SAMSUNG ANDROID OS 9 WITH KNOX 3.X SUPPLEMENTAL PROCEDURES

24 July 2020

Developed by Samsung and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. 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 upon 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 MDM vendors to offer a single foundation for customers to deploy Android Enterprise, while adding necessary Samsung Knox features on top to comply with their security requirements.

2. ANDROID ENTERPRISE

AE provides basic security protections, management policies, and network functions. However, AE alone lacks the necessary controls to deploy a Samsung Android mobile device that meets the configuration standards for DoD Information Assurance (IA).

3. KNOX PLATFORM FOR ENTERPRISE

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

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

The following KPE features must be configured, in addition to AE features, for this Security Technical Implementation Guide (STIG):

- Knox Workspace (for Corporately Owned Personally Enabled [COPE] use case)
- Knox Common Criteria (CC) mode
- Knox access control policy (for COPE use case)
- Knox password constraints: Maximum sequential or repeating characters and numbers
- Knox certificate: Revocation checking and Online Certificate Status Protocol (OCSP)
- Knox audit logging
- Knox encryption: External storage encryption (optional if removable storage is disabled)
- Knox restrictions: Allowed Bluetooth profiles
- Knox restrictions: Disallowing "Share Via List" feature
- Knox restrictions: USB host mode exception list, enabled for DeX mode
- Knox restrictions: Disallowing unsecured Wi-Fi hotspots
- Knox restrictions: Disallowing autofill in Samsung Internet app
- Knox restrictions: Disallowing Google Accounts auto sync
- Knox Exchange ActiveSync: Disabling password recovery

Figure 3-1: Knox Platform Diagram

For additional information, visit:

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

3.1   KPE Security Highlights

3.1.1   Hardware-Backed Security

3.1.1.1 Trusted Environment

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

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

Knox features that use the trusted environment include:

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

3.1.1.2 Knox Verified Boot

Starting with Samsung Galaxy S10, KPE introduces Knox Verified Boot (KVB). KVB is a new, more complete integration of Android Verified Boot (AVB).

KVB will be enabled by default on new devices released with Knox 3.3 but will not be available to older devices with firmware updates to Knox 3.3.

KVB in built on top of Trusted Boot but performs component checks earlier, in the boot loader, where validations can be made before user data is accessed. This provides stronger data protection, as devices can be reflashed before data is exposed.

All devices will continue to support Trusted Boot.

3.1.1.3 Hardware Fuses

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

- Device Health Attestation checks fail.
- Knox Keystore removes the cryptographic keys used by SDP, preventing access to data marked as "sensitive".
- Knox Workspace no longer operates, preventing access to the secure enterprise apps and "protected" data within.

3.1.2   App isolation

Android provides both app isolation and group of app isolation.

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

Apps are isolated from each other in the Android Sandbox.

AE offers work profiles to provide basic security for group of app isolation.

With AE work profiles on Samsung Android mobile devices, KPE provides additional features to enhance app security, such as:

- Real-time kernel protection (RKP)
- Secure enterprise apps
- Hardware-backed storage of certificates and keys

KPE offers Knox Workspace to provide enhanced security for group of app isolation.

Knox Workspace builds on the basic security of AE work profiles and provides enhanced security, which provides additional features, such as:

- Hardware-backed integrity checks
- SDP

3.1.3   Data Protection

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

- User authentication:

    o Device password: This STIG enforces that the user configures a strong password that meets the standards for DoD IA: a minimum password length of six alphanumeric characters, with a maximum of two sequential or repeating characters and numbers. On first boot, any NIAP-certified biometric authentication mechanism enabled will not function until the user successfully authenticates with the device password.

    o Knox Workspace password: This STIG allows for the One Lock Workspace lock type. One Lock allows for the Knox Workspace and device to share the device lock screen for authentication. This means that when the user authenticates to unlock the device, they also authenticate to unlock the Knox Workspace at the same time. Likewise, when the device locks, the Knox Workspace also locks. Note that One Lock use is optional, and if not used, device and/or biometric authentication must be set up for Workspace independently.

    o Biometric authentication: Fingerprint and iris authentication are NIAP certified as compliant with the Protection Profile for Mobile Device Fundamentals (MDFPP) and available for use in this STIG. The Galaxy S10 (and newer) devices do not have an iris scanner but have face recognition authentication. Face recognition is not currently NIAP certified as compliant with MDFPP and, therefore, the STIG requires this feature to be disabled.

- Encryption of device data:

    o Protected data: Data marked as "protected" is encrypted when the device is in the powered-off state. Encryption is NIAP certified as compliant with MDFPP.

    o 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 Knox APIs or by moving files to the Knox Workspace Chamber directory. SDP is NIAP certified as compliant with MDFPP and available for use in this STIG.

    o Encryption: The Galaxy S10 (and newer) devices use File-Based Encryption (FBE), and this STIG enforces that "Strong Protection" is enabled. Older devices use Full Device Encryption (FDE), and this STIG enforces that "Secure Startup" is enabled. Both "Strong Protection" and "Secure Startup" ensure that the encryption keys are

derived from the user password. On first boot, the user must successfully authenticate with the device password before the "protected" and "sensitive" data is decrypted.

- o Dual DAR: Knox 3.3 also introduces Dual Data-at-Rest (Dual DAR) for Galaxy S10 (and newer) devices compliant with Commercial Solutions for Classified Program (CSfC) DAR Capability Package (CP). See section 4.3 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, providing the ability to configure a separate VPN for the Knox Workspace as well as for individual apps. Knox 3.3 introduces several VPN improvements. See section 4.4 for more information.

3.2   Manageability highlights

3.2.1   Deployment

In Samsung Android, the management app is called the device policy controller (DPC). The DPC can enforce policies in two deployment types:

- Android Enterprise, where a DPC manages the device in Device Owner (DO) mode, and another manages the Workspace in Profile Owner (PO) mode. Note that the most common case is usually two instances of the same application, tied to a single MDM console. The COBO use case uses a DPC in the DO mode of operation. The COPE use case uses a DPC in the DO mode of operation to manage the device and a second DPC in the PO mode of operation to manage the Workspace.

- Legacy mode, where the DPC manages both the device and Legacy Workspace in "classic" Device Admin (DA) mode. For both COBO and COPE, a single DPC operating in "legacy" mode manages the device/Workspace.

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

Both 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.

