
  - Protected data: Data marked as “protected” is encrypted when the device is in the powered-off state. Encryption is NIAP certified as compliant with MDFPP.
  - Sensitive data: The KPE feature SDP encrypts data marked as “sensitive” when the device is in the locked state in addition to the powered-off state. The file can be marked as “sensitive” using KPE APIs or by moving files to the KPE Workspace/Work profile Chamber directory. SDP is NIAP certified as compliant with MDFPP and available for use in this STIG.
  - Encryption: The Galaxy S10 (and newer) devices use File-Based Encryption (FBE), and this STIG enforces that “Strong Protection” is enabled. Devices launched with Android 10 enforce “Strong Protection” and do provide an option for the user to disable it. Older devices use Full Device Encryption (FDE), and this STIG enforces that “Secure Startup” is enabled. Both “Strong Protection” and “Secure Startup” ensure that the encryption keys are derived from the user password. On first boot, the user must successfully authenticate with the device password before the “protected” and “sensitive” data is decrypted.
  - Dual DAR: Knox 3.3 also introduces Dual Data-at-Rest (Dual DAR) for Galaxy S10 (and newer) devices compliant with Commercial Solutions for Classified Program (CSfC) DAR Capability Package (CP). See Section 5.2 for more information.

- Encryption of network data: This STIG does not mandate the use of a virtual private network (VPN); however, KPE offers a wide selection of advanced VPN features, providing the ability to configure a separate VPN for the KPE Workspace/Work profile as well as for individual apps.

4.2 Manageability Highlights

4.2.1 Device Management

Samsung Android devices support administrator configuration and management via third-party Mobile Device Management tools. Devices support both Android Enterprise and Android Legacy management deployment types. Knox Platform for Enterprise is built on top of these frameworks, providing additional policies and services that can be accessed and configured by the Management tool.

This STIG allows for any Management tool that allows an administrator to configure and subsequently use platform APIs to apply the configuration.

For MDM solutions, one or more management applications are installed on the device, which are known as Device Policy Controllers (DPCs). These applications in general connect to a back-end MDM service to receive configuration data, as configured by an administrator via an MDM console, and subsequently use platform APIs to apply the configuration.

Samsung Android devices support a number of deployment use cases, with two specifically considered within the scope of this STIG:

- Corporate Owned Personally Enabled (COPE): An enterprise-owned device for business and personal use. A KPE Workspace/Work profile is configured to separate work applications and data from personal applications and data.
- Corporate Owned Business Only (COBO): Configuration of a device for work use only, with a single space for work applications and data. Personal applications and data are prohibited.

This STIG uses Android Enterprise and/or Knox Platform for Enterprise policies, enforced by a Management tool, to deploy devices in a compliant configuration. Both Android Enterprise and Android Legacy deployment types support COPE and COBO use cases, with this STIG providing the appropriate configuration.

Additional details on the deployment uses cases and corresponding configuration can be found in Section 6.

4.2.2 Knox Mobile Enrollment

Knox Mobile Enrollment (KME) is a free service to automate device enrollment either individually or in bulk. It is the quickest and most automated way to enroll a large number of devices to the MDM/Enterprise Mobility Management (EMM) for corporate use. Once an IT administrator registers a device with the service, the device user simply has to turn it on and connect to Wi-Fi or 3G/4G/5G during the initial device setup process.

The International Mobile Equipment Identity (IMEI) or serial number of purchased devices are uploaded and registered to the administrator's KME account by a participating Knox Deployment Program (KDP) reseller on behalf of the administrator. The administrator can then configure this set of devices for enrollment.

KME core features include:

- Asset control – If a KME enrolled device is factory reset, the MDM/EMM software will be automatically reinstalled and the user will be reenrolled.
- Automated MDM/EMM enrollment – Automatically signs in to MDM/EMM agents with user credentials provided by the IT administrator.
- Streamlined device setup process – Skip unwanted setup steps, such as Google/Samsung/Carrier account registration
- Widely supported – Supports almost all MDM/EMM solutions.
- Supports Android Enterprise and Android Legacy deployments.

Android Enterprise offers zero-touch service, with functionality similar to Samsung's KME. To help alleviate the burden for operators and resellers to integrate both services, Google and Samsung have developed a common client library for service providers that will integrate both Android zero-touch-capable devices and Samsung KME-capable Android devices.

For additional information on KME, visit https://www.samsungknox.com/en/solutions/it-solutions/knox-mobile-enrollment.

4.2.3 E-FOTA

Enterprise Firmware Over-the-Air (E-FOTA) is an enterprise solution that controls operating system versions on Samsung Android mobile devices to ensure the latest security patches are deployed to devices on schedule. IT administrators can test updates before deployment, ensuring compatibility between in-house apps and new operating system versions.

E-FOTA core features include:

- Selective update operating system versions
- No user interaction needed
- Schedule updates
- Forced update to target devices

For additional information, visit https://www.samsungknox.com/en/solutions/it-solutions/samsung_e-fota.

4.2.4 Accelerating Delivery of Knox Features to Customers

Samsung KPE supports OEMConfig, an Android standard that enables OEMs to create custom device features and controls that can be immediately and consistently offered by EMM providers. The premise of OEMconfig is simple: Allow an OEM-provided app to configure all of the customized OEM-specific features on the device instead of having EMMs build support for every OEM-specific feature in their products. OEMConfig leverages a feature of Android Enterprise known as managed configurations and is part of the standard published on the Appconfig community.

