GOOGLE ANDROID 14
SUPPLEMENTAL PROCEDURES

24 July 2024

Developed by Google 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

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. GOOGLE PIXEL DEVICES

Google offers a series of devices running the Android 14 mobile operating system (MOS). The following table lists all the devices covered in this STIG.

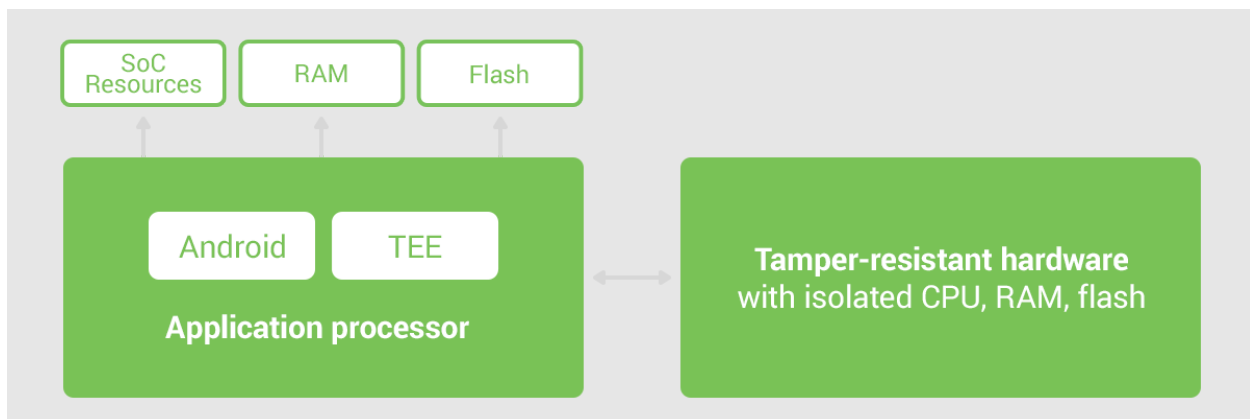**Table 1-1: Devices Covered in Google Android 14 STIG**

Product	System on Chip (SoC)	Kernel	Titan
Google Pixel 7 Pro/7	Google Tensor G2	5.15	M2
Google Pixel 6 Pro/6/6a	Google Tensor	5.10	M2
Google Pixel 5a-5G/5/4a-5G	Qualcomm Snapdragon 765	4.19	M
Google Pixel 4a	Qualcomm Snapdragon 730	4.14	M
Google Pixel 4 XL/4	Qualcomm Snapdragon 855	4.14	M

Google manufactures some of the phones in two variants, differing in size (normal and large, "XL," or "Pro") or build materials (entry and premium). The only differences between variants of a given device are build materials, screen type and size, battery capacity, and RAM and flash storage. The XL or Pro phones are physically larger and have larger screen sizes, battery capacity, and, where applicable, RAM (not all XL devices have more RAM). Storage options vary with each release, and the customer may select an option at purchase.

1.1 Titan M and Titan M2 – Tamper-Resistant Hardware

Google Pixel devices ship with tamper-resistant hardware (Titan M and M2) to perform security-critical operations. Titan chips have additional protections against physical tampering and share only very limited resources with the main application processor, significantly reducing its attack surface and the potential of side channel attacks.

Figure 1-1: Tamper-Resistant Hardware Provides Numerous Protections on the Device

2.   ANDROID SECURITY OVERVIEW

2.1   Android Operating System

Android is an open-source operating system built on the Linux kernel that provides an environment for multiple apps to run simultaneously. These apps are signed and isolated into application sandboxes associated with their application signature. The application sandbox defines the privileges available to the application. Apps are generally built using Android Runtime and interact with the operating system through a framework that describes system services, platform APIs, and message formats. Other high-level and lower-level languages, such as C/C++, are allowed and operate within the same application sandbox.

2.1.1   Security-Enhanced Linux (SELinux)

Android uses SELinux to enforce mandatory access control (MAC) over all processes and apps, including processes running with root and superuser privileges. SELinux provides a centralized auditable security policy that can be used to strongly separate processes from one another. Android devices implement SELinux policy on a per-domain basis in enforcing mode. Illegitimate actions that violate policy are blocked, and all violations (denials) are logged by the kernel.