3.2.2   Knox Mobile Enrollment

Knox Mobile Enrollment (KME) is a free service to automate device enrollment either individual or in bulk. It is the quickest and most automated way to enroll a large number of devices to your MDM/EMM for corporate use. Once an IT administrator registers a device with the service, the

device user simply has to turn it on and connect to Wi-Fi or 3G/4G/5G during the initial device setup process.

There is no need for International Mobile Equipment Identity (IMEI) management and verification, and participating Knox Deployment Program (KDP) resellers register the purchased devices on your behalf.

KME core features include:

- Asset control: If a KME enrolled device is factory reset, the MDM/EMM software will be automatically reinstalled and the user will be re-enrolled.

- 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: Almost all MDM/EMM solutions are supported.

- Now supports Google Device Owner mode.

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

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

3.2.3 E-FOTA

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

E-FOTA core features include:

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

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

3.2.4 Accelerating Delivery of Knox Features to Customers

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

To support OEMConfig, Samsung will be releasing the Knox Service Plugin (KSP) app by spring 2019. 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.

4. SPOTLIGHT

4.1 Samsung DeX

Samsung DeX is DoD approved, and this STIG provides configuration information to enable its use. DeX is a unique product that lets you use your 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. You can connect a keyboard and mouse.

- 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.

4.1.1 Accessories

To use Samsung DeX, you will need 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.

4.2 UX Updates for Knox Workspace

KPE 3.2 removes the "folder" and "launcher" Workspace styles. The App screen now provides a convenient tabbed interface to switch between Personal and Workspace apps. Apps in the Workspace are still clearly badged to identify them as work managed apps.

Figure 4-1: App Screen with Tabbed Interface
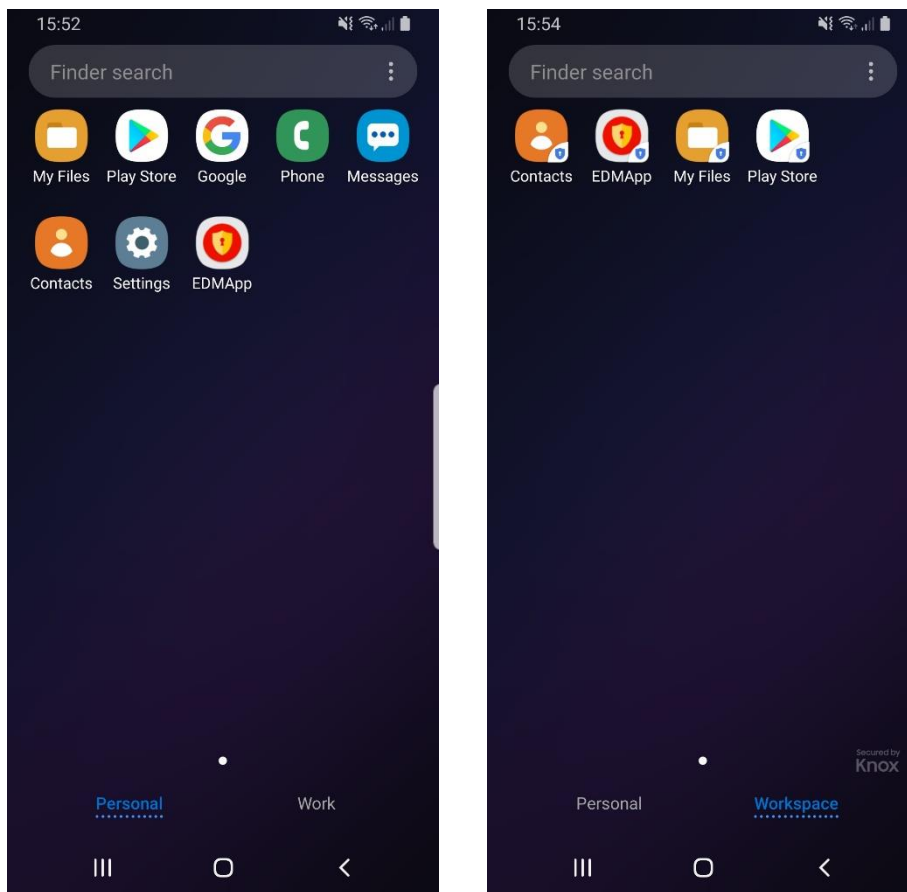
KPE 3.2 removes the Workspace settings apps. The device settings now integrate the Workspace setting, giving the user one central place to change settings.

4.3   Dual DAR

Starting with Samsung Galaxy S10, KPE introduces Dual Data-at-Rest (DAR) for data in the Knox Workspace compliant with Commercial Solutions for Classified Program (CSfC) DAR CP, which can be viewed at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/dar-cp.pdf.

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

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

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

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

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

4.4   VPN Improvements and Enhancements

KPE 3.3 includes several enhancements that improve user experience and performance of VPN clients on the Knox framework. The enhancements include but are not limited to the following:

- Support multi-app tunneling: These enhancements improve user experience when using VPN tunnels that impact more than one app at a time. As a result of these enhancements, users can connect with and start using business apps immediately after the VPN tunnel is established.

- Synchronize Knox events with Android networking events: These enhancements improve the performance of VPN clients by synchronizing Knox events with Android networking events. This change means the Knox Workspace recognizes that the VPN client is connected without any delay.

Provide ongoing network flow information for NPA purposes: This new feature improves the performance of EMM-based Network Performance Assessment tools by providing information about network data flow while the connection is ongoing. This feature means administrators now have the ability to configure their EMM-based NPA tools to receive network statistics while a network connection is ongoing. This functionality is especially useful in cases where network sessions last for a long time.

4.5   Common Criteria (CC) Settings

Since the release of the Samsung Android 9 STIG earlier this year 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. And there has been confusion related to 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 set of Common Criteria configuration settings in the STIG have been assigned a Severity Category Code (CAT) of CAT I to CAT III, depending on the risk and impact of the vulnerability for non-compliance. One control, "CC Mode", is an API that implements nine separate functional changes on the mobile device (see requirement KNOX-09-000710/KNOX-09-000715 for more details).

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

- Features enforced by policy:
    - Enable Knox Common Criteria (CC) Mode
    - Enable external storage encryption or disallow mount physical media
    - Minimum password quality
    - Disable face
    - Password recovery
    - Password history length
    - Revocation check
    - OCSP check
    - Max password failures for local wipe
- User Based Enforcement (UBE):
    - Secure Startup only for devices prior to Galaxy S10

To be 100% compliant with Common Criteria (CC) mode of operation all of the policies must be correctly configured. However, due to operational or deployment constraints, there may be cases where it may be required to deviate by not configuring selected problematic policies. 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 as such should be considered individually by the AO.