To support OEMConfig, Samsung provides the Knox Service Plugin (KSP) app. All EMM vendors that have validated their solutions for Android Enterprise can immediately support Samsung KPE features as they are updated through the Knox Service Plugin app.

KSP can only be used for Android Enterprise deployments and is not compatible with Android Legacy deployments.

Please refer to the following guide to using KSP to configure STIG policies on an Android Enterprise deployment:

- https://docs.samsungknox.com/knox-service-plugin/admin-guide/STIG-guidelines.htm

5. SPOTLIGHT

5.1 Samsung DeX

Samsung DeX is DoD approved, and this STIG provides configuration information to enable its use. DeX allows for the use of the device as if it were a laptop or desktop computer.

DeX supports three different modes:

- DeX mode: The device's screen appears on the connected monitor. A keyboard and mouse can be connected.
- Screen Mirroring: The device's screen is duplicated on the connected monitor.
- Dual-Mode: The device's screen and the connected monitor can be used at the same time.

5.1.1 Accessories

Use of Samsung DeX requires one of the following accessories:

- DeX station
- DeX pad
- Multi-port adapter
- USB Type-C to HDMI adapter
- DeX cable

Because the STIG does not permit the use of Human Interface Device (HID) Bluetooth profile, only USB HID devices (keyboards, mice, etc.) can be used with DeX.

5.2 Dual DAR

Starting with Samsung Galaxy S10, KPE introduced Dual DAR for data in the Work profile compliant with CSfC DAR CP, which can be viewed at:
https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/dar-cp.pdf.

Dual DAR encryption allows enterprises to secure their work data with two layers of encryption, which provides protection even while in the powered-off or unauthenticated state.

Galaxy S10 and later devices support a design solution that uses File Encryption (FE) as the inner layer and Platform Encryption (PE) as the outer layer. This solution uses passwords to provide access to classified data. Once a user inputs the correct password, the platform is decrypted, which then provides access to user data. Next, the user authenticates to the FE, which in turn decrypts the user's classified files.

The PE solution relies on the device to implement the requirements specified in the MDFPP along with the CSfC selected requirements. The FE solution will comply with the current requirements of NIAP's Protection Profile for Application Software (ASPP) as well as the ASPP Extended Package: File Encryption.

For additional information, visit https://docs.samsungknox.com/whitepapers/knox-platform/DualDAR.htm.

Deploying and configuring Dual DAR is beyond the scope of this STIG.

5.3 Common Criteria (CC) Settings

Since the release of the previous Samsung Android 9 STIG, some DoD mobile service providers have had a number of challenges implementing a few of the STIG settings, mainly due to MDM products not supporting key controls. There has also been some confusion related to Severity Category Code (CAT) II controls that are included in the set of controls required for full compliance with the device Common Criteria evaluation.

DoD policy requires that only mobile devices that have passed Common Criteria evaluation be used in the DoD. The STIG enforces the same set of device configurations that were required in the Common Criteria evaluation. The Common Criteria configuration settings in the STIG have been assigned a Severity Category Code of CAT I to CAT III, depending on the risk and impact of the vulnerability for non-compliance. One control, “CC Mode”, is an API that implements nine separate functional changes on the mobile device (see requirement KNOX-10-010800 for more details).

The set of Common Criteria configuration settings in the STIG includes both Management tool managed policy controls and a User Based Enforcement (UBE) control:

- Features enforced by policy:
  - Enable Knox CC Mode
  - Enable external storage encryption or disallow mount physical media
  - Minimum password quality
  - Disable face
  - OCSP check and/or Revocation check
  - Max password failures for local wipe
- UBE:
  - Secure Startup/Strong Protection

Note: The “Password history length” and “Password Recovery” policies are no longer required.

To be 100% compliant with CC Mode of operation, all of the policies must be configured correctly. However operational or deployment constraints may require that selected problematic policies not be configured. The AO must determine if the risk is acceptable to deviate from any STIG-required configuration setting.

When deviating from the STIG, there is no single severity category for non-compliance with respect to the overall configuration. This is because each individual policy has a different degree of risk associated with non-compliance and should be considered individually by the AO.

5.4 LegacyWorkspace Deprecation

The creation of KPE Legacy Workspace is no longer supported in device models that launch with Knox 3.4 or later. This has no impact on current deployments. To understand the impact this has on new deployments, refer to the following table:

Table 5-1: Impact of LegacyWorkspace Deprecation

Use Case	Devices launched with Knox 3.4 and later (e.g., Note10)	Devices launched prior to Knox 3.4
COBO	No Impact. Can be deployed using either Android Enterprise or Android Legacy.	No impact. Can be deployed using either Android Enterprise or Android Legacy.
COPE	**Impact: Can ONLY be deployed using Android Enterprise.**	No impact. Can be deployed using either Android Enterprise or Android Legacy.

Note: Although Android Legacy deployments can still be used in the short term, it is strongly discouraged due to Device Admin (DA) deprecation, which is the mode of operation used to manage Android Legacy deployments.

5.5 Secure Startup Clarification

Secure Startup offers additional security only when a device is powered off until first authentication. For deployments with operational needs that require users’ devices to always be powered on (e.g., so users do not miss important emergency alerts or can always be responsive for mission needs), it can be assumed that the users have always authenticated once and therefore Secure Startup is not offering additional security. In this situation, the AO may decide to accept the risk and deviate from the STIG configuration.

