SAMSUNG ANDROID 12 WITH KNOX 3.X SUPPLEMENTAL PROCEDURES

27 July 2022

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 the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. 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. Samsung continues to work with Google to simplify mobility for customers and reduce duplication. Knox features are 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 AE while adding necessary Samsung Knox features on top to comply with their security requirements.

This STIG is fully harmonized with Google's Android platform STIG configuration. The AE security policies listed cover the baseline STIG requirements. Knox policies can augment the deployment to provide additional features, and in some cases may be used in substitution of AE policies to alleviate customer pain points when there is a gap in coverage due to management tool limitations. With this harmonization, the previous Legacy deployment that utilized Device Admin (DA) is now deprecated for use and no longer supported.

The following configurations are available for Samsung Galaxy devices running Android 12:

- To support COBO: Fully managed device:
  - Device Owner (DO) privileges are assigned to an MDM or similar application to apply policies and restrictions to the device as a whole.
- To support COPE (management-over-privacy): Fully managed device with App Separation:
  - DO privileges are assigned to an MDM or similar application to apply policies and restrictions to the device as a whole. In addition, using Knox App Separation feature, a group of apps are isolated from the rest of the system, supporting use cases such as the isolation of non-work approved apps or the separation of highest-trust tier apps.
- To support COPE (privacy-over-management): Work profile on company-owned device:
  - A work profile is created on a company-owned device, enabling the use of the device for personal purposes and work purposes in a separate profile. The work profile is managed by a Profile Owner (PO) that can apply certain configurations to the device as a whole that respect the user's privacy.
- To support BYOD: Work profile on personally owned device:
  - A work profile is created on a personally owned device. The work profile is managed by a Profile Owner (PO) that can apply configurations to the Work Profile only, with the exception of very few policies that can be applied to the device.

2. INTRODUCTION

Android Enterprise (AE) provides baseline security protections, management policies, and network functions that fully cover the STIG requirements. Samsung Android mobile devices can leverage Samsung-specific security features and hardware to enhance security beyond the configuration standards required for DoD Information Assurance (IA). In other words, AE covers the STIG baseline requirements, while the Samsung-specific security features (Knox Platform for Enterprise [KPE]) provide additional benefits for customers who require them.

KPE differentiating features when compared with AE include software features such as App Separation, DeX, Mobile hotspot management, SD card encryption, sensitive data protection[1], on-device firewall management, audit logs, network platform analytics, customizable keyguard, Dual Data at Rest (DualDAR), and hardware features as discussed in section 5.1.1, Hardware-Backed Security

Figure 2-1: AE and KPE

[1] Sensitive Data Protection (SDP) will be deprecated starting from Android 13; it will be replaced by the AE-equivalent – Storage Area Encryption (SAE).

3. ANDROID 12 USER PRIVACY

Android 12 continues to build on the increased emphasis on improving user privacy, as introduced in Android 11. Therefore, AE has few controls over the personal profile. Personal apps in the personal profile cannot be configured, monitored, or enumerated by an MDM.

This situation can be mitigated by DoD mobile service providers interested in more control of personal apps by:

- Implementing zero-touch enrollment or Knox Mobile Enrollment (KME) forces old and new devices to remove all personal apps at enrollment, and then MDM can control which apps can be downloaded via app block list or app allow list. (See Section 5.2.2 for more detail.)
- Alternately, for a fully managed device (COBO), use Knox Service Plugin (KSP) to allow installation of personal apps. (See Section 6.1 for more detail.)

4. ANDROID ENTERPRISE (AE)

4.1 App Isolation

Android provides both app isolation and group of apps isolation.

The core app isolation technology is called SE for Android, which is an adaptation of SELinux to Android. This technology denies applications access to resources unless otherwise allowed by a Samsung-built policy. Applications are given labels so they cannot access data of other applications or of the same application installed under a different user.

Groups of apps may be isolated by the creation of a work profile. This results in the installation of the apps under a different Android user. While communication is allowed between apps installed under the same user, for instance through the Binder framework, this is prohibited by the Android framework for non-system apps installed under different users, contributing to a further isolation of these apps.

The creation of a work profile is not possible under Android 12 when the device has been enrolled as a fully managed device (COBO). However, Samsung provides an alternative mechanism for app separation in the COBO scenario using the Knox App Separation feature. This mechanism can be enabled or disabled by an IT administrator via the KSP. By installing KSP on the target device, IT administrators can specify which apps they want to see isolated on compatible UEM consoles. These apps will be installed via Managed Play under a secondary Android user while being disabled under the main user. No launchable system apps are enabled under the secondary user by default. Similar to work profiles, no sharing between users is allowed, strengthening the isolation of these apps as a group.