4.6 Note 10 Legacy Deprecation

The Samsung Note 10 is the first Samsung device to not include support for KPE (Legacy). Note 10 device will require to be deployed using the AE (KPE) deployment configuration.

4.7 Secure Startup Clarification

Secure Startup only offers additional security when a device is powered off until 1st authentication. For deployments that have operational needs that require Users to have devices always powered on, for example so that Users do not miss important emergency alerts or can always be responsive for mission needs, it can be assumed that the Users have always authenticated once and therefore Secure Startup is not offering additional security. In this situation, the AO may decide to accept the risk and deviate from the STIG configuration.

5. USE CASES

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

- Corporately Owned, Personally Enabled (COPE): An enterprise-owned device for business and personal use. This use case entails a significant degree of enterprise control over configuration and possibly software inventory. The enterprise elects to provide users with mobile devices and additional applications (such as VPN or email clients) to maintain control of their enterprise data and security of their networks. COPE deployment uses the Workspace in Knox Platform for Enterprise to maintain a separation between personal and work data and applications. Please refer to Sections 6 and 8 of this document to support the COPE configuration

- Corporate Owned, Business Only (COBO): COBO prohibits personal use of a mobile device; therefore, there is no configuration for the personal space. Please refer to Section 7 to support the COBO configuration. The COBO use case includes the following examples:

  o Using device to host low-security work area and the Workspace to host high-security work area (this configuration is not in the scope of this document).

  o DualDAR-enabled Workspace to support high-security requirements such as CSfC DAR CP (this configuration is not in the scope of this document).

Depending upon MDM policy support and DoD mobile service provider deployment choices, the above use cases can be implemented using deployment options as summarized in the following table.

Table 5-1: User Case and Deployment Options

Deployment Use Cases	Deployment options with KPE	Supplemental Document Reference	Configuration Document
COBO	KPE(Legacy): DA	Section 7	Samsung Android OS 9 Knox 3-x COBO KPE(Legacy) V1R1 Configuration Tables
	KPE(AE): DO		Samsung Android OS 9 Knox 3-x COBO KPE(AE) V1R1 Configuration Tables
COPE	KPE(Legacy): DA	Section 6 and 8	Samsung Android OS 9 Knox 3-x COPE KPE(Legacy) V1R1 Configuration Tables
	KPE(AE): (DO+ PO)		Samsung Android OS 9 Knox_3-x COPE KPE(AE) V1R1 Configuration Tables

6. CONFIGURATION OF THE PERSONAL SPACE

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 space and work space are set up on the Samsung Android 9 device.

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

- The site Authorizing Official (AO) has approved full access to the Google Play app store for the personal space, including downloading and installing Google Play apps into the personal space and syncing personal data on the device with personal cloud data storage accounts[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 space (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. Currently Samsung KPE Workspaces are the only NIAP-certified technology or application for Samsung mobile devices.

- The site MDM is configured to restrict the download of apps from all third-party app stores.

- The MDM or user restricts the use of DoD VPN profiles within the personal space.

- 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-09-000350 for more information.

This STIG assumes that all of the conditions above have been met and allows full user access to the personal space. If the AO has not approved unrestricted use of the personal space, the AO should consider implementing the following COPE Configuration Policy Rules for Non-Work Environment policy controls: Table 6-1 for KPE(Legacy) Deployment, and Table 6-2 for KPE (AE) deployment.

---

[1] It is recommended that the AO provide guidance on types of apps that should be avoided in the Google app store due to known risky functions or behaviors.
[2] UBE controls cannot be managed by the site MDM server and, therefore, must be managed by the mobile device user. See *Configuration of COPE Workspace* section in this document for more information.

Table 6-1: Optional COPE KPE (Legacy) Configuration Policy Rules for "Restricted" Non-Work Environment

Policy Vendor	Policy Group	Policy Rule	Settings	Related Requirement
AE	Android lock screen restrictions	disable unredacted notifications	Select	KNOX-09-000285
KPE	Knox application	application installation whitelist	Add each AO-approved package	KNOX-09-000075
KPE	Knox application	system application disable list	Add all non-AO-approved system app packages. Add all system app packages that have been identified as having non-DoD-approved characteristics. Add all pre-installed public cloud backup system apps.	KNOX-09-000045, KNOX-09-000105, KNOX-09-000865
KPE	Knox restrictions	Disable Android Beam	Select	KNOX-09-000805
KPE	Knox restrictions	Disallow share via list	Select	KNOX-09-000775
KPE	Knox restrictions	allow auto-fill	Unselect	KNOX-09-000585
KPE	Knox restrictions	allow google accounts auto sync	Unselect	KNOX-09-000865
KPE	Knox restrictions	allow google backup	Unselect	KNOX-09-000865

Table 6-2: Optional COPE KPE(AE) Configuration Policy Rules for "Restricted" Non-Work Environment

Policy Vendor	Policy Group	Policy Rule	Settings	Related Requirement	Comment
AE	Android device owner management	enable backup service	Unselect	KNOX-09-000860	
AE	Android lock screen restrictions	disable unredacted notifications	Select	KNOX-09-000280	
KPE	Android user restrictions	disallow autofill	Select	KNOX-09-000610	

Policy Vendor	Policy Group	Policy Rule	Settings	Related Requirement	Comment
AE	Android user restrictions	disallow outgoing beam	Select	KNOX-09-000800	
KPE	Knox application	application installation whitelist	Add each AO-approved package.	KNOX-09-000070	Confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2.
KPE	Knox application	system application disable list	Add all non-AO-approved system app packages. Add all system app packages that have been identified as having non-DoD-approved characteristics. Add all pre-installed public cloud backup system apps.	KNOX-09-000040, KNOX-09-000100, KNOX-09-000860	Confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #2.
KPE	Knox restrictions	Disallow share via list	Select	KNOX-09-000770	
KPE	Knox restrictions	allow auto-fill	Unselect	KNOX-09-000580	
KPE	Knox restrictions	allow google accounts auto sync	Unselect	KNOX-09-000860	
AE	managed Google Play	application installation whitelist	Add each AO-approved package.	KNOX-09-000070	For KNOX-09-000070, confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #1.