6. USE CASES

The mobile device may be operated in a number of use cases relevant to Government deployment. In the majority of DoD use cases, the mobile device will be DoD owned (Corporate Owned), and therefore the Bring Your Own Device (BYOD) use case is not considered in this STIG. The following Corporate Owned use cases are supported in this STIG:

- Corporately Owned, Personally Enabled (COPE): An enterprise-owned device for business and personal use. This use case entails a significant degree of enterprise control over configuration and possibly software inventory. The enterprise elects to provide users with mobile devices and additional applications (such as VPN or email clients) to maintain control of their enterprise data and network security. COPE deployment uses the KPE Workspace/Work profile to maintain a separation between personal and work data and applications. Refer to Sections 7 and 9 of this document to support the COPE configuration
- Corporate Owned, Business Only (COBO): COBO prohibits personal use of a mobile device; therefore, there is no provision for the use of Personal Applications and data. The COBO use case includes the following examples:
    - Configuration of a device for work use only, with a single space for work applications and data, with no use of a KPE Workspace/Work profile for separation of personal applications, which is prohibited. Refer to Section 8 to support this COBO configuration.
    - Using device to host low-security work area and the Workspace/Work profile to host high-security work area. (This configuration is not in the scope of this document.)
    - DualDAR-enabled Work profile to support high-security requirements such as CSfC DAR CP. (This configuration is not in the scope of this document.)

As mentioned previously, Samsung Android devices support both Android Enterprise and Android Legacy device management modes. Both support the COPE and COBO use cases described above:

- Android Enterprise
    - For a COPE use case, a DPC manages the device in Device Owner (DO) mode. A Work profile is also created that is managed by a separate DPC in Profile Owner (PO) mode, which resides inside the Work profile. The DPC in DO mode can apply device-wide policies and policies for the Personal Environment (outside the Work profile). The DPC in PO mode can apply policies and configuration for the Work profile only. Note that the most common case is usually two instances of the same application tied to a single MDM console.
    - For the COBO use case, a DPC manages the device in DO mode. The DPC can manage and apply policies for the device as a whole. No Work profile is created.
    - In both use cases, the DPCs apply Android Enterprise policies using Android API implemented by the Android Device Policy Manager (DPM) module. Additionally, the DPC can apply KPE policies using Samsung KPE APIs, in addition to Android

Enterprise policies, to create a STIG-compliant configuration on Samsung Galaxy devices.

- Android Legacy
    - For both COPE and COBO, a single DPC in Device Admin (DA) mode is installed.
    - For COPE, the DPC manages both the device and the KPE Workspace, with the DPC residing outside the Workspace.
    - For COBO, the DPC manages and applies policies for the device as a whole. No KPE Workspace is created.
    - As above, a DPC in DA mode can call allowed Android DPM APIs and KPE APIs to create a STIG-compliant configuration.

Android DA depreciation is only effective for EMM Applications targeting API level 29 (see https://developers.google.com/android/work/device-admin-deprecation). Apps not targeting this API level will continue to work. Apart from the KPE API createContainer() (Legacy container creation), all other KPE APIs can be called in AE mode. EMM Applications that target API level 29 and rely on DPM deprecated API for DPC in DA mode can call alternative APIs offered by KPE to comply with this STIG.

In certain deployments, it may be beneficial to employ a combined approach where the device is managed and monitored by an MDM but is mainly restricted by a local device administrator. This is compatible with both the Legacy and Android Enterprise modes. In an Android Enterprise configuration, the device is managed by the MDM in the Device Owner mode, and further restrictions are applied by a local device administrator, whereas in the Legacy case, two device administrator applications coexist on the device. In either case, this allows for a flexible deployment where policies can be adjusted by an authorized IT administrator on-site.

Note: Both Android Legacy and Android Enterprise deployments are supported in this STIG, but it is recommended that DoD mobile service providers start migrating to Android Enterprise as soon as possible.

6.1 Configuration Approach

This STIG classifies device management policies as being “Device/Asset” policies or “Work Environment” policies.

- Device/Asset Policies are applied at the device level regardless of whether the COPE or COBO use case is being deployed by the administrator.
- Work Environment Policies are applied to the KPE Workspace/Work profile in the COPE use case (where the KPE Workspace/profile is the Work Environment), or to the “main user” in the COBO use case (where these is no separate KPE Workspace/Work profile configured for the device and therefore the Work Environment is the device as a whole).

This STIG uses AE and/or KPE policies to deploy Samsung Android devices for the COPE or COBO uses cases in either the Android Enterprise or Android Legacy deployment types. A combination of AE and KPE policies may be defined in this STIG configuration for both the “Device/Asset” grouping and the “Work Environment” grouping.

To support this approach, this STIG provides configuration tables with separate “Device/Asset” and “Work Environment” groupings.

Depending on Management tool policy support and DoD mobile service provider deployment choices, the use cases defined in Section 6 above can be implemented using deployment options as summarized in the following table:

Table 6-1: User Case and Deployment Options

Deployment Use Cases	Deployment/ Enrollment Type	Supplemental Document Reference	Configuration Document
COBO	Android Legacy managed device	Section 8	Apply policies in “Device/Asset” and “Work Environment” tables to the device.
	Android Enterprise Fully managed device		Apply policies in “Device/Asset” and “Work Environment” tables to the device.
COPE	Android Legacy managed device with Workspace	Sections 7 and 9	Apply policies in “Device/Asset” table to the device and policies in “Work Environment” table to the Legacy Workspace.
	Android Enterprise Fully managed device with work profile		Apply policies in “Device/Asset” table to the device and policies in “Work Environment” table to the work profile.

