SAMSUNG ANDROID OS 15 WITH KNOX 3.X SUPPLEMENTAL PROCEDURES

30 January 2025

Developed by Samsung and DISA for the DOD

Trademark Information

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

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

The Samsung Android 15 with Knox 3.x STIG is compatible with the Google Android 15 STIG, and the configuration is based on the same set of Android Enterprise (AE) policies, with no additional Knox Platform for Enterprise (KPE) policies or license required for compliance.

However, KPE policies may be used with a free license to give a richer AE experience. This can allow additional features to be used while remaining STIG compliant. It also provides a means to achieve compliance with the Knox Service Plugin (KSP) when Mobile Device Managers (MDMs) and Enterprise Mobility Managers (EMMs) do not implement some of the required controls.

2. ARTIFICAL INTELLIGENCE RESTRICTIONS

The artificial intelligence (AI) strategy implemented in the STIG is to disable access to all AI features/apps that process device data in the cloud and to allow all AI features/apps that process device data locally on the device. When Google Workspace or Google Cloud are disabled/not used on a Google device, Google AI features (such as Google Gemini business and enterprise editions) cannot be used.

Services that use on-device inference (e.g., Google Gemini Nano and its associated developer API, AICore) can be used. Applications will need to build a user interface to present on-device inference created through AICore. For example, the Voice Recorder app on Pixel devices uses on-device AI to transcribe voice recordings and uses AICore summaries of conversations. Crucially, AICore does not send any data off of the device, and processing is handled in Google Private Compute Core on the device only. Updates to AICore and the underlying model, Gemini Nano, can be updated through Google Play.

Sites can install a managed configuration to Chrome to block access to specified AI websites or web-based AI tools (such as ChatGPT).

3. SAMSUNG GALAXY DEVICES

Samsung offers a series of devices running the Android 15 mobile operating system (MOS). This STIG covers any Samsung Galaxy device listed in the DODIN Approved Product List for Samsung Android 15 devices. At the time of writing, the following devices are in evaluation for inclusion:

- Samsung Galaxy TBD/S24/S23/S22/S21.
- Samsung Galaxy Z Fold 6/5/4/3.
- Samsung Galaxy Z Flip 6/5/4/3.
- Samsung Galaxy Tab TBD/S9/S8.
- Samsung Galaxy XCover 6 Pro.
- Samsung Galaxy A53/A52.

Samsung manufactures each device model in several variants. Differences include higher specification components such as screen size, connectivity type, and available memory.

For the full list of supported devices, including specific device variants, refer to the DODIN Approved Product List for Samsung Android OS 15 devices at https://aplits.disa.mil/processAPList.action.

4. KNOX PLATFORM FOR ENTERPRISE (KPE)

KPE is built on top of Android Enterprise (AE) and therefore contains all the security features provided by AE, adding advanced security features to provide a richer AE experience. As the details of AE are already well documented—refer to Google's Android 15 Supplemental document—this section will provide details only on security features and Android 15 changes specific to KPE.

Figure 4-1: AE and KPE

SAMSUNG
Knox Platform
for Enterprise
Android
enterprise

4.1 Licensing

KPE licenses are obtained from a Knox reseller free of charge and must be activated on the MDM/EMM. During activation, the device will validate the license with the Samsung Knox License Management (KLM) server. Once validated, all the KPE features and APIs will become available for use.

4.2 Knox On-Premise Servers

While all services necessary to enable KPE are hosted in the cloud, it is possible to deploy and manage on-site using the Samsung Knox On-Premise server. Installation packages are available for both Windows and Linux, with maintenance support from Samsung.

DOD customers are expected to host the Knox On-Premise servers on enterprise-managed servers.

The Knox On-Premise server includes:

- KLM: The license management and compliance system used to activate KPE services.
- Global Server Load Balancing (GSLB): A dictionary server for KPE services. During license activation, the server will return the URLs for the different KPE services to the device.

