SAMSUNG ANDROID OS 11 WITH KNOX 3.X SUPPLEMENTAL PROCEDURES

Version 1, Release 1

20 November 2020

Developed by Samsung and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. GLOSSARY

Acronym	Meaning
AO	Authorizing Official
API	Application Programming Interface
BYOD	Bring Your Own Device
CC	Common Criteria
COBO	Corporate Owned Business Only
COPE	Corporate Owned Personally Enabled
DA	Device Admin
DeX	Desktop Experience
DISA	Defense Information Systems Agency
DO	Device Owner
DoD	Department of Defense
DPC	Device Policy Controller
EDM	Enterprise Device Manager
HID	Human Interface Device
KPE	Knox Platform for Enterprise
KSP	Knox Service Plugin
MDM	Mobile Device Management
PO	Profile Owner
STIG	Security Technical Implementation Guide
USB	Universal Serial Bus
VPN	Virtual Private Network

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 AE while adding necessary Samsung Knox features on top to comply with their security requirements.

Samsung has deployed these changes in a phased way so customers can adjust to the new frameworks. Knox Workspaces are supported for all devices released prior to Knox 3.4 (e.g., S10). For devices released after Android 8.0 Oreo, work profiles on personally owned devices (work profiles – P) and work profiles on company-owned devices (work profiles – C) may be created through AE. Work profile – P enrollments would be used to implement a Bring Your own Device (BYOD) use case, whereas work profile – C enrollments would be used to

implement a Corporate Owned Personally Enabled (COPE) use case. Both enrollment types will benefit from the KPE features after a KPE license is activated.
Also, AE has promoted the deprecation of Device Admin (DA) for Enterprise use, with a shift in focus to consumer security. This Security Technical Implementation Guide (STIG) continues to support DA with its Legacy configuration. Samsung achieves this by providing alternative APIs for controls deprecated under Android 10 in AE through the Enterprise Device Manager (EDM). This allows sites time to migrate to AE deployments.

The following configurations are available for Samsung Galaxy devices running Android 11:

- 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. DA applications may also be installed and enforce policies.
  - For Legacy deployments, DA privileges are assigned to an MDM or similar application to apply policies and restrictions to the device as a whole. Other DA applications may also be installed and enforce policies.
- 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. DA applications may also be installed and enforce policies. 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.
- 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 configurations to the device as a whole that respect the user's privacy. DA applications may also be installed and enforce policies. Current COPE deployments featuring a DO and a PO will transition to this model when their device is upgraded to Android 11.
- Work profile on personally owned device:
  - A work profile is created on a personally owned device. This setting is not within the scope of this document.
- DA + Knox Workspace:
  - Legacy Knox Workspaces may be created in a Samsung Galaxy device released prior to Knox 3.4 with a DA.

3. ANDROID ENTERPRISE (AE)

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).

KPE differentiating features when compared with AE include sensitive data protection, on-device firewall management, audit logs, network platform analytics customizable keyguard, and Dual Data at Rest (DualDAR).

4. ANDROID 11 USER PRIVACY

Android 11 has increased emphasis on improving user privacy. Therefore Android Enterprise 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.)

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 meet the configuration standards 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

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)
- 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.
- KPE Keystore removes the cryptographic keys used by SDP, preventing access to data marked as "sensitive".
- KPE Workspace/Work profile no longer operates, preventing access to the secure enterprise apps and "protected" data within.

5.1.2 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 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.

For non-legacy deployments, the creation of a work profile is only possible under Android 11 when no app has been assigned DO privileges. Samsung provides an alternative mechanism for app separation in this 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.

5.1.3 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 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:
  - 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 KPE Workspace/ 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 11 use File-Based Encryption (FBE). Devices launched with Android 10 include a "Strong Protection" control. When "Strong Protection" is activated on devices released with Android 10, or for devices released with Android 11, the user must successfully authenticate with the device password after boot before the "protected" and "sensitive" data is decrypted.
  - 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 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 Knox Workspace and the personal profile under legacy deployments as well as for individual apps under any deployment.

5.2 Manageability Highlights

5.2.1 Device Management

Samsung Android devices support administrator configuration and management via third-party MDM 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 permits an administrator to configure and subsequently use platform APIs to apply the configuration.

For MDM solutions, one or more management applications, which are 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 Knox Workspace/Work profile is configured to separate work applications and data from personal applications and data.
- 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 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 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 7.

5.2.2 Knox Mobile Enrollment (KME)

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 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 Android Enterprise and Android Legacy deployments.

- 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).

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. 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.

5.2.3 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

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.

5.2.4 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 Android Enterprise 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 Android Enterprise 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. IT administrators will be able not only to activate app separation through their UEM console but also to allowlist 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 app allowlist.

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

6. SPOTLIGHT

6.1 App Separation

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 running Android 11.

The activation of this feature and the list of apps to be isolated must be enable 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.

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

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.

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/whitepapers/knox-platform/DualDAR.htm

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

6.4 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 three separate functional changes on the mobile device (see requirement KNOX-11-020100/ KNOX-11-020200 for more details). In previous Samsung STIGs, "CC Mode" had been categorized with a higher severity level, but with recent improvements making security features non-configurable and secure by default, it has been reassessed and is now categorized as CAT III for this STIG.