7. CONFIGURATION OF THE PERSONAL ENVIRONMENT

This section is not applicable for the COBO use case. Section 1.1 of the Overview document states that the scope of this STIG includes the COPE use case where both a Personal Environment and Work Environment are set up on the Samsung Android 10 device.

DoD mobile service providers may allow users full access to the Google Play app store for the Personal Environment, 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 Environment, including downloading and installing Google Play apps into the Personal Environment and syncing personal data on the device with personal cloud data storage accounts[1]. 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 Environment (guidance can be added to user training or the User Agreement).
- Site mobile devices are configured with a technology used for data separation between work apps and data and personal apps and data that is NIAP certified.
- The site Management tool is configured to restrict the download of apps from all third-party app stores.
- The Management tool or user restricts the use of DoD VPN profiles within the Personal Environment.
- 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)[2]. See STIG requirement KNOX-10-009900 for more information.

This STIG assumes that all of the conditions above have been met and allows full user access to the Personal Environment. If the AO has not approved unrestricted use of the Personal Environment, the AO should consider implementing the appropriate policies from the "Work Environment" table in the Configuration Table document to the device.

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

[2] UBE controls cannot be managed by the site Management tool and, therefore, must be managed by the mobile device user. See *Configuration of COPE Workspace/Work Profile* section in this document for more information.

8. CONFIGURATION OF COBO

This section is not applicable for the COPE use case. In the COBO use case, a KPE Workspace/Work profile is not required to provide isolation from personal applications, and the Managed Device mode provides a secure environment for enterprise applications and data.

9. CONFIGURATION OF COPE WORKSPACE/WORK PROFILE

9.1 Overview

The KPE Workspace/Work profile provides a Work Environment that is isolated and independent from a Personal Environment for enterprise applications and data when implementing the COPE use case. Enterprise applications and data are placed inside the Work Environment, while personal applications and data reside outside the Work Environment but within the Personal Environment. The Personal Environment has separate resources than the Work Environment.

9.2 Work Environment Isolation

The KPE Workspace/Work profile provides a completely separated Android environment with its own applications and data. Various security mechanisms, such as Security Enhancements (SE) for Android policies, provide isolation of Work Environment applications and data from applications and data within the Personal Environment. A Work Environment does not restrict the user’s ability to allow certain data to pass through to/from the Personal Environment. An administrator must explicitly restrict this behavior through APIs as indicated in the STIG configuration table.

10. PROCEDURES

10.1 Device Wipe

Samsung Android devices can be wiped by a factory data reset or management tool or when the failed authentication limit is reached.

Pre-installed apps in the Data partition will be wiped from the device after a device wipe.
If any of those apps are configured in the application disable list, the policy will no longer be effective, and the user would not be prevented from installing them.

The only solution is to both uninstall/disable the unwanted apps and then use either application installation whitelisting or blacklisting.

- For application installation whitelisting, the unwanted apps will be implicitly blacklisted (all apps blacklisted), and the unwanted apps will not be whitelisted.
- For application installation blacklisting, the unwanted apps will be explicitly blacklisted.

Application installation blacklisting should only be used if the AO has not approved unrestricted use of personal apps in the COPE use case.

10.2 Strong Protection

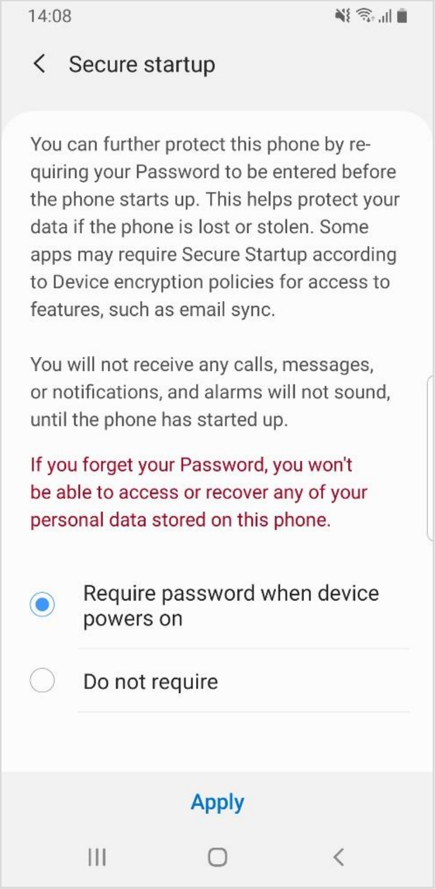
Strong Protection is enabled by default on S10 (or newer) devices, and users must not disable it. When the administrator (Management tool) has enabled Knox CC Mode, the setting will be enforced, allowing users only to enable it, and will prohibit disablement.

10.3 Secure Startup (S9, Tab S4)

Secure Startup must be enabled by users of S9, and Tab S4 must be installed with Samsung Android Q. When the administrator (Management tool) has enabled Knox CC Mode, the setting will be enforced, allowing users only to enable it, and will prohibit disablement.

The Secure Startup screen is shown below.