Policy Vendor	Policy Group	Policy Rule	Settings	Related Requirement	Comment
AE	managed Google Play	system application disable list	Add all non-AO-approved system app packages. Add all system app packages that have been identified as having non-DoD-approved characteristics. Add all pre-installed public cloud backup system apps.	KNOX-09-000040, KNOX-09-000100, KNOX-09-000860	Confirm if Method #1 or Method #2 is used at the Samsung device site. This configuration is only required for Method #1.

7. CONFIGURATION OF COBO

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

Samsung Android OS 9 with Knox 3.x Supplemental Procedures
24 July 2020
DISA
Developed by Samsung and DISA for the DoD

17

UNCLASSIFIED

8. CONFIGURATION OF COPE WORKSPACE

8.1 Overview

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

8.2 Workspace Isolation

The Knox Workspace provides a completely separated Android environment with its own applications and data. Various security mechanisms, such as Security Enhancements (SE) for Android policies, provide isolation of Know Workspace applications and data from applications and data outside the Knox Workspace. A newly created Knox Workspace does not restrict the user's ability to allow data to pass through the Knox Workspace. An administrator must explicitly restrict this behavior through APIs as indicated in the STIG configuration table.

9.   PROCEDURES

9.1   Device Wipe

Samsung Android devices can be wiped by a Factory Data Reset, MDM, or when the failed authentication limit is reached.

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

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

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

- For application installation blacklisting, the unwanted apps will be explicitly blacklisted.

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

9.2   Strong Protection

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

9.3   Secure Startup (S8, S9, Tab S4)

Secure Startup must be enabled by users of S8, S9, and Tab S4 installed with Samsung Android Pie. When the administrator (MDM) has enabled Knox CC mode, the setting will be enforced, allowing users only to enable it, and will prohibit disablement.

The Secure Startup screen is shown below.

Figure 9-1: Secure Startup Screen
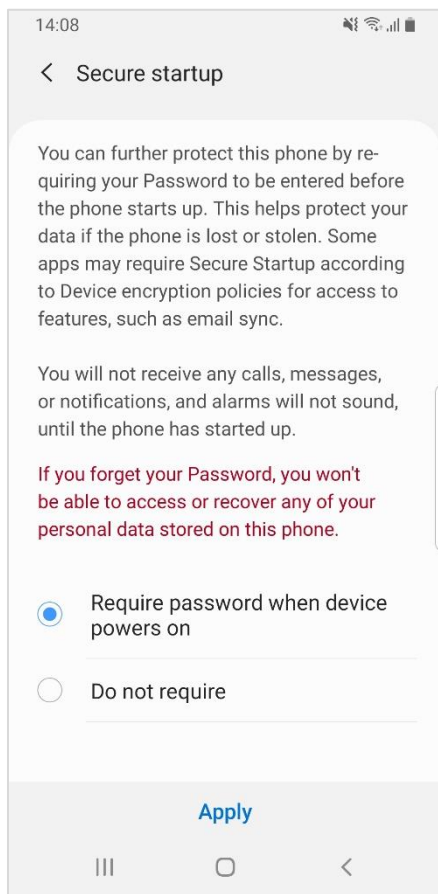
10. SPECIAL GUIDANCE

10.1 Whitelisting vs. Blacklisting

MDMs implement the Samsung whitelist and blacklist policies in slightly different ways. This section is to help clarify the intention of this STIG's configuration and how it might be achieved on the MDM console.

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

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

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

Refer to your MDM's documentation to determine how whitelisting/blacklisting is implemented. To understand the underlying KPE API's behavior, apply the following logic:

- To whitelist and allow only the things that are listed: Add the allowed items to the whitelist and configure the blacklist to include everything else. To include everything on a list, a wildcard (".*") may be used.

- To blacklist and allow everything but the items that are listed: **Do not configure the whitelist** and add the disallowed items to the blacklist. The whitelist should not be configured because it would override the blacklist, causing it have no effect.

10.2 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.

11. INFRASTRUCTURE

11.1 Knox SDK

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

Some policies, such as application whitelist and password requirements, must be applied separately for the personal area and 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.

11.2 Knox Licensing

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

11.3 Knox On-Premise Servers

All services necessary to enable Knox services on the device are hosted on the cloud. However, the Samsung Knox On-Premise server is also available for Enterprises wanting to deploy and manage Knox services on premise. DoD implementations are expected to install, configure, and manage the Knox On-Premise servers on enterprise-managed servers. Samsung provides the On-Premise server install packages, which are available for both Windows and Linux.

The Knox On-Premise server includes the following components:

- Knox License Management (KLM): The license management and compliance system for Samsung Knox. KLM is used to activate Knox services on supported devices.

- Global Server Load Balancing (GSLB): A dictionary server for the various services (e.g., KLM server). The URL for the GSLB server is coded into the enterprise-provided Knox license. During activation, the GSLB server will return the endpoints (URL) for the various services to the device agents.

An enterprise that decides to deploy the Knox On-Premise server will request the appropriate Knox license from the Knox reseller. The enterprise will provide its On-Premise GSLB server URL, which will be encoded into the Knox license.

The MDM agent will pass the Knox license to a KLM agent running off the device. This agent will connect to the GSLB server, which will return the KLM server URL. The agent then connects to the KLM server to obtain Knox license validation.

12. DOD PKI PUREBRED

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

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

- Users are responsible for maintaining positive control of their credentialed devices. The DoD PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and to report any loss of control so the credentials can be revoked.

- Upon device retirement, turn in, or reassignment, ensure a factory data reset is performed prior to device handoff. Follow mobility service provider decommissioning procedures as applicable.

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

13. SAMSUNG KNOX FOR ANDROID USER-BASED ENFORCEMENT

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

13.1   Calendar Alarm

The default Samsung pre-installed Calendar application allows users to create events that include event title, location, date and time, and also notification alarms for the event. When the alarm is configured, at the specified time the event details will be shown on the device screen, even when the device is in a locked state. Users should be trained to not configure this option or to not include any sensitive information in the event title and location.

13.2   Content Transferring and Screen Mirroring

Samsung devices include various ways that allow the user to transfer files on their device to other devices and to display content from their device on select Samsung Smart TVs.