A standard KPE license contains the URL to the GSLB server in the cloud. To use the on-premise solution, licenses must instead contain the on-premise GSLB URL. To do this, the URL must be provided to the Knox reseller so the correct license can be created.

During license activation, the device will first connect to the GSLB using the URL contained in the license. The GSLB will return a URL to the KLM server. The device will then use this server to validate the license.

4.3 Software Development Kit (SDK)

The Knox SDK provides APIs to configure additional features and security controls. They may be used by customers with deployment needs beyond what is required by the STIG. These APIs can be used to configure restrictions on the device and a Work Profile. The Work Profile can be fully managed by a management tool using a variety of policies that are independent of the device policies.

Some policies, such as password requirements, must be applied separately for the personal area and Work Profile. Others, such as disabling Wi-Fi, can only be applied at a devicewide level.

4.4 Unified Work Profile

In Android 13, Samsung completed the implementation of fully unifying KPE and AE Work Profiles. Previously, there were differences in the default policies between the two when a KPE license was activated.

4.5 Sensitive Data Protection (SDP)

Knox SDP has been deprecated in Knox for Android 14. The protection of sensitive data now uses the AE Storage Area Encryption (SAE) solution.

Knox provides the **Chamber directory** within the Work Profile to allow users to quickly protect work files as sensitive data. To use the feature, a user need only move a file within the folder. The file will instantly be protected by the SAE solution.

4.6 Trusted Execution Environment (TEE)

Samsung Galaxy devices include a TEE—a secondary isolated environment from the Android platform. It is implemented using secure ARM TrustZone technology.

The TEE is responsible for performing sensitive operations such as file system encryption and:

- Real-Time Kernel Protection (RKP).
- Knox Verified Boot (KVB).
- Device Attestation.
- Certificate Management.

In addition to the TEE, some Samsung Galaxy devices include an embedded Secure Element (eSE).

4.7 Knox Verified Boot (KVB)

KVB is a Samsung-specific implementation of Android Verified Boot (AVB) v2. The core differences are:

Table 4-1: KVB Table

AVB	KVB
Checks the integrity of the kernel and platform components.	Extends the chain of trust to earlier bootloaders and other partitions, including Kernel, System, Vendor, and Product. This provides integrity and authenticity, as well as assurance that the device is booting using trusted components that are all from an aligned set of binaries.

4.8 Hardware Fuses

KPE uses a hardware fuse to permanently detect if a Samsung Galaxy device has ever booted into an unapproved state. When a hardware fuse is set, it is physically damaged in the hardware and cannot be reversed.

KVB sets the fuse when it detects failures of certain critical security checks, including:

- Attempts to load nontrusted boot components.
- Security Enhancements (SE) for Android having been disabled.

The fuse is checked during normal operation, and if set, triggers the following security measures:

- Device Health Attestation checks fail.
- Device requires factory data reset to remove unofficial software components.
- Work profile is disabled, preventing access to enterprise apps and data within.

4.9 Dual Data-at-Rest (DualDAR)

KPE implements a solution to provide DualDAR compliant with Commercial Solutions for Classified Program (CSfC) DAR Capability Package (CP).

DualDAR allows for Work Profile data to be secured with two layers of encryption, which provides protection when powered off and when powered on in an unauthenticated state.

Deploying and configuring DualDAR is beyond the scope of this STIG.

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

To view the CSfC DAR CP, visit https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/dar-cp.pdf.

4.10 Knox Mobile Enrollment (KME)

KME (desktop and cloud) is a free-to-use service to automate single/bulk enrollment of devices to the MDM/EMM. KME is approved for STIG use and highly recommended for DOD use.

To use KME, the International Mobile Equipment Identity (IMEI) or serial number of purchased devices is uploaded by a participating Knox Deployment Program (KDP) reseller on behalf of the administrator. Once that is registered to the administrator's KME account, the administrator can configure the devices for enrollment. The enrollment occurs automatically when the device user turns on the device and connects to the internet during the initial device setup process.