Figure 10-1: Secure Startup Screen



Secure startup

You can further protect this phone by requiring your Password to be entered before the phone starts up. This helps protect your data if the phone is lost or stolen. Some apps may require Secure Startup according to Device encryption policies for access to features, such as email sync.

You will not receive any calls, messages, or notifications, and alarms will not sound, until the phone has started up.

If you forget your Password, you won't be able to access or recover any of your personal data stored on this phone.

● Require password when device powers on

○ Do not require

10.4 Unenrollment

KPE/AE provide API(s) to wipe the device, and these API(s) must be called by the management tool as part of retiring/unenrollment of Samsung devices. When transferring a device to a new user, the Samsung device should be wiped by the administrator (Management tool) via the management tool or by a factory data reset. In either case, the administrator (Management tool) should ensure the device has been wiped.

11. SPECIAL GUIDANCE

11.1 Whitelisting vs. Blacklisting

Management tools implement the Samsung whitelist and blacklist policies in slightly different ways. This section is to help clarify the intention of this STIG's configuration and how it might be achieved by the Management tool.

Whitelisting and blacklisting are two ways to filter things. Whitelisting will allow only the things that are listed. Blacklisting will allow everything except the things that are listed.

Some Management tools might provide whitelisting and blacklisting exactly as described here, allowing either a whitelist or blacklist to be configured but not both. This is the same as the intention in the STIG configurations.

However, some Management tools might provide whitelisting and blacklisting, allowing both to be configured.

Refer to the Management tool's documentation to determine how whitelisting/blacklisting is implemented.

To understand the underlying KPE API's behavior, apply the following logic:

- To whitelist and allow only the things that are listed – Add the allowed items to the whitelist and configure the blacklist to include everything else. To include everything on a list, use a wildcard (".*").
- To blacklist and allow everything but the items that are listed – **Do not configure the whitelist** and add the disallowed items to the blacklist. The whitelist should not be configured because it would override the blacklist, causing it to have no effect.

11.2 Samsung Android Device Disposal

For Samsung Android devices that have never 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:

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

12. INFRASTRUCTURE

12.1 Knox SDK

The Samsung Knox 3.x SDK provides various APIs for third-party Management tool solution vendors to configure Knox security components that can be used to implement several STIG controls. These APIs can be used to configure restrictions on the device and a Workspace. The KPE Workspace/Work profile can be fully managed by a Management tool 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 Workspace. 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.

12.2 Knox Licensing

The MDM is required to activate a KPE license prior to getting access to the full range of Samsung KPE features and APIs. KPE 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.

12.3 Knox On-Premise Servers

All services necessary to enable KPE 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 KPE 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 KPE 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 KPE 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 KPE license from the Knox reseller. The enterprise will provide its On-Premise GSLB server URL, which will be encoded into the KPE license.

The MDM agent will pass the KPE 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 obtain KPE license validation.

13. 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 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 (see Section 10.4). Follow mobility service provider decommissioning procedures as applicable.

Additional information is available at https://cyber.mil/pki-pke/purebred/.

14. 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 Management tools, the mitigation must include proper training of individual users.

14.1 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.

14.2 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 “SmartThings” 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 Management tool controls or can explicitly disable the application package that implements the service.

14.3 Accessory Use (DeX Station, USB Dongle)

Certain accessories can provide wired networking capabilities to Samsung Android devices. For example, the Samsung DeX Station provides the capability to connect the Samsung Android device to external monitor, keyboard, mouse, and Ethernet cable via LAN port. USB to Ethernet adapters/dongles also provide wired networking capabilities to Samsung Android devices. Connecting a Samsung Android device to a DoD network via any accessory that provides wired networking capabilities is prohibited.

Users should be trained to not connect the DeX Station to a DoD network via an Ethernet cable. See STIG requirement KNOX-10-0011200.

14.4 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.

Wi-Fi Sharing can be disabled via the Settings application (Settings >> Connections >> Mobile Hotspot and tethering >> Mobile Hotspot >> Wi-Fi Sharing).

Users should be trained to disable Samsung Wi-Fi Sharing. See STIG requirement KNOX-10-011800.

14.5 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.

14.6 Secure Startup/Strong Protection

Strong Protection protects Samsung Android devices that use File-Based Encryption (FBE). As FBE allows different files to be encrypted with different keys, files required for the device to start up are encrypted with default cryptographic keys, whereas the user’s apps and protected data can be encrypted with different cryptographic keys.

When enabled, Strong Protection replaces the default cryptographic keys used to encrypt the user’s apps and protected data with keys derived from the user password. This allows the device to decrypt files required to boot with default cryptographic keys, and the user's apps and protected data are decrypted the first time the user successfully authenticates after reboot. This feature must be enabled for a Samsung Android device to be in the NIAP-certified CC Mode of operation. Strong Protection is enabled by default on S10 (or newer) devices installed with Samsung Android Pie. Users of S10 (or newer) devices should be trained to never disable Strong Protection. When the administrator (Management tool) has enabled Knox CC Mode, users will only have the capability to enable Strong Protection and will be prohibited from disabling it. See STIG requirement KNOX-10-012700.