The "Quick Connect" and "Samsung Connect" features (device model dependent) are accessed from the notification bar and display a list of scanned devices that the user's device can connect to. The user can select a device from this list to transfer selected files to (either via Wi-Fi Direct or Bluetooth) or to do screen mirroring. Depending on the selected device's capabilities, either Miracast or DLNA technology will be used to provide screen mirroring. Both Miracast and DLNA will work over a Wi-Fi Direct connection or with devices connected to the same Wi-Fi access point. Whereas Miracast renders whatever is on the device screen to the target device, DLNA requires the playback on the target device.

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

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

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

Users should be trained to not enable these options unless they are authorized to do so and they visually verify the recipient device. Users should be trained to not enable these options unless using an approved DoD screen mirroring technology with FIPS 140-2 validated Wi-Fi. Miracast must only be used with TVs, monitors, and Miracast dongles with FIPS 140-2 validated Wi-Fi clients.

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

13.3 Certificate Removal

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

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

Users should be trained to not remove DoD root and intermediate PKI certificates. See STIG requirements KNOX-09-001070, KNOX-09-001075, KNOX-09-001080, and KNOX-09-001085.

13.4 Accessory Use (DeX Station, USB Dongle)

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

Users should be trained to not connect the DeX Station to a DoD network via an Ethernet cable. See STIG requirements KNOX-09-000360 and KNOX-09-000365.

13.5 Samsung Wi-Fi Sharing

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

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

Users should be trained to disable Samsung Wi-Fi Sharing. See STIG requirements KNOX-09-000820 and KNOX-09-000825.

13.6 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.

13.7 Secure Startup/Strong Protection

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

When enabled, Strong Protection replaces the default cryptographic keys used to encrypt the user's apps and protected data with keys derived from the user password. This allows the device to decrypt files required to boot with default cryptographic keys, and the user's apps and protected data are decrypted the first time the user successfully authenticates after reboot. This feature must be enabled for a Samsung Android device to be in the NIAP-certified CC mode of operation. Strong Protection is enabled by default on S10 (or newer) devices installed with Samsung Android Pie. Users of S10 (or newer) devices should be trained to never disable Strong Protection. When the administrator (MDM) has enabled Knox CC Mode, users will only have the capability to enable Strong Protection and will be prohibited from disabling it. See STIG requirements KNOX-09-001480/KNOX-09-001485.

Secure Startup protects Samsung Android devices that use Full Disk Encryption (FDE). When enabled, Secure Startup replaces the default cryptographic keys with keys derived from the user password. The user must successfully authenticate at startup so the whole device can be decrypted before continuing to boot. This feature must be enabled for a Samsung Android device to be in the NIAP-certified CC mode of operation. Secure Startup is disabled by default on S8, S9, and Tab S4 installed with Samsung Android Pie and must be enabled by users (see Section 9.3). Users of S8, S9, and Tab S4 devices should be trained to enable Secure Startup and to never disable it. When the Administrator (MDM) has enabled Knox CC Mode, users will only have the capability to enable Secure Startup and will be prohibited from disabling it. See STIG requirements KNOX-09-001420/KNOX-09-001425.

14. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES

The Samsung Knox for Android supports application disable policies that allow administrators to disable core and preinstalled applications[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.

14.1 Public Cloud Backup Applications

Android allows users to back up and sync application data, user files, and settings to Google servers or other third-party cloud services, such as Samsung accounts and Dropbox. Samsung Knox for Android supports policy to disable Google backup, but other third-party services are disabled using application disable policies. The administrator must identify any such service pre-installed on the Workspace and disable these applications unless use is approved by the AO. This list includes:

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

14.2 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 Connect (Quick Connect)

14.3 Mobile Printing

Mobile printing applications provide the capability for wireless printing from a Samsung Android device. Setting up wireless printing from a mobile device to a DoD network-connected printer is problematic due to the print server requirements listed in the MultiFunction Device STIG and the DoD Wi-Fi network requirements listed in the Network Infrastructure STIG. If a mobile device is directly connected to a DoD network via a VPN or Wi-Fi connection, it may be able to print to network printers if the printer drivers or a printer app is installed. Android 9.x comes with a built-in print service that allows communication with most commercial printers. This package is covered in Table 14-1: System Apps for Disablement.

---

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

14.4 Core and Preinstalled Applications

14.4.1 Introduction

The core and preinstalled application lists below may not reflect the exact list on any specific device that is being reviewed. Small modifications to app names or app package names can be expected between various carriers' operating system (OS) builds. Also, additional apps not on the lists may be included in an OS build, or the OS build may not include all apps on a list. The app lists below should be compared to the list of apps installed on a device being reviewed.

14.4.2 Disabled Core and Preinstalled Applications

Tables 14-1: System Apps for Disablement (Non-DoD-Approved Characteristics and 14-2: System Apps for Disablement (Other Characteristics) list system apps (core/pre-installed applications) that must be disabled for STIG compliance unless the AO has approved the use of the application. Each section includes guidance explaining how to apply configuration for the different use cases.

DoD Commands and Agencies should fully vet these apps using the Application Software Protection Profile (APPSWPP) prior to approving their use. Note that depending on many factors, including how the device was provisioned, Android upgrade path, and carrier modifications, many of these applications may be already disabled or not installed.

14.4.2.1 System Apps for disablement (non-DoD-approved characteristics)

- **Guidance for COBO and COPE Workspace:**

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

   o back up mobile device data to non-DoD cloud servers (including user and application access to cloud backup services);

   o transmit mobile device diagnostic data to non-DoD servers;

   o voice assistant application if available when mobile device is locked;

   o voice dialing application if available when mobile device is locked;

   o allows synchronization of data or applications between devices associated with user; and

   o allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other mobile devices or printers.

   Related requirements: KNOX-09-000100, KNOX-09-000105, KNOX-09-000120, KNOX-09-000125, KNOX-09-000860, KNOX-09-000865, KNOX-09-000870, and KNOX-09-000870.

- **Guidance for COPE Personal:**

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

  Related requirements: KNOX-09-000110, and KNOX-09-000115.

Table 14-1: System Apps for Disablement (Non-DoD-Approved Characteristics)

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

Application Name	Application Package Name	Characteristic
Cloud	com.vcast.mediamanager	Back up MD data to non-DoD cloud servers (including user and application access to cloud backup services) Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers
Default Print Service	com.android.bips	Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers
Samsung Print Service Plugin	com.sec.app.samsungprintservice	Allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers
Smart Switch	com.sec.android.easyMover	Allows synchronization of data or applications between devices associated with user
Smart Switch Agent	com.sec.android.easyMover.Agent	Allows synchronization of data or applications between devices associated with user
Setup & Transfer	com.synchronoss.dcs.att.r2g	Allows synchronization of data or applications between devices associated with user

14.4.2.2 System Apps for Disablement (Other Characteristics)

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

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

  Related requirements: KNOX-09-000040, KNOX-09-000045, KNOX-09-000050, and KNOX-09-000055.