The set of Common Criteria configuration settings in the STIG includes both Management tool managed policy controls:

- Features enforced by policy:
  - Enable Knox CC Mode (notice that AE CC Mode does not provide the same policy coverage as Knox CC Mode, and the activation of this control would not suffice to leave the device in a compliant state)
  - 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

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.

6.5 Legacy Knox Workspace and COPE (DO+PO) Deprecation

The creation of Knox Workspace is no longer supported in device models that launch with Knox 3.4 or later. This has no impact on current deployments (i.e., devices released with an earlier version of Knox than 3.4 will continue to support the Knox Workspace). Devices deployed in COPE mode featuring a DO and a PO will transition to a work profile on the corporate-owned device setting when upgraded to Android 11. The DO will be removed, while the PO will benefit from an extended API that will allow it to apply device-wide configurations.

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

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), and therefore the BYOD use case is not considered in this STIG. The following Corporate Owned use cases are supported in this STIG:

- 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 Knox Workspace/Work profile to maintain a separation between personal and work data and applications. Refer to Sections 8 and 10 of this document to support the COPE configuration
- 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 Knox Workspace/Work profile for separation of personal applications, which is prohibited. Refer to Section 9 to support this COBO configuration.
  - Using app separation to allow for the isolated use of non-work approved apps.
  - 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 Work profile is created that is managed by a DPC in Profile Owner (PO) mode, which resides inside the Work profile. The device will detect that it is company-owned and the DPC in PO mode will have its privileges extended so that it can apply both allowed device-wide and Work profile policies.
  - 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 DA mode is installed.
  - For COPE, the DPC manages both the device and the Knox 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 deprecation 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 Device Owner or Profile 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.

7.1 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. Notice that for AE COPE deployments, these polices are set by the extended PO residing inside the Work profile.
- Work Environment Policies are applied to the Knox Workspace/Work profile in the COPE use case (where the Knox Workspace/Work profile is the Work Environment), or to the “main user” in the COBO use case (since there is no separate Knox 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 uses a naming convention for the Policy Group configuration within the configuration tables. Configuration for the “Device/Asset” is prefixed

with “Device”, and configuration for the “Work Environment” is prefixed with “Work profile/Workspace”.

If a DoD mobile service provider wishes to deploy with the Knox app separation feature, it must be implemented using the COBO AE fully managed device and the policies in “Table 2: Configuration Policy Rules for COBO” within the “AE Configuration Tables” 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 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	Android Legacy managed device	Section 9	Apply policies in “Table 2: Configuration Policy Rules for COBO” within the “Legacy Configuration Tables” document.
	Android Enterprise Fully managed device		Apply policies in “Table 2: Configuration Policy Rules for COBO” within the “AE Configuration Tables” document.
COPE	Android Legacy managed device with Legacy Workspace	Sections 8 and 10	Apply policies in “Table 1: Configuration Policy Rules for COPE” within the “Legacy Configuration Tables” document.
	Android Enterprise work profile on company-owned device		Apply policies in “Table 1: Configuration Policy Rules for COPE” within the “AE Configuration Tables” document.

8. 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 Samsung Galaxy devices running Android 11.

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-11-018900 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 for 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.

9. CONFIGURATION OF COBO

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

10. CONFIGURATION OF COPE KNOX WORKSPACE/WORK PROFILE

10.1 Overview

The Knox 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 resources are separate from the ones in the Work Environment.

10.2 Work Environment Isolation

The Knox Workspace/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 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.

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.

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 allowlisting or denylisting.

- For application installation allowlisting, the unwanted apps will be implicitly denylisted (all apps denylisted), and the unwanted apps will not be allowlisted.
- For application installation denylisting, the unwanted apps will be explicitly denylisted.

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

11.2 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.

Please note that the device “recovery menu” is not a Management tool and should not be used to wipe the device.

12. SPECIAL GUIDANCE

12.1 Allowlisting vs. Denylisting

Samsung policies such as “app installation” and “account addition” make use of allowlists (referred to previously as whitelists) and denylists (referred to previously as blacklists).

Management tools implement the allowlist and denylist 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.

Allowlisting and denylisting are two ways to filter things. Allowlisting will allow only the things that are listed. Denylisting will allow everything except the things that are listed.

Some Management tools might provide allowlisting and denylisting exactly as described here, permitting either an allowlist or denylist to be configured but not both. This is the same as the intention in the STIG configurations.

However, some Management tools might provide allowlisting and denylisting, permitting both to be configured.

Refer to the Management tool’s documentation to determine how allowlisting/denylisting is implemented.

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

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

Note, for application management, app installation allowlist and denylist policies allow the administrator to manage what a user may or may not install or update, but the pre-installed apps must be managed using application disablement policy.

12.2 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.

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 implement several STIG controls. These APIs can be used to configure restrictions on the device and a Workspace. The Knox 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 allowlist 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.

13.2 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.

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, 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). 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.

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 the DeX Station to a DoD network via an Ethernet cable. See STIG requirement KNOX-11-0020900.