Secure Startup protects Samsung Android devices that use Full Disk Encryption (FDE). When enabled, Secure Startup replaces the default cryptographic keys with keys derived from the user password. The user must successfully authenticate at startup so the whole device can be decrypted before continuing to boot. This feature must be enabled for a Samsung Android device to be in the NIAP-certified CC Mode of operation. Secure Startup is disabled by default on S8, S9, and Tab S4 installed with Samsung Android Pie and must be enabled by users (see Section 10.3). Users of S8, S9, and Tab S4 devices should be trained to enable Secure Startup and to never disable it. When the Administrator (Management tool) has enabled Knox CC Mode, users will only have the capability to enable Secure Startup and will be prohibited from disabling it. See STIG requirement KNOX-10-012700.

15. APPLICATION DISABLE POLICIES

Samsung Android devices with Knox Platform for Enterprise support application disable policies that allow administrators to disable core and preinstalled applications[3] 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.

15.1 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. KPE 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 Workspace and disable these applications unless use is approved by the AO. This list includes:

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

15.2 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 Workspace and disable these applications unless use is approved by the AO. This list includes:

- Group Play
- Samsung SmartThings

15.3 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 and Network Printers STIG and the DoD Wi-Fi network requirements listed in the Network Infrastructure Policy 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 10 comes with a built-in print service that allows communication with most commercial printers. This package is covered in Table 15-1: System Apps for Disablement.

[3] 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).

15.4 Core and Preinstalled Applications

15.4.1 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.

15.4.2 Disabled Core and Preinstalled Applications

Tables 15-1: System Apps for Disablement (Non-DoD-Approved Characteristics) and 15-2: System Apps for Disablement (Other Characteristics) list system apps (core/pre-installed applications) that must be disabled for STIG compliance unless the AO has approved their use. Each section includes guidance explaining how to apply configuration for the different use cases.

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.

15.4.2.1 System Apps for Disablement (Non-DoD-Approved Characteristics)

- **Guidance for COBO and COPE Workspace**

  The system apps in the following table, unless the AO has approved the use of the app, **must** be disabled by inclusion on the "system application disable list", as they have been identified as having the following non-DoD-approved characteristics:

  - Back up mobile device data to non-DoD cloud servers (including user and application access to cloud backup services);
  - Transmit mobile device diagnostic data to non-DoD servers;
  - Voice assistant application if available when mobile device is locked;
  - Voice dialing application if available when mobile device is locked;
  - Allows synchronization of data or applications between devices associated with user; and
  - Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other mobile devices or printers.

  Related requirement: KNOX-10-009300

- **Guidance for COPE Personal Environment**

Only the system apps in the green rows in the following table, unless the AO has approved the use of the app, **must** be disabled by inclusion on the "system application disable list", as they have been identified to transmit mobile device diagnostic data to non-DoD servers.

Related requirement: KNOX-10-009200

Table 15-1: System Apps for Disablement (Non-DoD-Approved Characteristics)

Application Name	Application Package Name	Characteristic
Support & Protection	com.asurion.android.verizon.vms	Transmit MD diagnostic data to non-DoD servers
Samsung+	com.samsung.oh	Transmit MD diagnostic data to non-DoD servers
AT&T Remote Support	net.aetherpal.device	Transmit MD diagnostic data to non-DoD servers
AT&T Protect Plus	com.asurion.android.mobilerecovery.att	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services)
Android Setup	com.google.android.apps.restore	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services)
Samsung Cloud	com.samsung.android.scloud	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services)
ShortcutBNR	com.samsung.android.shortcutbackupservice	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services)
CloudGateway	com.samsung.android.slinkcloud	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services
	com.samsung.android.smartswitchassistant	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services)
Cloud	com.vcast.mediamanager	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services)

Application Name	Application Package Name	Characteristic
		Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers
Default Print Service	com.android.bips	Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers
Samsung Print Service Plugin	com.sec.app.samsungprintservice	Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers
Smart Switch	com.sec.android.easyMover	Allows synchronization of data or applications between devices associated with user
Smart Switch Agent	com.sec.android.easyMover.Agent	Allows synchronization of data or applications between devices associated with user
Setup & Transfer	com.synchronoss.dcs.att.r2g	Allows synchronization of data or applications between devices associated with user

15.4.2.2 System Apps for Disablement (Other Characteristics)

- **Guidance for COBO and COPE (Personal and Workspace)**

  The system apps in the following table, unless the AO has approved the use of the app, **must** be disabled by inclusion on the "system application disable list", as they have been identified as having characteristics that require disablement.

  Related requirements: KNOX-10-009200 and KNOX-10-009300

Table 15-2: System Apps for Disablement (Other Characteristics)

Application Name	Application Package Name	Characteristic
MobileKey	com.att.csoiam.mobilekey	Potential leak of DoD credentials, Personally Identifiable Information (PII)

Application Name	Application Package Name	Characteristic
AT&T Mobile Security	com.att.mobilesecurity	AT&T Mobile Security Basic includes AT&T Call Protect. Scans apps and files for malware and viruses, notifies if the operating system has been tampered with, alerts about company data breaches and provides helpful tips, ensures there is a pass code. Is a Device Administrator (DA) app.
Bixby Vision	com.samsung.android.visionintelligence	Bixby Vision's image and text recognition capabilities use cloud-based processing. This may leak sensitive DoD data.
Bixby Vision	com.samsung.android.visionprovider	Bixby Vision's image and text recognition capabilities use cloud-based processing. This may leak sensitive DoD data.
Samsung Health	com.sec.android.app.shealth	Potential leaks of PII, date of birth, face, home address, etc.
Cameralyzer	com.sec.factory.cameralyzer	Permissions requested do not match Activity behavior.
Find My Mobile	com.samsung.android.fmm	Remote Controls: Allows device to be controlled remotely using the Samsung account via the Internet, even when locked. Remote Unlock: Password will be securely stored by Samsung, allowing the user to unlock the phone in case of forgotten password.