Table 14-2: System Apps for Disablement (Other Characteristics)

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

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

14.4.2.3 System Apps That Must Not Be Disabled

There are many System Apps that should not be disabled, as they will have a negative impact on the performance and usability of the Samsung Android device. Table 14-3: System Apps That Must Not Be Disabled exists to capture specific packages that have known issues if disabled; however, this is not an exhaustive list of packages that should not be disabled.

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

o   Related requirements: KNOX-09-000040, KNOX-09-000045, KNOX-09-000050, KNOX-09-000055, KNOX-09-000100, KNOX-09-000105, KNOX-09-000110, KNOX-09-000115, KNOX-09-000120, KNOX-09-000125, KNOX-09-000860, KNOX-09-000865, KNOX-09-000870, and KNOX-09-000875.

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

o   Related requirements: KNOX-09-000070, KNOX-09-000075, KNOX-09-000080, and KNOX-09-000085.

Table 14-3: System Apps That Must Not Be Disabled

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

15. ADDITIONAL SAMSUNG FEATURES

15.1 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.

15.2 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:

1. For Samsung Android Knox 3.2 or later devices (Galaxy Note 9, Tab S4, and later):

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

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

        -allowWifiScanning()[6]

        -allowBLE()[7]

    c. Disable GPS in the optional STIG rule "Allow Location" on MDM for the device.

    d. Review all Google services and apps that may track device location and determine if the risk in using these apps in a designated OA is acceptable[8].

    Note: Operational impact of recommended STIG controls:

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

---

[4] A copy of DISA's "Google Location Tracking on Samsung Devices" whitepaper 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 (MDM) enforcing by policy, the device user can still use the device Wi-Fi radio to connect to Wi-Fi networks.
[7] When the administrator (MDM) disables Bluetooth scanning by enforcing the MDM policy, all Bluetooth functionality on the device is disabled. Alternately, the UBE control can be used to disable Bluetooth scanning, and the Bluetooth radio can still be used. See footnote 9 for additional information.
[8] See DoD CIO memo "Mobile Application Security Requirements", 06 Oct 2017, for information on reviewing mobile applications.

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

- Wi-Fi control disables apps and services from connecting to nearby devices.

     Impact: None expected. Connecting to nearby devices is a STIG-prohibited feature. There are no known tactical use cases for this feature at this time.

- When Bluetooth is disabled by the "allowBLE" MDM control, all Bluetooth functionality is disabled.

     Impact: Connecting the mobile device to Bluetooth peripherals and sensors or to a computer via Bluetooth will be disabled.

2. For older Samsung devices (Knox 3.1 and earlier):

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

   b. Disable Wi-Fi/Bluetooth Scanning (UBE Control): Go to Settings >> Google >> Location >> Improve Accuracy. Set "Wi-Fi scanning" to "Off" and set "Bluetooth scanning" to "Off".[9]

   c. Disable GPS in the optional STIG rule "Allow Location" on MDM for the device.

   d. Review all Google services and apps that may track device location and determine if the risk in using these apps in a designated OA is acceptable[10].

   Note: Operational impact of recommended STIG controls:

- Wi-Fi control disables apps and services from connecting to nearby devices.

     Impact: None expected. Connecting to nearby devices is a STIG-prohibited feature. There are no known tactical use cases for this feature at this time.

Full details of the APIs used to implement the location tracking policies listed in this section can be found on the Samsung Knox portal "Knox 3.x STIG Implementation Guide - Samsung Android OS 9 API table" page (https://support.samsungknox.com/hc/en-us/articles/360021444993). To filter the API details on the page to display only the policies listed in this section, select only the "Location Tracking" and one of "COBO KPE(AE)" "COBO KPE(LEGACY)" "COPE KPE(AE)" "COPE KPE(LEGACY)" checkboxes as appropriate to your deployment.

15.3 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 15-1 for recommended mitigations for specific STIG controls.

---

[9] When BLE scanning is disabled by the user changing the setting in "Settings" on the mobile device, the device user can still use the device Bluetooth radio to connect to Bluetooth devices. See footnote 7 for Wi-Fi scanning information.
[10] See DoD CIO memo "Mobile Application Security Requirements", 06 Oct 2017, for information on reviewing mobile applications.

As mentioned in Section 3.2.1 "Deployment", certain deployments may benefit from employing a combined approach where the device is managed by both an MDM and by a local device administrator. The tactical use case is one such deployment that would benefit.

The device could be managed by the remote MDM administrator 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 MDM 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.

Tables 15-2 and 15-3 are essentially the recommended Configuration Tables for the tactical use case. Table 15-2 is for the KPE(AE) Deployment Mode and Table 15-3 is for the KPE(Legacy) Deployment Mode. The STIG controls and mitigations listed in Table 15-1 are represented in Tables 15-2 and 15-3.

Note: Not all STIG controls listed in Tables 15-1, 15-2, and 15-3 are appropriate for every tactical use case.

Note: Specific MDM/EMM products may not support some of the risk mitigations listed in Table 15-1. Recommend DoD organizations consult with their MDM/EMM vendor and Samsung on how best to implement recommended mitigations.

Full details of the APIs used to implement the tactical use case policies listed in this section can be found on the Samsung Knox portal "Knox 3.x STIG Implementation Guide - Samsung Android OS 9 API table" page (https://support.samsungknox.com/hc/en-us/articles/360021444993). To filter the API details on the page to display only the policies listed in this section, select only the "Location Tracking" and one of "COBO KPE(AE)" "COBO KPE(LEGACY)" "COPE KPE(AE)" "COPE KPE(LEGACY)" checkboxes as appropriate to your deployment.