4.2 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 four 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 Profile password: This STIG does not require a separate password for the Work Profile.
- Encryption of device data:
  - Protected data: Data marked as “protected” is encrypted when the device is in the powered-off state and while in the powered-on state before the user first successfully inputs their credentials. 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 Work Profile

Chamber directory. SDP is NIAP certified as compliant with MDFPP and available for use in this STIG.

- Encryption: Samsung Galaxy devices supporting Android 12 use File-Based Encryption (FBE). The user must successfully authenticate with the device password after boot before the "protected" and "sensitive" data is decrypted.

4.3 Device Management

Samsung Android devices support administrator configuration and management via third-party MDM tools. Devices support AE with KPE being built on top, providing additional policies and services that can be accessed and configured by the Management tool.

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

For MDM solutions, management applications, also known as Device Policy Controllers (DPCs), are installed on the device. 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:

- COPE: An enterprise-owned device for business and personal use. A Work Profile is configured to separate work applications and data from personal applications and data.
- BYOD: A personally-owned device, on which the user must download an MDM client app that separates the device into a Work and Personal space just like in the COPE configuration. The difference being that in the BYOD case, the MDM has no visibility or control on the personal side, in contrast to the COPE configuration where limited visibility and control is granted to the MDM admin, while still respecting the user's privacy.

  Note: BYOD is not within scope for this STIG.
- COBO: Configuration of a device for work use only, with a single space for work applications and data. Personal applications and data are prohibited. App separation as described in Section 6.1 App Separation may be exploited to have a separate area where secondary apps may be installed. This facilitates the installation of non-work approved apps, such as those of ride-hailing services, which may assist employees on business trips.

This STIG uses AE policies, enforced by a Management tool, to deploy devices in a compliant configuration. AE supports COBO, COPE, and BYOD use cases, with this STIG providing the appropriate configuration. **Note:** BYOD is not within scope for this STIG.

This STIG does not require the use of KPE or need an activated KPE license for a device to be compliant. However, KPE can be used on top of, or in some cases in substitution of, AE and the device will still be STIG-compliant. The STIG instructions note where KPE can be used to

provide more functionality that can be provided when using AE alone. The configuration table document also includes a table listing all KPE APIs that can be used to substitute for AE APIs, for cases where an MDM does not provide full AE coverage. Remember, KSP can be used to implement these KPE substitute APIs should the MDM not implement them innately. KPE requires a Knox License to operate, and the license is now free to customers.

Additional details on the deployment uses cases and corresponding configuration can be found in Section 7 Use Cases.

5. KNOX PLATFORM FOR ENTERPRISE (KPE)

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 enhance the security of the AE configuration which meets the standards baseline for DoD IA.

Figure 5-1: Knox Platform Diagram

For additional information, visit:

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

5.1 KPE Security Highlights

Samsung offers a proprietary set of security features to MDMs that can provide additional security sometimes on a more granular level upon request of AOs. This section will cover KPE features.

5.1.1 Hardware-Backed Security

5.1.1.1 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 filesystem-level 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)[2]
- Network Platform Analytics (NPA)

5.1.1.2 Knox Verified Boot (KVB)

Starting with Samsung Galaxy S10, KPE introduced 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.

5.1.1.3 Hardware Fuses

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

- Device Health Attestation checks fail.
- The device requires reset to wipe the data after detection of unofficial software components.
- Work profile no longer operates, preventing access to the secure enterprise apps and "protected" data within.

5.1.2 Data Protection

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

- User authentication:

[2] Marked for deprecation in Android 11 and will be removed from Android 13. It is replaced with SAE as part of a native AE feature.

  - Biometric authentication: Fingerprint authentication is NIAP certified as compliant with the Protection Profile for Mobile Device Fundamentals (MDFPP) and available for use in this STIG. The devices also support 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:
  - DualDAR: Knox 3.3 also introduces Dual Data-at-Rest (DualDAR) for Galaxy S10 (and newer) devices compliant with Commercial Solutions for Classified Program (CSfC) DAR Capability Package (CP). See Section 6.3 DualDAR 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, such as providing the ability to configure different VPNs for the Work Profile and the Personal profile under legacy deployments as well as for individual apps under any deployment.