15.4.2.3 System Apps That Must Not Be Disabled

Many system apps should not be disabled, as they will have a negative impact on the performance and usability of the Samsung Android device. Table 15-3: System Apps That Must Not Be Disabled exists to capture specific packages that have known issues if disabled; however, this is not an exhaustive list of packages that should not be disabled.

- **Guidance for COBO and COPE (Personal and Workspace)**
  - The system apps in the following table **must not** be disabled by inclusion on the "system application disable list", as they are required for the correct operation of the Samsung Android device.

    - Related requirements: KNOX-10-009200, KNOX-10-009300, KNOX-10-001000, KNOX-10-001100, and KNOX-10-000800

  - The system apps in the following table **must** also be included on the "application installation whitelist" to allow installation of updates, as they are required to be kept up to date for the correct operation of the Samsung Android device.
    - Related requirement: KNOX-10-001000

Table 15-3: System Apps That Must Not Be Disabled

System App	Package Name
Android Market	com.google.android.finsky
Android Setup	com.google.android.setupwizard
Gmail	com.google.android.gm
Google Play Services	com.google.android.gms
Google Play Store	com.android.vending
Google Services Framework	com.google.android.gsf
Google Services Framework	com.google.android.gsf.login

16. ADDITIONAL SAMSUNG FEATURES

16.1 Samsung Wearables

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

16.2 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[4]. 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:

a. Have the user log on to the Google Account associated with the Android device and disable “Location History”.

b. Implement the following new KPE APIs to disable Wi-Fi and Bluetooth scanning[5]:

   -allowWifiScanning()[6]

   -allowBLE()[7]

c. Disable GPS in the optional STIG rule “Allow Location” on the Management tool 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[8].

   Note: Operational impact of recommended STIG controls:

   - Few Management tool products support these APIs at this time (April 2019).

     Impact: Site will need to use procedures for Knox 3.3 devices until its MDM supports the new APIs.

[4] 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.

[5] 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.

[6] When Wi-Fi scanning is disabled either by the user changing the setting in “Settings” on the mobile device or the administrator (Management tool) enforcing by policy, the device user can still use the device Wi-Fi radio to connect to Wi-Fi networks.

[7] When the administrator (Management tool) disables Bluetooth scanning by enforcing the Management tool 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.

[8] 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” Management tool 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.

Full details of the APIs used to implement the location tracking policies listed in this section can be found on the Samsung Knox portal “Knox 3.x STIG Implementation Guide - Samsung Android OS 10 API table” page (https://support.samsungknox.com/hc/en-us/articles/360041379213).

16.3 Tactical Use Case

Not all STIG requirements are appropriate for tactical use cases. AOs have the authority to POAM STIG requirements and accept risks after considering mitigation strategies. See Table 16-1 for recommended mitigations for specific STIG controls.

Certain deployments, including the tactical use case, may benefit from a combined approach where the device is managed by both a Management tool and a local device administrator.

The device could be managed by the remote administrator (Management tool) with the more relaxed tactical settings and could be dynamically restricted by the local device administrator when required, or it could be entirely managed by a local device administrator when no remote Management tool is required or available. In either case, this allows for a flexible deployment where policies can be adjusted by an authorized IT administrator on-site.

Table 16-2 is essentially the recommended Configuration Table for the tactical use case. The STIG controls and mitigations listed in Table 16-1 are represented in Table 16-2.

Note: Not all STIG controls listed in Tables 16-1 and 16-2 are appropriate for every tactical use case.

Note: Specific Management tool products may not support some of the risk mitigations listed in Table 16-1. DoD organizations should consult with their Management tool vendor and Samsung on how best to implement recommended mitigations.

Full details of the APIs used to implement the tactical use case policies listed in this section can be found on the Samsung Knox portal “Knox 3.x STIG Implementation Guide - Samsung Android OS 10 API table” page (https://support.samsungknox.com/hc/en-us/articles/360041379213).

Table 16-1: List of Tactical Changes to STIG Requirements with Recommended Mitigations

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
KNOX-10-000500	Disable (not wipe) the device after 10 consecutive failed authentication attempts and disable further authentication attempts; device can only be reenabled by the Management tool administrator.	Administrator maintains control of the device. Assets remain provisioned until the user authentication can be reconfigured. For devices prior to Galaxy S10 that implement Full Device Encryption, a "Secure Startup" lock screen will require authentication prior to decrypting the device. If the correct password is not entered within a predefined number of attempts, the device will be wiped regardless of any policies applied to the device.	None
KNOX-10-000100	Configure a minimum password length of four characters.	There is an emphasis on reducing head-down time.	Decrease allowed numbers of authentication failures to "5" or less. KNOX-10-000500
KNOX-10-000400	Do one of the following: - Method #1: Configure the device screen to lock after two hours of inactivity - Method #2: Configure Smart Lock (Trust Agent) to use Trusted Device.	Longer screen inactivity timeouts needed for some battlefield situations or quick screen unlock needed.	- Requires COBO deployment. If using Method #2: - On the Management tool, for the device, in the "Android trust agent" group, implement a trust agent whitelist by configuring "trust agent configuration" so only approved trust agents can be used.