Core KME features include:

- Retain asset control:
  - Persistent across factory data resets.
  - Bypass of Google factory reset protection.
- Automated sign-in of MDM/EMM.
  - Using IT-controlled user credentials.
- Streamlined and customizable device setup process.
- Automated installation of root and/or intermediate certificates.
  - For example, the DOD certificate bundle.

AE offers zero touch, and KME offers similar functionality. Samsung Galaxy devices support both services, with the latter taking precedence if a device is registered with both.

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

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

E-FOTA controls operating system versions on Samsung Galaxy devices to ensure the latest security patches are deployed to devices on schedule. IT administrators can test updates before rolling out to deployments, ensuring compatibility between in-house apps and new operating system versions. E-FOTA is approved for DOD use.

Core E-FOTA features include:

- Selective update of OS versions.
- Assigning of multiple devices to different OS versions in a single campaign.
- Automated upload of device identifiers by KDP resellers.
- Out-of-the-box installation of the E-FOTA client.
- Flexible license addition.

- No user interaction needed.
- Scheduled updates.
- Forced updates.
- Bypass of carrier FOTA restrictions.

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

4.12 Knox Service Plugin (KSP)

KSP is an app that allows Samsung to make new Knox features available immediately by dynamically extending the capabilities of any MDM/EMM that has been validated for AE. KSP is approved for DOD use.

The MDM/EMM console provides a dynamic interface to display the policies currently available in KSP and allows their configuration. When the IT administrator saves the KSP configuration on the console, the configuration is pushed to KSP via managed Google Play. KSP then enforces the policies on the Samsung Galaxy device on behalf of the MDM/EMM.

Refer to the following guide to using KSP to configure STIG policies:

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

4.13 Separated Apps

Separated Apps is an alternative solution to using a Work Profile to isolate apps and data from one group to another. Separated apps are approved for use in the DOD.

KSP or Managed Configurations must be used to enable this feature and configure the list of apps to be isolated in the Separated Apps folder. There are two options for separating apps:

- Inside: Isolate a specific list of apps within the folder.
- Outside: Isolate everything within the folder except for a specific list of apps.

To use this feature, deploy devices in the COBO use case and then use KSP to configure:

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/Outside—as required.
5. List of Apps to Separate >> “comma separated list of package names”.

Android 14 and later (Knox 3.10) includes the following improvements to the Separated Apps space:

- Allowing a list of applications to be installed both within and outside of the Separated Apps space.

- Supporting managed configurations for applications installed within the Separated Apps container.

4.14 Samsung DeX

DeX allows for the device to be used as if it were a laptop or desktop computer. DeX is approved for use in the DOD.

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.

Because the STIG configuration does not allow USB file transfer, DeX Drag & Drop mode is not usable.

Use of Samsung DeX requires one of the following accessories:

- DeX station.
- DeX pad.
- Multiport adapter.
- USB Type-C to HDMI adapter.
- DeX cable.
- USB cable with DeX companion app.

4.15 Galaxy AI

Galaxy AI, available on a limited set of Samsung Galaxy devices, provides a suite of productivity-improving features.

While many of these features require a logged-in Samsung account and cloud processing, several are able to run purely on the device. These features include:

- Voice Recorder text-to-speech and translation.
- Samsung Notes translation.
- Samsung interpreter for live voice translation.

Samsung provides KPE APIs to enforce that only on-device AI processing may be used, and this configuration can be enforced through KSP.

More information is available at https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/data-processing-for-galaxy-ai/.