Table 15-1: List of Tactical Changes to STIG Requirements with Recommended Mitigations

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
V-80331 KNOX-09-000430 KNOX-09-000435	Disable (not wipe) the device after 10 consecutive failed authentication attempts and disable further authentication attempts; device can only be re-enabled by the MDM 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
V-80315 KNOX-09-000370 KNOX-09-000375	Configure a minimum password length of four characters.	Unlocking the device with alphanumeric password on a keyboard can be problematic in battle gear. In addition, there is an emphasis on reducing head-down time.	Decrease allowed numbers of authentication failures to "5" or less. KNOX-09-000430, KNOX-09-000435
V-80315 KNOX-09-001440 KNOX-09-001445	Configure a minimum password quality of "PIN".	PIN pad use is required for many tactical use cases. In addition, there is an emphasis on reducing head-down time.	Decrease allowed numbers of authentication failures to "5" or less. KNOX-09-000430, KNOX-09-000435

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
V-80327 **KNOX-09-000400** **KNOX-09-000405**	Do one of the following: - Method #1: Configure the device screen to lock after two hours of inactivity - Method #2: Configure Smart Lock (Trust Agent) to use Trusted Device.	Longer screen inactivity timeouts needed for some battlefield situations or quick screen unlock needed.	- Require COBO deployment If using Method #2: - On the MDM console, for the device, in the "Android trust agent" group, implement a trust agent whitelist by configuring "trust agent configuration" so only approved trust agents can be used.
V-000000 **KNOX-09-000130** **KNOX-09-000135**	Enable unknown app installation sources.	Change required so apps can be downloaded from SD cards or sources other than Google Play and an MDM app catalog.	- Require COBO deployment - Require apps be downloaded from other AO-approved app repository (for example, DoD-app store)
V-80357 **KNOX-09-000660** **KNOX-09-000665**	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.
V-80335 **KNOX-08-010300**	Enable Trust Agents and configure a list of trusted devices using "Trusted Device".	The user authentication mechanism would be bypassed so that the user need not unlock the device while flying or on patrol. The device would lock automatically when separated from the	Enable Trust Agent whitelist on MDM 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

STIG Requirement Identifiers	Tactical Use Case Configuration	Tactical Application Notes	DoD Recommended Mitigations
		Trusted Device, enabling user authentication mechanisms.	be disabled for the Trust Agent Whitelist to operate correctly.
KNOX-09-000920 **KNOX-09-000925**	Enable developer modes.	Mock Locations and USB debugging are required for some tactical use cases.	Require COBO deployment.
V-80387 **KNOX-09-000680** **KNOX-09-000840** **KNOX-09-000685** **KNOX-09-000845**	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
V-80371 **KNOX-09-000730** **KNOX-09-000735**	Enable manual Date Time changes.	In some tactical situations, the user needs to be able to change the device time so it is different from the time of the local wireless carrier.	None
V-80373 **KNOX-09-000750** **KNOX-09-000755**	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 15-2: KPE(AE) Configuration Policy Rules for Tactical Use Case

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-09-000010	AE	Android lock screen restrictions	max password failures for local wipe	0+	0	KNOX-09-000430	This configuration is only required if: - implementing KTACT-09-000020 - when not implementing KTACT-09-000020 but as part of a recommended mitigation for either KTACT-09-000030/40. If configured as part of a recommended mitigation for either KTACT-09-000030/40, use a setting of "5", and not "0" as stated here.
KTACT-09-000020	KPE	Knox password constraints	max password failures for device disable	0+	10	KNOX-09-000430	If also implementing either KTACT-09-000030/40, the recommended mitigation is to use a setting of "5",

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
							and not "10" as stated here.
KTACT-09-000030	AE	Android password constraints	minimum password length	0+	4	KNOX-09-000370	DoD recommended mitigation: See "Comment" section of KTACT-09-000010/20.
KTACT-09-000040	AE	Android password constraints	minimum password quality	None, Pattern, PIN, Alphabetic, Alphanumeric, Complex, Biometric	PIN	KNOX-09-001440	DoD recommended mitigation: See "Comment" section of KTACT-09-000010/20.
KTACT-09-000050	AE	Android lock screen restrictions	max time to screen lock	0+	2 hours	KNOX-09-000400	This is Method #1. If configuring this, do not configure KTACT-09-000060. If possible, using a Remote MDM or Local Admin: Implement policy with "Tactical setting" only while on mission and set "Non-tactical setting" after return

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
							from mission. Requires COBO use case.
KTACT-09-000060	AE	Android trust agent	trust agent configuration	Configure	Enable "trusted device" feature.	KNOX-09-000400	This is Method #2. If configuring this, do not configure KTACT-09-000050, or KTACT-09-000130. Requires COBO use case.
KTACT-09-000070	AE	Android user restrictions	disallow install unknown sources	Select/Unselect	Unselect	KNOX-09-000130	Require apps be downloaded from other AO-approved app repository (for example, DoD-app store). If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" for as long as required to install apps/ updates, and set "Non-tactical

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
							setting" afterward. Requires COBO use case.
KTACT-09-000080	KPE	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-09-000660	If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" only while on mission and set "Non-tactical setting" after return from mission.
KTACT-09-000090	AE	Android user restrictions	disallow debugging features	Select/Unselect	Unselect	KNOX-09-000920	If possible, using a remote MDM 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 Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-09-000100	AE	Android user restrictions	disallow usb file transfer	Select/Unselect	Unselect	KNOX-09-000680 KNOX-09-000840	If possible, using a remote MDM 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-09-000110	AE	Android user restrictions	disallow config date time	Select/Unselect	Unselect	KNOX-09-000730	If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" only as required to correct the date/time while on mission deployment.
KTACT-09-000120	KPE	Knox restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON, CSC, HID, HUB, MAS, MIS,	HID MAS	KNOX-09-000750	If possible, using a remote MDM or local admin: Implement policy with "Tactical

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
				PER, PHY, PRI, STI, VEN, VID, WIR			setting" only during pre-mission device configuration and set to "Non-tactical setting" prior to mission deployment.
KTACT-09-000130	AE	Android lock screen restrictions	disable trust agents	Select/Unselect	Unselect	KNOX-09-000470	If implementing KTACT-09-000060, do not implement this policy as stated here. Use the STIG configuration table setting. Otherwise, the "trust agent configuration" will not operate correctly.