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
KNOX-10-008000	Enable unknown app installation sources.	Change required so apps can be downloaded from SD cards or sources other than Google Play and a Management tool app catalog.	- Requires COBO deployment. - Requires apps be downloaded from other AO-approved app repository (for example, DoD app store).
KNOX-10-001400	Enable other Bluetooth profiles based on mission need.	Examples of other Bluetooth profiles required for connection to tactical equipment: 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.
KNOX-10-002100	Enable Trust Agents and configure a list of trusted devices using “Trusted Device”.	The user authentication mechanism would be bypassed so the user need not unlock the device while flying or on patrol. The device would lock automatically when separated from the Trusted Device, enabling user authentication mechanisms.	Enable Trust Agent whitelist on Management tool so only approved trust agent can be used by configuring “trust agent configuration” policy. If implementing this mitigation, do not enable Trust Agents as this needs to be disabled for the Trust Agent Whitelist to operate correctly.
KNOX-10-002800	Enable developer modes.	Mock Locations and USB debugging are required for some tactical use cases.	Requires COBO deployment.
KNOX-10-003500 **KNOX-10-003700**	Enable USB mass storage mode.	Required to side-load tactical apps and data and to allow backup of data to locally connected systems after return from mission.	None

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
KNOX-10-010200	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
KNOX-10-011200	In addition to "HID" also include "MAS" (mass storage device) in the USB host mode exception list.	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.

Table 16-2: Configuration Policy Rules for Tactical Use Case

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-10-000010	Password Requirements	Max password failures for local wipe	0+	0	KNOX-10-000500	This configuration is only required if: - implementing KTACT-10-000020 - not implementing KTACT-10-000020 but as part of a recommended mitigation for either KTACT-10-000030/40. If configured as part of a recommended mitigation for either KTACT-10-000030/40, use a setting of "5" and not "0" as stated here.

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-10-000020	KPE Password Requirements	Max password failures for device disable	0+	10	KNOX-10-000500	If also implementing either KTACT-10-000030/40, the recommended mitigation is to use a setting of "5" and not "10" as stated here.
KTACT-10-000030	Password Requirements	Minimum password length	0+	4	KNOX-10-000100	DoD recommended mitigation: See "Comment" section of KTACT-10-000010/20.
KTACT-10-000050	Password Requirements	Max time to screen lock	0+	2 hours	KNOX-10-000400	This is Method #1. If configuring this, do not configure KTACT-10-000060. If possible, using a Remote Management tool or Local Admin: Implement policy with "Tactical setting" only while on mission and set "Non-tactical setting" after return from mission. Requires COBO use case.
KTACT-10-000060	Restrictions	Trust Agent configuration	Configure	Enable "trusted device" feature	KNOX-10-000400	This is Method #2. If configuring this, do not configure KTACT-10-000050, or KTACT-10-000130. Requires COBO use case.

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-10-000070	Restrictions	Install unknown sources	Allow/ Disallow	Allow	KNOX-10-008000	Requires apps be downloaded from other AO-approved app repository (for example, DoD-app store). If possible, using a remote Management tool or local admin: Implement policy with "Tactical setting" for as long as required to install apps/updates and set "Non-tactical setting" afterward. Requires COBO use case.
KTACT-10-000080	Knox Bluetooth	Allowed profiles	HSP, HFP, BPAP, A2DP, AVRCP, SPP, NAP, BNEP, HID, BPP, DUN, SAP	Enable "all" profiles that may be required for any mission need	KNOX-10-001400	If possible, using a remote Management tool or local admin: Implement policy with "Tactical setting" only while on mission and set "Non-tactical setting" after return from mission.
KTACT-10-000090	Restrictions	Debugging features	Allow/ Disallow	Allow	KNOX-10-002800	If possible, using a remote Management tool or local admin: Implement policy with "Tactical setting" only as long as Mock Locations/ USB debugging is required

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
						and set “Non-tactical setting” afterward. Requires COBO use case.
KTACT-10-000100	Restrictions	USB file transfer	Allow/ Disallow	Allow	KNOX-10-003500 KNOX-10-003700	If possible, using a remote Management tool or local admin: Implement policy with “Tactical setting” only to side-load tactical apps/data and to allow backup of data to locally connected systems after return from mission and set to “Non-tactical setting” when completed.
KTACT-10-000110	#1: Restrictions #2: Restrictions #3: KPE Date Time	#1: Config Date Time #2: Set auto (network) time required #3: Date Time Change	#1: Allow/ Disallow #2: Require/ Do not require #3: Enable/ Disable	#1: Allow #2: Do not Require #3: Enable	KNOX-10-010200	If possible, using a remote Management tool or local admin: Implement policy with “Tactical setting” only as required to correct the date/time while on mission deployment.
KTACT-10-000120	KPE Restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON,	HID MAS	KNOX-10-011200	If possible, using a remote Management tool or local admin: Implement policy with “Tactical setting” only during pre-mission device

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
			CSC, HID, HUB, MAS, MIS, PER, PHY, PRI, STI, VEN, VID, WIR			configuration and set to "Non-tactical setting" prior to mission deployment.
KTACT-10-000130	Restrictions	Trust Agents	Allow/ Disallow	Allow	KNOX-10-002300	If implementing KTACT-10-000060, do not implement this policy as stated here. Use the STIG configuration table setting. Otherwise, the "trust agent configuration" will not operate correctly.