5. USE CASES

Samsung Galaxy devices may be operated in a number of use cases relevant to government deployment. In the majority of DOD use cases, the mobile device will be DOD owned (Corporate Owned). The following use cases are supported in this STIG:

Table 5-1: Deployment Type

Use Case	AE Deployment type	Implementation Detail
COBO	**Fully managed device.** Contains only work apps and data that is visible and managed by the organization.	During AE enrollment, a device policy controller (DPC) is installed and activated in Device Owner (DO) mode.
COPE	**Work profile on company-owned device.** **Personal profile:** Contains personal apps and data that is not visible to the organization. Only a small number of policies, which respect the user's privacy, may be enforced. **Work profile:** Contains work apps and data, visible and managed by the organization.	During AE enrollment, a DPC is installed and activated in Profile Owner (PO) mode.

In all use cases, the DPCs apply AE policies using Android API implemented by the Android Device Policy Manager (DPM) module. Additionally, the DPC may apply KPE policies using Samsung KPE APIs when a free-of-charge KPE license is activated.

5.1 Configuration Approach

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

5.2 COBO

In the COBO use case, a 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.

5.3 COPE with Work Profile

In the COPE use case, two completely isolated and independent profiles are available: Personal and Work. Enterprise applications and data reside within the Work Profile, while personal applications and data reside within the Personal Profile. This use case provides limited visibility and control while respecting the user's privacy.

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

DualDAR may be enabled in the Work Profile to support high-security requirements such as CSfC DAR CP. (This configuration is not in the scope of this document.)

5.3.1 Configuration of the Personal Profile

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

- The site authorizing official (AO) has approved access to the Google Play app store for the Personal Profile, including downloading and installing Google Play apps into the Personal Profile and syncing personal data on the device with personal cloud data storage accounts[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 Profile (guidance can be added to user training or the User Agreement).
- Site mobile devices are configured with a technology used for data separation between work apps and data and personal apps and data that is NIAP certified.
- The site management tool is configured to restrict the download of apps from all third-party app stores.
- The management tool or user restricts the use of DOD VPN profiles within the Personal Profile.
- Site mobile device users receive training on known Google Play application risks and required STIG controls that must be enabled by the user (User-Based Enforcement)[2]. Refer to STIG requirement KNOX-15-009400 for more information.

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

[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. Refer to Section 8, User-Based Enforcement, in this document for more information.

5.4 COPE With Separated Apps

KPE includes an additional security feature, Separated Apps, to allow organizations that require more management and less privacy of the personal profile in the COPE use case.

If a DOD mobile service provider wants to deploy with the Knox app separation feature, it must be implemented using the policies in the Configuration Tables document in Table 1: Configuration Policy Rules for COBO. The app separation policies listed in the same document in Table 4-2: KSP App Separation must then be applied.

Table 5-2: Deployment Type With Separated Apps

Use Case	AE Deployment Type	Implementation Detail
COPE	**Fully managed device, then activate KPE Separated Apps.** Contains work apps and data, visible and managed by the organization. **Separated Apps folder:** Contains personal apps and data that is **visible and managed** by the organization. **Note:** It is also possible to deploy the work apps and data in the Separated Apps folder, with personal and apps and data outside.	During AE enrollment, a DPC is installed and activated in DO mode. KSP can then enable KPE Separated Apps and configure which apps to install in the folder.

5.5 Nonstandard Deployment Considerations

Not all STIG requirements are appropriate for all deployments (for example, tactical deployments). AOs have the authority to develop a Plan of Action and Milestones (POA&M) for STIG requirements and accept risks after considering mitigation strategies.

These types of deployments may also benefit from a combined management approach where the device is managed by both a management tool and a local device administrator tool.

For example, 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. Alternatively, 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.

6. PROCEDURES

6.1 Device Wipe

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

6.2 Unenrollment

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

7. SPECIAL GUIDANCE

7.1 Samsung Android Device Disposal

For Samsung Android devices that have never been exposed to classified data, follow this procedure prior to disposing of (or transferring to another user) a mobile device via site property disposal procedures.