5.2 Manageability Highlights

5.2.1 Knox Mobile Enrollment (KME)

KME (desktop and cloud), **approved for STIG use, and highly recommended for DoD use**, 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 configures 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 is 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 reinstalled automatically 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 AE.
- Allows bypass of Google factory reset protection.
- Allows specifying root or intermediate certificates that will be installed during KME enrollment (for example, the installation of the DoD Root and intermediate certificate bundle).

AE 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. Notice that Samsung Galaxy devices support both AE zero-touch enrollment and KME, with the latter taking precedence if a device is registered with both services.

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

5.2.2 Enterprise Firmware Over-the-Air (E-FOTA)

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

Knox E-FOTA One, in particular, has several benefits in comparison to other E-FOTA solutions. These include the ability to assign multiple device models to different firmware releases in a single campaign; the automatic uploading of device identifiers to Knox E-FOTA by resellers participating in the KDP; out-of-the-box installation of the Knox E-FOTA client app; and the possibility of adding licenses as needed to support more devices while keeping current licenses active. Knox E-FOTA also supports bypassing the carrier FOTA restrictions.

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

5.2.3 Accelerating Delivery of Knox Features to Customers

Samsung KPE supports OEMConfig, an Android standard that enables original equipment manufacturers (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 AE known as "managed configurations" and is part of the standard published on the Appconfig community.

Samsung supports OEMConfig through the KSP app. All EMM vendors that have validated their solutions for AE can immediately support Samsung KPE features as they are updated through the Knox Service Plugin app. For this to happen, Samsung publishes an XML schema that defines

the controls supported by KSP and is linked to the KSP's manifest file. UEM developers implement logic to pull this schema from Managed Google Play and render an interface for administrators to interact with these controls. This interface is updated with each new release of KSP. After the IT administrator saves their configuration, the MDM pushes the configuration to Managed Google Play, which relays it to KSP. KSP applies the policies requested by the IT administrator and returns the result of the configuration process using Google's Feedback SDK. IT administrators can view any configuration failures and associated error messages on the UEM console.

The aforementioned mechanisms are used for IT administrators to configure the app separation control described in Section 6.1 App Separation. IT administrators will be able to activate app separation through their UEM console and restrict the apps that may be installed in the space associated with it. KSP will then use the feedback channel to report the successful or unsuccessful termination of the app separation process as well as of any update to the list of installable apps.

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

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

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

6. SPOTLIGHT

6.1 App Separation

Introduced in Android 11, KPE App Separation allows an IT admin to mitigate risks from one group of apps to another. It removes the burden of vetting every app while allowing the user to be more productive by installing the non-enterprise apps they desire. The separation mechanism is available when deploying the COBO use case with an AE fully managed Samsung Galaxy device.

The activation of this feature and the list of apps to be isolated must be enabled and configured by IT administrators through KSP.

There are two use cases for separation:

- Isolate a specific list of apps (Inside).
- Isolate everything except for a specific list of apps (Outside).

6.1.1 Inside Use Case

If app separation is configured for the "Inside" use case, the list of specified apps will be installed inside of the app separation folder, while apps not in the list will be installed outside.

To configure this use case, do the following within KSP:

1. Application Separation
2. App Separation policies [Allow List Policy] >> CONFIGURE
3. Enable App Separation policies [enable]
4. Location for Separate Apps installation [Outside/Inside] >> Inside
5. List of Apps to Separate >> "comma separated list of package names"

6.1.2 Outside Use Case

If app separation is configured for the "Outside" use case, the list of specified apps will be installed outside of the app separation folder, while apps not in the list will be installed inside.

To configure this use case, do the following within KSP:

1. Application Separation
2. App Separation policies [Allow List Policy] >> CONFIGURE
3. Enable App Separation policies [enable]
4. Location for Separate Apps installation [Outside/Inside] >> Outside
5. List of Apps to Separate >> "comma separated list of package names"

6.2 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.

Due to the STIG configuration disallowing USB file transfer, DeX Drag & Drop mode is not usable.

6.2.1 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
- USB cable with DeX companion app

6.3 DualDAR

Starting with Samsung Galaxy S10, KPE introduced DualDAR 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

DualDAR 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.

DualDAR has been designed since its inception to respect the privacy requirements enforced by AE for work profiles on company-owned devices.

For additional information, visit:
https://docs.samsungknox.com/admin/whitepaper/kpe/DualDAR.htm

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

6.4 Common Criteria (CC) Settings

As Samsung continues to harmonize with Google and remove duplication, KPE CC mode API is now marked for deprecation in Android 12 for removal in Android 13. Starting with this STIG, the use of AE Common Criteria mode will be required. To allow customers time to migrate to the new API, KPE CC mode can continue to be used within this STIG as all required security behaviors are implemented by both KPE and AE CC mode implementations for Samsung Android devices.