Table 15-3: KPE(Legacy) Configuration Policy Rules for Tactical Use Case

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-09-000015	AE	Android lock screen restrictions	max password failures for local wipe	0+	0	KNOX-09-000435	This configuration is only required if: - implementing KTACT-09-000025 - when not implementing KTACT-09-000025 but as part of a recommended mitigation for either KTACT-09-000035/45. If configured as part of a recommended mitigation for either KTACT-09-000035/45, use a setting of "5", and not "0" as stated here.
KTACT-09-000025	KPE	Knox password constraints	max password failures for device disable	0+	10	KNOX-09-000435	If also implementing either KTACT-09-000035/45, the recommended mitigation is to use a setting of "5",

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
							and not "10" as stated here.
KTACT-09-000035	AE	Android password constraints	minimum password length	0+	4	KNOX-09-000375	DoD recommended mitigation: See "Comment" section of KTACT-09-000015/25.
KTACT-09-000045	AE	Android password constraints	minimum password quality	None, Pattern, PIN, Alphabetic, Alphanumeric, Complex, Biometric	PIN	KNOX-09-001445	DoD recommended mitigation: See "Comment" section of KTACT-09-000015/25.
KTACT-09-000055	AE	Android lock screen restrictions	max time to screen lock	0+	2 hours	KNOX-09-000405	This is Method #1. If configuring this, do not configure KTACT-09-000065. If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" only while on mission and set "Non-tactical setting" after return

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
							from mission. Requires COBO use case.
KTACT-09-000065	AE	Android trust agent	trust agent configuration	Configure	Enable "trusted device" feature.	KNOX-09-000405	This is Method #2. If configuring this, do not configure KTACT-09-000055 or KTACT-09-000135. Requires COBO use case.
KTACT-09-000075	KPE	Knox restrictions	allow install unknown sources	Select/Unselect	Select	KNOX-09-000135	Require apps be downloaded from other AO-approved app repository (for example, DoD-app store). If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" for as long as required to install apps/updates and set "Non-tactical

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
							setting" afterward. Requires COBO use case.
KTACT-09-000085	KPE	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-09-000665	If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" only while on mission and set "Non-tactical setting" after return from mission.
KTACT-09-000095	KPE	Knox restrictions	allow developer mode	Select/Unselect	Select	KNOX-09-000925	If possible, using a remote MDM 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 Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
KTACT-09-000105	KPE	Knox restrictions	disable USB media player	Select/Unselect	Unselect	KNOX-09-000685 KNOX-09-000845	If possible, using a remote MDM 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-09-000115	KPE	Knox Date Time	date time change enabled	Select/Unselect	Select	KNOX-09-000735	If possible, using a remote MDM or local admin: Implement policy with "Tactical setting" only as required to correct the date/time while on mission deployment.
KTACT-09-000125	KPE	Knox restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON, CSC, HID, HUB, MAS, MIS,	HID MAS	KNOX-09-000750	If possible, using a remote MDM or local admin: Implement policy with "Tactical

UID	Policy Vendor	Policy Group	Policy Rule	Options	Tactical Setting	Related Requirement	Comment
				PER, PHY, PRI, STI, VEN, VID, WIR			setting" only during pre-mission device configuration and set to "Non-tactical setting" prior to mission deployment.
KTACT-09-000135	AE	Android lock screen restrictions	disable trust agents	Select/Unselect	Unselect	KNOX-09-000475	If implementing KTACT-09-000065, do not implement this policy as stated here. Use the STIG configuration table setting. Otherwise, the "trust agent configuration" will not operate correctly.

16. OPTIONAL CONTROLS

DoD wireless service providers should consider including the following optional controls, if warranted, based on the operational environment and use case implemented.

Table 16-1: Optional Controls

Vendor	Policy Group	Policy Rule	Options	Fix
AE	Android trust agent	trust agent configuration	Configure	See section 15.3 Tactical Use Case.
KPE	Knox RCP	allow move files to workspace	Select/Unselect	This policy applies to the Workspace only.
KPE	Knox location	allow location	Passive, Network, GPS	An administrator can enable or disable specific location providers (i.e., passive, network, GPS).
KPE	Knox NFC	allow NFC	Select/Unselect	This setting applies to both the device and the Workspace if one exists.
KPE	Knox password constraints	disable fingerprint	Select/Unselect	This policy can be independently applied to both the device and the Workspace if one exists.
AE	Android lock screen restrictions	disable fingerprint	Select/Unselect	This policy can be independently applied to both the device and the Workspace if one exists.
KPE	Knox password constraints	disable iris	Select/Unselect	This policy can be independently applied to both the Device and the Workspace if one exists.
AE	Android lock screen restrictions	disable iris	Select/Unselect	This policy can be independently applied to both the device and the Workspace if one exists.
KPE	Knox password constraints	max password failures for device disable	0+	See section 15.3: Tactical Use Case.
KPE	Knox restrictions	allow BLE	Select/Unselect	See section 15.2: Google Location Tracking on Samsung Devices.
KPE	Knox restrictions	allow Wi-Fi scanning	Select/Unselect	See section 15.2: Google Location Tracking on Samsung Devices.

Vendor	Policy Group	Policy Rule	Options	Fix
KPE	Knox restrictions	allow Wi-Fi tethering	Select/Unselect	This setting applies to both the device and the Workspace if one exists.
KPE	Knox restrictions	allow Bluetooth tethering	Select/Unselect	This setting applies to both the device and the Workspace if one exists.
AE	Android user restriction	disallow config tethering	Select/Unselect	This policy disallows user from configuring tethering and portable hotspots. This setting applies to both the device and the Workspace if one exists.
KPE	Knox restrictions	allow camera	Select/Unselect	If disabled for the device, will also disable for the Workspace if one exists, but can be applied to only disable for the Workspace.
AE	Android camera	disable camera	Select/Unselect	If disabled for the device, will also disable for the Workspace if one exists, but can be applied to only disable for the Workspace.
KPE	Knox restrictions	allow microphone	Select/Unselect	This policy only disables the microphone used for recording, not the phone application microphone. If disabled for the device, will also disable for the Workspace if one exists, but can be applied to only disable for the Workspace.
AE	Android user restrictions	disallow unmute microphone	Select/Unselect	This policy can only be applied to the device and will have no effect on the Workspace.

Full details of the APIs used to implement the optional policies listed in this section can be found on the Samsung Knox portal "Knox 3.x STIG Implementation Guide - Samsung Android OS 9 API table" page (https://support.samsungknox.com/hc/en-us/articles/360021444993). To filter the API details on the page to display only the policies listed in this section, select only the "Location Tracking" and one of "COBO KPE(AE)" "COBO KPE(LEGACY)" "COPE KPE(AE)" "COPE KPE(LEGACY)" checkboxes as appropriate to your deployment.