2.1.2   Trusted Execution Environment

Android devices have a secondary isolated environment called a Trusted Execution Environment (TEE). This enables further separation from any untrusted code. The capability is typically implemented using secure hardware such as ARM TrustZone technology.

The TEE is responsible for some of the most security-critical operations on the device, including:

- Lock screen passcode verification.
- Fingerprint template matching.
- Protection and management of KeyStore keys.

2.2   Over-the-Air (OTA) Updates

OTA updates, which include baseband processor updates, use public key chaining to the root public key, a hardware-protected key whose SHA-256 hash resides inside the application processor. The update is installed only if the verification check is successful. Android also provides rollback protection for OTA updates to prevent a user from installing a previous version of software.
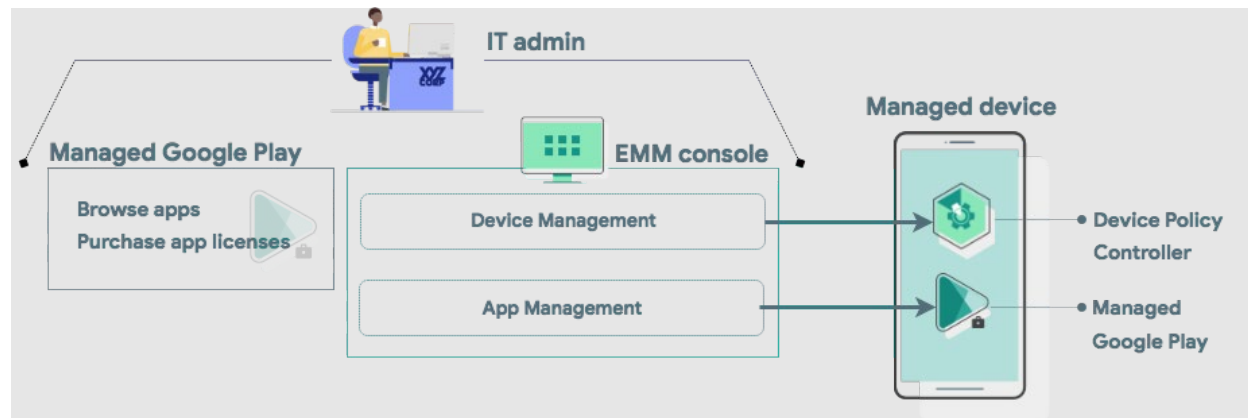
Administrators of fully managed devices can install system updates via a system update file. Manual system updates allow IT administrators to do the following:

- Test an update on a small number of devices before installing them widely.
- Avoid duplicate downloads on bandwidth-limited networks.
- Stagger installations or update devices only when not being used.

3. ANDROID ENTERPRISE

An Android Enterprise solution is a combination of three components: The Enterprise Mobility Management/Mobile Device Management (EMM/MDM) console, a device policy controller (DPC), which is the EMM/MDM agent, and managed Google Play (not covered here).

Figure 3-1: Components of an Android Enterprise Solution

3.1 EMM/MDM Console

EMM solutions typically take the form of an EMM console—a web application that allows IT administrators to manage their organization, devices, and apps. To support these functions for Android, the console must be integrated with the application programming interfaces (APIs) and user interface (UI) components provided by Android Enterprise.

3.2 DPC (Device Policy Controller)

All Android devices managed by an organization through an EMM console must install a DPC app during setup. A DPC is an agent that applies the management policies set in the EMM console to devices. Depending on which development option is chosen, the EMM solution can be coupled with Android's DPC or with a custom user-developed DPC.

End users can provision a fully managed or dedicated device using a DPC identifier (e.g., "afw#") or by scanning a QR code created by the EMM according to the implementation guidelines defined in the Play EMM API developer documentation.

- The EMM's DPC must be publicly available on Google Play, and the end user must be able to install the DPC from the device setup wizard by entering a DPC-specific identifier or scanning a QR code generated by the EMM.
- Once installed, the EMM's DPC must guide the user through the process of provisioning a fully managed or dedicated device.

3

3.3   Work Profile Security

Work profile mode is initiated when the DPC initiates a managed provisioning flow. The work profile is based on the Android multiuser concept, where the work profile functions as a separate Android user segregated from the primary profile. The work profile shares common UI real estate with the primary profile. Apps, notifications, and widgets from the work profile appear next to their counterparts from the primary profile and are always badged to indicate the type of app.