7. 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). The following use cases are supported in this STIG:

- COPE: An enterprise-owned device for business and personal use. This use case provides limited visibility and control while respecting User's privacy. 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 Work profile to maintain a separation between personal and work data and applications. Refer to Sections 8 Configuration of the Personal Profile and Section 10 Configuration of COPE Work Profile of this document to support the COPE configuration.
    - DualDAR-enabled Work profile to support high-security requirements such as CSfC DAR CP. (This configuration is not in the scope of this document.)
- 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 Knox Work profile for separation of personal applications, which is prohibited. Refer to Section 9 Configuration of COBO to support this COBO configuration.
    - Using app separation to allow for the isolated use of non-work approved apps.
- BYOD: A personal device brought into the Work Profile after being equipped with an MDM agent that creates a work profile where work-specific apps/data are subject to security policies. The non-work profile (personal profile) is almost[3] free from any restrictions. This implies that certain features such as disabling Bluetooth/Wi-Fi sharing are not present as this would inhibit the personal side of the device as well. The lack of some restrictions[4] are covered by UBEs discussed later on in this STIG (Section 15).

  Note: This information is included for completeness. BYOD is not currently approved for DoD use, except for several limited pilots.

Samsung Android devices support the COBO, COPE, and BYOD use cases described above.

In all use cases, the DPCs apply AE policies using Android API implemented by the Android Device Policy Manager (DPM) module. Additionally, the DPC may apply KPE policies using Samsung KPE APIs, in addition to AE policies.

[3] Few restrictions can be applied to the Personal Profile of BYOD. For example, lock screen and password restrictions.
[4] As for COBO and COPE, AE policies will simply disable Bluetooth in general, thereby prohibiting any usage of the wireless protocol for sharing.

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. The device is managed by the MDM in Device Owner or Profile Owner mode, and further restrictions are applied by a local device administrator. In either case, this allows for a flexible deployment where policies can be adjusted by an authorized IT administrator on-site.

7.1 Tactical Use Case

Not all STIG requirements are appropriate for tactical use cases. AOs have the authority to POA&M STIG requirements and accept risks after considering mitigation strategies.

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.

7.2 Configuration Approach

This STIG uses AE policies to deploy Samsung Android devices for the COBO, COPE, and BYOD uses cases in the AE deployment type.

Despite this, in some cases KPE can be used in place of an AE policy to provide extra functionality while maintaining STIG compliance. In other cases, in which the MDM does not provide full AE coverage, KPE policies may be used in substitution of AE policies. For these instances the STIG includes additional information in both the instructions and the configuration table comment column.

If a DoD mobile service provider wishes to deploy with the Knox app separation feature, it must be implemented using the policies in “Table 1: Configuration Policy Rules for COBO” configuration table document. The app separation policies listed in “Table 4: KSP App Separation” within the same document must then be applied.

Depending on management tool policy support and DoD mobile service provider deployment choices, the use cases defined in Section 7 Use Cases above can be implemented using deployment options as summarized in the following table:

Table 7-1: User Case and Deployment Options

Deployment Use Cases	Deployment/ Enrollment Type	Supplemental Document Reference	Configuration Document
COBO	AE Fully managed device	Section 9 Configuration of COBO	Apply policies in "Table1: Configuration Policy Rules for COBO" within the configuration tables document.
COPE	AE work profile on company-owned device	Sections 8 Configuration of the Personal Profile and Section 10 Configuration of COPE Work Profile	Apply policies in "Table 2: Configuration Policy Rules for COPE" within the "configuration table document.
BYOD	AE work profile on personal-owned device	Section 10 Configuration of COPE Work Profile	NA

8. CONFIGURATION OF THE PERSONAL PROFILE

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 Profile and Work Profile are set up on Samsung Galaxy devices running Android 12.

DoD mobile service providers may allow users access to the Google Play app store for the Personal Profile, 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 AO has approved access to the Google Play app store for the Personal Profile, including downloading and installing Google Play apps into the Personal Profile and syncing personal data on the device with personal cloud data storage accounts[5]. 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 Profile (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 Profile.
- 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)[6]. See STIG requirement KNOX-12-110290/KNOX-12-210290 for more information.