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

8. DOD PKI PUREBRED

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

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

- Users are responsible for maintaining positive control of their credentialed devices. The DOD PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and 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 (refer to Section 5.2, Unenrollment). Follow mobility service provider decommissioning procedures as applicable.

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

9. 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.

9.1 Calendar Alarm

The default Samsung preinstalled 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 must be trained to not configure this option or to not include any sensitive information in the event title and location.

9.2 Content Transferring and Screen Mirroring

Samsung devices include various ways that allow the user to transfer files on their device to other devices and 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 **Android Auto** 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 Connected Devices >> Android Auto 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 must 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/FIPS 140-3 validated Wi-Fi. Miracast must only be used with TVs, monitors, and Miracast dongles with FIPS 140-2/FIPS 140-3 validated Wi-Fi clients.

Note: The administrator can also restrict the underlying connection method (Bluetooth, Wi-Fi Direct, etc.) via management tool controls or can explicitly disable the application package that implements the service. Specifically disabling Wi-Fi Direct and Bluetooth Sharing can be performed via AE and KPE APIs.

9.3 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 must be trained to not connect these types of accessories (DeX Station, USB dongle) to a DOD network via an Ethernet cable. Refer to STIG requirement KNOX-15-007200.

9.4 VPN Profiles

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

Users must 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.

9.5 Samsung Wi-Fi Sharing

This training is required only if using either the Bring Your Own Device (BYOD) use case or KPE as directed in the STIG to allow the use of mobile hotspots and tethering. Allowing their use requires KPE to be used to disallow "Open" mobile hotspots, but there is no control to disallow the use of Wi-Fi Sharing.

Wi-Fi Sharing is an option included in Samsung mobile hotspot tethering settings. 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 >> Network name >> Advanced >> Wi-Fi Sharing).

Users must be trained to disable/not enable Samsung Wi-Fi Sharing. Refer to STIG requirement KNOX-15-009700.

9.6 Wi-Fi Hotspots

This training is required on COPE and COBO devices as directed in the STIG to educate users on how to set suitably secure passwords for mobile hotspot sharing.

Mobile hotspot sharing is an option included in the Connections area of the settings application. It allows a Samsung device user to share their mobile data connection with other Wi-Fi enabled devices, but a weak password or no password could allow unauthorized devices to access a DOD device.

A user must configure the mobile hotspot securely to reduce the risk of an unauthorized device connecting to that hotspot. This can be achieved by setting a 15-character complex hotspot password and configuring the security to be WPA2/WPA3-personal in Settings >> Connections >> Mobile Hotspot and tethering >> Mobile Hotspot >> Password. The 15-character complex password is set by default in Android.

10. ADDITIONAL CONSIDERATIONS

10.1 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.

10.2 Google Location Tracking on Samsung Devices

DOD policy memorandum "Use of Geolocation-Capable Devices, Applications, and Services," 03 August 2018, prohibits the use of geolocation-capable devices, applications, and services on DOD mobile devices in designated operational areas (OAs). Independent researchers and DISA analysis have determined that even when **Location History** is disabled, Google continues to store location data on the mobile device[3]. 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. Disable GPS with **Location** as **Disallow** on the **Management** tool for the device.
c. 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[4].
d. KSP can be used where MDM/EMM capability is missing. The guidance to implement policies to disable Wi-Fi/Bluetooth scanning with KSP are listed in Table 9-1: Disable Location Tracking Implementation Guidance.

Table 10-1: Disable Location Tracking Implementation Guidance

Policy Group	Policy Rule	Instructions
Advanced Restriction	Wi-Fi scanning	1. Devicewide 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. Devicewide 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] 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.
[4] Refer to DOD CIO memo "Mobile Application Security Requirements," 06 Oct 2017, for information on reviewing mobile applications.

Policy Group	Policy Rule	Instructions
		3. Advanced Restriction policies (Premium). 4. Enable Advanced Restrictions controls [enable]. 5. Allow Bluetooth scanning [disable].

Note:

- 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.