With the work profile, enterprise data does not intermix with personal application data. The work profile has its own apps, downloads folder, settings, and KeyChain. It is encrypted using its own encryption key and can have its own passcode to gate access.

The work profile is provisioned upon installation, and the user can only remove it by removing the entire work profile. Administrators can remotely instruct the device policy client to remove the work profile when, for example, a user leaves the organization or a device is lost or stolen. Whether the user or an IT administrator removes the work profile, user data in the primary profile remains on the device.

A DPC running in profile owner mode can require users to specify a security challenge for apps running in the work profile. The system shows the security challenge when the user attempts to open any work apps. If the user successfully completes the security challenge, the system unlocks the work profile and decrypts it if necessary.

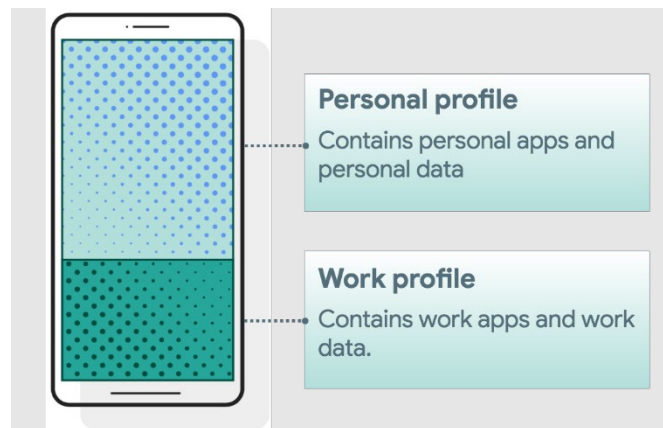### 3.3.1   COPE Deployments and User Privacy

Google Android 14 devices deployed using COPE will have enhanced privacy for users. Personal apps in the personal profile cannot be configured, monitored, or enumerated by an MDM. Allowlists and blocklists should be used to permit or block specific applications from use in the personal profile. It is highly recommended that DOD mobile service providers deploy/redeploy all Android phones using Zero-Touch with personal app allowlists/blocklists to provide visibility on which personal apps are installed on managed devices.

4. DEVICE CONFIGURATION

Work profiles on company-owned devices are for government-furnished devices used for both work and personal purposes. The organization still manages the entire device; however, the separation of work data and apps into a work profile allows organizations to enforce two separate sets of policies. For example:

- A stronger set of policies for the work profile that applies to all work apps and data.
- A more lightweight set of policies for the personal profile that applies to the user's personal apps and data.

Figure 4-1: Personal Profile and Work Profile

5. PROCEDURES

5.1 Device Wipe

Google Android devices can be wiped by a factory data reset, EMM, or when the failed authentication limit is reached. Preinstalled 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 will not be prevented from installing them.

The only solution is to both uninstall/disable the unwanted apps and use either application installation allowlisting or blocklisting.

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

Application installation blocklisting must only be used if the Authorizing Official (AO) has not approved unrestricted use of personal apps where a personal and work profile exists.

6. SPECIAL GUIDANCE

6.1   Google Android Device Disposal

Follow the procedure below prior to disposing of (or transferring to another user) Android devices that have never been exposed to classified data using site property disposal procedures for mobile devices.

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

6.2   Configuration of the Personal Space

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

- The site AO has approved 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. 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.) on the Google Android 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, Android Enterprise is the only NIAP-certified technology for application separation for Google Android mobile devices.

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

- The EMM 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).
    - Refer to STIG requirement GOOG-14-009800 for more information.

7. DOD PKI PUREBRED

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

Requirements for Google Android 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. Follow mobility service provider decommissioning procedures as applicable.

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

8. ADDITIONAL CONSIDERATIONS

8.1 Wearables

The use of virtual reality (VR) wearables with a DOD-owned Google Android 14 device is prohibited. VR wearables are considered a personal use product with no DOD mission requirement.

8.2 Google Location Tracking

DOD policy memorandum "Use of Geolocation-Capable Devices, Applications, and Services," dated 03 August 2018, prohibits the use of geolocation-capable devices, applications, and services on DOD mobile devices in designated operational areas. Independent research and DISA analysis has determined that even when "Location History" is disabled, Google continues to store location data on the mobile device[1]. Therefore, AOs should consider additional actions to limit Google tracking mobile devices when these devices are used in operational areas.

---

[1] 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.