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

[5] 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.
[6] UBE controls cannot be managed by the site Management tool and, therefore, must be managed by the mobile device user. See Section 10 *Configuration of COPE/BYOD Work Profile* section in this document for more information.

9. CONFIGURATION OF COBO

This section is not applicable for the COPE use case. In the COBO use case, an AE 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. App Separation may be enabled to allow non-enterprise applications to be installed in the COBO use case.

10. CONFIGURATION OF COPE WORK PROFILE

10.1 Overview

In a COPE device, there are two completely isolated and independent profiles available; Personal and Work. Enterprise applications and data reside within the Work Profile, while personal applications and data reside within the Personal Profile.

Note: BYOD information is included for completeness. BYOD is not currently approved for DoD use, except for several limited pilots.

10.2 Work Profile Isolation

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

10.3 COPE and BYOD Difference

The BYOD use case behaves in a very similar way to the COPE use case with the difference being that with BYOD, the MDM admins have limited visibility and control while respecting User's privacy within the Personal Profile due to the phone being personally-owned and not company-owned. Sections 8 Configuration of the Personal Profile details the functions the AO is able to perform on the Personal Profile in the case of the COPE deployment; they are not applicable to the Personal Profile in BYOD deployments.

11. PROCEDURES

11.1 Device Wipe

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

11.2 Unenrollment

As part of retiring/unenrollment of Samsung devices or for transferring a device to a new user, those devices must be wiped by the administrator in the correct manner, using a wipe policy provided by a management tool. **Using the "recover menu" is not an approved method**, and can lead to operational issues; for example, Factory Reset Protection (FRP).

12. SPECIAL GUIDANCE

12.1 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.

13. INFRASTRUCTURE

13.1 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 enable additional features, or provide additional security controls as may be required for customers with additional deployment needs beyond what is required by the STIG. These APIs can be used to configure restrictions on the device and a Work Profile. The Knox 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 password requirements, must be applied separately for the personal area and Work Profile. Others, such as disabling Wi-Fi, can only be applied at a device-wide level.

13.2 Knox Licensing (FREE)

Note: KPE licenses are now provided free of charge.

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 free and obtained 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.

13.3 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 and support for maintenance, which are available for both Windows and Linux.

The Knox On-Premise server includes the following components:

- 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.

14. 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 11.2 Unenrollment). Follow mobility service provider decommissioning procedures as applicable.

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

15. 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.

15.1 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, the event details will be shown on the device screen at the specified time, 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.

15.2 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” feature (device model dependent) is accessed from the notification bar and displays a list of scanned devices that can form a connection with the user’s device. 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 Digital Living Network Alliance (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, visually verify the recipient device, and use 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. Specifically disabling Wi-Fi Direct and Bluetooth Sharing can only be performed via KPE APIs. AE APIs are less granular and simply disable Wi-Fi or Bluetooth as a general service.

Note that none of the aforementioned wireless restrictions are possible to enforce for the BYOD use case; users must be trained/instructed not to share over Bluetooth/Wi-Fi in certain circumstances (UBE).

15.3 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 an 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 these types of accessories (DeX Station, USB dongle) to a DoD network via an Ethernet cable. See STIG requirement KNOX-12-210130.

15.4 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.

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 have determined that even when "Location History" is disabled, Google continues to store location data on the mobile device[7]. 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:
   -allowWifiScanning()[8]
   -allowBLE()[9]
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[10].
   Note: Operational impact of recommended STIG controls:
   - Few Management tool products support these APIs at this time (October 2020).
   - Impact: Site will need to use procedures for Knox 3.2 (or later) devices until its MDM supports the new APIs. For AE deployments, KSP can be used where MDM capability is missing. The guidance to implement these policies are listed in Table 16-1: Policy Implementation Guidance

[7] 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.
[8] 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.
[9] 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.
[10] See DoD CIO memo "Mobile Application Security Requirements", 06 Oct 2017, for information on reviewing mobile applications.

Table 16-1: Disable Location Tracking Implementation Guidance

Policy Group	Policy Rule	Instructions
Advanced Restriction	Wi-Fi scanning	1. Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) 2. Enable device policy controls [enable] 3. Advanced Restriction policies (Premium) 4. Enable Advanced Restrictions controls [enable] 5. Allow Wi-Fi scanning [disable]
Advanced Restriction	Bluetooth scanning	1. Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) 2. Enable device policy controls [enable] 3. Advanced Restriction policies (Premium) 4. Enable Advanced Restrictions controls [enable] 5. Allow Bluetooth scanning [disable]

- 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.