15.4 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 this 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-11-022100.

15.5 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.

16. 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.

16.1 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 in the Work Environment and disable these applications unless use is approved by the AO. This list includes:

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

16.2 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
- Music Share
- Direct Share

16.3 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

[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).

or Wi-Fi connection, it may be able to print to network printers if the printer drivers or a printer app is installed. Android 11 comes with a built-in print service that allows communication with most commercial printers.

16.4 Core and Preinstalled Applications

DoD Commands and Agencies should fully vet core and preinstalled 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 core and preinstalled applications may be already disabled or not installed.

For non-AE enrollments (Legacy), using the list of apps that are disabled when the same device is AE enrolled is recommended to provide a baseline configuration.

17. ADDITIONAL SAMSUNG FEATURES

17.1 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.

17.2 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 (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

[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.

where MDM capability is missing. The guidance to implement these policies are listed below:

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.

17.3 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 17-1 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 17-2 is essentially the recommended Configuration Table for the tactical use case. The STIG controls and mitigations listed in Table 17-1 are represented in Table 17-2.

Note: Not all STIG controls listed in Tables 17-1 and 17-2 are appropriate for every tactical use case.

Note: Specific Management tool products may not support some of the risk mitigations listed in Table 17-1. DoD organizations should consult with their Management tool vendor and Samsung on how best to implement recommended mitigations.

Table 17-1: List of Tactical Changes to STIG Requirements with Recommended Mitigations

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
KNOX-11-000700/ KNOX-11-000800	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-11-000100/ KNOX-11-000200	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-11-000700/ KNOX-11-000800
KNOX-11-000500/ KNOX-11-000600	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 are 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 allowlist 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-11-015300/ KNOX-11-015400	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-11-002500/ KNOX-11-002600	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-11-003900/ KNOX-11-004000	Enable Trust Agents and configure a list of trusted devices using “Trusted Device”.	The user authentication mechanism would be bypassed so the user does not need to 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 allowlist 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 Allowlist to operate correctly.
KNOX-11-005300/ KNOX-11-005400	Enable developer modes.	Mock Locations and USB debugging are required for some tactical use cases.	Requires COBO deployment.
KNOX-11-006700/ KNOX-11-006800 KNOX-11-007100/ KNOX-11-007200	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
KNOX-11-019300/ KNOX-11-019400	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

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
KNOX-11-020900/ KNOX-11-021000	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 17-2: Configuration Policy Rules for Tactical Use Case

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-11-000010	Password Requirements	Max password failures for local wipe	0+	0	KNOX-11-000700	This configuration is only required if: - implementing KTACT-11-000020 - not implementing KTACT-11-000020 but as part of a recommended mitigation for either KTACT-11-000030/40. If configured as part of a recommended mitigation for either KTACT-11-000030/40, use a setting of "5" and not "0" as stated here.
KTACT-11-000020	KPE Password Requirements	Max password failures for device disable	0+	10	KNOX-11-000700	If also implementing either KTACT-11-000030/40, the recommended mitigation is to use a setting of "5" and not "10" as stated here.

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-11-000030	Password Requirements	Minimum password length	0+	4	KNOX-11-000100	DoD recommended mitigation: See "Comment" section of KTACT-11-000010/20.
KTACT-11-000050	Password Requirements	Max time to screen lock	0+	2 hours	KNOX-11-000500	This is Method #1. If configuring this, do not configure KTACT-11-000060. 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-11-000060	Restrictions	Trust Agent configuration	Configure	Enable "trusted device" feature	KNOX-11-000500	This is Method #2. If configuring this, do not configure KTACT-11-000050, or KTACT-11-000130. Requires COBO use case.
KTACT-11-000070	Restrictions	Install unknown sources	Allow/ Disallow	Allow	KNOX-11-015300	Requires apps be downloaded from other AO-approved app repository (for example, DoD-app store).

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
						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-11-000080	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-11-002500	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-11-000090	Restrictions	Debugging features	Allow/ Disallow	Allow	KNOX-11-005300	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 and set "Non-tactical setting" afterward. Requires COBO use case.

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-11-000100	Restrictions	USB file transfer	Allow/ Disallow	Allow	KNOX-11-006700 KNOX-11-007200	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-11-000110	#1: Restrictions #2: KPE Date Time	#1: Config Date Time #2: Date Time Change	#1: Allow/ Disallow #2: Enable/ Disable	#1: Allow #2: Enable	KNOX-11-019300	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-11-000120	KPE Restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON, CSC, HID, HUB, MAS, MIS, PER, PHY, PRI,	HID MAS	KNOX-11-020900	If possible, using a remote Management tool or local admin: Implement policy with "Tactical setting" only during pre-mission device configuration and set to "Non-tactical setting" prior to mission deployment.

UID	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
			STI, VEN, VID, WIR			
KTACT-11-000130	Restrictions	Trust Agents	Allow/ Disallow	Allow	KNOX-11-004300	If implementing KTACT-11-000060, do not implement this policy as stated here. Use the STIG configuration table setting. Otherwise, the "trust agent configuration" will not operate correctly.